I

(Zakonodajni akti)

DIREKTIVE

DIREKTIVA (EU) 2016/1148 EVROPSKEGA PARLAMENTA IN SVETA

z dne 6. julija 2016

o ukrepih za visoko skupno raven varnosti omrežij in informacijskih sistemov v Uniji

EVROPSKI PARLAMENT IN SVET EVROPSKE UNIJE STA –

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

ob upoštevanju predloga Evropske komisije,

po posredovanju osnutka zakonodajnega akta nacionalnim parlamentom,

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

v skladu z rednim zakonodajnim postopkom ([2]),

ob upoštevanju naslednjega:

(1) Omrežja in informacijski sistemi ter storitve imajo ključno vlogo v družbi. Njihova zanesljivost in varnost sta bistveni za gospodarske in družbene dejavnosti ter zlasti za delovanje notranjega trga.

(2) Obseg, pogostost in posledice varnostnih incidentov so vse večji ter pomenijo veliko grožnjo delovanju omrežij in informacijskih sistemov. Ti sistemi lahko postanejo tudi tarča namernih škodljivih dejanj, katerih namen je povzročitev škode ali prekinitev delovanja sistemov. Takšni incidenti lahko ovirajo gospodarske dejavnosti, ustvarjajo znatne finančne izgube, slabijo zaupanje uporabnikov in povzročajo veliko škodo gospodarstvu Unije.

(3) Omrežja in informacijski sistemi, zlasti internet, imajo bistveno vlogo pri zagotavljanju lažjega čezmejnega pretoka blaga, storitev in ljudi. Zaradi te transnacionalne razsežnosti lahko namerne ali nenamerne znatne prekinitve delovanja teh sistemov, ne glede na to, kje se zgodijo, vplivajo na posamezne države članice in Unijo kot celoto. Varnost omrežij in informacijskih sistemov je zato bistvena za nemoteno delovanje notranjega trga.

(4) Na podlagi vidnega napredka, ki ga je Evropski forum držav članic dosegel pri razpravah in izmenjavi dobrih političnih praks, vključno z oblikovanjem načel za evropsko sodelovanje pri kibernetskih krizah, bi bilo treba ustanoviti skupino za sodelovanje, sestavljeno iz predstavnikov držav članic, Komisije in Agencije Evropske unije za varnost omrežij in informacij (v nadaljnjem besedilu: agencija ENISA), da se podpre in zagotovi lažje strateško

([1]) UL C 271, 19.9.2013, str. 133.

([2]) Stališče Evropskega parlamenta z dne 13. marca 2014 (še ni objavljeno v Uradnem listu) in stališče Sveta v prvi obravnavi z dne 17. maja 2016 (še ni objavljeno v Uradnem listu). Stališče Evropskega parlamenta z dne 6. julija 2016 (še ni objavljeno v Uradnem listu).

sodelovanje med državami članicami na področju varnosti omrežij in informacijskih sistemov. Za učinkovito in vključujoče delovanje te skupine morajo imeti vse države članice minimalne zmogljivosti in strategijo za zagotavljanje visoke ravni varnosti omrežij in informacijskih sistemov na svojem ozemlju. Poleg tega bi morale za izvajalce bistvenih storitev in ponudnike digitalnih storitev veljati varnostne zahteve in zahteve za priglasitev, da bi se spodbudila kultura obvladovanja tveganja in zagotovilo poročanje o najresnejših incidentih.

(5) Obstoječe zmogljivosti ne zadostujejo za zagotavljanje visoke ravni varnosti omrežij in informacijskih sistemov v Uniji. Raven pripravljenosti držav članic je zelo različna, zato se tudi pristopi po Uniji med seboj močno razlikujejo. Zaradi tega je raven varstva potrošnikov in podjetij različna, prizadeta pa je tudi celotna raven varnosti omrežij in informacijskih sistemov v Uniji. Pomanjkanje skupnih zahtev za izvajalce bistvenih storitev in ponudnike digitalnih storitev obenem onemogoča vzpostavitev globalnega in učinkovitega mehanizma za sodelovanje na ravni Unije. Univerze in raziskovalni centri imajo odločilno vlogo pri spodbujanju raziskav, razvoja in inovacij na teh področjih.

(6) Za učinkovito odzivanje na izzive na področju varnosti omrežij in informacijskih sistemov je zato potreben globalni pristop na ravni Unije, ki bo obsegal skupne minimalne zahteve za vzpostavitev in načrtovanje zmogljivosti, izmenjavo informacij ter sodelovanje in skupne varnostne zahteve za izvajalce bistvenih storitev in ponudnike digitalnih storitev. Vendar izvajalcem bistvenih storitev in ponudnikom digitalnih storitev nič ne preprečuje, da izvajajo varnostne ukrepe, ki so strožji od tistih, ki so določeni v tej direktivi.

(7) Da bi bili zajeti vsi ustrezni incidenti in tveganja, bi se morala ta direktiva uporabljati tako za izvajalce bistvenih storitev kot tudi ponudnike digitalnih storitev. Vendar se obveznosti izvajalcev bistvenih storitev in ponudnikov digitalnih storitev ne bi smele uporabljati za podjetja, ki zagotavljajo javna komunikacijska omrežja ali javno dostopne elektronske komunikacijske storitve v smislu Direktive Evropskega parlamenta in Sveta 2002/21/ES ([1]), za katera veljajo posebne zahteve glede varnosti in celovitosti, določene v navedeni direktivi; prav tako se ne bi smele uporabljati za ponudnike storitev zaupanja v smislu Uredbe (EU) št. 910/2014 Evropskega parlamenta in Sveta ([2]), za katere veljajo varnostne zahteve iz navedene uredbe.

(8) Ta direktiva ne bi smela posegati v možnost vsake države članice, da sprejme potrebne ukrepe, s katerimi zavaruje bistvene interese svoje varnosti, zaščiti javni red in javno varnost ter omogoči preiskovanje, odkrivanje in pregon kaznivih dejanj. V skladu s členom 346 Pogodbe o delovanju Evropske unije (PDEU) nobena država članica ni dolžna dajati informacij, za katere meni, da bi bilo njihovo razkritje v nasprotju z bistvenimi interesi njene varnosti. V tem smislu so pomembni Sklep Sveta 2013/488/EU ([3]) in sporazumi o nerazkritju informacij ali neuradni sporazumi o nerazkritju informacij, kot je semaforski protokol (Traffic Light Protocol).

(9) Sektorski pravni akti Unije, ki vsebujejo pravila o varnosti omrežij in informacijskih sistemov, že urejajo ali pa morda še bodo urejali nekatere sektorje ekonomije. Kadar ti pravni akti Unije vsebujejo določbe, ki uvajajo zahteve glede varnosti omrežij in informacijskih sistemov ali priglasitve incidentov, bi se morale te določbe uporabljati, če vsebujejo zahteve, ki so po učinku najmanj enake obveznostim iz te direktive. V tem primeru bi morale države članice uporabljati določbe iz sektorskih pravnih aktov Unije, tudi tiste, ki se nanašajo na pristojnost, in ne bi smele izvesti postopka določitve izvajalcev bistvenih storitev, kot je določeno v tej direktivi. V zvezi s tem bi morale države članice Komisijo obvestiti o uporabi takih določb *lex specialis*. Pri ugotavljanju, ali so zahteve glede varnosti omrežij in informacijskih sistemov ter priglasitve incidentov iz sektorskih pravnih aktov Unije enakovredne zahtevam iz te direktive, bi bilo treba upoštevati samo določbe ustreznih pravnih aktov Unije in njihovo uporabo v državah članicah.

(10) Varnostne zahteve iz pravnih aktov Unije v sektorju vodnega prometa, ki veljajo za podjetja, ladje, pristaniško infrastrukturo, pristanišča in storitve ladijskega prometa, se nanašajo na vse dejavnosti, med drugim na radijske in telekomunikacijske sisteme, računalniške sisteme in omrežja. Med obvezne postopke, ki jih je treba izpolnjevati, sodi priglasitev vseh incidentov, ki bi zato morala šteti za *lex specialis*, če so te zahteve najmanj enakovredne ustreznim zahtevam iz te direktive.

([1]) Direktiva Evropskega parlamenta in Sveta 2002/21/ES z dne 7. marca 2002 o skupnem regulativnem okviru za elektronska komunikacijska omrežja in storitve (okvirna direktiva) (UL L 108, 24.4.2002, str. 33).

([2]) Uredba (EU) št. 910/2014 Evropskega parlamenta in Sveta z dne 23. julija 2014 o elektronski identifikaciji in storitvah zaupanja za elektronske transakcije na notranjem trgu in o razveljavitvi Direktive 1999/93/ES (UL L 257, 28.8.2014, str. 73).

([3]) Sklep Sveta 2013/488/EU z dne 23. septembra 2013 o varnostnih predpisih za varovanje tajnih podatkov EU (UL L 274, 15.10.2013, str. 1).

(11) Države članice bi morale pri določanju izvajalcev v sektorju vodnega prometa upoštevati obstoječe in prihodnje mednarodne zakonike in smernice, zlasti tiste, ki jih je oblikovala Mednarodna pomorska organizacija, da se posameznim izvajalcem v pomorskem sektorju zagotovi usklajen pristop.

(12) Urejanje in nadzor v bančnem sektorju in sektorju infrastruktur finančnega trga sta na ravni Unije že visoko harmonizirana v okviru primarnega in sekundarnega prava Unije, pa tudi standardov, oblikovanih v sodelovanju z evropskimi nadzornimi organi. Uporaba in nadzor teh zahtev sta v okviru bančne unije zagotovljena z enotnim mehanizmom nadzora. Za države članice, ki niso del bančne unije, ju zagotavljajo ustrezni bančni regulativni organi držav članic. Na drugih področjih urejanja finančnega sektorja pa Evropski sistem finančnega nadzora prav tako zagotavlja visoko stopnjo enakosti in konvergence nadzornih praks. Tudi Evropski organ za vrednostne papirje in trge ima neposredno nadzorno vlogo nad določenimi subjekti, in sicer bonitetnimi agencijami in repozitoriji sklenjenih poslov.

(13) Operativno tveganje je ključen del bonitetne ureditve in nadzora v bančnem sektorju in sektorju infrastruktur finančnega trga. Zajema vse dejavnosti, vključno z varnostjo, celovitostjo in odpornostjo omrežij in informacijskih sistemov. Zahteve glede teh sistemov, ki so pogosto strožje od zahtev iz te direktive, so določene v številnih pravnih aktih Unije, vključno s: pravili o dostopu do dejavnosti kreditnih institucij in bonitetnem nadzoru kreditnih institucij in investicijskih podjetij ter pravili o bonitetnih zahtevah za kreditne institucije in investicijska podjetja, ki vključujejo zahteve glede operativnega tveganja; pravili o trgih finančnih instrumentov, ki vključujejo zahteve glede ocene tveganja za investicijska podjetja in regulirane trge; pravili o izvedenih finančnih instrumentih OTC, centralnih nasprotnih strankah in repozitorijih sklenjenih poslov, ki vsebujejo zahteve glede operativnega tveganja za centralne nasprotne stranke in repozitorije sklenjenih poslov; in pravili o izboljšanju ureditve poravnav vrednostnih papirjev v Uniji in o centralnih depotnih družbah, ki vsebujejo zahteve glede operativnega tveganja. Poleg tega so zahteve za priglasitev incidentov del običajne nadzorne prakse v finančnem sektorju in pogosto vključene v priročnike o nadzoru. Navedena pravila in zahteve bi države članice morale upoštevati pri izvajanju *lex specialis*.

(14) Evropska centralna banka je v mnenju z dne 25. julija 2014 ([1]) navedla, da ta direktiva ne posega v ureditev po pravu Unije, vzpostavljeno za nadzor, ki ga Eurosistem opravlja nad plačilnimi sistemi in sistemi poravnave. Primerno bi bilo, da organi, pristojni za tovrsten nadzor, in pristojni organi iz te direktive izmenjavajo izkušnje o zadevah glede varnosti omrežij in informacijskih sistemov. Enako velja za članice Evropskega sistema centralnih bank, ki niso del Eurosistema, vendar nadzorujejo plačilne sisteme in sisteme poravnave na podlagi nacionalnega prava in predpisov.

(15) Spletna tržnica potrošnikom in trgovcem omogoča sklepanje pogodb o spletni prodaji in pogodb o spletnih storitvah s trgovci, ki so v okviru nje tudi dokončno sklenjene. Vanjo ne bi smele biti vključene spletne storitve, ki služijo le kot posrednik do storitev tretjih strani, prek katerih se nazadnje pogodba lahko sklene. Zato ne bi smela vključevati spletnih storitev, ki primerjajo cene določenih izdelkov ali storitev različnih trgovcev in nato uporabnika preusmerjajo k izbranemu trgovcu za nakup izdelka. Računalniške storitve, ki jih zagotavlja spletna tržnica, lahko vključujejo obdelavo transakcij, zbiranje podatkov ali profiliranje uporabnikov. Trgovine z aplikacijami, ki delujejo kot spletne trgovine in omogočajo digitalno distribucijo aplikacij ali programske opreme tretjih strani, štejejo za vrsto spletne tržnice.

(16) Spletni iskalnik uporabniku omogoča iskanje po načeloma vseh spletiščih na podlagi poizvedbe v zvezi s katero koli temo. Lahko pa se osredotoči tudi na iskanje po spletiščih v določenem jeziku. Opredelitev pojma spletnega iskalnika iz te direktive ne bi smela obsegati funkcij iskanja, ki so omejene na vsebino določenega spletišča, ne glede na to, ali funkcijo iskanja zagotavlja zunanji iskalnik. Obsegati ne bi smela niti spletnih storitev, ki primerjajo cene določenih izdelkov ali storitev različnih trgovcev in nato uporabnika preusmerjajo k izbranemu trgovcu za nakup izdelka.

(17) Storitve računalništva v oblaku zajemajo raznolike dejavnosti, ki jih je mogoče zagotavljati po različnih modelih. V tej direktivi izraz „storitve računalništva v oblaku“ zajema storitve, ki omogočajo dostop do prožnega in po obsegu prilagodljivega nabora deljivih računalniških virov. Ti „računalniški viri“ obsegajo vire, kot so omrežja, strežniki ali druga infrastruktura, shranjevanje, aplikacije in storitve. Izraz „prožen“ se nanaša na računalniške vire, ki jih ponudnik storitev v oblaku prilagodljivo dodeljuje, ne glede na geografsko lokacijo virov, da bi se tako lahko odzvali na spremembe v povpraševanju. Izraz „prilagodljiv nabor“ opisuje take računalniške vire, ki se

([1]) UL C 352, 7.10.2014, str. 4.

zagotavljajo in sproščajo glede na povpraševanje, da bi se tako število razpoložljivih virov hitro povečalo ali zmanjšalo odvisno od delovne obremenitve. Izraz „deljiv“ opisuje take računalniške vire, ki se zagotavljajo več uporabnikom, ki si delijo isti dostop do storitve, vendar se obdelava za vsakega uporabnika opravi ločeno, čeprav storitev opravlja ista elektronska oprema.

(18) Stičišče omrežij medsebojno povezuje omrežja. Stičišče omrežij ne zagotavlja dostopa do omrežja oziroma ni ponudnik ali nosilec prenosa. Prav tako stičišče omrežij ne zagotavlja drugih storitev, ki se ne nanašajo na medsebojno povezljivost, čeprav to izvajalcu stičišča omrežij ne preprečuje nudenja teh drugih storitev. Stičišče omrežij medsebojno povezuje tehnično in organizacijsko ločena omrežja. Izraz „avtonomni sistem“ opisuje tehnično samostojno omrežje.

(19) Države članice bi morale biti pristojne, da določijo, kateri subjekti izpolnjujejo merila iz opredelitve pojma izvajalec bistvenih storitev. Da bi zagotovili usklajen pristop, bi morale vse države članice skladno uporabljati opredelitev pojma izvajalec bistvenih storitev. V ta namen ta direktiva določa oceno subjektov, delujočih v določenih sektorjih in podsektorjih, pripravo seznama bistvenih storitev, razmislek o skupnem seznamu medsektorskih dejavnikov za ugotavljanje, ali bi imel incident pomemben negativen vpliv, postopek posvetovanja, pri katerem sodelujejo ustrezne države članice v primeru subjektov, ki storitve ponujajo v več kot eni državi članici, in podporo skupine za sodelovanje pri določanju izvajalcev bistvenih storitev. Države članice bi morale redno pregledovati in po potrebi posodabljati seznam izvajalcev, ki so bili določeni, da bi bile morebitne spremembe na trgu tako točno odražene. Nazadnje, države članice bi morale Komisiji poslati informacije, potrebne za oceno, v kakšnem obsegu je skupna metodologija pripomogla k skladni uporabi te opredelitve pojma v državah članicah.

(20) Države članice bi morale pri določanju izvajalcev bistvenih storitev vsaj za vsak podsektor iz te direktive oceniti, katere storitve morajo šteti za bistvene za ohranitev ključnih družbenih in gospodarskih dejavnosti ter ali subjekti, ki so bili uvrščeni na seznam sektorjev in podsektorjev iz te direktive ter ponujajo te storitve, izpolnjujejo merila za določitev izvajalcev. Pri oceni, ali subjekt ponuja storitev, ki je bistvena za ohranitev ključnih družbenih ali gospodarskih dejavnosti, je dovolj, da se preuči, ali ta subjekt ponuja storitev, ki je vključena na seznam bistvenih storitev. Dokazati bi bilo tudi treba, da je zagotavljanje bistvene storitve odvisno od omrežij in informacijskih sistemov. Nazadnje, države članice bi morale pri oceni, ali bi incident pomembno negativno vplival na zagotavljanje storitve, upoštevati več medsektorskih dejavnikov ter po potrebi tudi dejavnike, značilne za posamezni sektor.

(21) Za namene določitve izvajalcev bistvenih storitev pomeni sedež v državi članici učinkovito in dejansko izvajanje dejavnosti na podlagi stabilnih ureditev. Pravna oblika takih ureditev, bodisi prek podružnice ali prek odvisne družbe, ki je pravna oseba, v tem pogledu ni odločujoči dejavnik.

(22) Možno je, da subjekti v sektorjih in podsektorjih iz te direktive zagotavljajo tako bistvene storitve kakor tudi druge storitve, ki ne štejejo za bistvene. Na primer, v sektorju zračnega prometa letališča zagotavljajo storitve, ki jih država članica lahko šteje za bistvene, kot je upravljanje vzletno-pristajalnih stez, pa tudi številne storitve, ki lahko ne štejejo za bistvene, kot je zagotavljanje nakupovalnih površin. Za izvajalce bistvenih storitev bi morale veljati posebne varnostne zahteve, vendar le za tiste storitve, ki štejejo za bistvene. Države članice bi za namen določitve izvajalcev bistvenih storitev zato morale sestaviti seznam storitev, ki štejejo za bistvene.

(23) Na seznam storitev bi morale biti uvrščene vse storitve, ki se zagotavljajo na ozemlju določene države članice in izpolnjujejo zahteve iz te direktive. Državam članicam bi moralo biti omogočeno, da obstoječi seznam dopolnijo z vključitvijo novih storitev. Države članice bi morale seznam storitev uporabljati kot referenčno točko pri določanju izvajalcev bistvenih storitev. Na podlagi seznama se določijo vrste bistvenih storitev v katerem koli sektorju iz te direktive, ki se jih tako loči od nebistvenih dejavnosti, za katere je lahko pristojen kateri koli subjekt v katerem koli sektorju. Seznam storitev, ki ga sestavi vsaka država članica, bi služil kot dodatni element za oceno regulativne prakse vsake države članice, da bi tako zagotovili splošno raven usklajenosti postopka določitve izvajalcev bistvenih storitev med državami članicami.

(24) Kadar subjekt zagotavlja bistveno storitev v dveh ali več državah članicah, bi se zadevne države članice za namene postopka določitve izvajalcev bistvenih storitev morale medsebojno dvo- ali večstransko posvetovati. Ta postopek posvetovanja je državam članicam v pomoč pri oceni kritične narave izvajalca z vidika čezmejnega učinka, in tako vsaki vpleteni državi članici omogoči predstavitev stališč glede tveganj, povezanih s storitvami, ki se zagotavljajo. Zadevne države članice bi morale pri tem postopku upoštevati mnenja ena druge in bi morale imeti možnost, da v zvezi s tem zaprosijo za pomoč skupine za sodelovanje.

(25) Države članice bi morale po zaključenem postopku določitve izvajalcev bistvenih storitev sprejeti nacionalne ukrepe za določitev, za katere subjekte veljajo obveznosti v zvezi z varnostjo omrežij in informacijskih sistemov. V ta namen bi lahko sprejele seznam vseh izvajalcev bistvenih storitev ali nacionalne ukrepe, vključno z objektivnimi količinsko opredeljivimi merili, kot sta obseg produkcije izvajalca ali število uporabnikov, na podlagi katerih je mogoče določiti, za katere subjekte veljajo obveznosti v zvezi z varnostjo omrežij in informacijskih sistemov. Nacionalni ukrepi, ne glede na to, ali že obstajajo ali so bili sprejeti v okviru te direktive, bi morali zajemati vse pravne ukrepe ter upravne ukrepe in politike, ki omogočajo določitev izvajalcev bistvenih storitev v skladu s to direktivo.

(26) Da bi se za zadevni sektor odrazil pomen izvajalcev bistvenih storitev, ki so bili določeni, bi morale države članice upoštevati število in velikost teh izvajalcev, na primer glede na tržni delež ali proizvedene ali prenesene količine, ne da bi morale pri tem razkriti informacije, iz katerih bi bilo mogoče razbrati, katere izvajalce so določile.

(27) Države članice bi pri ugotavljanju, ali bi incident pomembno negativno vplival na zagotavljanje bistvene storitve, morale upoštevati več različnih faktorjev, kot je število uporabnikov, ki so od storitve odvisni pri zasebnih ali poslovnih namenih. Zadevna storitev se lahko uporablja neposredno, posredno ali s posredovanjem. Države članice bi morale pri oceni morebitnega vpliva, ki bi ga incident glede na svoj obseg in trajanje lahko imel na ekonomske in družbene dejavnosti ali javno varnost, oceniti, koliko časa bo verjetno poteklo, preden bi prekinitev povzročila negativne posledice.

(28) Za namen ugotavljanja, ali bi incident pomembno negativno vplival na zagotavljanje storitve, bi bilo treba poleg medsektorskih dejavnikov upoštevati tudi dejavnike, značilne za posamezni sektor. Kar zadeva dobavitelje energije, bi ti dejavniki lahko vključevali količino ali delež ustvarjene električne energije na nacionalni ravni; za dobavitelje nafte količino na dan; za zračni promet, vključno z letališči in letalskimi prevozniki, železniški promet in morska pristanišča delež nacionalnega prometa in število potnikov ali tovornih operacij na leto; za bančni sektor ali infrastrukture finančnega trga njihov sistemski pomen glede na skupna sredstva ali razmerje med temi skupnimi sredstvi in BDP; za zdravstveni sektor število bolnikov v oskrbi ponudnika na leto; za sektor pridobivanja in čiščenja vode ter preskrbe z njo obseg, število in vrste uporabnikov, ki se oskrbujejo z vodo, vključno na primer z bolnicami, javnimi službami, organizacijami ali posamezniki, ter obstoj nadometnih virov vode, ki oskrbujejo isto geografsko območje.

(29) Da bi dosegli in ohranjali visoko raven varnosti omrežij in informacijskih sistemov, bi morala vsaka država članica imeti nacionalno strategijo za varnost omrežij in informacijskih sistemov, v kateri bi določila strateške cilje in konkretne ukrepe politik, ki jih je treba izvesti.

(30) Glede na razlike v nacionalnih strukturah upravljanja in zaradi varovanja že obstoječih sektorskih dogovorov ali nadzornih in regulativnih organov Unije ter da bi se izognili podvajanju, bi države članice morale imeti možnost imenovati več kot en pristojni nacionalni organ, odgovoren za izvajanje nalog, povezanih z varnostjo omrežij in informacijskih sistemov izvajalcev bistvenih storitev in ponudnikov digitalnih storitev po tej direktivi.

(31) Za zagotavljanje lažjega čezmejnega sodelovanja in komunikacije ter za učinkovito izvajanje te direktive je nujno, da vsaka država članica brez poseganja v sektorske regulativne ureditve imenuje nacionalno enotno kontaktno točko, odgovorno za usklajevanje vprašanj v zvezi z varnostjo omrežij in informacijskih sistemov ter za čezmejno sodelovanje na ravni Unije. Pristojni organi in enotne kontaktne točke bi morali imeti ustrezne tehnične, finančne in človeške vire, da bi lahko uspešno in učinkovito opravljali dodeljene naloge ter tako dosegli cilje te direktive. Ker je namen te direktive z ustvarjanjem zaupanja izboljšati delovanje notranjega trga, je treba organom držav članic omogočiti učinkovito sodelovanje z ekonomskimi akterji in jih ustrezno strukturirati.

(32) Pristojni organi ali skupine za odzivanje na incidente na področju računalniške varnosti (v nadaljnjem besedilu: skupine CSIRT) bi morali prejemati priglasitve incidentov. Enotne kontaktne točke ne bi smele neposredno prejemati priglasitev incidentov, razen če niso istočasno v vlogi pristojnega organa ali skupine CSIRT. Kljub temu pa bi pristojni organ ali skupina CSIRT morala imeti možnost, da enotni kontaktni točki naložita, da priglasitve incidentov pošlje enotnim kontaktnim točkam drugih držav članic, na katere je incident vplival.

(33) Da bi bile države članice in Komisija dobro obveščene, bi morala enotna kontakta točka poslati skupini za sodelovanje zbirno poročilo, podatki v tem zbirnem poročilu pa bi morali biti anonimizirani, da se ohranita zaupnost priglasitev ter identiteta izvajalcev bistvenih storitev in ponudnikov digitalnih storitev, saj informacije o identiteti subjektov priglasiteljev niso potrebne za izmenjavo najboljših praks v skupini za sodelovanje. V zbirnem poročilu bi morale biti navedene informacije o številu prejetih priglasitev in narava priglašenih incidentov, kot so vrsta, resnost ali trajanje kršitev varnosti.

(34) Države članice bi morale imeti ustrezne tehnične in organizacijske zmogljivosti za preprečevanje, odkrivanje in ublažitev incidentov in tveganj v omrežjih in informacijskih sistemih ter za odzivanje nanje. Zato bi morale države članice zagotoviti, da imajo dobro delujoče skupine CSIRT, znane tudi kot skupine za odzivanje na računalniške grožnje (v nadaljnjem besedilu: skupine CERT), ki izpolnjujejo osnovne zahteve, da bi se tako zajamčile učinkovite in združljive zmogljivosti za obvladovanje incidentov in tveganj in zagotovilo učinkovito sodelovanje na ravni Unije. Da bi te zmogljivosti in sodelovanje lahko koristili vsem vrstam izvajalcev bistvenih storitev in ponudnikov digitalnih storitev, bi morale države članice zagotoviti, da je za vsako vrsto odgovorna ena od določenih skupin CSIRT. Mednarodno sodelovanje na področju kibernetske varnosti je pomembno, zato bi morali skupinam CSIRT poleg sodelovanja v mreži skupin CSIRT, vzpostavljeni s to direktivo, omogočiti sodelovanje tudi v mrežah mednarodnega sodelovanja.

(35) Večino omrežij in informacijskih sistemov upravljajo zasebna podjetja, zato je sodelovanje med javnim in zasebnim sektorjem bistvenega pomena. Izvajalce bistvenih storitev in ponudnike digitalnih storitev bi bilo treba spodbujati, da za zagotavljanje varnosti omrežij in informacijskih sistemov vzpostavijo lastne neformalne mehanizme sodelovanja. Skupini za sodelovanje bi morali omogočiti, da k posvetovanjem po potrebi pritegne zadevne deležnike. Za uspešno spodbujanje izmenjave informacij in najboljših praks je treba zagotoviti, da izvajalci bistvenih storitev in ponudniki digitalnih storitev, ki pri njej sodelujejo, zaradi tega sodelovanja ne bodo v slabšem položaju.

(36) ENISA bi morala državam članicam in Komisiji pomagati s strokovnim znanjem in nasveti ter zagotavljati lažjo izmenjavo najboljših praks. Pri uporabi te direktive bi se Komisija morala posvetovati z ENISA, to možnost pa bi morale imeti tudi države članice. Da bi države članice razvile zmogljivosti in pridobile znanje, bi morala biti skupina za sodelovanje tudi forum za izmenjavo najboljših praks ter razpravo o zmogljivostih in pripravljenosti držav članic, poleg tega pa bi morala na prostovoljni osnovi pomagati svojim članom pri oceni nacionalnih strategij s področja varnosti omrežij in informacijskih sistemov, pri razvoju zmogljivosti in pri oceni vaj v zvezi z varnostjo omrežij in informacijskih sistemov.

(37) Kjer je to primerno, bi morali državam članicam omogočiti, da pri uporabi te direktive uporabijo ali prilagodijo obstoječe organizacijske strukture ali strategije.

(38) Zadevne naloge skupine za sodelovanje in agencije ENISA so soodvisne in se medsebojno dopolnjujejo. Na splošno bi ENISA morala skupini za sodelovanje pomagati pri opravljanju nalog, in sicer v skladu s ciljem ENISA, določenim v Uredbi (EU) št. 526/2013 Evropskega parlamenta in Sveta ([1]), da pomaga institucijam, organom, uradom in agencijam Unije ter državam članicam pri izvajanju politik, potrebnih za izpolnjevanje pravnih in regulativnih zahtev v zvezi z varnostjo omrežij in informacijskih sistemov v veljavnih in prihodnjih pravnih aktih Unije. ENISA bi morala pomagati zlasti na področjih, ki se prekrivajo z njenimi nalogami, kot so določene v Uredbi (EU) št. 526/2013, to je analiza strategij s področja varnosti omrežij in informacijskih sistemov, pomoč pri organizaciji in izvedbi vaj v zvezi z varnostjo omrežij in informacijskih sistemov na ravni Unije ter izmenjava informacij in najboljših praks o ozaveščanju in usposabljanju. Sodelovati bi morala tudi pri razvoju smernic za merila, značilna za posamezni sektor, namenjena določitvi, kako pomemben je vpliv incidenta.

([1]) Uredba (EU) št. 526/2013 Evropskega parlamenta in Sveta z dne 21. maja 2013 o Agenciji Evropske unije za varnost omrežij in informacij (ENISA) in razveljavitvi Uredbe (ES) št. 460/2004 (UL L 165, 18.6.2013, str. 41).

(39) Za spodbujanje večje varnosti omrežij in informacijskih sistemov bi morala skupina za sodelovanje po potrebi sodelovati z zadevnimi institucijami, organi, uradi in agencijami Unije, da bi z njimi izmenjavala znanje in najboljše prakse ter jim svetovala o varnostnih vidikih omrežij in informacijskih sistemov, ki bi lahko vplivali na njihovo delo, pri tem pa ravnati v skladu z obstoječimi ureditvami za izmenjavo zaupnih informacij. Pri sodelovanju z organi kazenskega pregona v zvezi z varnostnimi vidiki omrežij in informacijskih sistemov, ki bi lahko vplivali na njihovo delo, bi morala uporabljati obstoječe informacijske poti in vzpostavljena omrežja.

(40) Informacije o incidentih so vse bolj dragocene za širšo javnost in podjetja, zlasti mala in srednja podjetja. Na nacionalni ravni so v nekaterih primerih že dostopne na spletu v jeziku posamezne države ter zlasti navajajo incidente in pojave z nacionalno razsežnostjo. Ker podjetja vse pogosteje poslujejo prek meja, državljani pa uporabljajo spletne storitve, bi bilo treba informacije o incidentih zagotavljati v zbirni obliki na ravni Unije. Sekretariat mreže skupin CSIRT naj vzdržuje spletno mesto oziroma na obstoječem spletnem mestu gosti namensko stran, na kateri so širši javnosti na voljo splošne informacije o večjih incidentih, ki so se zgodili v Uniji, pri čemer je posebna pozornost namenjena interesom in potrebam podjetij. Skupine CSIRT, ki sodelujejo v mreži skupin CSIRT, naj na prostovoljni osnovi prispevajo informacije za objavo na tem spletnem mestu, ne vključijo pa tajnih ali občutljivih informacij.

(41) Če informacije štejejo za zaupne v skladu s predpisi Unije in nacionalnimi predpisi o poslovni tajnosti, bi bilo to zaupnost treba zagotoviti pri izvajanju dejavnosti in izpolnjevanju ciljev te direktive.

(42) Vaje, ki simulirajo različne scenarije incidentov v realnem času, so nujne za preskus pripravljenosti in sodelovanja držav članic glede varnosti omrežij in informacijskih sistemov. Sklop vaj, imenovan CyberEurope, ki jih je usklajevala ENISA in v katerih so sodelovale države članice, je koristno orodje za preskušanje in pripravo priporočil o možnostih izboljšanja obvladovanja incidentov na ravni Unije. Ker države članice trenutno niso zavezane, niti da vaje načrtujejo niti da v njih sodelujejo, bi vzpostavitev mreže skupin CSIRT po tej direktivi državam članicam morala omogočiti sodelovanje v vajah na podlagi natančnega načrtovanja in strateških izbir. Skupina za sodelovanje, ustanovljena po tej direktivi, bi morala obravnavati strateške odločitve glede vaj zlasti, vendar ne izključno, kar zadeva rednost vaj in načrtovanje scenarijev. ENISA bi morala v skladu s svojim mandatom podpreti organizacijo in izvedbo vaj na ravni Unije ter v ta namen skupini za sodelovanje in mreži skupin CSIRT zagotoviti strokovno znanje in jima svetovati.

(43) Zaradi globalne narave varnostne problematike, ki zadeva omrežja in informacijske sisteme, je potrebno tesnejše mednarodno sodelovanje, da se izboljšajo varnostni standardi in okrepi izmenjava informacij ter spodbudi skupen globalen pristop do varnostnih vprašanj.

(44) Za zagotavljanje varnosti omrežij in informacijskih sistemov so v veliki meri odgovorni izvajalci bistvenih storitev in ponudniki digitalnih storitev. Z ustreznimi regulativnimi zahtevami in prostovoljnimi sektorskimi praksami bi bilo treba spodbujati in razvijati kulturo obvladovanja tveganja, ki vključuje oceno tveganja in izvajanje ustreznih varnostnih ukrepov za zadevna tveganja. Za učinkovito delovanje skupine za sodelovanje in mreže skupin CSIRT je bistvena tudi vzpostavitev zanesljivih enakih konkurenčnih pogojev, da se zagotovi učinkovito sodelovanje vseh držav članic.

(45) Ta direktiva se uporablja le za tiste javne uprave, ki so opredeljene kot izvajalci bistvenih storitev. Države članice so zato odgovorne za zagotavljanje varnosti omrežij in informacijskih sistemov javnih uprav, ki ne sodijo v področje uporabe te direktive.

(46) Med ukrepe za obvladovanje tveganj spadajo ukrepi za prepoznavanje tveganj incidentov, preprečevanje in odkrivanje incidentov ter njihovo obvladovanje, in ukrepi za ublažitev njihovih učinkov. Varnost omrežij in informacijskih sistemov obsega varnost shranjenih, prenesenih in obdelanih podatkov.

(47) Pristojnim organom bi morali tudi v prihodnje omogočiti, da sprejmejo nacionalne smernice glede okoliščin, v katerih morajo izvajalci bistvenih storitev priglasiti incidente.

(48) Številna podjetja v Uniji so pri zagotavljanju storitev odvisna od ponudnikov digitalnih storitev. Ker bi bile nekatere digitalne storitve lahko pomembno sredstvo za uporabnike, vključno z izvajalci bistvenih storitev, in ker ti uporabniki morda nimajo vedno na voljo drugih enakovrednih možnosti, bi se morala ta direktiva uporabljati tudi za ponudnike takšnih storitev. Varnost, neprekinjenost in zanesljivost vrste digitalnih storitev iz te direktive so ključne za nemoteno delovanje številnih podjetij. Prekinitev take digitalne storitve bi lahko preprečila zagotavljanje drugih storitev, ki so od nje odvisne, in bi tako lahko vplivala na ključne ekonomske in družbene dejavnosti v Uniji. Take digitalne storitve bi tako lahko bile ključnega pomena za nemoteno delovanje podjetij, ki so od njih odvisna, ter zlasti za udeležbo teh podjetij na notranjem trgu in čezmejno trgovino v Uniji. Ta direktiva se uporablja za tiste ponudnike digitalnih storitev, za katere se šteje, da ponujajo digitalne storitve, od katerih so številna podjetja v Uniji vse bolj odvisna.

(49) Ponudniki digitalnih storitev bi morali zagotavljati raven varnosti, ki ustreza stopnji tveganja za varnost digitalnih storitev, ki jih zagotavljajo, in pomenu njihovih storitev za dejavnosti drugih podjetij v Uniji. Stopnja tveganja za izvajalce bistvenih storitev, ki so pogosto bistvene za ohranjanje ključnih družbenih in gospodarskih dejavnosti, je v praksi višja od stopnje tveganja za ponudnike digitalnih storitev. Zato bi morale biti varnostne zahteve za ponudnike digitalnih storitev manj stroge. Ponudnikom digitalnih storitev bi morali omogočiti, da se sami odločijo za sprejetje ukrepov, ki se jim zdijo primerni za obvladovanje tveganj, ki ogrožajo varnost njihovih omrežij in informacijskih sistemov. Zaradi čezmejne narave ponudnikov digitalnih storitev, bi se moral zanje uporabljati bolj usklajen pristop na ravni Unije. Z izvedbenimi akti bi morali zagotoviti lažjo določitev in izvajanje tovrstnih ukrepov.

(50) Čeprav proizvajalci strojne in razvijalci programske opreme niso izvajalci bistvenih storitev ali ponudniki digitalnih storitev, njihovi izdelki krepijo varnost omrežij in informacijskih sistemov. Izvajalcem bistvenih storitev in ponudnikom digitalnih storitev zato pomembno pomagajo pri varstvu njihovih omrežij in informacijskih sistemov. Za to strojno in programsko opremo se že uporabljajo obstoječi predpisi o odgovornosti za izdelek.

(51) S tehničnimi in organizacijskimi ukrepi, naloženimi izvajalcem bistvenih storitev in ponudnikom digitalnih storitev, ne bi smeli predpisovati, da se določen komercialni izdelek informacijske in komunikacijske tehnologije oblikuje, razvije ali proizvede na določen način.

(52) Izvajalci bistvenih storitev in ponudniki digitalnih storitev bi morali zagotavljati varnost omrežij in informacijskih sistemov, ki jih uporabljajo. To so predvsem zasebna omrežja in informacijski sistemi, ki jih upravlja njihovo notranje osebje za IT ali pa za njihovo varnost skrbi zunanji izvajalec. Zahteve glede varnosti in priglasitve bi morali za zadevne izvajalce bistvenih storitev in ponudnike digitalnih storitev veljati ne glede na to, ali omrežja in informacijske sisteme vzdržujejo sami ali njihov zunanji izvajalec.

(53) Da ne bi bili izvajalci bistvenih storitev in ponudniki digitalnih storitev nesorazmerno finančno in upravno obremenjeni, bi morale biti zahteve sorazmerne s tveganjem, ki ga pomenita zadevno omrežje in informacijski sistem, pri čemer bi bilo treba upoštevati dovršenost takih ukrepov. V primeru ponudnikov digitalnih storitev se te zahteve ne bi smele uporabljati za mikro- in mala podjetja.

(54) Kadar javne uprave držav članic uporabljajo storitve ponudnikov digitalnih storitev, zlasti storitve računalništva v oblaku, bi morda hotele od ponudnikov teh storitev zahtevati, naj poleg ukrepov, ki jih ponudniki digitalnih storitev običajno zagotavljajo v skladu s to direktivo, sprejmejo dodatne varnostne ukrepe. Zato bi jim bilo treba omogočiti, da to storijo s pogodbenimi obveznostmi.

(55) Opredelitve pojmov spletna tržnica, spletni iskalnik in storitve računalništva v oblaku so v tej direktivi določene za poseben namen te direktive in ne posegajo v druge instrumente.

(56) Ta direktiva državam članicam ne bi smela preprečevati sprejetja nacionalnih ukrepov, na podlagi katerih morajo organi javnega sektorja zagotoviti specifične varnostne zahteve v okviru pogodb za storitve računalništva v oblaku. Vsi ti nacionalni ukrepi bi se morali uporabljati za zadevni organ javnega sektorja in ne za ponudnika storitev računalništva v oblaku.

(57) Zaradi temeljnih razlik med izvajalci bistvenih storitev, zlasti njihove neposredne povezanosti s fizično infrastrukturo, in ponudniki digitalnih storitev, zlasti njihove čezmejne narave, bi morali v tej direktivi sprejeti ločen pristop do stopnje harmonizacije za obe skupini subjektov. Kar zadeva izvajalce bistvenih storitev, bi morali državam članicam omogočiti, da določijo zadevne izvajalce in naložijo strožje zahteve od tistih v tej direktivi. Države članice ne bi smele določiti ponudnikov digitalnih storitev, saj bi se morala ta direktiva uporabljati za vse ponudnike digitalnih storitev, ki sodijo v njeno področje uporabe. Kar zadeva varnostne zahteve in zahteve glede priglasitve, bi morali ta direktiva in izvedbeni akti, sprejeti na njeni podlagi, zagotoviti tudi visoko stopnjo harmonizacije za ponudnike digitalnih storitev. To bi moralo omogočiti enotno obravnavo ponudnikov digitalnih storitev v Uniji, sorazmerno z njihovo naravo in stopnjo tveganja, ki bi mu lahko bili izpostavljeni.

(58) Brez poseganja v obveznosti, ki jih imajo države članice na podlagi prava Unije, ta direktiva državam članicam ne bi smela preprečiti, da varnostne zahteve in zahteve glede priglasitve uvedejo za subjekte, ki niso ponudniki digitalnih storitev s področja uporabe te direktive.

(59) Pristojni organi bi morali ustrezno pozornost nameniti ohranjanju neformalnih in zanesljivih poti za izmenjavo informacij. Pri obveščanju javnosti o incidentih, priglašenih pristojnim organom, bi bilo treba najti ravnotežje med interesom javnosti, da je obveščena o nevarnostih, na eni strani, ter morebitno škodo za ugled in poslovanje izvajalcev bistvenih storitev in ponudnikov digitalnih storitev, ki priglasijo incidente, na drugi strani. Pri izvajanju obveznosti priglasitve bi morali pristojni organi in skupine CSIRT posebno pozorno paziti, da informacije o ranljivosti izdelka ostanejo strogo zaupne, dokler se varnost znova ne vzpostavi.

(60) Pri ponudnikih digitalnih storitev bi se morale ob upoštevanju narave njihovih storitev in postopkov izvajati blage ter odzivne naknadne nadzorne dejavnosti. Zadevni pristojni organ bi moral zato ukrepati – zlasti takrat, ko se je incident že zgodil – le na podlagi predloženih dokazov, ki mu jih na primer predloži sam ponudnik digitalne storitve, drug pristojni organ, vključno s pristojnim organom druge države članice, ali uporabnik storitve, da ponudnik digitalne storitve ne ravna v skladu z zahtevami iz te direktive. Pristojni organ torej ne bi smel biti splošno obvezan, da nadzoruje ponudnike digitalnih storitev.

(61) Pristojni organi bi morali imeti potrebna sredstva za opravljanje svojih nalog, vključno s pooblastili za pridobivanje zadostnih informacij za oceno ravni varnosti omrežij in informacijskih sistemov.

(62) Incidenti so lahko posledica kriminalnih dejavnosti, ki se preprečujejo, preiskujejo in preganjajo z usklajevanjem in sodelovanjem med izvajalci bistvenih storitev, ponudniki digitalnih storitev, pristojnimi organi in organi kazenskega pregona. V primeru suma, da je incident povezan s hudimi kaznivimi dejanji po pravu Unije ali nacionalnem pravu, bi morale države članice izvajalce bistvenih storitev in ponudnike digitalnih storitev spodbujati, da incident, za katerega sumijo, da je hudo kaznivo dejanje, prijavijo ustreznim organom kazenskega pregona. Kjer je to ustrezno, je priporočljivo, da Evropski center za boj proti kibernetski kriminaliteti (EC3) in ENISA zagotavljata lažje usklajevanje med pristojnimi organi in organi kazenskega pregona različnih držav članic.

(63) V številnih primerih je zaradi incidentov ogrožena varnost osebnih podatkov. Zato bi morali pristojni organi in organi za varstvo podatkov pri odpravljanju kršitev varnosti osebnih podatkov, nastalih zaradi incidentov, med seboj sodelovati in si izmenjevati pomembne informacije.

(64) Pristojnost glede ponudnikov digitalnih storitev bi morali podeliti državi članici, v kateri ima ponudnik digitalnih storitev glavni sedež v Uniji, ki je načeloma tista država članica, kjer je glavna uprava ponudnika v Uniji. Sedež pomeni, da se dejavnost izvaja dejansko in učinkovito na podlagi stabilnih ureditev. Pravna oblika takih ureditev, bodisi prek podružnice ali odvisne družbe, ki je pravna oseba, v tem pogledu ni odločujoči dejavnik. To merilo

ne bi smelo biti odvisno od tega, ali so omrežja in informacijski sistemi fizično locirani na tistem mestu; prisotnost in uporaba teh sistemov sami po sebi ne pomenita tega glavnega sedeža in zato nista merili za ugotavljanje glavnega sedeža.

(65) Ponudnik digitalnih storitev brez sedeža v Uniji, ki nudi storitve v Uniji, bi moral določiti predstavnika. Da bi ugotovili, ali tak ponudnik digitalnih storitev le-te nudi v Uniji, bi bilo treba preveriti, ali je jasno, da namerava ponudnik digitalnih storitev svoje storitve nuditi posameznikom v eni ali več državah članicah. Sama dostopnost spletnega mesta ponudnika digitalnih storitev ali spletnega mesta posrednika v Uniji ali elektronskega naslova in drugih kontaktnih podatkov ali uporaba jezika, ki se običajno uporablja v tretji državi, v kateri ima ponudnik digitalnih storitev sedež, ne zadošča za določitev takšne namere. Vendar se lahko z dejavniki, kot je uporaba jezika ali valute, ki se običajno uporablja v eni ali več državah članicah, z možnostjo naročanja storitev v tem drugem jeziku, ali navedba strank ali uporabnikov, ki so v Uniji, jasno pokaže, da namerava ponudnik digitalnih storitev nuditi storitve v Uniji. Predstavnik bi moral delovati v imenu ponudnika digitalnih storitev, pristojni organi ali skupine CSIRT pa bi morali imeti možnost, da navežejo stik s predstavnikom. Ponudnik digitalnih storitev bi moral predstavnika pisno izrecno določiti, da v njegovem imenu izvaja njegove obveznosti na podlagi te direktive, vključno s priglasitvijo incidentov.

(66) Standardizacija varnostnih zahtev je proces, ki ga narekuje trg. Za zagotovitev usklajene uporabe varnostnih standardov bi morale države članice spodbujati uporabo ali upoštevanje določenih standardov ter tako zagotoviti visoko raven varnosti omrežij in informacijskih sistemov na ravni Unije. ENISA bi morala državam članicam pomagati s svetovanjem in smernicami. V ta namen bi bilo morda v pomoč, če bi oblikovali harmonizirane standarde, kar bi morali storiti v skladu z Uredbo (EU) št. 1025/2012 Evropskega parlamenta in Sveta ([1]).

(67) Subjektom, ki ne sodijo na področje uporabe te direktive, se lahko zgodijo incidenti, ki pomembno vplivajo na storitve, ki jih ponujajo. Kadar ti subjekti menijo, da je priglasitev pojava takšnih incidentov v javnem interesu, bi jim bilo treba omogočiti, da to storijo prostovoljno. Te priglasitve bi morali obdelati ustrezni organi držav članic ali skupine CSIRT, kadar takšna obdelava za zadevne države članice ne pomeni nesorazmernega ali neupravičenega bremena.

(68) Za zagotovitev enotnih pogojev za izvajanje te direktive bi bilo treba na Komisijo prenesti izvedbena pooblastila za določitev postopkovnih ureditev, potrebnih za delovanje skupine za sodelovanje, ter zahtev glede varnosti in priglasitve, ki se uporabljajo za ponudnike digitalnih storitev. Navedena pooblastila bi bilo treba izvajati v skladu z Uredbo (EU) št. 182/2011 Evropskega parlamenta in Sveta ([2]). Komisija bi morala pri sprejemanju izvedbenih aktov o postopkovnih ureditvah, potrebnih za delovanje skupine za sodelovanje, v največji možni meri upoštevati mnenje ENISA.

(69) Komisija bi morala pri sprejemanju izvedbenih aktov o varnostnih zahtevah za ponudnike digitalnih storitev v največji možni meri upoštevati mnenje ENISA in se posvetovati z zainteresiranimi deležniki. Komisija bi tudi morala upoštevati naslednje primere: glede varnosti sistemov in infrastrukture: fizično in okoljsko varnost, zanesljivost oskrbe, nadzor dostopa do omrežij in informacijskih sistemov ter celovitost omrežij in informacijskih sistemov; glede obvladovanja incidentov: postopke za obvladovanje incidentov, zmogljivost zaznavanja incidentov, poročanje in obveščanje o incidentih; glede upravljanja neprekinjenega poslovanja: strategijo za neprekinjenost storitve in načrte izrednih ukrepov, sanacijske zmogljivosti po incidentih; in glede spremljanja, revidiranja in preskušanja: politike spremljanja in vodenja evidenc, izvajanje načrtov izrednih ukrepov, preskušanje omrežij in informacijskih sistemov, ocene varnosti in spremljanje skladnosti.

(70) Pri izvajanju te direktive bi se Komisija morala po potrebi povezati z ustreznimi sektorskimi odbori in organi, ustanovljenimi na ravni Unije na področjih, zajetih v tej direktivi.

([1]) Uredba (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 (UL L 316, 14.11.2012, str. 12).

([2]) Uredba (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 (UL L 55, 28.2.2011, str. 13).

(71) Komisija bi morala redno v posvetovanju z zainteresiranimi deležniki pregledovati to direktivo, zlasti da bi ugotovila, ali jo je treba prilagoditi spremenjenim družbenim, političnim, tehnološkim ali tržnim razmeram.

(72) Za izmenjavo informacij o tveganjih in incidentih v skupini za sodelovanje in mreži skupin CSIRT ter za izpolnjevanje zahtev za priglasitev incidentov pristojnim nacionalnim organom ali skupinam CSIRT bi lahko bila potrebna obdelava osebnih podatkov. Taka obdelava bi morala potekati v skladu z Direktivo 95/46/ES Evropskega parlamenta in Sveta ([1]) in Uredbo (ES) št. 45/2001 Evropskega parlamenta in Sveta ([2]). Pri izvajanju te direktive bi se morala po potrebi uporabljati Uredba Evropskega parlamenta in Sveta (ES) št. 1049/2001 ([3]).

(73) V skladu s členom 28(2) Uredbe (ES) št. 45/2001 je bilo opravljeno posvetovanje z Evropskim nadzornikom za varstvo podatkov, ki je svoje mnenje podal dne 14. junija 2013 ([4]).

(74) Ker cilja te direktive, in sicer zagotavljanja visoke skupne ravni varnosti omrežij in informacijskih sistemov v Uniji, države članice ne morejo zadovoljivo doseči, temveč se zaradi učinkov ukrepov lažje doseže na ravni Unije, lahko Unija sprejme ukrepe v skladu z načelom subsidiarnosti iz člena 5 Pogodbe o Evropski uniji. V skladu z načelom sorazmernosti iz navedenega člena ta direktiva ne presega tistega, kar je potrebno za doseganje navedenega cilja.

(75) 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 podati izjavo. To direktivo bi bilo treba izvajati v skladu s temi pravicami in načeli –

SPREJELA NASLEDNJO DIREKTIVO:

POGLAVJE I

SPLOŠNE DOLOČBE

Člen 1

Predmet urejanja in področje uporabe

1. Ta direktiva določa ukrepe za doseganje visoke skupne ravni varnosti omrežij in informacijskih sistemov v Uniji, da bi izboljšali delovanje notranjega trga.

2. V ta namen ta direktiva:

(a) določa obveznosti vseh držav članic, da sprejmejo nacionalne strategije za varnost omrežij in informacijskih sistemov;

(b) vzpostavlja skupino za sodelovanje, da bi podprli in zagotovili lažje strateško sodelovanje in izmenjavo informacij med državami članicami ter okrepili zaupanje med njimi;

(c) vzpostavlja mrežo skupin za odzivanje na incidente na področju računalniške varnosti (v nadaljnjem besedilu: mreža skupin CSIRT), da bi prispevali h krepitvi zaupanja med državami članicami ter spodbudili hitro in učinkovito operativno sodelovanje;

([1]) Direktiva 95/46/ES Evropskega parlamenta in Sveta z dne 24. oktobra 1995 o varstvu posameznikov pri obdelavi osebnih podatkov in o prostem pretoku takih podatkov (UL L 281, 23.11.1995, str. 31).
([2]) Uredba (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 (UL L 8, 12.1.2001, str. 1).
([3]) Uredba Evropskega parlamenta in Sveta (ES) št. 1049/2001 z dne 30. maja 2001 o dostopu javnosti do dokumentov Evropskega parlamenta, Sveta in Komisije (UL L 145, 31.5.2001, str. 43).
([4]) UL C 32, 4.2.2014, str. 19.

(d) določa varnostne zahteve in zahteve glede priglasitve za izvajalce bistvenih storitev in za ponudnike digitalnih storitev;

(e) določa obveznosti držav članic glede določitve pristojnih nacionalnih organov, enotnih kontaktnih točk in skupin CSIRT, katerih naloge so povezane z varnostjo omrežij in informacijskih sistemov.

3. Varnostne zahteve in zahteve glede priglasitve iz te direktive se ne uporabljajo za podjetja, za katera veljajo zahteve iz členov 13a in 13b Direktive 2002/21/ES, niti za ponudnike storitev zaupanja, za katere veljajo zahteve iz člena 19 Uredbe (EU) št. 910/2014.

4. Ta direktiva se uporablja brez poseganja v Direktivo Sveta 2008/114/ES ([1]) in direktivi 2011/93/EU ([2]) in 2013/40/EU ([3]) Evropskega parlamenta in Sveta.

5. Brez poseganja v člen 346 PDEU se informacije, ki so zaupne v skladu s predpisi Unije in nacionalnimi predpisi, na primer o poslovni tajnosti, s Komisijo in drugimi ustreznimi organi izmenjajo le, če je takšna izmenjava potrebna za uporabo te direktive. Izmenjava informacij je omejena na obseg, ki je ustrezen in sorazmeren glede na namen te izmenjave. Pri takšni izmenjavi informacij se ohranijo zaupnost zadevnih informacij ter zaščitijo varnost in poslovni interesi izvajalcev bistvenih storitev in ponudnikov digitalnih storitev.

6. Ta direktiva ne posega v ukrepe, ki jih države članice sprejmejo za zaščito svojih temeljnih državnih funkcij, zlasti za zaščito nacionalne varnosti,vključno z ukrepi za zaščito informacij, za katere države članice menijo, da bi njihovo razkritje bilo v nasprotju s temeljnimi interesi njihove varnosti, ter za ohranitev javnega reda in miru, predvsem za omogočanje preiskovanja, odkrivanja in pregona kaznivih dejanj.

7. Kadar sektorski pravni akt Unije zahteva, da izvajalec bistvenih storitev ali ponudnik digitalnih storitev zagotovi varnost svojih omrežij in informacijskih sistemov ali priglasi incidente, se uporabljajo zadevne določbe tega sektorskega pravnega akta Unije, če so takšne zahteve po učinku vsaj enakovredne obveznostim iz te direktive.

Člen 2

Obdelava osebnih podatkov

1. Obdelava osebnih podatkov na podlagi te direktive se izvaja v skladu z Direktivo 95/46/ES.

2. Obdelava osebnih podatkov s strani institucij in organov Unije na podlagi te direktive se izvaja v skladu z Uredbo (ES) št. 45/2001.

Člen 3

Minimalna harmonizacija

Države članice lahko brez poseganja v člen 16(10) in svoje obveznosti na podlagi prava Unije sprejmejo ali ohranijo določbe za doseganje višje stopnje varnosti omrežja in informacijskih sistemov.

([1]) Direktiva Sveta 2008/114/ES z dne 8. decembra 2008 o ugotavljanju in določanju evropske kritične infrastrukture ter o oceni potrebe po izboljšanju njene zaščite (UL L 345, 23.12.2008, str. 75).

([2]) Direktiva 2011/93/EU Evropskega parlamenta in Sveta z dne 13. decembra 2011 o boju proti spolni zlorabi in spolnemu izkoriščanju otrok ter otroški pornografiji in nadomestitvi Okvirnega sklepa Sveta 2004/68/PNZ (UL L 335, 17.12.2011, str. 1).

([3]) Direktiva 2013/40/EU Evropskega parlamenta in Sveta z dne 12. avgusta 2013 o napadih na informacijske sisteme in nadomestitvi Okvirnega sklepa Sveta 2005/222/PNZ (UL L 218, 14.8.2013, str. 8).

Člen 4

Opredelitev pojmov

V tej direktivi se uporabljajo naslednje opredelitve pojmov:

1. „omrežje in informacijski sistem“ pomeni:

   (a) elektronsko komunikacijsko omrežje v smislu točke (a) člena 2 Direktive 2002/21/ES;

   (b) vsako napravo ali skupino med seboj povezanih ali sorodnih naprav, od katerih ena ali več na podlagi programa opravlja samodejno obdelavo digitalnih podatkov, ali

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

2. „varnost omrežij in informacijskih sistemov“ pomeni zmožnost omrežij in informacijskih sistemov, da na določeni ravni zaupanja preprečijo vse dogodke, ki ogrožajo razpoložljivost, avtentičnost, celovitost ali zaupnost shranjenih, prenesenih ali obdelanih podatkov ali pripadajočih storitev, ki jih navedena omrežja in informacijski sistemi zagotavljajo ali so prek njih dostopne;

3. „nacionalna strategija za varnost omrežij in informacijskih sistemov“ pomeni okvir s strateškimi cilji in prednostnimi nalogami na področju varnosti omrežij in informacijskih sistemov na nacionalni ravni;

4. „izvajalec bistvenih storitev“ pomeni javni ali zasebni subjekt, ki spada med vrste iz Priloge II in izpolnjuje merila, določena v členu 5(2);

5. „digitalna storitev“ pomeni storitev v smislu točke (b) člena 1(1) Direktive (EU) 2015/1535 Evropskega parlamenta in Sveta ([1]), ki spada med vrste storitev iz Priloge III;

6. „ponudnik digitalnih storitev“ pomeni vsako pravno osebo, ki zagotavlja digitalno storitev;

7. „incident“ pomeni vsak dogodek, ki ima dejanski negativen učinek na varnost omrežij in informacijskih sistemov;

8. „obvladovanje incidentov“ pomeni vse postopke, ki podpirajo odkrivanje, analizo in zajezitev incidentov ter odzivanje nanje;

9. „tveganje“ pomeni vsako razumno določljivo okoliščino ali dogodek, ki ima lahko negativen učinek na varnost omrežja in informacijskih sistemov;

10. „predstavnik“ pomeni vsako fizično ali pravno osebo s sedežem v Uniji, ki je izrecno določena, da deluje v imenu ponudnika digitalnih storitev, ki nima sedeža v Uniji, in s katero lahko nacionalni pristojni organ ali skupina CSIRT vzpostavi stik namesto s ponudnikom digitalnih storitev, kar zadeva obveznosti tega ponudnika digitalnih storitev na podlagi te direktive;

11. „standard“ pomeni standard v smislu točke 1 člena 2 Uredbe (EU) št. 1025/2012;

12. „specifikacija“ pomeni tehnično specifikacijo v smislu točke 4 člena 2 Uredbe (EU) št. 1025/2012;

13. „stičišče omrežij“ pomeni omrežno zmogljivost, ki omogoča medsebojno povezavo več kot dveh neodvisnih avtonomnih sistemov, predvsem zaradi izmenjave internetnega prometa; stičišče omrežij zagotavlja medsebojno povezavo le avtonomnih sistemov; stičišče omrežij omogoča izmenjavo internetnega prometa med katerima koli sodelujočima avtonomnima sistemoma, brez prehoda prek tretjega avtonomnega sistema, prav tako pa ne spreminja takšnega prometa ali kako drugače posega vanj;

14. „sistem domenskih imen“ pomeni hierarhičen porazdeljen sistem dodeljevanja imen v omrežju, ki posreduje poizvedbe za domenska imena;

([1]) Direktiva (EU) 2015/1535 Evropskega parlamenta in Sveta z dne 9. septembra 2015 o določitvi postopka za zbiranje informacij na področju tehničnih predpisov in pravil za storitve informacijske družbe (UL L 241, 17.9.2015, str. 1).

15. „ponudnik storitev sistema domenskih imen“ pomeni subjekt, ki zagotavlja storitve sistema domenskih imen na internetu;

16. „register domenskih imen najvišje ravni“ pomeni subjekt, ki upravlja in izvaja registracijo imen internetnih domen v okviru določene domene najvišje ravni;

17. „spletna tržnica“ pomeni digitalno storitev, ki omogoča potrošnikom in/ali trgovcem, kot so opredeljeni v točki (a) oziroma točki (b) člena 4(1) Direktive 2013/11/EU Evropskega parlamenta in Sveta ([1]), da na spletišču spletne tržnice ali spletišču trgovca, ki uporablja računalniške storitve spletne tržnice, s trgovci sklenejo pogodbe o spletni prodaji ali pogodbe o spletnih storitvah;

18. „spletni iskalnik“ pomeni digitalno storitev, ki uporabnikom na podlagi poizvedbe na katero koli temo v obliki ključne besede, fraze ali drugega vnosa omogoča iskanje po načeloma vseh spletiščih ali spletiščih v določenem jeziku, ponudi pa povezave do strani z informacijami o zahtevani vsebini;

19. „storitev računalništva v oblaku“ pomeni digitalno storitev, ki omogoča dostop do prožnega in po obsegu prilagodljivega nabora deljivih računalniških virov.

Člen 5

Določitev izvajalcev bistvenih storitev

1. Države članice za vsak sektor in podsektor iz Priloge II do 9. novembra 2018 določijo izvajalce bistvenih storitev s sedežem na svojem ozemlju.

2. Merila za določitev izvajalcev bistvenih storitev iz točke 4 člena 4 so naslednja:

(a) subjekt zagotavlja storitev, ki je bistvena za ohranitev ključnih družbenih in/ali gospodarskih dejavnosti;

(b) zagotavljanje te storitve je odvisno od omrežij in informacijskih sistemov; ter

(c) incident bi imel pomemben negativen vpliv na zagotavljanje te storitve.

3. Za namene odstavka 1 vsaka država članica pripravi seznam storitev iz točke (a) odstavka 2.

4. Kadar subjekt zagotavlja storitev iz točke (a) odstavka 2 v dveh ali več državah članicah, se te države članice za namene odstavka 1 posvetujejo med seboj. To posvetovanje se opravi pred sprejetjem sklepa o določitvi.

5. Države članice redno in vsaj vsaki dve leti po 9. maju 2018 pregledajo in po potrebi posodobijo seznam določenih izvajalcev bistvenih storitev.

6. Skupina za sodelovanje v skladu z nalogami iz člena 11 podpira države članice, da pri določanju izvajalcev bistvenih storitev uporabijo usklajen pristop.

7. Države članice za namene pregleda iz člena 23 najpozneje do 9. novembra 2018 in nato vsaki dve leti Komisiji predložijo potrebne informacije, da lahko slednja oceni izvajanje te direktive, zlasti skladnost pristopov držav članic za določanje izvajalcev bistvenih storitev. Te informacije zajemajo vsaj:

(a) nacionalne ukrepe, ki omogočajo določitev izvajalcev bistvenih storitev;

([1]) Direktiva 2013/11/EU Evropskega parlamenta in Sveta z dne 21. maja 2013 o alternativnem reševanju potrošniških sporov ter spremembi Uredbe (ES) št. 2006/2004 in Direktive 2009/22/ES (Direktiva o alternativnem reševanju potrošniških sporov) (UL L 165, 18.6.2013, str. 63).

(b) seznam storitev iz odstavka 3;

(c) število izvajalcev bistvenih storitev, določenih za vsak sektor iz Priloge II, in navedbo njihovega pomena za ta sektor;

(d) prage, kadar obstajajo, za določitev ustrezne ravni opravljanja storitev glede na število uporabnikov, ki so odvisni od te storitve, kot je določeno v točki (a) člena 6(1), ali glede na pomen zadevnega izvajalca bistvenih storitev, kot je določeno v točki (f) člena 6(1).

Da bi prispevala k zagotavljanju primerljivih informacij, lahko Komisija ob najdoslednejšem upoštevanju mnenja ENISA sprejme ustrezne tehnične smernice glede parametrov informacij iz tega odstavka.

Člen 6

Pomemben negativen vpliv

1. Države članice pri določanju, kako pomemben je negativen vpliv iz točke (c) člena 5(2), upoštevajo vsaj naslednje medsektorske dejavnike:

(a) število uporabnikov, ki so odvisni od storitve zadevnega subjekta;

(b) odvisnost drugih sektorjev iz Priloge II od storitve tega subjekta;

(c) stopnjo in trajanje vpliva, ki bi ga incidenti lahko imeli na gospodarske in družbene dejavnosti ali javno varnost;

(d) tržni delež tega subjekta;

(e) geografsko razširjenost, kar zadeva območje, ki bi ga incident lahko prizadel;

(f) pomen subjekta za ohranitev zadostne ravni storitve ob upoštevanju razpoložljivosti alternativnih načinov za zagotavljanje zadevne storitve.

2. Pri odločanju, ali bi incident imel pomemben negativen vpliv, države članice po potrebi upoštevajo tudi sektorske dejavnike.

POGLAVJE II

NACIONALNI OKVIRI ZA VARNOST OMREŽIJ IN INFORMACIJSKIH SISTEMOV

Člen 7

Nacionalna strategija za varnost omrežij in informacijskih sistemov

1. Vsaka država članica sprejme nacionalno strategijo za varnost omrežij in informacijskih sistemov, v kateri določi strateške cilje ter ustrezne ukrepe politike in regulativne ukrepe, da bi dosegla in vzdrževala visoko raven varnosti omrežja in informacijskih sistemov, pri čemer zajame vsaj sektorje iz Priloge II in storitve iz Priloge III. V nacionalni strategiji za varnost omrežij in informacijskih sistemov se obravnavajo zlasti:

(a) cilji in prednostne naloge nacionalne strategije za varnost omrežij in informacijskih sistemov;

(b) okvir upravljanja za dosego ciljev in prednostnih nalog nacionalne strategije za varnost omrežij in informacijskih sistemov, vključno z vlogami in odgovornostmi vladnih organov in drugih ustreznih akterjev;

(c) opredelitev ukrepov v zvezi s pripravljenostjo, odzivanjem in ponovno vzpostavitvijo, vključno s sodelovanjem med javnim in zasebnim sektorjem;

(d) opredelitev programov izobraževanja, ozaveščanja in usposabljanja v zvezi z nacionalno strategijo za varnost omrežij in informacijskih sistemov;

(e) opredelitev načrtov raziskav in razvoja v zvezi z nacionalno strategijo za varnost omrežij in informacijskih sistemov;

(f) načrt ocene tveganja za prepoznavanje tveganj;

(g) seznam različnih akterjev, vključenih v izvajanje nacionalne strategije za varnost omrežij in informacijskih sistemov.

2. Države članice lahko pri oblikovanju nacionalnih strategij za varnost omrežij in informacijskih sistemov zaprosijo za pomoč ENISA.

3. Države članice sporočijo svoje nacionalne strategije za varnost omrežij in informacijskih sistemov Komisiji v treh mesecih po njihovem sprejetju. Pri tem lahko izvzamejo dele strategije, ki so povezane z nacionalno varnostjo.

Člen 8

Pristojni nacionalni organi in enotna kontaktna točka

1. Vsaka država članica določi enega ali več pristojnih nacionalnih organov za varnost omrežij in informacijskih sistemov (v nadaljnjem besedilu: pristojni organ), pri čemer zajame vsaj sektorje iz Priloge II in storitve iz Priloge III. Države članice lahko to vlogo dodelijo obstoječemu organu ali organom.

2. Pristojni organi spremljajo uporabo te direktive na nacionalni ravni.

3. Vsaka država članica določi enotno nacionalno kontaktno točko za varnost omrežij in informacijskih sistemov (v nadaljnjem besedilu: enotna kontaktna točka). Države članice lahko to vlogo dodelijo obstoječemu organu. Kadar država članica določi le en pristojni organ, je ta tudi enotna kontaktna točka.

4. Enotna kontaktna točka ima povezovalno vlogo in tako zagotavlja čezmejno sodelovanje organov držav članic z ustreznimi organi drugih držav članic ter s skupino za sodelovanje iz člena 11 in mrežo skupin CSIRT iz člena 12.

5. Države članice zagotovijo, da imajo pristojni organi in enotne kontaktne točke ustrezne vire, da učinkovito in uspešno opravljajo dodeljene naloge ter tako izpolnjujejo cilje te direktive. Države članice zagotovijo tudi učinkovito, uspešno in varno sodelovanje določenih predstavnikov v skupini za sodelovanje.

6. Pristojni organi in enotna kontaktna točka se po potrebi in v skladu z nacionalnim pravom posvetujejo z ustreznimi nacionalnimi organi kazenskega pregona in nacionalnimi organi za varstvo podatkov ter z njimi sodelujejo.

7. Vsaka država članica Komisijo nemudoma uradno obvesti o določitvi pristojnega organa in enotne kontaktne točke, njunih nalogah in vseh poznejših spremembah, povezanih z določitvijo in nalogami. Vsaka država članica objavi določitev pristojnega organa in enotne kontaktne točke. Komisija objavi seznam določenih enotnih kontaktnih točk.

Člen 9

Skupine za odzivanje na incidente na področju računalniške varnosti (skupine CSIRT)

1. Vsaka država članica določi eno ali več skupin CSIRT, ki izpolnjujejo zahteve iz točke 1 Priloge I ter so pristojne za obvladovanje incidentov in tveganj v skladu z natančno določenim postopkom, pri čemer zajame vsaj sektorje iz Priloge II in storitve iz Priloge III. Skupina CSIRT se lahko ustanovi v okviru pristojnega organa.

2. Države članice zagotovijo, da imajo skupine CSIRT ustrezne vire za učinkovito izvajanje nalog iz točke 2 Priloge I.

Države članice zagotovijo tudi učinkovito, uspešno in varno sodelovanje svojih skupin CSIRT v mreži skupin CSIRT iz člena 12.

3. Države članice zagotovijo, da imajo njihove skupine CSIRT dostop do ustrezne, varne in odporne komunikacijske in informacijske infrastrukture na nacionalni ravni.

4. Države članice Komisijo obvestijo o pristojnostih svojih skupin CSIRT in o glavnih elementih njihovega postopka za obvladovanje incidentov.

5. Države članice lahko pri oblikovanju nacionalnih skupin CSIRT zaprosijo za pomoč ENISA.

Člen 10

Sodelovanje na nacionalni ravni

1. Kadar so pristojni organ, enotna kontaktna točka in skupine CSIRT iste države članice ločeni subjekti, sodelujejo pri izpolnjevanju obveznosti, ki jih določa ta direktiva.

2. Države članice zagotovijo, da so pristojni organi ali skupine CSIRT obveščeni o incidentih, priglašenih na podlagi te direktive. Kadar država članica sklene, da skupine CSIRT ne prejemajo priglasitev, se tem skupinam v obsegu, potrebnem za opravljanje njihovih nalog, zagotovi dostop do podatkov o incidentih, ki jih v skladu s členom 14(3) in (5) priglasijo izvajalci bistvenih storitev ali v skladu s členom 16(3) in (6) ponudniki digitalnih storitev.

3. Države članice zagotovijo, da pristojni organi ali skupine CSIRT obvestijo enotne kontaktne točke o incidentih, priglašenih na podlagi te direktive.

Enotna kontaktna točka do 9. avgusta 2018 in nato vsako leto skupini za sodelovanje predloži zbirno poročilo o prejetih priglasitvah, vključno s številom priglasitev in vrsto priglašenih incidentov, ter ukrepih, sprejetih v skladu s členom 14(3) in (5) ter členom 16(3) in (6).

POGLAVJE III

SODELOVANJE

Člen 11

Skupina za sodelovanje

1. Da bi podprli in olajšali strateško sodelovanje in izmenjavo informacij med državami članicami, okrepili zaupanje ter dosegli visoko skupno raven varnosti omrežij in informacijskih sistemov v Uniji, se ustanovi skupina za sodelovanje.

Skupina za sodelovanje opravlja svoje naloge na podlagi dvoletnih delovnih programov iz drugega pododstavka odstavka 3.

2. Skupino za sodelovanje sestavljajo predstavniki držav članic, Komisije in ENISA.

Skupina za sodelovanje lahko k sodelovanju po potrebi povabi predstavnike ustreznih deležnikov.

Komisija zagotovi sekretariat.

3. Skupina za sodelovanje ima naslednje naloge:

(a) strateško usmerja dejavnosti mreže skupin CSIRT, vzpostavljene na podlagi člena 12;

(b) izmenjuje najboljše prakse glede izmenjave informacij v zvezi s priglasitvijo incidentov iz člena 14(3) in (5) ter člena 16(3) in (6);

(c) izmenjuje najboljše prakse med državami članicami in v sodelovanju z ENISA državam članicam pomaga pri krepitvi zmogljivosti za zagotavljanje varnosti omrežij in informacijskih sistemov;

(d) obravnava zmogljivosti in pripravljenost držav članic ter na prostovoljni osnovi ocenjuje nacionalne strategije za varnost omrežij in informacijskih sistemov in učinkovitost skupin CSIRT, pri tem pa določa najboljše prakse;

(e) izmenjuje informacije in najboljše prakse o ozaveščanju in usposabljanju;

(f) izmenjuje informacije in najboljše prakse o raziskavah in razvoju v zvezi z varnostjo omrežij in informacijskih sistemov;

(g) z ustreznimi institucijami, organi, uradi in agencijami Unije po potrebi izmenjuje izkušnje o vprašanjih v zvezi z varnostjo omrežij in informacijskih sistemov;

(h) s predstavniki ustreznih evropskih organizacij za standardizacijo razpravlja o standardih in specifikacijah iz člena 19;

(i) zbira informacije o najboljših praksah v zvezi s tveganji in incidenti;

(j) vsako leto preuči zbirna poročila iz drugega pododstavka člena 10(3);

(k) obravnava delo glede vaj v zvezi z varnostjo omrežij in informacijskih sistemov, izobraževalnih programov in usposabljanj, tudi delo ENISA;

(l) s pomočjo ENISA izmenjuje najboljše prakse glede tega, kako države članice določajo izvajalce bistvenih storitev, tudi glede čezmejnih odvisnosti v zvezi s tveganji in incidenti;

(m) obravnava načine za poročanje o priglasitvah incidentov iz členov 14 in 16.

Skupina za sodelovanje do 9. februarja 2018 in nato vsaki dve leti določi delovni program glede ukrepov, ki jih je treba izvesti za uresničitev svojih ciljev in nalog, ki morajo biti skladni s cilji te direktive.

4. Skupina za sodelovanje za namene pregleda iz člena 23 do 9. avgusta 2018 ter nato vsako leto in pol pripravi poročilo, v katerem oceni izkušnje, pridobljene s strateškim sodelovanjem na podlagi tega člena.

5. Komisija sprejme izvedbene akte, s katerimi določi postopkovne ureditve, potrebne za delovanje skupine za sodelovanje. Te izvedbene akte sprejme v skladu s postopkom pregleda iz člena 22(2).

Za namene prvega pododstavka Komisija predloži odboru iz člena 22(1) prvi osnutek izvedbenega akta do 9. februarja 2017.

Člen 12

Mreža skupin CSIRT

1. Da bi prispevali h krepitvi zaupanja med državami članicami ter spodbudili hitro in učinkovito operativno sodelovanje, se ustanovi mreža nacionalnih skupin CSIRT.

2. Mrežo skupin CSIRT sestavljajo predstavniki tovrstnih skupin držav članic in CERT-EU. Komisija sodeluje v mreži skupin CSIRT kot opazovalka. ENISA zagotovi sekretariat in dejavno podpira sodelovanje med skupinami CSIRT.

3. Mreža skupin CSIRT ima naslednje naloge:

(a) izmenjuje informacije o storitvah, dejavnostih in zmogljivostih za sodelovanje skupin CSIRT;

(b) na prošnjo predstavnika skupine CSIRT iz države članice, na katero bi lahko vplival določen incident, izmenjuje in obravnava poslovno neobčutljive informacije o incidentu in z njim povezanih tveganjih; vendar lahko vsaka skupina CSIRT države članice zavrne, da bi prispevala k tej obravnavi, če bi to lahko negativno vplivalo na preiskavo incidenta;

(c) na prostovoljni osnovi izmenjuje in daje na voljo nezaupne informacije v zvezi s posameznimi incidenti;

(d) na prošnjo predstavnika skupine CSIRT države članice obravnava in po možnosti opredeli usklajen odziv na incident, ki je v pristojnosti te iste države članice;

(e) državam članicam zagotavlja podporo pri obravnavi čezmejnih incidentov na podlagi njihove prostovoljne medsebojne pomoči;

(f) obravnava, preučuje in določa nadaljnje oblike operativnega sodelovanja, tudi glede:

  (i) kategorij tveganj in incidentov;

  (ii) zgodnjega opozarjanja;

  (iii) medsebojne pomoči;

  (iv) načel in načinov usklajevanja pri odzivanju držav članic na čezmejna tveganja in incidente;

(g) skupino za sodelovanje obvešča o svojih dejavnostih in nadaljnjih oblikah operativnega sodelovanja, obravnavanih v skladu s točko (f), ter zaprosi za usmeritve v zvezi s tem;

(h) obravnava izkušnje, pridobljene pri vajah v zvezi z varnostjo omrežij in informacijskih sistemov, tudi tistih, ki jih organizira ENISA;

(i) na prošnjo posamezne skupine CSIRT obravnava njene zmogljivosti in pripravljenost;

(j) izdaja smernice, da olajša konvergenco operativnih praks glede uporabe določb tega člena v zvezi z operativnim sodelovanjem.

4. Mreža skupin CSIRT za namene pregleda iz člena 23 do 9. avgusta 2018 ter vsako leto in pol zatem pripravi poročilo, v katerem oceni izkušnje, pridobljene z operativnim sodelovanjem na podlagi tega člena, vključno s sklepi in priporočili. To poročilo se predloži tudi skupini za sodelovanje.

5. Mreža skupin CSIRT določi svoj poslovnik.

Člen 13

Mednarodno sodelovanje

Unija lahko v skladu s členom 218 PDEU sklene mednarodne sporazume s tretjimi državami ali mednarodnimi organizacijami, ki omogočajo in urejajo njihovo sodelovanje pri nekaterih dejavnostih skupine za sodelovanje. V takih sporazumih se upošteva potreba po zagotavljanju ustreznega varstva podatkov.

POGLAVJE IV

VARNOST OMREŽJA IN INFORMACIJSKIH SISTEMOV IZVAJALCEV BISTVENIH STORITEV

Člen 14

Varnostne zahteve in priglasitev incidentov

1. Države članice zagotovijo, da izvajalci bistvenih storitev sprejmejo ustrezne in sorazmerne tehnične in organizacijske ukrepe za obvladovanje tveganj za varnost omrežij in informacijskih sistemov, ki jih uporabljajo pri svojih dejavnostih. Ob upoštevanju stanja tehnike se s temi ukrepi zagotovi raven varnosti omrežij in informacijskih sistemov, primerna obstoječemu tveganju.

2. Države članice zagotovijo, da izvajalci bistvenih storitev sprejmejo ustrezne ukrepe za preprečitev in zmanjšanje vpliva incidentov, ki vplivajo na varnost tistih omrežij in informacijskih sistemov, ki se uporabljajo za zagotavljanje takšnih bistvenih storitev, da bi zagotovili neprekinjeno izvajanje teh storitev.

3. Države članice zagotovijo, da izvajalci bistvenih storitev pristojnemu organu ali skupini CSIRT brez nepotrebnega odlašanja priglasijo incidente s pomembnim vplivom na neprekinjeno izvajanje bistvenih storitev, ki jih zagotavljajo. Priglasitev zajema informacije, na podlagi katerih lahko pristojni organ ali skupina CSIRT določi morebiten čezmejni vpliv incidenta. Priglasitev ne sme nalagati priglasitelju dodatne odgovornosti.

4. Da bi določili, kako pomemben je vpliv incidenta, se upoštevajo zlasti naslednji parametri:

(a) število uporabnikov, ki jih je prizadela motnja pri zagotavljanju bistvene storitve;

(b) trajanje incidenta;

(c) geografska razširjenost, kar zadeva območje, na katerega vpliva incident.

5. Pristojni organ ali skupina CSIRT na podlagi informacij, ki jih v priglasitvi zagotovi izvajalec bistvenih storitev, obvesti drugo prizadeto državo članico oziroma države članice, če ima incident pomemben vpliv na neprekinjenost izvajanja bistvenih storitev v tej državi članici. Pristojni organ ali skupina CSIRT pri tem v skladu s pravom Unije ali nacionalno zakonodajo, ki je skladna s pravom Unije, zaščiti varnost in poslovne interese izvajalca bistvenih storitev ter zaupnost informacij, ki jih slednji zagotovi v svoji priglasitvi.

Kadar okoliščine omogočajo, pristojni organ ali skupina CSIRT izvajalcu bistvenih storitev, ki priglasi incident, predloži ustrezne informacije glede nadaljnjih ukrepov na podlagi njegove priglasitve, na primer informacije, ki bi lahko prispevale k učinkovitemu obvladovanju incidentov.

Enotna kontaktna točka na zahtevo pristojnega organa ali skupine CSIRT priglasitve iz prvega pododstavka posreduje enotnim kontaktnim točkam drugih prizadetih držav članic.

6. Pristojni organ ali skupina CSIRT lahko po posvetovanju z izvajalcem bistvenih storitev, ki je priglasil incident, obvesti javnost o posameznih incidentih, kadar je ozaveščenost javnosti potrebna za preprečitev incidenta ali obravnavo incidenta, ki je v teku.

7. Pristojni organi, ki sodelujejo v okviru skupine za sodelovanje, lahko oblikujejo in sprejmejo smernice o okoliščinah, v katerih morajo izvajalci bistvenih storitev priglasiti incidente, vključno s parametri iz odstavka 4, na podlagi katerih se določi, kako pomemben je vpliv incidenta.

Člen 15

Izvajanje in izvrševanje

1. Države članice zagotovijo, da imajo pristojni organi potrebna pooblastila in sredstva, da ocenijo, ali izvajalci bistvenih storitev izpolnjujejo obveznosti iz člena 14 ter s tem povezane posledice za varnost omrežij in informacijskih sistemov.

2. Države članice zagotovijo, da ima pristojni organ pooblastila in sredstva, da od izvajalcev bistvenih storitev zahteva, da predložijo:

(a) informacije, potrebne za oceno varnosti njihovih omrežij in informacijskih sistemov, vključno z dokumentiranimi varnostnimi pravili;

(b) dokaze o učinkovitem izvajanju varnostnih pravil, na primer rezultate pregleda varnosti, ki ga izvede pristojni organ ali kvalificiran revizor, pri čemer dajo v primeru pregleda s strani kvalificiranega revizorja rezultate, vključno z ustreznimi dokazi, na voljo pristojnemu organu.

Kadar zahtevajo take informacije ali dokaze, pristojni organi navedejo namen zahteve in opredelijo, katere informacije so potrebne.

3. Pristojni organ lahko po oceni informacij ali rezultatov pregledov varnosti iz odstavka 2 izvajalcem bistvenih storitev da zavezujoča navodila za odpravo ugotovljenih pomanjkljivosti.

4. Pristojni organ pri obravnavi incidentov, katerih posledica je kršitev varstva osebnih podatkov, tesno sodeluje z organi za varstvo podatkov.

POGLAVJE V

VARNOST OMREŽJA IN INFORMACIJSKIH SISTEMOV PONUDNIKOV DIGITALNIH STORITEV

Člen 16

Varnostne zahteve in priglasitev incidentov

1. Države članice zagotovijo, da ponudniki digitalnih storitev določijo in sprejmejo ustrezne in sorazmerne tehnične in organizacijske ukrepe za obvladovanje tveganj za varnost omrežij in informacijskih sistemov, ki jih uporabljajo pri zagotavljanju storitev iz Priloge III v Uniji. Ob upoštevanju stanja tehnike se s temi ukrepi zagotovi raven varnosti omrežij in informacijskih sistemov, primerna obstoječemu tveganju, in upoštevajo naslednji elementi:

(a) varnost sistemov in zmogljivosti;

(b) obvladovanje incidentov;

(c) upravljanje neprekinjenega poslovanja;

(d) spremljanje, revidiranje in preizkušanje;

(e) skladnost z mednarodnimi standardi.

2. Države članice zagotovijo, da ponudniki digitalnih storitev sprejmejo ukrepe za preprečitev in zmanjšanje vpliva incidentov, ki ogrožajo varnost njihovih omrežij in informacijskih sistemov, na storitve iz Priloge III, ki se zagotavljajo v Uniji, da bi zagotovili neprekinjeno izvajanje teh storitev.

3. Države članice zagotovijo, da ponudniki digitalnih storitev vsak incident, ki ima pomemben vpliv na zagotavljanje storitve iz Priloge III, ki jo ponujajo v Uniji, brez nepotrebnega odlašanja priglasijo pristojnemu organu ali skupini CSIRT. Priglasitev zajema informacije, na podlagi katerih lahko pristojni organ ali skupina CSIRT določi pomembnost morebitnega čezmejnega vpliva. Priglasitev ne sme nalagati priglasitelju dodatne odgovornosti.

4. Pri določitvi stopnje vpliva incidenta se upoštevajo zlasti naslednji parametri:

(a) število uporabnikov, na katere vpliva incident, zlasti uporabnikov, ki so odvisni od storitve pri zagotavljanju lastnih storitev;

(b) trajanje incidenta;

(c) geografska razširjenost, kar zadeva območje, na katerega vpliva incident;

(d) v kakšnem obsegu je moteno delovanje storitve;

(e) obseg vpliva na gospodarske in družbene dejavnosti.

Obveznost priglasitve incidenta velja le, kadar ima ponudnik digitalnih storitev dostop do informacij, potrebnih za oceno vpliva incidenta glede na parametre iz prvega pododstavka.

5. Kadar je izvajalec bistvenih storitev pri zagotavljanju storitve, ki je bistvena za ohranitev ključnih družbenih in gospodarskih dejavnosti, odvisen od tretjega ponudnika digitalnih storitev, ta izvajalec priglasi vsak znaten vpliv na neprekinjeno izvajanje bistvenih storitev, ki je posledica incidenta, ki vpliva na ponudnika digitalnih storitev.

6. Kadar je to ustrezno in zlasti če incident iz odstavka 3 zadeva dve ali več držav članic, pristojni organ ali skupina CSIRT obvesti druge prizadete države članice. Pristojni organi, skupine CSIRT in enotne kontaktne točke pri tem v skladu s pravom Unije ali nacionalno zakonodajo, ki je skladna s pravom Unije, zaščitijo varnost in poslovne interese ponudnika digitalnih storitev ter zaupnost predloženih informacij.

7. Pristojni organ ali skupina CSIRT in, kadar je to ustrezno, organi ali skupine CSIRT drugih zadevnih držav članic lahko po posvetovanju z zadevnim ponudnikom digitalnih storitev obvestijo javnost o posameznih incidentih ali zahtevajo, da to stori ponudnik digitalnih storitev, kadar je ozaveščenost javnosti potrebna za preprečitev incidenta ali obravnavo incidenta, ki je v teku, ali kadar je razkritje incidenta kako drugače v javnem interesu.

8. Komisija sprejeme izvedbene akte, da se podrobneje opredeli elemente iz odstavka 1 in parametre, navedene v odstavku 4 tega člena. Ti izvedbeni akti se sprejmejo v skladu s postopkom pregleda iz člena 22(2) do 9. avgusta 2017.

9. Komisija lahko sprejme izvedbene akte, s katerimi določi obliko in postopke, ki se uporabljajo za zahteve glede priglasitve. Ti izvedbeni akti se sprejmejo v skladu s postopkom pregleda iz člena 22(2).

10. Brez poseganja v člen 1(6) države članice za ponudnike digitalnih storitev ne uvedejo nikakršnih nadaljnjih varnostnih zahtev ali zahtev glede priglasitve.

11. Poglavje V se ne uporablja za mikropodjetja in mala podjetja, kakor so opredeljena v Priporočilu Komisije 2003/361/ES ([1]).

([1]) Priporočilo Komisije 2003/361/ES z dne 6. maja 2003 o opredelitvi mikro-, malih in srednjih podjetij (UL L 124, 20.5.2003, str. 36).

Člen 17

Izvajanje in izvrševanje

1. Države članice zagotovijo, da pristojni organi po potrebi ukrepajo z izvajanjem naknadnih nadzornih ukrepov, kadar se jim predložijo dokazi, da ponudnik digitalnih storitev ne izpolnjuje zahtev iz člena 16. Takšne dokaze lahko predloži pristojni organ druge države članice, v kateri se storitev zagotavlja.

2. Pristojni organi imajo za namene odstavka 1 potrebna pooblastila in sredstva, da od ponudnikov digitalnih storitev zahtevajo da:

(a) predložijo informacije, potrebne za oceno varnosti njihovega omrežja in informacijskih sistemov, vključno z dokumentiranimi varnostnimi pravili;

(b) odpravijo vsakršno neizpolnjevanje zahtev iz člena 16.

3. Če ima ponudnik digitalnih storitev glavni sedež ali predstavnika v eni državi članici, omrežja in informacijske sisteme pa v eni ali več drugih državah članicah, pristojni organ države članice glavnega sedeža ali predstavnika in pristojni organi teh drugih držav članic po potrebi sodelujejo in si pomagajo. Takšna pomoč in sodelovanje lahko zajemata izmenjavo informacij med zadevnimi pristojnimi organi in zahteve za sprejem nadzornih ukrepov iz odstavka 2.

Člen 18

Pristojnost in teritorialnost

1. Za namene te direktive se šteje, da ponudnik digitalnih storitev sodi v pristojnost države članice, v kateri ima glavni sedež. Za ponudnika digitalnih storitev se šteje, da ima glavni sedež v državi članici, če ima v tej državi članici glavno upravo.

2. Ponudnik digitalnih storitev, ki nima sedeža v Uniji, vendar v njej zagotavlja storitve iz Priloge III, določi predstavnika v Uniji. Predstavnik ima sedež v eni od držav članic, v katerih se zagotavljajo storitve. Šteje se, da ponudnik digitalnih storitev sodi v pristojnost države članice, v kateri ima predstavnik sedež.

3. Določitev predstavnika s strani ponudnika digitalnih storitev ne posega v sodne postopke, ki se lahko sprožijo proti samemu ponudniku digitalnih storitev.

POGLAVJE VI

STANDARDIZACIJA IN PROSTOVOLJNA PRIGLASITEV

Člen 19

Standardizacija

1. Za pospešitev usklajenega izvajanja člena 14(1) in (2) ter člena 16(1) in (2) države članice spodbujajo uporabo evropskih ali mednarodno sprejetih standardov in specifikacij, pomembnih za varnost omrežij in informacijskih sistemov, ne da bi predpisale uporabo določene vrste tehnologije ali ji dajale prednost.

2. ENISA v sodelovanju z državami članicami pripravi nasvete in smernice za tehnična področja, ki se upoštevajo v zvezi z odstavkom 1, ter za že obstoječe standarde, vključno z nacionalnimi standardi držav članic, s katerimi bi lahko zajeli navedena področja.

Člen 20

Prostovoljna priglasitev

1. Brez poseganja v člen 3 lahko subjekti, ki niso bili določeni kot izvajalci bistvenih storitev in niso ponudniki digitalnih storitev, prostovoljno priglasijo incidente, ki imajo pomemben vpliv na neprekinjeno izvajanje storitev, ki jih zagotavljajo.

2. Države članice pri obdelavi priglasitev ravnajo v skladu s postopkom iz člena 14. Pred prostovoljnimi priglasitvami lahko prednostno obdelajo obvezne priglasitve. Prostovoljne priglasitve se obdelajo le, kadar takšna obdelava zadevnim državam članicam ne pomeni nesorazmernega ali neupravičenega bremena.

Prostovoljna priglasitev subjektu priglasitelju ne sme naložiti nikakršnih obveznosti, ki zanj ne bi veljale, če ne bi opravil priglasitve.

POGLAVJE VII

KONČNE DOLOČBE

Člen 21

Kazni

Države članice določijo pravila o kaznih, ki se uporabljajo za kršitve nacionalnih določb, sprejetih na podlagi te direktive, in sprejmejo vse potrebne ukrepe za zagotovitev, da se te kazni izvajajo. Te kazni morajo biti učinkovite, sorazmerne in odvračilne. Države članice o teh pravilih in ukrepih uradno obvestijo Komisijo do 9. maja 2018 ter jo brez odlašanja uradno obvestijo o vsakršni naknadni spremembi, ki nanje vpliva.

Člen 22

Postopek v odboru

1. Komisiji pomaga Odbor za varnost omrežij in informacijskih sistemov. Ta odbor je odbor v smislu Uredbe (EU) št. 182/2011.

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

Člen 23

Pregled

1. Komisija do 9. maja 2019 Evropskemu parlamentu in Svetu predloži poročilo, v katerem oceni skladnost pristopa držav članic pri določanju izvajalcev bistvenih storitev.

2. Komisija redno pregleduje delovanje te direktive ter o tem poroča Evropskemu parlamentu in Svetu. V ta namen in zaradi nadaljnje krepitve strateškega in operativnega sodelovanja Komisija upošteva poročila skupine za sodelovanje in mreže skupin CSIRT o izkušnjah, pridobljenih na strateški in operativni ravni. Komisija pri pregledu oceni tudi sezname iz prilog II in III ter skladnost pri določanju izvajalcev bistvenih storitev in storitev v sektorjih iz Priloge II. Prvo poročilo predloži do 9. maja 2021.

Člen 24

Prehodni ukrepi

1. Brez poseganja v člen 25 in da bi državam članicam zagotovili dodatne možnosti ustreznega sodelovanja v obdobju prenosa, skupina za sodelovanje in mreža skupin CSIRT začneta naloge iz člena 11(3) in člena 12(3) opravljati do 9. februarja 2017.

2. Skupina za sodelovanje, da bi države članice spodbudila k uporabi skladnega pristopa pri določanju izvajalcev bistvenih storitev, v obdobju od 9. februarja 2017 do 9. novembra 2018 obravnava postopek, vsebino in vrsto nacionalnih ukrepov, ki omogočajo določitev izvajalcev bistvenih storitev v določenem sektorju v skladu z merili iz členov 5 in 6. Skupina za sodelovanje na zahtevo države članice obravnava tudi specifičen osnutek nacionalnih ukrepov te države članice, ki omogoča določitev izvajalcev bistvenih storitev v določenem sektorju v skladu z merili iz členov 5 in 6.

3. Države članice do 9. februarja 2017 in za namene tega člena zagotovijo ustrezno zastopanost v skupini za sodelovanje in mreži skupin CSIRT.

Člen 25

Prenos

1. Države članice sprejmejo in objavijo zakone in druge predpise, potrebne za uskladitev s to direktivo, do 9. maja 2018. O tem takoj obvestijo Komisijo.

Države članice začnejo te predpise uporabljati 10. maja 2018.

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

2. Države članice Komisiji sporočijo besedilo temeljnih določb nacionalnega prava, sprejetih na področju, ki ga ureja ta direktiva.

Člen 26

Začetek veljavnosti

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

Člen 27

Naslovniki

Ta direktiva je naslovljena na države članice.

V Strasbourgu, 6. julija 2016

Za Evropski parlament	*Za Svet*
Predsednik	*Predsednik*
M. SCHULZ	I. KORČOK

PRILOGA I

ZAHTEVE ZA SKUPINE ZA ODZIVANJE NA INCIDENTE NA PODROČJU RAČUNALNIŠKE VARNOSTI (CSIRT) IN NJIHOVE NALOGE

Zahteve za skupine CSIRT in njihove naloge so ustrezno in jasno opredeljene ter podprte z nacionalno politiko in/ali zakonodajo. Vključujejo naslednje:

1. Zahteve za skupine CSIRT

   (a) Skupine CSIRT zagotavljajo visoko stopnjo razpoložljivosti svojih komunikacijskih storitev tako, da preprečujejo kritične točke odpovedi in vzpostavijo več kanalov, po katerih se drugi lahko kadar koli obrnejo nanje in one obrnejo na druge. Poleg tega se komunikacijski kanali jasno opredelijo ter jih uporabniki in partnerji dobro poznajo.

   (b) Uradi skupin CSIRT in podporni informacijski sistemi se nahajajo na varnih krajih.

   (c) Neprekinjeno poslovanje:

      (i) skupine CSIRT imajo ustrezen sistem za upravljanje in usmerjanje zahtevkov, da se poenostavi njihova predaja;

      (ii) skupine CSIRT imajo ustrezno osebje, s katerim lahko zagotovijo stalno razpoložljivost;

      (iii) skupine CSIRT uporabljajo infrastrukturo, katere neprekinjeno delovanje je zagotovljeno. V ta namen se zagotovijo redundantni sistemi in nadomestni delovni prostor;

   (d) skupine CSIRT imajo možnost, da po želji sodelujejo v mednarodnih mrežah za sodelovanje.

2. Naloge skupin CSIRT

   (a) Naloge skupin CSIRT obsegajo vsaj naslednje:

      (i) spremljanje incidentov na nacionalni ravni;

      (ii) zagotavljanje zgodnjega opozarjanja, opozoril, obvestil in razširjanja informacij o tveganjih in incidentih deležnikom;

      (iii) odzivanje na incidente;

      (iv) opravljanje dinamičnih analiz tveganja in incidentov ter spremljanje razmer;

      (v) sodelovanje v mreži skupin CSIRT.

   (b) Skupine CSIRT sodelujejo z zasebnim sektorjem.

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

      (i) postopke za obvladovanje incidentov in tveganj;

      (ii) sheme za klasifikacijo incidentov, tveganj in informacij.

PRILOGA II

VRSTE SUBJEKTOV ZA NAMENE TOČKE 4 ČLENA 4

Sektor	Podsektor	Vrsta subjekta
1. Energija	(a) Elektrika	— elektroenergetska podjetja, kot so opredeljena v točki 35 člena 2 Direktive 2009/72/ES Evropskega parlamenta in Sveta ([1]), ki opravljajo dejavnosti „dobave“, kot je opredeljena v točki 19 člena 2 navedene direktive
		— operaterji distribucijskega sistema, kot so opredeljeni v točki 6 člena 2 Direktive 2009/72/ES
		— operaterji prenosnega sistema, kot so opredeljeni v točki 4 člena 2 Direktive 2009/72/ES
	(b) Nafta	— upravljavci naftovodov
		— upravljavci obratov za proizvodnjo, rafiniranje in predelavo nafte ter upravljavci skladišč in transporta nafte
	(c) Plin	— dobavitelji, kot so opredeljeni v točki 8 člena 2 Direktive 2009/73/ES Evropskega parlamenta in Sveta ([2])
		— operaterji distribucijskega sistema, kot so opredeljeni v točki 6 člena 2 Direktive 2009/73/ES
		— operaterji prenosnega sistema, kot so opredeljeni v točki 4 člena 2 Direktive 2009/73/ES
		— operaterji skladiščnega sistema, kot so opredeljeni v točki 10 člena 2 Direktive 2009/73/ES
		— operaterji sistema za UZP, kot so opredeljeni v točki 12 člena 2 Direktive 2009/73/ES
		— podjetja plinskega gospodarstva, kot so opredeljena v točki 1 člena 2 Direktive 2009/73/ES
		— upravljavci obratov za rafiniranje in predelavo zemeljskega plina
2. Promet	(a) Zračni promet	— letalski prevozniki, kot so opredeljeni v točki 4 člena 3 Uredbe (ES) št. 300/2008 Evropskega parlamenta in Sveta ([3])
		— upravni organi letališča, kot so opredeljeni v točki 2 člena 2 Direktive 2009/12/ES Evropskega parlamenta in Sveta ([4]), letališča, kot so opredeljena v točki 1 člena 2 navedene direktive, vključno z jedrnimi letališči iz oddelka 2 Priloge II k Uredbi (EU) št. 1315/2013 Evropskega parlamenta in Sveta ([5]), ter subjekti, ki upravljajo pomožne objekte, naprave in sredstva na letališčih

Sektor	Podsektor	Vrsta subjekta
		— kontrolorji upravljanja prometa, ki zagotavljajo kontrolo zračnega prometa (ATC), kot je opredeljena v točki 1 člena 2 Uredbe (ES) št. 549/2004 Evropskega parlamenta in Sveta ([6])
	(b) Železniški promet	— upravljavci infrastrukture, kot so opredeljeni v točki 2 člena 3 Direktive 2012/34/EU Evropskega parlamenta in Sveta ([7])
		— prevozniki v železniškem prometu, kot so opredeljeni v točki 1 člena 3 Direktive 2012/34/EU, vključno z upravljavci objektov za izvajanje železniških storitev, kot so opredeljeni v točki 12 člena 3 navedene direktive
	(c) Vodni promet	— prevozna podjetja za potniški in tovorni promet po kopenskih vodah, morju in obalnih vodah, kot so za področje vodnega prometa opredeljena v Prilogi I k Uredbi (ES) št. 725/2004 Evropskega parlamenta in Sveta ([8]), brez posameznih plovil, ki jih upravljajo ta podjetja
		— upravni organi pristanišč, kot so opredeljena v točki 1 člena 3 Direktive Evropskega parlamenta in Sveta 2005/65/ES ([9]), vključno z njihovimi pristaniškimi zmogljivostmi, kot so opredeljene v točki 11 člena 2 Uredbe (ES) št. 725/2004, ter subjekti, ki izvajajo dela in upravljajo opremo v pristaniščih
		— upravljavci sistemov za nadzor plovbe, kot so opredeljeni v točki (o) člena 3 Direktive 2002/59/ES Evropskega parlamenta in Sveta ([10])
	(d) Cestni prevoz	— cestni organi, kot so opredeljeni v točki 12 člena 2 Delegirane uredbe Komisije (EU) 2015/962 ([11]), odgovorni za kontrolo upravljanja prometa
		— upravljavci inteligentnih prometnih sistemov, kot so opredeljeni v točki 1 člena 4 Direktive 2010/40/EU Evropskega parlamenta in Sveta ([12])
3. Bančništvo		Kreditne institucije, kot so opredeljene v točki 1 člena 4 Uredbe (EU) št. 575/2013 Evropskega parlamenta in Sveta ([13])
4. Infrastruktura finančnega trga		— upravljavci mest trgovanja, kot so opredeljena v točki 24 člena 4 Direktive 2014/65/EU Evropskega parlamenta in Sveta ([14])
		— centralne nasprotne stranke (CNS), kot so opredeljene v točki 1 člena 2 Uredbe (EU) št. 648/2012 Evropskega parlamenta in Sveta ([15])
5. Zdravstveni sektor	Zdravstvenovarstvene ustanove (vključno z bolnišnicami in zasebnimi klinikami)	Izvajalci zdravstvenega varstva, kot so opredeljeni v točki (g) člena 3 Direktive 2011/24/EU Evropskega parlamenta in Sveta ([16])

Sektor	Podsektor	Vrsta subjekta
6. Oskrba s pitno vodo in njena distribucija		Dobavitelj in distributer „vode, namenjene za prehrano ljudi“, kot je opredeljena v točki 1(a) člena 2 Direktive Sveta 98/83/ES ([17]), vendar brez distributerjev, za katere je distribucija vode za prehrano ljudi le del splošne dejavnosti distribucije drugih dobrin in blaga, ki ne štejejo za bistvene storitve
7. Digitalna infrastruktura		— stičišča omrežij
		— ponudniki storitev sistema domenskih imen
		— upravljavci registra domenskih imen najvišje ravni

([1]) Direktiva 2009/72/ES Evropskega parlamenta in Sveta z dne 13. julija 2009 o skupnih pravilih notranjega trga z električno energijo in o razveljavitvi Direktive 2003/54/ES (UL L 211, 14.8.2009, str. 55).
([2]) Direktiva 2009/73/ES Evropskega parlamenta in Sveta z dne 13. julija 2009 o skupnih pravilih notranjega trga z zemeljskim plinom in o razveljavitvi Direktive 2003/55/ES (UL L 211, 14.8.2009, str. 94).
([3]) Uredba (ES) št. 300/2008 Evropskega parlamenta in Sveta z dne 11. marca 2008 o skupnih pravilih na področju varovanja civilnega letalstva in o razveljavitvi Uredbe (ES) št. 2320/2002 (UL L 97, 9.4.2008, str. 72).
([4]) Direktiva 2009/12/ES Evropskega parlamenta in Sveta z dne 11. marca 2009 o letaliških pristojbinah (UL L 70, 14.3.2009, str. 11).
([5]) Uredba (EU) št. 1315/2013 Evropskega parlamenta in Sveta z dne 11. decembra 2013 o smernicah Unije za razvoj vseevropskega prometnega omrežja in razveljavitvi Sklepa št. 661/2010/EU (UL L 348, 20.12.2013, str. 1).
([6]) Uredba (ES) št. 549/2004 Evropskega parlamenta in Sveta z dne 10. marca 2004 o določitvi okvira za oblikovanje enotnega evropskega neba (okvirna uredba) (UL L 96, 31.3.2004, str. 1).
([7]) Direktiva 2012/34/EU Evropskega parlamenta in Sveta z dne 21. novembra 2012 o vzpostavitvi enotnega evropskega železniškega območja (UL L 343, 14.12.2012, str. 32).
([8]) Uredba (ES) št. 725/2004 Evropskega parlamenta in Sveta z dne 31. marca 2004 o povečanju zaščite na ladjah in v pristaniščih (UL L 129, 29.4.2004, str. 6).
([9]) Direktiva Evropskega parlamenta in Sveta 2005/65/ES z dne 26. oktobra 2005 o krepitvi varnosti v pristaniščih (UL L 310, 25.11.2005, str. 28).
([10]) Direktiva 2002/59/ES Evropskega parlamenta in Sveta z dne 27. junija 2002 o vzpostavitvi sistema spremljanja in obveščanja za ladijski promet ter o razveljavitvi Direktive Sveta 93/75/EGS (UL L 208, 5.8.2002, str. 10).
([11]) Delegirana uredba Komisije (EU) 2015/962 z dne 18. decembra 2014 o dopolnitvi Direktive 2010/40/EU Evropskega parlamenta in Sveta v zvezi z opravljanjem storitev zagotavljanja prometnih informacij v realnem času po vsej EU (UL L 157, 23.6.2015, str. 21).
([12]) Direktiva 2010/40/EU Evropskega parlamenta in Sveta z dne 7. julija 2010 o okviru za uvajanje inteligentnih prometnih sistemov v cestnem prometu in za vmesnike do drugih vrst prevoza (UL L 207, 6.8.2010, str. 1).
([13]) Uredba (EU) št. 575/2013 Evropskega parlamenta in Sveta z dne 26. junija 2013 o bonitetnih zahtevah za kreditne institucije in investicijska podjetja ter o spremembi Uredbe (EU) št. 648/2012 (UL L 176, 27.6.2013, str. 1).
([14]) Direktiva 2014/65/EU Evropskega parlamenta in Sveta z dne 15. maja 2014 o trgih finančnih instrumentov ter spremembi Direktive 2002/92/ES in Direktive 2011/61/EU (UL L 173, 12.6.2014, str. 349).
([15]) Uredba (EU) št. 648/2012 Evropskega parlamenta in Sveta z dne 4. julija 2012 o izvedenih finančnih instrumentih OTC, centralnih nasprotnih strankah in repozitorijih sklenjenih poslov (UL L 201, 27.7.2012, str. 1).
([16]) Direktiva 2011/24/EU Evropskega parlamenta in Sveta z dne 9. marca 2011 o uveljavljanju pravic pacientov pri čezmejnem zdravstvenem varstvu (UL L 88, 4.4.2011, str. 45).
([17]) Direktiva Sveta 98/83/ES z dne 3. novembra 1998 o kakovosti vode, namenjene za prehrano ljudi (UL L 330, 5.12.1998, str. 32).

PRILOGA III

VRSTE DIGITALNIH STORITEV ZA NAMENE TOČKE 5 ČLENA 4

1. Spletna tržnica
2. Spletni iskalnik
3. Storitev računalništva v oblaku