Službeni list Europske unije

L 194

Svezak 59.

Hrvatsko izdanje

Zakonodavstvo

19. srpnja 2016.

Sadržaj

HR

Akti čiji su naslovi tiskani običnim slovima jesu oni koji se odnose na svakodnevno upravljanje poljoprivrednim pitanjima, a općenito vrijede ograničeno razdoblje.

Naslovi svih drugih akata tiskani su masnim slovima, a prethodi im zvjezdica.

I.

(Zakonodavni akti)

DIREKTIVE

DIREKTIVA (EU) 2016/1148 EUROPSKOG PARLAMENTA I VIJEĆA

od 6. srpnja 2016.

o mjerama za visoku zajedničku razinu sigurnosti mrežnih i informacijskih sustava širom Unije

EUROPSKI PARLAMENT I VIJEĆE EUROPSKE UNIJE,

uzimajući u obzir Ugovor o funkcioniranju Europske unije, a posebno njegov članak 114.,

uzimajući u obzir prijedlog Europske komisije,

nakon prosljeđivanja nacrta zakonodavnog akta nacionalnim parlamentima,

uzimajući u obzir mišljenje Europskoga gospodarskog i socijalnog odbora ([1]),

u skladu s redovnim zakonodavnim postupkom ([2]),

budući da:

(1) Mrežni i informacijski sustavi i usluge imaju ključnu ulogu u društvu. Njihova pouzdanost i sigurnost ključne su za gospodarske i društvene aktivnosti, a posebno za funkcioniranje unutarnjeg tržišta.

(2) Sigurnosni incidenti sve su većeg razmjera, učestalosti i utjecaja te predstavljaju veliku prijetnju funkcioniranju mrežnih i informacijskih sustava. Ti sustavi također mogu postati meta za namjerne štetne radnje kojima je cilj nanijeti štetu ili prekinuti rad sustavâ. Takvi incidenti mogu ugroziti izvršavanje gospodarskih aktivnosti, prouzročiti znatne financijske gubitke, narušiti povjerenje korisnika i nanijeti znatnu štetu gospodarstvu Unije.

(3) Mrežni i informacijski sustavi, a ponajprije internet, imaju ključnu ulogu u pojednostavljivanju prekograničnog kretanja robe, usluga i ljudi. Zbog takve transnacionalne prirode sustavâ, znatan poremećaj u njihovu radu, bez obzira na to je li on namjeran ili nenamjeran te bez obzira na to gdje do njega dođe, može utjecati na pojedine države članice te na Uniju u cjelini. Stoga je sigurnost mrežnih i informacijskih sustava ključna za neometano funkcioniranje unutarnjeg tržišta.

(4) Na temelju znatnog napretka koji je unutar Europskog foruma država članica postignut u poticanju rasprava i razmjeni dobrih političkih praksi, uključujući razvoj načela za europsku suradnju za kibernetičke krize, trebalo bi uspostaviti skupinu za suradnju sastavljenu od predstavnikâ država članica, Komisije i Agencije Europske unije za mrežnu i informacijsku sigurnost („ENISA”) kako bi se podržala i pospješila strateška suradnja među državama

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

([2]) Stajalište Europskog parlamenta od 13. ožujka 2014. (još nije objavljeno u Službenom listu) i stajalište Vijeća u prvom čitanju od 17. svibnja 2016. (još nije objavljeno u Službenom listu). Stajalište Europskog parlamenta od 6. srpanj 2016. (još nije objavljeno u Službenom listu).

članicama u pogledu sigurnosti mrežnih i informacijskih sustava. Da bi ta skupina bila djelotvorna i uključiva, nužno je da sve države članice raspolažu minimalnim sposobnostima i strategijom za osiguravanje visoke razine sigurnosti mrežnih i informacijskih sustava na svojem državnom području. Osim toga, zahtjevi za sigurnost i obavješćivanje trebali bi se primjenjivati na operatore ključnih usluga i na pružatelje digitalnih usluga kako bi se promicala kultura upravljanja rizicima i osiguralo da najozbiljniji incidenti budu prijavljeni.

(5) Postojeće sposobnosti nisu dovoljne za osiguranje visoke razine sigurnosti mrežnih i informacijskih sustava unutar Unije. Države članice imaju vrlo različite razine pripravnosti, što je dovelo do postojanja rascjepkanih pristupa širom Unije. To rezultira nejednakom razinom zaštite potrošača i poduzeća te narušava ukupnu razinu sigurnosti mrežnih i informacijskih sustava unutar Unije. Nepostojanje zajedničkih zahtjeva za operatore ključnih usluga i pružatelje digitalnih usluga onemogućuje uspostavu globalnog i učinkovitog mehanizma suradnje na razini Unije. Sveučilišta i istraživački centri imaju odlučujuću ulogu u poticanju istraživanja, razvoja i inovacije u tim područjima.

(6) Stoga je za djelotvoran odgovor na izazove u pogledu sigurnosti mrežnih i informacijskih sustava potreban globalan pristup na razini Unije koji bi obuhvatio zajedničke minimalne zahtjeve za izgradnju kapaciteta i planiranje, razmjenu informacija, suradnju te zajedničke sigurnosne zahtjeve za operatore ključnih usluga i pružatelje digitalnih usluga. Međutim, operatore ključnih usluga i pružatelje digitalnih usluga ne sprečava se da provode sigurnosne mjere koje su strože od onih predviđenih ovom Direktivom.

(7) Kako bi se obuhvatilo sve relevantne incidente i rizike, ova Direktiva trebala bi se primjenjivati i na operatore ključnih usluga i na pružatelje digitalnih usluga. Međutim, obveze za operatore ključnih usluga i pružatelje digitalnih usluga ne bi se smjele odnositi na poduzeća koja pružaju javne komunikacijske mreže ili javno dostupne elektroničke komunikacijske usluge, kako je određeno Direktivom 2002/21/EZ Europskog parlamenta i Vijeća ([1]) i na koje se primjenjuju posebni zahtjevi u pogledu sigurnosti i cjelovitosti utvrđeni u toj Direktivi, a te obveze ne bi se trebale primjenjivati ni na pružatelje usluga povjerenja u smislu Uredbe (EU) br. 910/2014 Europskog parlamenta i Vijeća ([2]), na koje se primjenjuju sigurnosni zahtjevi utvrđeni u toj Uredbi.

(8) Ovom Direktivom ne bi se trebalo dovoditi u pitanje mogućnost da svaka država članica poduzme mjere koje su potrebne za osiguranje zaštite osnovnih interesa njezine sigurnosti, za zaštitu javne politike i javne sigurnosti te za omogućivanje istrage, otkrivanja i kažnjavanja kaznenih djela. U skladu s člankom 346. Ugovora o funkcioniranju Europske unije (UFEU) nijednu državu članicu ne treba obvezivati na davanje podataka za čije otkrivanje smatra da je u suprotnosti s temeljnim interesima njezine sigurnosti. U tom kontekstu važni su Odluka Vijeća 2013/488/EU ([3]) te sporazumi o povjerljivosti podataka, ili neformalni sporazumi o povjerljivosti podataka kao što je Protokol o semaforu.

(9) Određeni sektori gospodarstva već su uređeni, ili će možda biti regulirani u budućnosti, pravnim aktima Unije specifičnim za pojedini sektor koji sadrže pravila u vezi sa sigurnošću mrežnih i informacijskih sustava. Kad god ti pravni akti Unije sadrže odredbe kojima se propisuju zahtjevi za sigurnost mrežnih i informacijskih sustava ili za obavijesti o incidentima, te odredbe trebale bi se primjenjivati ako su njima propisani zahtjevi po učinku barem jednaki obvezama iz ove Direktive. Države članice zatim bi trebale primjenjivati odredbe takvih pravnih akata Unije specifičnih za pojedini sektor, među ostalim odredbe koje se odnose na nadležnost, te ne bi trebale provoditi postupak identifikacije operatora ključnih usluga kako je to određeno u ovoj Direktivi. U tom kontekstu države članice Komisiji bi trebale dostaviti podatke o primjeni takvih odredbi koje predstavljaju *lex specialis*. Pri određivanju toga jesu li zahtjevi za sigurnost mrežnih i informacijskih sustava i za obavijesti o incidentima koji su sadržani u pravnim aktima Unije za pojedini sektor istovjetni zahtjevima sadržanima u člancima ove Direktive u obzir bi se trebale uzeti samo odredbe relevantnih pravnih akata Unije i njihova primjena u državama članicama.

(10) Za sektor vodnog prometa, sigurnosnim zahtjevima za poduzeća, brodove, lučke objekte, luke i službe za nadzor i upravljanje pomorskim prometom na temelju pravnih akata Unije obuhvaćene su sve aktivnosti, što uključuje radijske i telekomunikacijske sustave te računalne sustave i mreže. Među obveznim postupcima koje treba slijediti je izvješćivanje o svim incidentima i stoga bi se trebali smatrati *lex specialisom*, u onoj mjeri u kojoj su ti zahtjevi barem jednakovrijedni odgovarajućim odredbama ove Direktive.

([1]) Direktiva 2002/21/EZ Europskog parlamenta i Vijeća od 7. ožujka 2002. o zajedničkom regulatornom okviru za elektroničke komunikacijske mreže i usluge (Okvirna direktiva) (SL L 108, 24.4.2002., str. 33.).

([2]) Uredba (EU) br. 910/2014 Europskog parlamenta i Vijeća od 23. srpnja 2014. o elektroničkoj identifikaciji i uslugama povjerenja za elektroničke transakcije na unutarnjem tržištu i stavljanju izvan snage Direktive 1999/93/EZ (SL L 257, 28.8.2014., str. 73.).

([3]) Odluka Vijeća 2013/488/EU od 23. rujna 2013. o sigurnosnim propisima za zaštitu klasificiranih podataka EU-a (SL L 274, 15.10.2013., str. 1.).

(11) Pri identifikaciji operatora u sektoru vodnog prometa države članice trebale bi uzeti u obzir postojeće i buduće međunarodne kodekse i smjernice, posebno one koje je razvila Međunarodna pomorska organizacija, kako bi pojedinačnim pomorskim operatorima na raspolaganju bio usklađen pristup.

(12) Regulacija i nadzor u sektorima bankarske infrastrukture i infrastrukture financijskog tržišta usklađeni su do visokog stupnja na razini Unije primjenom primarnog i sekundarnog prava Unije i standardima koji su razvijeni zajedno s europskim nadzornim tijelima. U okviru bankovne unije primjenu i nadzor tih zahtjeva osigurava jedinstveni nadzorni mehanizam. Za države članice koje ne čine dio bankovne unije to osiguravaju odgovarajuća bankarska regulatorna tijela država članica. Za druga područja regulacije financijskog sektora visok stupanj preklapanja i konvergencija nadzornih praksi također osigurava Europski sustav financijskog nadzora. Europsko nadzorno tijelo za vrijednosne papire i tržišta kapitala također ima izravnu nadzornu ulogu za određene subjekte, osobito agencije za kreditni rejting i trgovinske repozitorije.

(13) Operativni rizik ključan je dio bonitetne regulative i nadzora u sektorima bankarske infrastrukture i infrastrukture financijskog tržišta. On obuhvaća sve aktivnosti, među ostalim sigurnost, cjelovitost i otpornost mrežnih i informacijskih sustava. Zahtjevi u pogledu tih sustava, koji često prelaze zahtjeve predviđene ovom Direktivom, utvrđeni su u više pravnih akata Unije, uključujući: pravila o pristupu aktivnostima kreditnih institucija i bonitetnom nadzoru kreditnih institucija i investicijskih društava, pravila o bonitetnim zahtjevima za kreditne institucije i investicijska društva, koja uključuju zahtjeve u pogledu operativnog rizika; pravila o tržištu financijskih instrumenata, koja uključuju zahtjeve u pogledu procjene rizika za investicijska društva i za regulirana tržišta; pravila o neuvrštenim (OTC) izvedenicama, središnjoj drugoj ugovornoj strani i trgovinskom repozitoriju, koja uključuju zahtjeve u pogledu operativnog rizika za središnje druge ugovorne strane i trgovinske repozitorije; te pravila za poboljšavanje namire vrijednosnih papira u Uniji i pravila o središnjim depozitorijima vrijednosnih papira, koja uključuju zahtjeve u pogledu operativnog rizika. Nadalje, zahtjevi za obavješćivanje o incidentima dio su uobičajene nadzorne prakse u financijskom sektoru te su često obuhvaćeni nadzornim priručnicima. Države članice trebale bi razmotriti ta pravila i zahtjeve kod primjene *lex specialisa*.

(14) Kao što je Europska središnja banka navela u svom mišljenju od 25. srpnja 2014 ([1]), ova Direktiva ne utječe na režim na temelju prava Unije za nadzor Eurosustava nad platnim sustavom i sustavom namire. Bilo bi primjereno da tijela nadležna za takav nadzor razmjenjuju iskustva o pitanjima povezanim sa sigurnošću mrežnih i informacijskih sustava s nadležnim tijelima prema ovoj Direktivi. Isto vrijedi i za članove Europskog sustava središnjih banaka koji nisu dio europodručja, a koji obavljaju takav nadzor platnog sustava i sustava namire na temelju nacionalnih zakona i propisa.

(15) Internetsko tržište potrošačima i trgovcima omogućuje da putem interneta sklapaju kupoprodajne ugovore ili ugovore o uslugama s trgovcima te je krajnje odredište za sklapanje tih ugovora. Ne bi trebalo obuhvaćati internetske usluge koje imaju samo posredničku ulogu za usluge koje pružaju treće strane putem kojih se na kraju može sklopiti ugovor. Stoga ono ne bi trebalo obuhvaćati internetske usluge kojima se uspoređuje cijena određenih proizvoda ili usluga kod različitih trgovaca te se korisnika zatim preusmjerava na preporučenog trgovca radi kupovine tog proizvoda. Računalne usluge koje pružaju internetska tržišta mogu uključivati obradu transakcija, agregiranje podataka ili izradu profila korisnika. Trgovine aplikacijama, koje djeluju kao internetske trgovine kojima se omogućuje digitalna distribucija aplikacija ili softverskih programa trećih strana, trebaju se smatrati vrstom internetskih tržišta.

(16) Internetske tražilice korisniku omogućuju da obavlja pretraživanja u načelu svih internetskih stranica na temelju upita o bilo kojoj temi. Alternativno, mogu biti usmjerene na internetske stranice na određenom jeziku. Definicija internetske tražilice predviđena u ovoj Direktivi ne bi trebala obuhvaćati funkcije pretraživanja koje su ograničene na sadržaj određene internetske stranice, bez obzira na to pruža li tu funkciju pretraživanja neka vanjska tražilica. Ne bi trebala ni obuhvaćati internetske usluge kojima se uspoređuje cijena određenih proizvoda ili usluga kod različitih trgovaca te se korisnika zatim preusmjerava na preporučenog trgovca radi kupovine tog proizvoda.

(17) Usluge računalstva u oblaku obuhvaćaju širok raspon aktivnosti koje se mogu pružati na temelju različitih modela. Za potrebe ove Direktive pojam „usluge računalstva u oblaku” obuhvaća usluge kojima se omogućuje pristup nadogradivom i elastičnom skupu djeljivih računalnih resursa. Ti računalni resursi obuhvaćaju resurse poput mreža, poslužitelja ili drugih infrastruktura, pohrane, aplikacija i usluga. Pojam „nadogradivi” odnosi se na računalne usluge koje pružatelj usluga u oblaku dodjeljuje na fleksibilan način, bez obzira na zemljopisnu lokaciju resursâ, s ciljem rješavanja fluktuacija u potražnji. Pojam „elastičan skup” upotrebljava se za opisivanje

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

onih računalnih resursa koji se predviđaju i isporučuju u skladu s potražnjom, kako bi se raspoloživi resursi mogli brzo povećati i smanjiti ovisno o radnom opterećenjem. Pojam „djeljivi" upotrebljava se za opisivanje onih računalnih resursa koji se pružaju većem broju korisnika koji dijele zajednički pristup toj usluzi, ali da se obrada provodi odvojeno za svakog korisnika, iako se usluga pruža preko iste elektroničke opreme.

(18) Funkcija središta za razmjenu internetskog prometa (IXP) međusobno je povezivanje mreža. IXP ne pruža pristup mreži te ne djeluje kao pružatelj prijenosa ni kao nositelj prijenosa. Također, IXP ne pruža ni druge usluge koje nisu vezane za međusobno povezivanje, iako to operatora IXP-a ne sprečava da pruža i nepovezane usluge. IXP služi međusobnom povezivanju mreža koje su tehnički i organizacijski odvojene. Pojam „autonomni sustav" upotrebljava se za opisivanje mreže koja je tehnički samostalna.

(19) Državama članicama trebalo bi povjeriti zadaću utvrđivanja subjekata koji ispunjavaju kriterije iz definicije operatora ključnih usluga. Kako bi se osigurao dosljedan pristup, definicija operatora ključnih usluga trebala bi se dosljedno primjenjivati u svim državama članicama. Ovom se Direktivom u tu svrhu predviđa procjena subjekata koji djeluju u specifičnim sektorima i podsektorima, izrada popisa ključnih usluga, razmatranje zajedničkog popisa međusektorskih čimbenika za utvrđivanje bi li potencijalni incident imao znatan negativan učinak, postupak savjetovanja u kojem bi sudjelovale relevantne države članice u slučaju da je riječ o subjektima koji pružaju usluge u više od jedne države članice te potpora skupine za suradnju u postupku identifikacije. Kako bi se osiguralo da popis identificiranih operatora točno odražava moguće promjene na tržištu, države članice trebale bi ga redovito preispitivati i, prema potrebi, ažurirati. Naposljetku, države članice Komisiji bi trebale dostaviti informacije potrebne za procjenu opsega u kojem je ta zajednička metodologija omogućila dosljednu primjenu te definicije u državama članicama.

(20) U postupku identifikacije operatora ključnih usluga države članice trebale bi, barem za svaki podsektor iz ove Direktive, procijeniti koje usluge treba smatrati ključnima za održavanje ključnih društvenih i gospodarskih aktivnosti te ispunjavaju li subjekti iz sektorâ i podsektorâ iz ove Direktive koji te usluge pružaju kriterije za identifikaciju operatora. Prilikom procjene toga pruža li neki subjekt uslugu koja je ključna za održavanje ključnih društvenih ili ekonomskih djelatnosti dovoljno je provjeriti pruža li taj subjekt uslugu koja se nalazi na popisu ključnih usluga. Nadalje, trebalo bi dokazati da to pružanje ključne usluge ovisi o mrežnim i informacijskim sustavima. Naposljetku, prilikom procjene toga bi li incident imao znatan negativan učinak na pružanje usluge, države članice u obzir bi trebale uzeti niz međusektorskih čimbenika, kao i, prema potrebi, čimbenike specifične za pojedine sektore.

(21) Za potrebe identifikacije operatora ključne usluge poslovni nastan u državi članici podrazumijeva učinkovito i stvarno obavljanje djelatnosti u okviru stabilnih aranžmana. Pravni oblik takvih aranžmana, bilo posredstvom podružnice ili društva kćeri s pravnom osobnošću, nije odlučujući čimbenik u tom pogledu.

(22) Moguće je da subjekti koji djeluju u sektorima i podsektorima navedenima u ovoj Direktivi mogu pružati i ključne i sporedne usluge. Na primjer, u sektoru zračnog prometa zračne luke pružaju usluge koje bi države članice mogle smatrati ključnim uslugama, poput upravljanja uzletno-sletnim stazama, ali i niz usluga koje bi se mogle smatrati sporednima, kao što je ponuda trgovačkih prostora. Posebni sigurnosni zahtjevi trebali bi se na operatore ključnih usluga primjenjivati samo s obzirom na one usluge koje se smatraju ključnima. U svrhu identificiranja operatora države članice stoga bi trebale izraditi popis usluga koje smatraju ključnima.

(23) Popis usluga trebao bi sadržavati sve usluge koje se pružaju na državnom području određene države članice koje ispunjavaju zahtjeve iz ove Direktive. Države članice trebale bi biti u mogućnosti dopuniti postojeći popis dodavanjem novih usluga. Popis usluga trebao bi poslužiti kao referentna točka za države članice i omogućiti identifikaciju operatora ključnih usluga. Njegova je svrha identificiranje vrsta ključnih usluga u bilo kojem sektoru iz ove Direktive, po čemu bi ih se na taj način razlikovalo od sporednih djelatnosti za koje bi neki subjekt koji djeluje u određenom sektoru mogao biti odgovoran. Popis usluga koji sastavlja svaka država članica služio bi kao dodatna informacija u procjeni regulatorne prakse svake države članice s ciljem osiguravanja opće razine dosljednosti među državama članicama u postupku identifikacije.

(24) Ako subjekt pruža ključnu uslugu u dvjema državama članicama ili više njih, te države članice trebale bi se za potrebe postupka identifikacije uključiti u međusobne bilateralne ili multilateralne rasprave. Cilj je tog postupka savjetovanja pomoći im da procijene kritičnost operatora u pogledu prekograničnog učinka, čime se svakoj dotičnoj državi članici omogućuje da predstavi svoja stajališta o rizicima povezanima s pruženim uslugama. Države članice trebale bi u okviru tog postupka u obzir uzeti mišljenje drugih država članica i trebale bi moći u tom pogledu zatražiti pomoć skupine za suradnju.

(25) Kao rezultat postupka identifikacije države članice trebale bi donijeti nacionalne mjere radi utvrđivanja na koje se subjekte primjenjuju obveze u pogledu sigurnosti mrežnih i informacijskih sustava. Taj rezultat može se postići izradom popisa na kojem se navode svi operatori ključnih usluga ili donošenjem nacionalnih mjera, što uključuje objektivne mjerljive kriterije, kao što su podaci o učinku operatora ili broj korisnika, koji omogućuju da se utvrdi koji subjekti podliježu obvezama u pogledu sigurnosti mrežnih i informacijskih sustava. Nacionalne mjere, bilo da one već postoje ili su donesene u kontekstu ove Direktive, trebale bi uključivati sve pravne mjere, administrativne mjere i politike kojima se omogućuje identifikacija operatora ključnih usluga u okviru ove Direktive.

(26) Kako bi dale naznaku važnosti, u odnosu na dotični sektor, identificiranih operatora ključnih usluga, države članice trebale bi uzeti u obzir broj i veličinu tih operatora, na primjer u pogledu tržišnog udjela ili količine koja je proizvedena ili prenesena, a da pritom ne moraju odati informacije koje bi otkrile koji su operatori identificirani.

(27) Radi utvrđivanja bi li neki incident imao značajan negativan učinak na pružanje ključne usluge, države članice trebale bi uzeti u obzir različite faktore poput broja fizičkih osoba i pravnih subjekata koji se oslanjanju na tu uslugu u privatne ili poslovne svrhe. Korištenje tom uslugom može biti izravno, neizravno ili posredno. Pri procjeni učinka koji bi incident mogao imati, u pogledu težine i trajanja, na gospodarske i društvene aktivnosti ili javnu sigurnost, države članice trebale bi također procijeniti vjerojatno razdoblje do nastupanja negativnog učinka prekida.

(28) Osim međusektorskih čimbenika države članice trebale bi u obzir uzeti i čimbenike za pojedine sektore da bi se utvrdilo bi li incident imao znatan negativan učinak na pružanje neke usluge. U pogledu dobavljača energije takvi faktori mogli bi uključivati količinu ili udio proizvedene nacionalne energije; za dobavljače nafte, dnevnu količinu; za zračni promet, što uključuje zračne luke i zračne prijevoznike, željeznički promet i morske luke, udio u opsegu nacionalnog prometa i godišnji broj putnika ili prevezenog tereta; za bankarsku infrastrukturu ili infrastrukturu financijskog tržišta, njihovu sustavnu važnost koja se temelji na ukupnoj imovini ili omjeru te ukupne imovine i BDP-a; za zdravstveni sektor, godišnji broj pacijenata kojima se pruža zdravstvena skrb; za proizvodnju i obradu vode te za vodoopskrbu, količinu te broj i vrste opskrbljenih korisnika, što primjerice uključuje bolnice, organizacije javnih službi ili pojedince, te postojanje alternativnih izvora vode za isto zemljopisno područje.

(29) Da bi se postigla i održavala visoka razina sigurnosti mrežnih i informacijskih sustava, svaka država članica trebala bi imati nacionalnu strategiju za sigurnost mrežnih i informacijskih sustava u kojoj će biti definirani strateški ciljevi i konkretna politička djelovanja koja treba poduzeti.

(30) S obzirom na razlike u nacionalnim upravljačkim strukturama i radi zaštite već postojećih sektorskih rješenja ili nadzornih i regulatornih tijela Unije te kako bi se izbjegla udvostručivanja, države članice trebale bi biti u mogućnosti odrediti više od jednog nadležnog nacionalnog tijela čija je odgovornost izvršavanje zadaća povezanih sa sigurnošću mrežnih i informacijskih sustava operatorâ ključnih usluga i pružateljâ digitalnih usluga u okviru ove Direktive.

(31) Da bi se olakšala prekogranična suradnja i komunikacija i da bi se omogućila djelotvorna provedba ove Direktive, nužno je da svaka država članica, ne dovodeći u pitanje sektorska regulatorna rješenja, odredi jedinstvenu nacionalnu kontaktnu točku odgovornu za koordinaciju pitanjâ sigurnosti mrežnih i informacijskih sustava te za prekograničnu suradnju na razini Unije. Nadležnim tijelima i jedinstvenim kontaktnim točkama trebalo bi osigurati odgovarajuće tehničke, financijske i ljudske resurse kako bi im se omogućilo djelotvorno i učinkovito izvršavanje zadaća koje su im dodijeljene te time postizanje ciljeva ove Direktive. Budući da je cilj ove Direktive poboljšanje funkcioniranja unutarnjeg tržišta izgradnjom povjerenja i pouzdanja, tijela u državama članicama moraju biti u stanju djelotvorno surađivati s gospodarskim subjektima te biti strukturirana na odgovarajući način.

(32) Nadležna tijela ili timovi za odgovor na računalne sigurnosne incidente (CSIRT-ovi) trebali bi zaprimati obavijesti o takvim incidentima. Jedinstvene kontaktne točke ne bi trebale izravno zaprimati obavijesti o incidentima, osim ako također obavljaju dužnost nadležnog tijela ili CSIRT-a. Međutim, nadležno tijelo ili CSIRT jedinstvenoj kontaktnoj točki trebali bi moći naložiti da obavijesti o incidentima proslijedi jedinstvenim kontaktnim točkama u drugim pogođenim državama članicama.

(33) Da bi se osiguralo učinkovito pružanje informacija državama članicama i Komisiji, jedinstvena kontaktna točka trebala bi podnositi sažeto izvješće skupini za suradnju te bi ono trebalo biti anonimizirano kako bi se očuvala povjerljivost obavijesti i identitet operatora ključnih usluga i pružatelja digitalnih usluga zato što podaci o identitetu subjekta koji je obavijest podnio nisu potrebni za razmjenu najbolje prakse u okviru skupine za suradnju. Sažeto izvješće trebalo bi sadržavati informacije o broju zaprimljenih obavijesti, kao i naznaku prirode incidenata o kojima je zaprimljena obavijest, primjerice o vrsti povreda sigurnosti, njihovoj ozbiljnost ili trajanju.

(34) Države članice trebale bi biti dostatno opremljene, u smislu tehničkih i organizacijskih sposobnosti, za sprečavanje i otkrivanje incidenata i rizika u mrežnim i informacijskim sustavima, davanje odgovora na njih i njihovo ublažavanje. Države članice stoga bi trebale osigurati da njihovi CSIRT-ovi, također poznati i kao timovi za odgovor na računalne opasnosti („CERT-ovi”), dobro funkcioniraju i da poštuju ključne zahtjeve kako bi se zajamčile djelotvorne i uskladive sposobnosti za rješavanje incidenata i rizika te kako bi se osigurala učinkovita suradnja na razini Unije. Kako bi sve vrste operatora ključnih usluga i pružatelja digitalnih usluga imale koristi od takvih sposobnosti i suradnje, države članice trebale bi osigurati da imenovani CSIRT-ovi pokrivaju sve njih. S obzirom na važnost međunarodne suradnje za kibersigurnost CSIRT-ovi bi trebali moći, uz mrežu CSIRT-ova uspostavljenu ovom Direktivom, sudjelovati i u međunarodnim mrežama suradnje.

(35) Budući da većinom mrežnih i informacijskih sustava upravljaju privatni subjekti, suradnja javnog i privatnog sektora od ključne je važnosti. Operatore ključnih usluga i pružatelje digitalnih usluga trebalo bi poticati da slijede vlastite neformalne mehanizme suradnje s ciljem osiguravanja sigurnosti mrežnih i informacijskih sustava. Skupina za suradnju trebala bi biti u mogućnosti, prema potrebi, pozvati relevantne dionike na sudjelovanje u raspravama. Kako bi se učinkovito poticalo dijeljenje informacija i najbolje prakse, ključno je osigurati da operatori ključnih usluga i pružatelji digitalnih usluga koji sudjeluju u takvom dijeljenju zbog suradnje ne dođu u nepovoljan položaj.

(36) ENISA bi državama članicama i Komisiji trebala pomoći pružanjem stručnog znanja i savjetovanjem te olakšavanjem razmjene najbolje prakse. Konkretno, u pogledu primjene ove Direktive Komisija bi se trebala, a države članice trebale bi se moći, savjetovati s ENISA-om. Za izgradnju sposobnost i unaprjeđivanje znanja među državama članicama skupina za suradnju također bi trebala služiti kao instrument za razmjenu najbolje prakse, rasprave o sposobnostima i pripravnosti država članica te, na dobrovoljnoj osnovi, pružati pomoć svojim članovima u ocjenjivanju nacionalnih strategija za sigurnost mrežnih i informacijskih sustava, izgradnji kapaciteta i ocjenjivanju vježbi koje se odnose na sigurnost mrežnih i informacijskih sustava.

(37) Prilikom primjene ove Direktive države članice bi, prema potrebi, trebale biti u mogućnosti koristiti se postojećim organizacijskim strukturama ili strategijama ili ih prilagoditi.

(38) Odgovarajuće zadaće skupine za suradnju i ENISA-e međuovisne su i međusobno se dopunjuju. ENISA bi općenito skupini za suradnju trebala pomagati u izvršavanju njezinih zadaća, u skladu s ciljem ENISA-e određenim u Uredbi (EU) br. 526/2013 Europskog parlamenta i Vijeća ([1]), osobito pomagati institucijama, tijelima, uredima i agencijama Unije i državama članicama u provedbi politika potrebnih za ispunjavanje pravnih i regulatornih zahtjeva u vezi sa sigurnošću mrežnih i informacijskih sustava u skladu s postojećim i budućim pravnim aktima Unije. ENISA bi konkretno trebala pružati pomoć u područjima koja odgovaraju njezinim vlastitim zadaćama, kako su određene u Uredbi (EU) br. 526/2013, osobito analiziranju strategija sigurnosti mrežnih i informacijskih sustava, podupiranju organizacije i provođenju vježbi Unije koje se odnose na sigurnost mrežnih i informacijskih sustava te razmjeni informacija i najbolje prakse za podizanje svijesti i osposobljavanja. ENISA bi također trebala biti uključena u razvoj smjernica za kriterije za pojedine sektore s ciljem utvrđivanja važnosti učinka pojedinog incidenta.

([1]) Uredba (EU) br. 526/2013 Europskog parlamenta i Vijeća od 21. svibnja 2013. o Agenciji Europske unije za mrežnu i informacijsku sigurnost (ENISA) i o stavljanju izvan snage Uredbe (EZ) br. 460/2004 (SL L 165, 18.6.2013., str. 41.).

(39) Radi promicanja napredne sigurnosti mrežnih i informacijskih sustava, skupina za suradnju bi, prema potrebi, trebala surađivati s odgovarajućim institucijama, tijelima, uredima i agencijama Unije s ciljem razmjene znanja i najbolje prakse i pružanja savjeta o aspektima sigurnosti mrežnih i informacijskih sustava koji bi mogli utjecati na njihov rad, poštujući pritom postojeće aranžmane za razmjenu povjerljivih informacija. Pri suradnji s tijelima za izvršavanje zakonodavstva u vezi sa sigurnosnim aspektima mrežnih i informacijskih sustava koji mogu utjecati na njihov rad, skupina za suradnju trebala bi poštovati postojeće informacijske kanale i uspostavljene mreže.

(40) Informacije o incidentima imaju sve veću vrijednost za javnost i poduzeća, posebno za mala i srednja poduzeća. U nekim slučajevima takve informacije na nacionalnoj razini već se pružaju putem internetskih stranica, na jeziku određene zemlje, pri čemu se najveća važnost većinom pridaje incidentima i događajima koji imaju nacionalnu dimenziju. Budući da poduzeća sve više djeluju preko granice i da se građani sve više koriste internetskim uslugama, informacije o incidentima u zbirnom obliku trebalo bi pružiti na razini Unije. Tajništvo mreže CSIRT-ova potiče se da vodi internetsku stranicu ili da na neku već postojeću internetsku stranicu uvrsti i posebnu stranicu na kojoj bi se javnosti na raspolaganje stavljale opće informacije o većim incidentima do kojih je došlo diljem Unije, s posebnim naglaskom na interese i potrebe poduzeća. CSIRT-ovi koji sudjeluju u mreži CSIRT-ova potiču se da na dobrovoljnoj osnovi pružaju informacije za objavu na toj internetskoj stranici bez uključivanja povjerljivih i osjetljivih informacija.

(41) Ako informaciju treba smatrati povjerljivom u skladu s Unijinim i nacionalnim pravilima o poslovnoj tajni, njezinu tajnost trebalo bi osigurati pri provedbi aktivnosti i pri ispunjavanju ciljeva postavljenih ovom Direktivom.

(42) Vježbe kojima se u realnom vremenu simuliraju scenariji incidenata ključne su za ispitivanja pripravnosti i suradnje država članica u pogledu sigurnosti mrežnih i informacijskih sustava. Ciklus vježbi CyberEurope kojim koordinira ENISA, uz sudjelovanje država članica, koristan je alat za testiranje i izradu preporuka o tome kako bi se rješavanje incidenata na razini Unije s vremenom trebalo poboljšati. Budući da države članice trenutačno nemaju obvezu planiranja vježbi ili sudjelovanja u njima, stvaranje mreže CSIRT-ova na temelju ove Direktive državama članicama trebalo bi omogućiti da sudjeluju u vježbama na temelju preciznog planiranja i strateških odabira. Skupina za suradnju uspostavljena na temelju ove Direktive trebala bi raspravljati o strateškim odlukama u vezi s vježbama, posebno, ali ne isključivo, u pogledu pravilnosti vježbi i izrade scenarija. ENISA bi u skladu sa svojim mandatom trebala pružiti potporu pri organizaciji i provođenju vježbi na razini Unije pružajući svoje stručno znanje i savjete skupini za suradnju i mreži CSIRT-ova.

(43) S obzirom na globalnu prirodu sigurnosnih problema koji utječu na mrežne i informacijske sustave postoji potreba za užom međunarodnom suradnjom radi unapređenja sigurnosnih standarda i razmjene podataka te za promicanjem zajedničkog globalnog pristupa pitanjima sigurnosti.

(44) Odgovornost za osiguranje sigurnosti mrežnih i informacijskih sustava uvelike snose operatori ključnih usluga i pružatelji digitalnih usluga. Kulturu upravljanja rizikom, među ostalim procjenu rizika i provedbu sigurnosnih mjera primjerenih riziku s kojim se suočava, trebalo bi poticati i razvijati prikladnim regulatornim zahtjevima i dobrovoljnim industrijskim praksama. Postavljanje pouzdanih ravnopravnih uvjeta također je ključno za učinkovito funkcioniranje skupine za suradnju i mreže CSIRT-ova, kako bi se osigurala djelotvorna suradnja svih država članica.

(45) Ova Direktiva primjenjuje se samo na one javne uprave koje su identificirane kao operatori ključnih usluga. Stoga su države članice odgovorne za osiguravanje sigurnosti mrežnih i informacijskih sustava javnih uprava koje ne pripadaju u područje primjene ove Direktive.

(46) Mjere za upravljanje rizikom uključuju mjere za utvrđivanje rizika od incidenata, sprječavanje, otkrivanje i rješavanje incidenata i ublažavanje njihova učinka. Sigurnost mrežnih i informacijskih sustava uključuje sigurnost podataka koji se pohranjuju, prenose i obrađuju.

(47) Nadležna tijela trebala bi i dalje imati mogućnost donošenja nacionalnih smjernica u vezi s okolnostima u kojima su operatori ključnih usluga dužni obavijestiti o incidentima.

(48) Mnoga poduzeća u Uniji se za pružanje svojih usluga oslanjaju na pružatelje digitalnih usluga. Budući da bi neke digitalne usluge mogle biti važan resurs za njihove korisnike, uključujući operatore ključnih usluga, te zato što je moguće da takvim korisnicima nije uvijek na raspolaganju alternativa, ova bi se Direktiva trebala primjenjivati i na pružatelje takvih usluga. Sigurnost, kontinuitet i pouzdanost vrsta digitalnih usluga navedenih u ovoj Direktivi ključni su za nesmetan rad mnogih poduzeća. Prekid neke od tih digitalnih usluga mogao bi onemogućiti pružanje drugih usluga koje se na tu uslugu oslanjaju te bi stoga mogao utjecati na ključne gospodarske i društvene aktivnosti u Uniji. Takve digitalne usluge stoga bi mogle biti od ključne važnosti za nesmetano funkcioniranje poduzeća koja ovise o njima te, osim toga, i za sudjelovanje takvih poduzeća na unutarnjem tržištu i u prekograničnoj trgovini diljem Unije. Pružatelji tih digitalnih usluga koji podliježu ovoj Direktivi jesu oni pružatelji za koje se smatra da nude digitalne usluge na koje se sve više oslanjaju mnoga poduzeća u Uniji.

(49) Pružatelji digitalnih usluga trebali bi osigurati razinu sigurnosti koja je u skladu sa stupnjem rizika kojima je izložena sigurnost usluga koje pružaju, s obzirom na važnost njihovih usluga za rad drugih poduzeća unutar Unije. U praksi je stupanj rizika za operatore ključnih usluga, koje su često neophodne za održavanje ključnih društvenih i gospodarskih aktivnosti, veći nego za pružatelje digitalnih usluga. Stoga bi sigurnosni zahtjevi za pružatelje digitalnih usluga trebali biti blaži. Pružatelji digitalnih usluga trebali bi i dalje imati slobodu poduzimanja mjera koje smatraju primjerenima za upravljanje rizicima kojima je izložena sigurnost njihovih mrežnih i informacijskih sustava. Zbog prekogranične prirode pružatelja digitalnih usluga na njih bi se trebao primjenjivati usklađeniji pristup na razini Unije. Provedbeni akti trebali bi olakšati specifikaciju i provedbu takvih mjera.

(50) Iako proizvođači hardvera i programski inženjeri nisu operatori ključnih usluga niti su pružatelji digitalnih usluga, njihovi proizvodi poboljšavaju sigurnost mrežnih i informacijskih sustava. Stoga oni imaju važnu ulogu jer operatorima ključnih usluga i pružateljima digitalnih usluga omogućuju da osiguraju svoje mrežne i informacijske sustave. Na takve hardverske i softverske proizvode već se primjenjuju postojeća pravila o odgovornosti za proizvode.

(51) Tehničke i organizacijske mjere nametnute operatorima ključnih usluga i pružateljima digitalnih usluga ne bi trebale uvjetovati definiran način za osmišljavanje, razvoj i proizvodnju određenog komercijalnog proizvoda informacijske i komunikacijske tehnologije.

(52) Operatori ključnih usluga i pružatelji digitalnih usluga trebali bi osigurati sigurnost mrežnih i informacijskih sustavâ kojima se koriste. To su ponajprije privatne mreže i sustavi kojima upravljaju njihovi vlastiti zaposlenici u IT-u ili vanjski zaposlenici koji se brinu o sigurnosti. Zahtjevi u pogledu sigurnosti i obavješćivanja trebali bi se primijeniti na relevantne operatore ključnih usluga i pružatelje digitalnih usluga bez obzira na to održavaju li sami svoje mrežne i informacijske sustave ili to eksternaliziraju.

(53) Da bi se izbjeglo nerazmjerno financijsko i administrativno opterećenje za operatore ključnih usluga i pružatelje digitalnih usluga, zahtjevi bi trebali biti razmjerni riziku kojemu je izložen dotični mrežni ili informacijski sustav, uzimajući u obzir suvremenost takvih mjera. U slučaju pružatelja digitalnih usluga ti zahtjevi ne bi se trebali primjenjivati na mikropoduzeća i mala poduzeća.

(54) Ako se javne uprave u državama članicama koriste uslugama koje nude pružatelji digitalnih usluga, posebno uslugama računalstva u oblaku, one bi od pružatelja takvih usluga mogle zahtijevati dodatne sigurnosne mjere koje premašuju ono što pružatelji digitalnih usluga obično nude u skladu sa zahtjevima ove Direktive. To bi trebali moći učiniti putem ugovorne obveze.

(55) Definicije internetskih tržišta, internetskih tražilica i usluga računalstva u oblaku u ovoj Direktivi namijenjene su za posebne svrhe ove Direktive i ne dovode u pitanje bilo koje druge instrumente.

(56) Ova Direktiva države članice ne bi trebala sprečavati da donesu nacionalne mjere kojima se od tijela javnog sektora zahtijeva osiguravanje posebnih sigurnosnih zahtjeva pri sklapanju ugovora za usluge računalstva u oblaku. Sve takve nacionalne mjere trebale bi se primjenjivati na dotično tijelo javnog sektora, a ne na pružatelja usluge računalstva u oblaku.

(57) S obzirom na bitne razlike između operatora ključnih usluga, posebno s obzirom na njihovu izravnu vezu s fizičkom infrastrukturom, i pružatelja digitalnih usluga, posebno s obzirom na njihovu prekograničnu prirodu, u okviru ove Direktive trebalo bi zauzeti diferencirani pristup u pogledu razine usklađivanja za te dvije skupine subjekata. Za operatore ključnih usluga države članice trebale bi moći identificirati relevantne operatore i nametnuti strože zahtjeve od onih koji su utvrđeni ovom Direktivom. Države članice ne bi trebale identificirati pružatelje digitalnih usluga jer bi se ova Direktiva trebala primjenjivati na sve pružatelje digitalnih usluga obuhvaćene područjem njezine primjene. Osim toga, ova Direktiva i na temelju nje doneseni provedbeni akti trebali bi osigurati visoku razinu usklađenosti u pogledu zahtjeva za sigurnost i obavješćivanje za pružatelje digitalnih usluga. To bi trebalo omogućiti da se prema pružateljima digitalnih usluga postupa ujednačeno diljem Unije, na način koji je razmjeran njihovoj prirodi i stupnju rizika kojem bi mogli biti izloženi.

(58) Ovom Direktivom državama članicama ne bi se smjelo spriječiti uvođenje zahtjeva za sigurnost i obavješćivanje za subjekte koji nisu pružatelji digitalnih usluga obuhvaćeni područjem primjene ove Direktive, ne dovodeći u pitanje obveze država članica u skladu s pravom Unije.

(59) Nadležna tijela trebala bi obratiti dužnu pozornost na očuvanje neformalnih i pouzdanih kanala za dijeljenje informacija. Objavom incidenata koji su prijavljeni nadležnim tijelima trebalo bi se na primjeren način uravnotežiti interes javnosti da bude informirana o prijetnjama i moguću štetu za ugled ili tržišnu štetu za operatore ključnih usluga i pružatelje digitalnih usluga koji incidente prijavljuju. U provedbi obveza obavješćivanja nadležna tijela i CSIRT-i posebno bi trebali obratiti pozornost na potrebu da se podaci o ranjivosti proizvoda drže u strogoj tajnosti prije objave odgovarajućih sigurnosnih popravaka.

(60) Pružatelji digitalnih usluga povjerenja trebali bi biti podvrgnuti manje opsežnim i reaktivnim naknadnim (*ex post*) nadzornim aktivnostima koje su opravdane zbog prirode njihovih usluga i djelatnosti. Dotična nadležna tijela stoga bi trebala poduzimati mjere samo ako im se pruže dokazi, primjerice od strane samog pružatelja digitalnih usluga, drugog nadležnog tijela, uključujući nadležno tijelo druge države članice, ili od strane korisnika te usluge, da neki pružatelj digitalnih usluga ne poštuje zahtjeve ove Direktive, posebno nakon pojave incidenta. Nadležno tijelo stoga ne bi trebalo imati opću obvezu nadzora pružatelja digitalnih usluga.

(61) Nadležna tijela trebala bi na raspolaganju imati sredstva potrebna za obavljanje njihovih dužnosti, što uključuje ovlasti za dobivanje informacija koje su potrebne kako bi se mogla odrediti razina sigurnosti mrežnih i informacijskih sustava.

(62) Incidenti mogu biti rezultat kriminalnih aktivnosti, a njihovo sprečavanje, istragu i kazneni progon podržava se koordinacijom i suradnjom operatora ključnih usluga, pružatelja digitalnih usluga, nadležnih tijela i tijela za izvršavanje zakonodavstva. Ako se sumnja da je incident povezan s aktivnostima koje su prema pravu Unije ili nacionalnom pravu ozbiljne kriminalne aktivnosti, države članice trebale bi operatore ključnih usluga i pružatelje digitalnih usluga poticati da odgovarajućim tijelima za izvršavanje zakonodavstva prijave incidente za koje se sumnja da su ozbiljne kriminalne naravi. Poželjno je da koordinaciju između nadležnih tijela i tijela za izvršavanje zakonodavstva različitih država članica, prema potrebi, olakšavaju Europski centar za kiberkriminal (EC3) i ENISA.

(63) U mnogim slučajevima osobni podaci ugroženi su zbog incidenata. U tom kontekstu nadležna tijela i tijela za zaštitu podataka trebala bi surađivati i razmjenjivati informacije o svim relevantnim temama za rješavanje kršenja tajnosti osobnih podataka uzrokovanih incidentima.

(64) Nadležnost u pogledu pružateljâ digitalnih usluga trebala bi se dodijeliti samo državi članici u kojoj dotični pružatelj digitalnih usluga ima svoj glavni poslovni nastan u Uniji, a što u načelu odgovara mjestu u kojem pružatelj ima svoje sjedište u Uniji. Poslovni nastan podrazumijeva učinkovito i stvarno obavljanje djelatnosti u okviru stabilnih aranžmana. Pravni oblik takvih aranžmana, bilo posredstvom podružnice ili društva kćeri s pravnom osobnošću, nije odlučujući čimbenik u tom pogledu. Taj kriterij ne bi trebao ovisiti o tome jesu li

mrežni i informacijski sustavi fizički smješteni na tom mjestu jer prisutnost tih sustava i korištenje njima ne predstavljaju sami po sebi takav glavni poslovni nastan te stoga nisu kriteriji za utvrđivanje glavnog poslovnog nastana.

(65) Ako pružatelj digitalnih usluga koji nema poslovni nastan u Uniji nudi usluge u Uniji, trebao bi imenovati predstavnika. Kako bi se utvrdilo nudi li takav pružatelj digitalnih usluga usluge u Uniji, trebalo bi provjeriti može li se zaključiti da pružatelj digitalnih usluga planira ponuditi usluge osobama u jednoj državi članici ili više njih. Sama dostupnost u Uniji internetskih stranica pružatelja digitalnih usluga ili posrednog davatelja takvih usluga ili adrese elektroničke pošte i drugih podataka za kontakt ili korištenje jezikom koji je općenito u uporabi u trećoj zemlji u kojoj pružatelj digitalnih usluga ima poslovni nastan nedovoljna je za utvrđivanje takve namjere. Međutim, čimbenici kao što su korištenje jezikom ili valutom koji su općenito u uporabi u jednoj državi članica ili više njih, s mogućnošću naručivanja usluga na tom drugom jeziku ili spominjanje kupaca ili korisnika koji se nalaze u Uniji, mogu jasno pokazati da pružatelj digitalnih usluga planira ponuditi usluge u Uniji. Predstavnik bi trebao djelovati u ime pružatelja digitalnih usluga te bi tog predstavnika trebala moći kontaktirati nadležna tijela ili CSIRT-ovi. Pružatelj digitalnih usluga predstavnika bi trebao pisanim ovlaštenjem izričito imenovati da djeluje u njegovo ime s obzirom na obveze tog pružatelja digitalnih usluga prema ovoj Direktivi, što uključuje izvješćivanja o incidentima.

(66) Standardizacija sigurnosnih zahtjeva proces je koji određuje tržište. Da bi se osigurala konvergentna primjena sigurnosnih standarda, države članice trebale bi poticati sukladnost ili usklađenost s posebnim standardima radi osiguranja visoke razine sigurnosti mrežnih i informacijskih sustava na razini Unije. ENISA bi davanjem savjeta i smjernica trebala pomagati državama članicama. U tu svrhu moglo bi biti korisno izraditi usklađene norme, koje bi trebalo izraditi u skladu s Uredbom (EU) br. 1025/2012 Europskog parlamenta i Vijeća ([1]).

(67) Subjektima koji nisu obuhvaćeni područjem primjene ove Direktive mogu se dogoditi incidenti koji imaju znatan učinak na usluge koje pružaju. Ako ti subjekti smatraju da bi bilo u javnom interesu da obavijeste o pojavi takvih incidenata, trebali bi to moći učiniti na dobrovoljnoj osnovi. Takve obavijesti trebali bi obrađivati nadležno tijelo ili CSIRT ako takva obrada ne predstavlja nerazmjerno ili nepotrebno opterećenje za dotične države članice.

(68) Radi osiguranja jedinstvenih uvjeta za provedbu ove Direktive, provedbene ovlasti trebalo bi dodijeliti Komisiji radi utvrđivanja postupovnih aranžmana potrebnih za funkcioniranje skupine za suradnju i za zahtjeve za sigurnost i obavješćivanje koji se primjenjuju na pružatelje digitalnih usluga. Te bi ovlasti trebalo izvršavati u skladu s Uredbom (EU) br. 182/2011 Europskog parlamenta i Vijeća ([2]). Pri donošenju provedbenih akata koji se odnose na postupovne aranžmane potrebne za funkcioniranje skupine za suradnju Komisija bi trebala što je više moguće uzimati u obzir mišljenje ENISA-e.

(69) Prilikom donošenja provedbenih akata o sigurnosnim zahtjevima za pružatelje digitalnih usluga, Komisija bi trebala u najvećoj mogućoj mjeri uzeti u obzir mišljenje ENISA-e i savjetovati se sa zainteresiranim dionicima. Nadalje, Komisiju se potiče da uzme u obzir sljedeće primjere: u pogledu sigurnosti sustava i postrojenja: fizičku sigurnost i sigurnost okoliša, sigurnost opskrbe, kontrolu pristupa mrežnim i informacijskim sustavima i cjelovitost mrežnih i informacijskih sustava; u pogledu rješavanja incidenata: postupke za rješavanje incidenata, sposobnost otkrivanja incidenata, izvješćivanja o incidentima i komunikaciju o njima; u pogledu upravljanja kontinuitetom poslovanja: strategije za kontinuitet pružanja usluga i krizne planove, sposobnosti za oporavak od katastrofa; te u pogledu praćenja, revizije i testiranja: politike praćenja i evidencija, vježbe kriznih planova, testiranje mrežnih i informacijskih sustava, sigurnosne procjene i praćenje sukladnosti.

(70) U provedbi ove Direktive Komisija bi, prema potrebi, trebala održavati vezu s relevantnim sektorskim odborima te relevantnim tijelima uspostavljenim na razini Unije, posebno u područjima koja obuhvaća ova Direktiva.

([1]) Uredba (EU) br. 1025/2012 Europskog parlamenta i Vijeća od 25. listopada 2012. o europskoj normizaciji, o izmjeni direktiva Vijeća 89/686/EEZ i 93/15/EEZ i direktiva 94/9/EZ, 94/25/EZ, 95/16/EZ, 97/23/EZ, 98/34/EZ, 2004/22/EZ, 2007/23/EZ, 2009/23/EZ i 2009/105/EZ Europskog parlamenta i Vijeća te o stavljanju izvan snage Odluke Vijeća 87/95/EEZ i Odluke br. 1673/2006/EZ Europskog parlamenta i Vijeća (SL L 316, 14.11.2012., str. 12.).

([2]) Uredba (EU) br. 182/2011 Europskog parlamenta i Vijeća od 16. veljače 2011. o utvrđivanju pravila i općih načela u vezi s mehanizmima nadzora država članica nad izvršavanjem provedbenih ovlasti Komisije (SL L 55, 28.2.2011., str. 13.).

(71) Komisija bi periodično trebala preispitivati ovu Direktivu, uz savjetovanje sa zainteresiranim dionicima, posebno u pogledu utvrđivanja toga postoji li potreba za njezinom izmjenom u svjetlu promjene društvenih, političkih, tehnoloških i tržišnih uvjeta.

(72) Pri dijeljenju informacija o rizicima i incidentima u okviru skupine za suradnju i mreže CSIRT-ova te pri poštovanju zahtjeva da se o incidentima obavijeste nadležna nacionalna tijela ili CSIRT-ovi mogla bi biti potrebna obrada osobnih podataka. Takva obrada trebala bi se provoditi u skladu s Direktivom 95/46/EZ Europskog parlamenta i Vijeća ([1]) i Uredbom (EZ) br. 45/2001 Europskog parlamenta i Vijeća ([2]). U primjeni ove Direktive bi, prema potrebi, trebalo primjenjivati Uredbu (EZ) br. 1049/2001 Europskog parlamenta i Vijeća ([3]).

(73) Izvršeno je savjetovanje s Europskim nadzornikom za zaštitu podataka u skladu s člankom 28. stavkom 2. Uredbe (EZ) br. 45/2001 te je on dao mišljenje 14. lipnja 2013. ([4]).

(74) S obzirom na to da cilj ove Direktive, to jest postizanje visoke zajedničke razine sigurnosti mrežnih i informacijskih sustava u Uniji, ne mogu dostatno ostvariti države članice, nego se zbog učinka djelovanja on na bolji način može ostvariti na razini Unije, Unija može donijeti mjere u skladu s načelom supsidijarnosti utvrđenim u članku 5. Ugovora o Europskoj uniji. U skladu s načelom proporcionalnosti utvrđenim u tom članku, ova Direktiva ne prelazi ono što je potrebno za ostvarivanje tog cilja.

(75) Ova Direktiva poštuje temeljna prava i uzima u obzir načela priznata Poveljom Europske unije o temeljnim pravima, posebno pravo na poštovanje privatnog života i komuniciranja, zaštitu osobnih podataka, slobodu poduzetništva, pravo na vlasništvo, pravo na djelotvoran pravni lijek pred sudom i pravo na saslušanje. Ova Direktiva trebala bi se provoditi u skladu s tim pravima i načelima,

DONIJELI SU OVU DIREKTIVU:

POGLAVLJE I.

OPĆE ODREDBE

Članak 1.

Predmet i područje primjene

1. Ovom Direktivom utvrđuju se mjere s ciljem postizanja visoke zajedničke razine sigurnosti mrežnih i informacijskih sustava unutar Unije kako bi se poboljšalo funkcioniranje unutarnjeg tržišta.

2. U tu svrhu, ovom Direktivom:

(a) utvrđuje se obveza za sve države članice da donesu nacionalnu strategiju za sigurnost mrežnih i informacijskih sustava;

(b) stvara se skupina za suradnju u svrhu podupiranja i olakšavanja strateške suradnje i razmjene informacija među državama članicama i razvijanja međusobnog povjerenja i pouzdanja;

(c) stvara se mreža timova za odgovor na računalne sigurnosne incidente („mreža CSIRT-ova”) kako bi se doprinijelo razvoju pouzdanja i povjerenja među državama članicama i promicalo brzu i učinkovitu operativnu suradnju;

([1]) Direktiva 95/46/EZ Europskog parlamenta i Vijeća od 24. listopada 1995. o zaštiti pojedinaca u vezi s obradom osobnih podataka i o slobodnom protoku takvih podataka (SL L 281, 23.11.1995., str. 31.).
([2]) Uredba (EZ) br. 45/2001 Europskog parlamenta i Vijeća od 18. prosinca 2000. o zaštiti pojedinaca u vezi s obradom osobnih podataka u institucijama i tijelima Zajednice i o slobodnom kretanju takvih podataka (SL L 8, 12.1.2001., str. 1.).
([3]) Uredba (EZ) br. 1049/2001 Europskog parlamenta i Vijeća od 30. svibnja 2001. o javnom pristupu dokumentima Europskog parlamenta, Vijeća i Komisije (SL L 145, 31.5.2001., str. 43.).
([4]) SL C 32, 4.2.2014., str. 19.

(d) utvrđuju se zahtjevi za sigurnost i obavješćivanje za operatore ključnih usluga i za pružatelje digitalnih usluga;

(e) utvrđuju se obveze za države članice da imenuju nacionalna nadležna tijela, jedinstvene kontaktne točke i CSIRT-ove čije su zadaće vezane uz sigurnost mrežnih i informacijskih sustava.

3. Zahtjevi za sigurnost i obavješćivanje iz ove Direktive ne primjenjuju se na poduzeća na koje se primjenjuju zahtjevi iz članaka 13.a i 13.b Direktive 2002/21/EZ ni na pružatelje usluga povjerenja na koje se primjenjuju zahtjevi iz članka 19. Uredbe (EU) br. 910/2014.

4. Ova Direktiva primjenjuje se ne dovodeći u pitanje Direktivu Vijeća 2008/114/EZ ([1]) i direktive 2011/93/EU ([2]) i 2013/40/EU ([3]) Europskog parlamenta i Vijeća.

5. Ne dovodeći u pitanje članak 346. UFEU-a, informacije koje se smatraju povjerljivima u skladu s pravilima Unije i nacionalnim pravilima, kao što su pravila o poslovnoj tajni, Komisiji i drugim relevantnim tijelima, ustupaju se samo u slučaju kad je takva razmjena nužna za primjenu ove Direktive. Razmijenjene informacije ograničuju se na ono što je relevantno i mora biti razmjerna svrsi takve razmjene. Pri takvoj razmjeni informacija čuva se povjerljivost tih informacija te se štite sigurnost i komercijalni interesi operatora ključnih usluga i pružatelja digitalnih usluga.

6. Ovom Direktivom ne dovode se u pitanje mjere koje države članice poduzimaju za zaštitu svojih temeljnih državnih funkcija, posebno za zaštitu nacionalne sigurnosti, što uključuje mjere za zaštitu informacija za čije otkrivanje države članice smatraju da bi bilo suprotno osnovnim interesima njihove sigurnosti, te za održavanje zakona i reda, posebno za to da se dopuste istraga, otkrivanje i kažnjavanje kaznenih djela.

7. Ako se pravnim aktom Unije za pojedini sektor od operatora ključnih usluga ili pružatelja digitalnih usluga zahtijeva da osiguraju ili sigurnost svojih mrežnih i informacijskih sustava ili da obavijeste o incidentima, pod uvjetom da su takvi zahtjevi po učinku barem jednaki obvezama utvrđenima u ovoj Direktivi, primjenjuju se te odredbe iz tog pravnog akta Unije za pojedini sektor.

Članak 2.

Obrada osobnih podataka

1. Obrada osobnih podataka na temelju ove Direktive provodi se u skladu s Direktivom 95/46/EZ.

2. Obrada osobnih podataka koju prema ovoj Direktivi provode institucije i tijela Unije provodi se u skladu s Uredbom (EZ) br. 45/2001.

Članak 3.

Minimalno usklađivanje

Ne dovodeći u pitanje članak 16. stavak 10. i obveze država članica u skladu s pravom Unije, države članice mogu donijeti ili zadržati odredbe čiji je cilj postizanje više razine sigurnosti mrežnih i informacijskih sustava.

([1]) Direktiva Vijeća 2008/114/EZ od 8. prosinca 2008. o utvrđivanju i označivanju europske kritične infrastrukture i procjeni potrebe poboljšanja njezine zaštite (SL L 345, 23.12.2008., str. 75.).

([2]) Direktiva 2011/93/EU Europskog parlamenta i Vijeća od 13. prosinca 2011. o suzbijanju seksualnog zlostavljanja i seksualnog iskorištavanja djece i dječje pornografije, te o zamjeni Okvirne odluke Vijeća 2004/68/PUP (SL L 335, 17.12.2011., str. 1.).

([3]) Direktiva 2013/40/EU Europskog parlamenta i Vijeća od 12. kolovoza 2013. o napadima na informacijske sustave i o zamjeni Okvirne odluke Vijeća 2005/222/PUP (SL L 218, 14.8.2013., str. 8.).

Članak 4.

Definicije

Za potrebe ove Direktive primjenjuju se sljedeće definicije:

1. „mrežni i informacijski sustav” znači:

   (a) elektronička komunikacijska mreža u smislu članka 2. točke (a) Direktive 2002/21/EZ;

   (b) bilo koji uređaj ili grupa povezanih ili srodnih uređaja, od kojih jedan ili više njih programski izvršava automatsku obradu digitalnih podataka; ili

   (c) digitalni podaci koji se pohranjuju, obrađuju, dobivaju ili prenose elementima opisanim u točkama (a) i (b) u svrhu njihova rada, uporabe, zaštite i održavanja;

2. „sigurnost mrežnih i informacijskih sustava” znači sposobnost mrežnih i informacijskih sustava da odolijevaju, na određenoj razini pouzdanosti, bilo kojoj radnji koja ugrožava dostupnost, autentičnost, cjelovitost ili povjerljivost pohranjenih ili prenesenih ili obrađenih podataka ili srodnih usluga koje ti mrežni i informacijski sustavi nude ili kojima omogućuju pristup;

3. „nacionalna strategija za sigurnost mrežnih i informacijskih sustava” znači okvir kojim se pružaju strateški ciljevi i prioriteti za sigurnost mrežnih i informacijskih sustava na nacionalnoj razini;

4. „operator ključne usluge” znači javni ili privatni subjekt tipa navedenog u Prilogu II., koji ispunjava kriterije utvrđene u članku 5. stavku 2.;

5. „digitalna usluga” znači usluga u smislu članka 1. stavka 1. točke (b) Direktive (EU) 2015/1535 Europskog parlamenta i Vijeća ([1]) tipa navedenog na popisu u Prilogu III.;

6. „pružatelj digitalnih usluga” znači bilo koja pravna osoba koja pruža neku digitalnu uslugu;

7. „incident” znači bilo koji događaj koji ima stvaran negativni učinak na sigurnost mrežnih i informacijskih sustava;

8. „rješavanje incidenta” znači svi postupci koji podupiru otkrivanje, analizu i zaustavljanje incidenta te odgovor na njega;

9. „rizik” znači bilo koja razumno prepoznatljiva okolnost ili događaj koji ima potencijalan negativni učinak na sigurnost mrežnih i informacijskih sustava;

10. „predstavnik” znači bilo koja fizička ili pravna osoba s poslovnim nastanom u Uniji koju je pružatelj digitalnih usluga koji nema poslovni nastan u Uniji izričito imenovao da djeluje u njegovo ime i kojoj se nacionalno nadležno tijelo ili CSIRT mogu obratiti umjesto tom pružatelju digitalnih usluga u pogledu obveza tog pružatelja digitalnih usluga iz ove Direktive;

11. „norma” znači norma u smislu članka 2. točke 1. Uredbe (EU) br. 1025/2012;

12. „specifikacija” znači tehnička specifikacija u smislu članka 2. točke 4. Uredbe (EU) br. 1025/2012;

13. „središte za razmjenu internetskog prometa (IXP)” znači mrežni instrument koji omogućuje međusobno povezivanje više od dvaju neovisnih autonomnih sustava, prvenstveno u svrhu olakšavanja razmjene internetskog prometa; IXP pruža međusobno povezivanje samo za autonomne sustave; za IXP nije potrebno da internetski promet između bilo kojih dvaju autonomnih sustava sudionika prođe kroz bilo koji treći autonomni sustav, on takav promet ne mijenja i ne utječe na njega ni na koji drugi način;

14. „sustav naziva domena (DNS)” znači hijerarhijsko raspoređeni sustav imenovanja na mreži koji šalje upite o nazivima domena;

([1]) Direktiva (EU) 2015/1535 Europskog parlamenta i Vijeća od 9. rujna 2015. o utvrđivanju postupka pružanja informacija u području tehničkih propisa i pravila o uslugama informacijskog društva (SL L 241, 17.9.2015., str. 1.).

15. „pružatelj DNS usluge” znači subjekt koji pruža DNS usluge na internetu;

16. „registri naziva vršnih domena” znači subjekt koji upravlja i rukuje registracijom naziva internetskih domena za određenu vršnu domenu (TLD);

17. „internetsko tržište” znači digitalna usluga koja potrošačima i/ili trgovcima, kako su utvrđeni u članku 4. stavku 1. točki (a) odnosno točki (b) Direktive 2013/11/EU Europskog parlamenta i Vijeća ([1]), omogućuje da na internetu sklapaju kupoprodajne ugovore i ugovore o uslugama s trgovcima na mrežnoj stranici tog internetskog tržišta ili na mrežnoj stranici tog trgovca koji se služi računalnim uslugama koje pruža internetsko tržište;

18. „internetska tražilica” znači digitalna usluga koja korisniku omogućuje da vrši pretraživanja u načelu svih internetskih stranica ili internetskih stranica na određenom jeziku na temelju upita o bilo kojoj temi koji je u obliku ključne riječi, rečenice ili nekog drugog unosa, a rezultat su poveznice na kojima se mogu pronaći informacije koje su povezane sa zatraženim sadržajem;

19. „usluga računalstva u oblaku” znači digitalna usluga kojom se pruža pristup nadogradivom i elastičnom skupu djeljivih računalnih resursa.

Članak 5.

Identifikacija operatora ključnih usluga

1. Do 9. studenoga 2018. za svaki sektor i podsektor iz Priloga II. države članice identificiraju operatore ključnih usluga s poslovnim nastanom na njihovom državnom području.

2. Kriteriji za identifikaciju operatora ključnih usluga iz članka 4. točke 4. jesu sljedeći:

(a) subjekt pruža uslugu koja je ključna za održavanje ključnih društvenih i/ili ekonomskih djelatnosti;

(b) pružanje takve usluge ovisi o mrežnim i informacijskim sustavima; i

(c) incident bi imao znatan negativan učinak na pružanje te usluge.

3. Za potrebe stavka 1. svaka država članica sastavlja popis usluga iz stavka 2. točke (a).

4. Za potrebe stavka 1. ako subjekt pruža uslugu kako je navedeno u stavku 2. točki (a) u dvije ili više država članica, te države članice uključuju se u međusobna savjetovanja. Savjetovanja se održavaju prije nego što bude donesena odluka o identificiranju.

5. Države članice redovito, a najmanje svake dvije godine nakon 9. svibnja 2018., preispituju i, prema potrebi, ažuriraju popis identificiranih operatora ključnih usluga.

6. Uloga skupine za suradnju u skladu sa zadaćama iz članka 11. jest podupirati države članice u zauzimanju dosljednog pristupa u postupku identifikacije operatora ključnih usluga.

7. Za potrebe preispitivanja iz članka 23. i najkasnije 9. studenoga 2018., a nakon toga svake dvije godine, države članice Komisiji dostavljaju podatke koji su potrebni kako bi se Komisiji omogućila procjena provedbe ove Direktive, posebno dosljednosti u pristupu država članica pri identifikaciji operatora ključnih usluga. Ti podaci obuhvaćaju barem:

(a) nacionalne mjere kojima se omogućuje identifikacija operatora ključnih usluga;

([1]) Direktiva 2013/11/EU Europskog parlamenta i Vijeća od 21. svibnja 2013. o alternativnom rješavanju potrošačkih sporova i izmjeni Uredbe (EZ) br. 2006/2004 i Direktive 2009/22/EZ (Direktiva o alternativnom rješavanju potrošačkih sporova) (SL L 165, 18.6.2013., str. 63.).

(b) popis usluga iz stavka 3.;

(c) broj operatora ključnih usluga identificiranih za svaki sektor iz Priloga II. te oznaku njihove važnosti u odnosu na taj sektor;

(d) pragove, ako postoje, za određivanje odgovarajuće razine opskrbe prema broju korisnika koji se oslanjaju na tu uslugu kako je navedeno u članku 6. stavku 1. točki (a) ili u skladu s važnošću tog određenog operatora ključnih usluga kako je navedeno u članku 6. stavku 1. točki (f).

Kako bi se doprinijelo tome da dostavljeni podaci budu usporedivi, Komisija, uzimajući u najvećoj mogućoj mjeri u obzir mišljenje ENISA-e, može donijeti odgovarajuće tehničke smjernice u pogledu parametara za informacije navedene u ovom stavku.

Članak 6.

Znatan negativan učinak

1. Pri utvrđivanju važnosti negativnog učinka iz točke (c) članka 5. stavka 2., države članice uzimaju u obzir barem sljedeće međusektorske čimbenike:

(a) broj korisnika koji se oslanjaju na usluge koje taj subjekt pruža;

(b) ovisnost drugih sektora iz Priloga II. o uslugama koje dotični subjekt pruža;

(c) mogući utjecaj incidenata, u pogledu njihova stupnja i trajanja, na gospodarske i društvene aktivnosti te na javnu sigurnost;

(d) tržišni udio tog subjekta;

(e) zemljopisnu raširenost u smislu područja na koje bi incident mogao utjecati;

(f) važnost subjekta za održavanje dostatne razine usluge, uzimajući u obzir raspoloživost alternativnih sredstava za pružanje te usluge.

2. Kako bi se utvrdilo bi li incident imao znatan negativan učinak, države članice također, prema potrebi, u obzir uzimaju čimbenike specifične za pojedini sektor.

POGLAVLJE II.

NACIONALNI OKVIRI ZA SIGURNOST MREŽNIH I INFORMACIJSKIH SUSTAVA

Članak 7.

Nacionalna strategija za sigurnost mrežnih i informacijskih sustava

1. Svaka država članica donosi nacionalnu strategiju za sigurnost mrežnih i informacijskih sustava, kojom se određuju strateški ciljevi te primjerena politika i regulatorne mjere s ciljem postizanja i održavanja visoke razine sigurnosti mrežnih i informacijskih sustava te koja obuhvaća barem sektore iz Priloga II. i usluge navedene u Prilogu III. Nacionalna strategija za sigurnost mrežnih i informacijskih sustava posebno se bavi sljedećim pitanjima:

(a) ciljevima i prioritetima nacionalnih strategija za sigurnost mrežnih i informacijskih sustava;

(b) upravljačkim okvirom za postizanje ciljeva i prioriteta nacionalne strategije za sigurnost mrežnih i informacijskih sustava, među ostalim ulogama i odgovornostima vladinih tijela i drugih relevantnih sudionika;

(c) određivanjem mjera u vezi s pripravnošću, odgovorom i ponovnom uspostavom, uključujući mehanizme suradnje između javnog i privatnog sektora;

(d) određivanjem programâ edukacije, podizanja razine svijesti i osposobljavanja povezanih sa strategijom sigurnosti mrežnih i informacijskih sustava;

(e) određivanjem istraživačkih i razvojnih planova u pogledu strategije za sigurnost mrežnih i informacijskih sustava;

(f) planom za procjenu rizika s ciljem prepoznavanja rizika;

(g) popisom različitih sudionika u provedbi nacionalne strategije za sigurnost mrežnih i informacijskih sustava.

2. Države članice mogu zatražiti podršku ENISA-e u razvijanju nacionalnih strategija za sigurnost mrežnih i informacijskih sustava.

3. Države članice priopćuju svoje nacionalne strategije za sigurnost mrežnih i informacijskih sustava Komisiji u roku od tri mjeseca od njihova donošenja. Pritom države članice mogu isključiti elemente strategije koji su povezani s nacionalnom sigurnosti.

Članak 8.

Nacionalna nadležna tijela i jedinstvene kontaktne točke

1. Svaka država članica imenuje jedno ili više nacionalnih nadležnih tijela za sigurnost mrežnih i informacijskih sustava („nadležno tijelo”) koja obuhvaćaju barem sektore iz Priloga II. i usluge iz Priloga III. Države članice mogu tu ulogu dodijeliti postojećem tijelu ili tijelima.

2. Nadležna tijela nadgledaju primjenu ove Direktive na nacionalnoj razini.

3. Svaka država određuje nacionalnu jedinstvenu kontaktnu točku za sigurnost mrežnih i informacijskih sustava („jedinstvena kontaktna točka”). Države članice mogu tu ulogu dodijeliti postojećem tijelu. Ako država članica odredi samo jedno nadležno tijelo, to nadležno tijelo također je i jedinstvena kontaktna točka.

4. Jedinstvena kontaktna točka izvršava funkciju povezivanja s ciljem osiguravanja prekogranične suradnje tijela države članice s relevantnim tijelima u drugim državama članicama te sa skupinom za suradnju iz članka 11. i mrežom CSIRT-ova iz članka 12.

5. Države članice osiguravaju da nadležna tijela i jedinstvene kontaktne točke imaju odgovarajuće resurse za učinkovitu i djelotvornu provedbu zadaća koje su im dodijeljene te da tako ispune ciljeve ove Direktive. Države članice osiguravaju učinkovitu, djelotvornu i sigurnu suradnju imenovanih predstavnika u skupini za suradnju.

6. Nadležna tijela i jedinstvena kontaktna točka, kad god je to prikladno i u skladu s nacionalnim pravom, savjetuju se s relevantnim nacionalnim tijelima za izvršavanje zakonodavstva i nacionalnim tijelima za zaštitu podataka te s njima surađuju.

7. Svaka država članica bez odgode obavješćuje Komisiju o imenovanju nadležnog tijela i jedinstvene kontaktne točke te njihovim zadaćama i svim naknadnim promjenama. Svaka država članica objavljuje imenovanje nadležnog tijela i jedinstvene kontaktne točke. Komisija objavljuje popis određenih jedinstvenih kontaktnih točaka.

Članak 9.

Timovi za odgovor na računalne sigurnosne incidente (CSIRT-ovi)

1. Svaka država članica imenuje jedan ili više CSIRT-ova koji udovoljavaju zahtjevima iz točke 1. Priloga I. i koji obuhvaćaju barem sektore iz Priloga II. i usluge iz Priloga III., odgovornih za rješavanje rizika i incidenata u skladu s točno propisanim postupkom. CSIRT se može osnovati unutar nadležnog tijela.

2. Države članice imenovanim CSIRT-ovima osiguravaju odgovarajuće resurse za učinkovito izvršavanje zadaća iz Priloga I. točke 2.

Države članice osiguravaju učinkovitu, djelotvornu i sigurnu suradnju svojih CSIRT-ova u mreži CSIRT-ova iz članka 12.

3. Države članice osiguravaju da CSIRT-ovi imaju pristup prikladnoj, sigurnoj i otpornoj infrastrukturi za komunikaciju i informiranje na nacionalnoj razini.

4. Države članice obavješćuju Komisiju o mandatu i glavnim elementima postupka za rješavanje incidenata svojih CSIRT-ova.

5. Države članice mogu zatražiti podršku ENISA-e u razvijanju nacionalnih CSIRT-ova.

Članak 10.

Suradnja na nacionalnoj razini

1. Ako su odvojeni, nadležno tijelo, jedinstvena kontaktna točka i CSIRT-ovi iste države članice surađuju u pogledu ispunjavanja obveza propisanih u ovoj Direktivi.

2. Države članice osiguravaju da bilo nadležna tijela ili CSIRT-ovi primaju obavijesti o incidentima podnesene u skladu s ovom Direktivom. Ako država članica odluči da CSIRT-ovi ne primaju obavijesti, CSIRT-ovima se, u onoj mjeri u kojoj je to potrebno za ispunjavanje njihovih zadaća, omogućuje pristup podacima o incidentima o kojima su obavijestili operatori ključnih usluga u skladu s člankom 14. stavcima 3. i 5. ili pružatelji digitalnih usluga, u skladu s člankom 16. stavcima 3. i 6.

3. Države članice osiguravaju da nadležna tijela ili CSIRT-ovi informiraju jedinstvene kontaktne točke o obavijestima o incidentima koje su im dostavljene u skladu s ovom Direktivom.

Do 9. kolovoza 2018., a nakon toga svake godine, jedinstvena kontaktna točka podnosi skupini za suradnju sažeto izvješće o zaprimljenim obavijestima, među ostalim o broju obavijesti i naravi incidenata o kojima ih se obavijestilo te o radnjama poduzetim u skladu s člankom 14. stavcima 3. i 5. te člankom 16. stavcima 3. i 6.

POGLAVLJE III.

SURADNJA

Članak 11.

Skupina za suradnju

1. U svrhu podupiranja i olakšavanja strateške suradnje i razmjene informacija među državama članicama te razvijanja povjerenja i pouzdanja s ciljem postizanja visoke zajedničke razine sigurnosti mrežnih i informacijskih sustava u Uniji, uspostavlja se skupina za suradnju.

Skupina za suradnju izvršava svoje zadaće na temelju dvogodišnjih programa rada iz stavka 3. drugog podstavka.

2. Skupina za suradnju sastoji se od predstavnika država članica, Komisije i ENISA-e.

Skupina za suradnju može, prema potrebi, pozvati predstavnike relevantnih zainteresiranih strana da sudjeluju u njezinu radu.

Komisija osigurava tajništvo.

3. Zadaće su skupine za suradnju:

(a) pružanje strateških smjernica za aktivnosti mreže CSIRT-ova osnovane prema članku 12.;

(b) razmjena najbolje prakse o razmjeni informacija povezanih s obavijestima o incidentima iz članka 14. stavaka 3. i 5. i članka 16. stavaka 3. i 6.;

(c) razmjena najbolje prakse među državama članicama i, u suradnji s ENISA-om, pomaganje državama članicama u izgradnji kapaciteta za sigurnost mrežnih i informacijskih sustava;

(d) rasprava o sposobnostima i pripravnosti država članica te, na dobrovoljnoj osnovi, obavljanje procjene nacionalnih strategija za sigurnost mrežnih i informacijskih sustava i učinkovitosti CSIRT-ova te utvrđivanje najbolje prakse;

(e) razmjena informacija i najbolje prakse u pogledu podizanja svijesti i osposobljavanja;

(f) razmjena informacija i najbolje prakse u pogledu istraživanja i razvoja u vezi sa sigurnošću mrežnih i informacijskih sustava;

(g) prema potrebi, razmjena iskustava o pitanjima povezanima sa sigurnošću mrežnih i informacijskih sustava u relevantnim institucijama, tijelima, uredima i agencijama Unije;

(h) rasprava o normama i specifikacijama iz članka 19. s predstavnicima relevantnih europskih organizacija za normizaciju;

(i) prikupljanje informacija o najboljoj praksi u pogledu rizika i incidenata;

(j) provjera, na godišnjoj osnovi, sažetih izvješća iz članka 10. stavka 3. drugog podstavka;

(k) rasprava o radu obavljenom u pogledu vježbi koje se odnose na sigurnost mrežnih i informacijskih sustava, programa za obrazovanje i osposobljavanja, uključujući rad ENISA-e;

(l) uz pomoć ENISA-e, razmjena najbolje prakse u pogledu identifikacije operatora ključnih usluga od strane država članica, među ostalim u pogledu prekograničnih ovisnosti u odnosu na rizike i incidente;

(m) rasprava o modalitetima za slanje obavijesti o incidentima iz članka 14. i 16.

Do 9. veljače 2018., a nakon toga svake dvije godine, skupina za suradnju sastavlja program rada u pogledu mjera koje treba poduzeti za provedbu svojih ciljeva i zadaća, a koje moraju biti u skladu s ciljevima ove Direktive.

4. Za potrebe preispitivanja iz članka 23. i najkasnije 9. kolovoza 2018., a nakon toga svakih godinu i pol, skupina za suradnju priprema izvješće o procjeni stečenog iskustva u pogledu strateške suradnje iz ovoga članka.

5. Komisija donosi provedbene akte kojima se utvrđuju postupovni aranžmani potrebni za funkcioniranje skupine za suradnju. Ti se provedbeni akti donose u skladu s postupkom ispitivanja iz članka 22. stavka 2.

Za potrebe prvog podstavka Komisija dostavlja prvi nacrt provedbenog akta odboru iz članka 22. stavka 1. do 9. veljače 2017.

Članak 12.

Mreža CSIRT-ova

1. S ciljem doprinosa razvoju povjerenja i pouzdanja među državama članicama te promicanju brze i učinkovite operativne suradnje osniva se mreža nacionalnih CSIRT-ova.

2. Mreža CSIRT-ova sastoji se od predstavnikâ CSIRT-ova iz država članica i iz CERT-EU-a. Komisija u mreži CSIRT-ova sudjeluje kao promatrač. ENISA osigurava tajništvo i aktivno podržava suradnju među CSIRT-ovima.

3. Zadaće su mreže CSIRT-ova:

(a) razmjena informacija o uslugama CSIRT-ova te njihovim aktivnostima i sposobnostima za suradnju;

(b) na zahtjev predstavnika CSIRT-a iz države članice na koju bi incident mogao utjecati, razmjenjivanje informacija koje nisu komercijalno osjetljive naravi, a odnose se na taj incident i s njime povezane rizike, te rasprava o tim informacijama; međutim, CSIRT svake države članice može odbiti davanje doprinosa takvoj raspravi ako postoji rizik da se u pitanje dovede istraga o incidentu;

(c) razmjena i stavljanje na raspolaganje na dobrovoljnoj osnovi informacija o pojedinačnim incidentima koje nisu povjerljive;

(d) na zahtjev predstavnika CSIRT-a države članice, razmatranje, a ako je to moguće, i određivanje koordiniranog odgovora na incident koji je utvrđen u području za koje je nadležna ista ta država članica;

(e) pružanje podrške državama članicama u rješavanju prekograničnih incidenata na temelju dobrovoljne uzajamne pomoći;

(f) rasprava o daljnjim oblicima operativne suradnje te njihovo istraživanje i utvrđivanje, među ostalim u odnosu na:

   i. kategorije rizika i incidenata;

   ii. rana upozorenja;

   iii. uzajamnu pomoć;

   iv. načela i načine koordinacije, kada države članice odgovaraju na prekogranične rizike i incidente;

(g) obavješćivanje skupine za suradnju o svojim aktivnostima i daljnjim oblicima operativne suradnje razmotrenima u skladu s točkom (f) te traženje smjernica u tom pogledu;

(h) rasprava o poukama stečenima u vježbama koje se odnose na sigurnost mrežnih i informacijskih sustava, među ostalim i onima koje organizira ENISA;

(i) na zahtjev pojedinačnog CSIRT-a, rasprava o sposobnostima i pripravnosti tog CSIRT-a;

(j) izdavanje smjernica radi olakšavanja konvergencije operativnih praksi s ciljem primjene odredaba ovoga članka u pogledu operativne suradnje.

4. Za potrebe preispitivanja iz članka 23. i najkasnije 9. kolovoza 2018., a nakon toga svakih godinu i pol, mreža CSIRT-ova priprema izvješće o procjeni stečenog iskustva u pogledu operativne suradnje iz ovoga članka, među ostalim zaključke i preporuke. To se izvješće dostavlja i skupini za suradnju.

5. Mreža CSIRT-ova utvrđuje vlastiti poslovnik.

Članak 13.

Međunarodna suradnja

Unija u skladu s člankom 218. UFEU-a može sklapati međunarodne sporazume s trećim državama ili međunarodnim organizacijama kojima im se dopušta i organizira sudjelovanje u nekim aktivnostima skupine za suradnju. Takvi sporazumi uzimaju u obzir potrebu da se osigura primjerena zaštita podataka.

POGLAVLJE IV.

SIGURNOST MREŽNIH I INFORMACIJSKIH SUSTAVA OPERATORA KLJUČNIH USLUGA

Članak 14.

Sigurnosni zahtjevi i obavješćivanje o incidentima

1. Države članice osiguravaju da operatori ključnih usluga poduzimaju odgovarajuće i razmjerne tehničke i organizacijske mjere za upravljanje rizicima kojima su izloženi mrežni i informacijski sustavi kojima se služe u svojem poslovanju. Uzimajući u obzir najnovija dostignuća tim se mjerama osigurava razina sigurnosti mrežnih i informacijskih sustava primjerena riziku kojem su izložene.

2. Države članice osiguravaju da operatori ključnih usluga poduzimaju odgovarajuće mjere za sprečavanje i svođenje na najmanju moguću mjeru učinaka incidenata koji utječu na sigurnost mrežnih i informacijskih sustava koji se koriste za pružanje takvih ključnih usluga s ciljem osiguravanja kontinuiteta tih usluga.

3. Države članice osiguravaju da operatori ključnih usluga bez neopravdane odgode obavješćuju nadležno tijelo ili CSIRT o incidentima koji imaju znatan učinak na kontinuitet ključnih usluga koje pružaju. Obavijesti sadržavaju informacije nadležnom tijelu ili CSIRT-u omogućuju da odredi sve prekogranične učinke incidenta. Strana koja šalje obavijest ne podliježe zbog toga povećanoj odgovornosti.

4. Kako bi se odredila važnost učinka nekog incidenta, osobito se uzimaju u obzir sljedeći parametri:

(a) broj korisnika pogođenih prekidom osnovnih usluga;

(b) trajanje incidenta;

(c) zemljopisna raširenost u smislu područja na koje bi incident mogao utjecati.

5. Na temelju informacija koje dostavlja operator ključnih usluga u svojem obavješćivanju, nadležno tijelo ili CSIRT obavješćuju drugu pogođenu državu članicu ili više njih ako incident ima znatan učinak na kontinuitet ključnih usluga u toj državi članici. Pritom nadležno tijelo ili CSIRT, u skladu s pravom Unije ili nacionalnim zakonodavstvom u skladu s pravom Unije, čuvaju sigurnost i komercijalne interese operatora ključnih usluga, kao i povjerljivost informacija koje je dostavio u svojem obavješćivanju.

Ako to dopuste okolnosti, nadležno tijelo ili CSIRT dostavljaju operatoru ključnih usluga koji je obavijest poslao relevantne informacije u pogledu daljnjeg postupanja po njegovoj obavijesti, primjerice informacije koje bi mogle doprinijeti djelotvornom rješavanju incidenta.

Na zahtjev nadležnog tijela ili CSIRT-a jedinstvena kontaktna točka obavijesti iz prvog podstavka prosljeđuje jedinstvenim kontaktnim točkama drugih pogođenih država članica.

6. Nakon savjetovanja s operatorom ključnih usluga koji je obavijest poslao, nadležno tijelo ili CSIRT mogu obavijestiti javnost o pojedinačnim incidentima ako je osviještenost javnosti nužna za sprečavanje incidenta ili rješavanje incidenta koji je u tijeku.

7. Nadležna tijela koja djeluju zajedno sa skupinom za suradnju mogu izraditi i donijeti smjernice u pogledu okolnosti u kojima su operatori ključnih usluga dužni obavijestiti o incidentu, među ostalim i o parametrima za određivanje važnosti učinka incidenta iz stavka 4.

Članak 15.

Provedba i izvršavanje

1. Države članice osiguravaju da nadležna tijela imaju potrebne ovlasti i sredstva za procjenu ispunjavaju li operatori ključnih usluga svoje obveze iz članka 14. te učinke toga na sigurnost mrežnih i informacijskih sustava.

2. Države članice osiguravaju da nadležno tijelo ima ovlasti i sredstva da od operatora ključnih uloga zatraži dostavu:

(a) informacija potrebnih za procjenu sigurnosti njihovih mrežnih i informacijskih sustava, među ostalim dokumentirane sigurnosne politike;

(b) dokaza o učinkovitoj provedbi sigurnosnih politika, primjerice rezultata revizije sigurnosti koju su obavili nadležno tijelo ili kvalificirani revizor te, u slučaju da je obavlja kvalificirani revizor, stavljanje tih rezultata, zajedno s dokazima na kojima se temelje, na raspolaganje nadležnom tijelu.

Prilikom traženja takvih informacija ili dokaza nadležno tijelo navodi svrhu zahtjeva i određuje koje su informacije potrebne.

3. Nakon procjene informacija ili rezultata revizije sigurnosti iz stavka 2., nadležno tijelo može izdavati obvezujuće upute operatorima ključnih usluga s ciljem ispravljanja utvrđenih nedostataka.

4. Nadležna tijela blisko surađuju s tijelima za zaštitu podataka u rješavanju incidenata koji za posljedicu imaju ugrožavanja osobnih podataka.

POGLAVLJE V.

SIGURNOST MREŽNIH I INFORMACIJSKIH SUSTAVA PRUŽATELJA DIGITALNIH USLUGA

Članak 16.

Sigurnosni zahtjevi i obavješćivanje o incidentima

1. Države članice osiguravaju da pružatelji digitalnih usluga poduzimaju odgovarajuće i razmjerne tehničke i organizacijske mjere za upravljanje rizicima kojima su izloženi mrežni i informacijski sustavi kojima se u Uniji služe u okviru pružanja usluga iz Priloga III. Uzimajući u obzir najnovija dostignuća tim se mjerama osigurava razina sigurnosti mrežnih i informacijskih sustava primjerena riziku kojem su izloženi te uz vođenje računa o sljedećim elementima:

(a) sigurnosti sustava i objekata;

(b) rješavanju incidenata;

(c) upravljanju kontinuitetom poslovanja;

(d) praćenju, reviziji i testiranju;

(e) sukladnosti s međunarodnim standardima.

2. Države članice osiguravaju da pružatelji digitalnih usluga poduzimaju mjere za sprečavanje i svođenje na najmanju moguću mjeru učinaka incidenata koji utječu na sigurnost njihovih mrežnih i informacijskih sustava na usluge iz Priloga III. koje se pružaju u Uniji, s ciljem osiguravanja kontinuiteta tih usluga.

3. Države članice osiguravaju da pružatelji digitalnih usluga bez nepotrebne odgode obavijeste nadležno tijelo ili CSIRT o svakom incidentu koji ima znatan učinak na pružanje neke od usluga iz Priloga III. koju oni nude unutar Unije. Obavijesti sadržavaju informacije s pomoću kojih nadležno tijelo ili CSIRT mogu odrediti važnost svakog prekograničnog učinka. Strana koja šalje obavijest ne podliježe zbog toga povećanoj odgovornosti.

4. Radi utvrđivanja je li učinak incidenta znatan, u obzir se osobito uzimaju sljedeći parametri:

(a) broj korisnika na koje incident utječe, osobito ako je riječ o korisnicima koji se na te usluge oslanjaju za pružanje vlastitih usluga;

(b) trajanje incidenta;

(c) zemljopisna raširenost u smislu područja na koje bi incident mogao utjecati;

(d) opseg poremećaja u funkcioniranju usluge;

(e) opseg utjecaja na gospodarsko i društveno djelovanje.

Obveza obavješćivanja o incidentu primjenjuje se samo ako pružatelj digitalnih usluga ima pristup informacijama potrebnima za procjenu učinka incidenta spram kriterija iz prvog podstavka.

5. Ako se operator ključnih usluga oslanja na trećeg pružatelja digitalnih usluga za pružanje usluge koja je neophodna za održavanje ključnih društvenih i gospodarskih aktivnosti, taj operator ključnih usluga obavijestit će o svakom znatnom učinku na kontinuitet ključnih usluga koji je prouzročen incidentom koji utječe na tog pružatelja digitalnih usluga.

6. Nadležno tijelo ili CSIRT prema potrebi obavješćuju ostale pogođene države članice, a osobito ako se incident iz stavka 3. odnosi na dvije ili više država članica. Pritom nadležna tijela, CSIRT-ovi i jedinstvene kontaktne točke, u skladu s pravom Unije ili nacionalnim zakonodavstvom u skladu s pravom Unije, čuvaju sigurnost i komercijalne interese pružatelja digitalnih usluga te povjerljivost dostavljenih informacija.

7. Nakon savjetovanja s dotičnim pružateljem digitalnih usluga, nadležno tijelo ili CSIRT te, prema potrebi, tijela ili CSIRT-ovi drugih pogođenih država članica, mogu javnost obavijestiti o pojedinačnim incidentima ili zatražiti od pružatelja digitalnih usluga da to učini ako je javnost potrebno obavijestiti s ciljem sprečavanja incidenta ili rješavanja incidenta koji je u tijeku ili ako je objavljivanje incidenta zbog nekog drugog razloga u javnome interesu.

8. Komisija donosi provedbene akte radi dodatnog utvrđivanja elemenata iz stavka 1. te parametara navedenih u stavku 4. ovog članka. Ti se provedbeni akti donose do 9. kolovoza 2017. u skladu s postupkom ispitivanja iz članka 22. stavka 2.

9. Komisija može donijeti provedbene akte kojima se utvrđuju oblici i postupci primjenljivi na zahtjeve za obavješćivanje. Ti se provedbeni akti donose u skladu s postupkom ispitivanja iz članka 22. stavka 2.

10. Ne dovodeći u pitanje članak 1. stavak 6., države članice ne nameću nikakve dodatne sigurnosne zahtjeve ni zahtjeve za obavješćivanje pružateljima digitalnih usluga.

11. Poglavlje V. ne primjenjuje se na mikropoduzeća i mala poduzeća kako su definirana u Preporuci Komisije 2003/361/EZ ([1]).

([1]) Preporuka Komisije 2003/361/EZ od 6. svibnja 2003. o definiciji mikropoduzeća te malih i srednjih poduzeća (SL L 124, 20.5.2003., str. 36.).

Članak 17.

Provedba i izvršavanje

1. Države članice osiguravaju da nadležna tijela, ako je potrebno, poduzmu *ex post* nadzorne mjere kada dobiju dokaze da pružatelj digitalnih usluga ne ispunjava zahtjeve utvrđene u članku 16. Takve dokaze može dostaviti nadležno tijelo druge države članice u kojoj se pruža usluga.

2. Za potrebe stavka 1. nadležna tijela imaju potrebne ovlasti i sredstva da mogu od pružatelja digitalnih usluga tražiti:

(a) dostavu informacija potrebnih za procjenu sigurnosti njihovih mrežnih i informacijskih sustava, među ostalim dokumentirane sigurnosne politike;

(b) otklanjanje svakog nepoštovanja zahtjeva utvrđenih u članku 16.

3. Ako pružatelj digitalnih usluga ima glavni poslovni nastan ili predstavnika u jednoj državi članici, ali se njegovi mrežni i informacijski sustavi nalaze u jednoj ili više država članica, nadležno tijelo države članice u kojoj se nalazi njegov glavni poslovni nastan ili predstavnik te nadležna tijela tih drugih država članica surađuju i međusobno si pomažu prema potrebi. Takva pomoć i suradnja mogu obuhvaćati razmjenu informacija između dotičnih nadležnih tijela i zahtjeve za poduzimanjem nadzornih mjera iz stavka 2.

Članak 18.

Nadležnost i teritorijalnost

1. Za potrebe ove Direktive smatra se da pružatelj digitalnih usluga pripada nadležnosti države članice u kojoj ima glavni poslovni nastan. Smatra se da pružatelj digitalnih usluga ima glavni poslovni nastan u onoj državi članici u kojoj ima sjedište.

2. Pružatelj digitalnih usluga koji nema nastan u Uniji, ali nudi usluge u Uniji kako je navedeno u Prilogu III., imenuje svojeg predstavnika u Uniji. Predstavnik ima sjedište u jednoj od država članica u kojima pružatelj nudi svoje usluge. Smatra se da pružatelj digitalnih usluga pripada nadležnosti one države članice u kojoj njegov predstavnik ima poslovni nastan.

3. Imenovanje predstavnika od strane pružatelja digitalnih usluga ne dovodi u pitanje pravne postupke koji bi se mogli pokrenuti protiv samog pružatelja digitalnih usluga.

POGLAVLJE VI.

NORMIZACIJA I OBAVJEŠĆIVANJE NA DOBROVOLJNOJ OSNOVI

Članak 19.

Normizacija

1. Države članice, s ciljem promicanja konvergentne provedbe članka 14. stavaka 1. i 2. te članka 16. stavaka 1. i 2., bez nametanja ili diskriminacije određene vrste tehnologije, potiču primjenu europskih ili međunarodno priznatih normi i specifikacija relevantnih za sigurnost mrežnih i informacijskih sustava.

2. ENISA u suradnji s državama članicama izrađuje savjete i smjernice u pogledu tehničkih područja koja treba razmotriti u odnosu na stavak 1. te u odnosu na postojeće norme, uključujući nacionalne norme država članica, kojima bi se ta područja mogla obuhvatiti.

Članak 20.

Obavješćivanje na dobrovoljnoj osnovi

1. Ne dovodeći u pitanje članak 3. subjekti koji nisu identificirani kao operatori ključnih usluga i nisu pružatelji digitalnih usluga obavješćuju na dobrovoljnoj osnovi o incidentima koji imaju znatan učinak na kontinuitet usluga koje pružaju.

2. Pri obradi obavijesti države članice djeluju u skladu s postupkom utvrđenim u članku 14. Države članice obradi obveznih obavijesti mogu dati prednost pred obradom obavijesti na dobrovoljnoj osnovi. Obavijesti na dobrovoljnoj osnovi obrađuju se samo ako takva obrada ne predstavlja nerazmjerno ili nepotrebno opterećenje za države članice o kojima je riječ.

Subjektu koji je obavijest podnio dobrovoljno ne nameću se zbog tog obavješćivanja nikakve obveze kojima ne bi podlijegao da nije podnio tu obavijest.

POGLAVLJE VII.

ZAVRŠNE ODREDBE

Članak 21.

Sankcije

Države članice utvrđuju pravila o sankcijama koje se primjenjuju na kršenja nacionalnih odredaba donesenih na temelju ove Direktive i poduzimaju sve potrebne mjere radi osiguranja njihove provedbe. Predviđene sankcije moraju biti učinkovite, proporcionalne i odvraćajuće. Države članice do 9. svibnja 2018. obavješćuju Komisiju o tim pravilima i mjerama te je bez odgode obavješćuju o svim naknadnim izmjenama koje na njih utječu.

Članak 22.

Postupak odbora

1. Komisiji pomaže Odbor za sigurnost mrežnih i informacijskih sustava. Navedeni odbor je odbor u smislu Uredbe (EU) br. 182/2011.

2. Pri upućivanju na ovaj stavak primjenjuje se članak 5. Uredbe (EU) br. 182/2011.

Članak 23.

Preispitivanje

1. Do 9. svibnja 2019. Komisija podnosi Europskom parlamentu i Vijeću izvješće s procjenom dosljednosti u pristupu država članica pri identifikaciji operatora ključnih usluga.

2. Komisija periodično preispituje funkcioniranje ove Direktive te podnosi izvješće Europskom parlamentu i Vijeću. U tu svrhu te s ciljem daljnjeg unapređivanja strateške i operativne suradnje Komisija uzima u obzir izvješća skupine za suradnju i mreže CSIRT-ova o iskustvu stečenom na strateškoj i operativnoj razini. Pri preispitivanju Komisija također procjenjuje popise iz priloga II. i III. te dosljednost u identifikaciji operatora ključnih usluga i usluga u sektorima iz Priloga II. Prvo se izvješće dostavlja do 9. svibnja 2021.

Članak 24.

Prijelazne mjere

1. Ne dovodeći u pitanje članak 25. te s ciljem da se državama članicama pruže dodatne mogućnosti za odgovarajuću suradnju tijekom razdoblja za prenošenje, skupina za suradnju i mreža CSIRT-ova počinju obavljati svoje zadaće utvrđene u članku 11. stavku 3. odnosno članku 12. stavku 3. najkasnije do 9. veljače 2017.

2. U razdoblju od 9. veljače 2017. do 9. studenoga 2018., a u svrhu podupiranja država članica u zauzimanju dosljednog pristupa u pogledu postupka identifikacije operatora ključnih usluga, skupina za suradnju raspravlja o postupku te sadržaju i vrsti nacionalnih mjera za omogućivanje identifikacije operatora ključnih usluga unutar određenog sektora u skladu s kriterijima određenim u člancima 5. i 6. Skupina za suradnju, na zahtjev države članice, raspravlja i o konkretnim nacrtima nacionalnih mjera te države članice za omogućivanje identifikacije operatora ključnih usluga u određenom sektoru u skladu s kriterijima određenima u člancima 5. i 6.

3. Do 9. veljače 2017., a za potrebe ovog članka države članice osiguravaju odgovarajuću zastupljenost u skupini za suradnju i mreži CSIRT-ova.

Članak 25.

Prenošenje

1. Države članice do 9. svibnja 2018. donose i objavljuju zakone i druge propise koji su potrebni radi usklađivanja s ovom Direktivom. One o tome odmah obavješćuju Komisiju.

One primjenjuju te mjere od 10. svibnja 2018.

Kada države članice donose te mjere, one sadržavaju upućivanje na ovu Direktivu ili se na nju upućuje prilikom njihove službene objave. Načine tog upućivanja određuju države članice.

2. Države članice Komisiji dostavljaju tekst glavnih odredaba nacionalnog prava koje donesu u području na koje se odnosi ova Direktiva.

Članak 26.

Stupanje na snagu

Ova Direktiva stupa na snagu dvadesetog dana od dana objave u *Službenom listu Europske unije*.

Članak 27.

Adresati

Ova je Direktiva upućena državama članicama.

Sastavljeno u Strasbourgu 6. srpnja 2016.

Za Europski parlament	*Za Vijeće*
Predsjednik	*Predsjednik*
M. SCHULZ	I. KORČOK

PRILOG I.

ZAHTJEVI U POGLEDU TIMOVA ZA ODGOVOR NA RAČUNALNE SIGURNOSNE INCIDENTE (CSIRT-ovi) I NJIHOVE ZADAĆE

Zahtjevi u pogledu CSIRT-ova i njihove zadaće propisno su i jasno definirani i poduprti nacionalnom politikom i/ili zakonodavstvom. Oni obuhvaćaju sljedeće:

1. Zahtjevi u pogledu CSIRT-ova:

   (a) CSIRT-ovi osiguravaju visoku razinu dostupnosti svojih usluga komuniciranja izbjegavanjem jedinstvenih točki prekida te u svakom trenutku raspolažu s nekoliko sredstava za mogućnost dvosmjernog kontaktiranja. Nadalje, komunikacijski kanali jasno su određeni i dobro poznati klijentima i suradnicima.

   (b) Prostori CSIRT-ova i informacijski sustavi za potporu smješteni su na sigurnim lokacijama.

   (c) Kontinuitet rada:

      i. CSIRT-ovi su opremljeni odgovarajućim sustavom za upravljanje zahtjevima i njihovim preusmjeravanjem, kako bi se olakšale primopredaje.

      ii. CSIRT-ovi imaju dovoljno zaposlenika kako bi se osigurala dostupnost u svako doba.

      iii. CSIRT-ovi se oslanjaju na infrastrukturu čiji je kontinuitet osiguran. U tu svrhu dostupni su redundantni sustavi i rezervni radni prostor.

   (d) CSIRT-ovi imaju mogućnost da, ako to žele, sudjeluju u međunarodnim mrežama za suradnju.

2. Zadaće CSIRT-ova:

   (a) Zadaće CSIRT-ova obuhvaćaju barem:

      i. praćenje incidenata na nacionalnoj razini;

      ii. pružanje ranih upozorenja i najava te informiranje relevantnih dionika o rizicima i incidentima;

      iii. odgovaranje na incidente;

      iv. pružanje dinamičke analize rizika i incidenata te pregleda situacije;

      v. sudjelovanje u mreži CSIRT-ova.

   (b) CSIRT-ovi uspostavljaju suradnju s privatnim sektorom.

   (c) CSIRT-ovi s ciljem olakšavanja suradnje promiču usvajanje i primjenu zajedničkih ili normiranih praksi za:

      i. postupke rješavanja incidenata i rizika;

      ii. planove za klasifikaciju incidenata, rizika i informacija.

PRILOG II.

VRSTE SUBJEKATA ZA POTREBE ČLANKA 4. TOČKE 4.

Sektor	Podsektor	Vrsta subjekta
1. Energetika	(a) električna energija	— elektroenergetsko poduzeće kako je definirano u članku 2. točki 35. Direktive 2009/72/EZ Europskog parlamenta i Vijeća ([1]), koje obavlja funkciju „opskrbe" kako je definirana u članku 2. točki 19. te Direktive
		— operatori distribucijskog sustava kako su definirani u članku 2. točki 6. Direktive 2009/72/EZ
		— operatori prijenosnog sustava kako su definirani u članku 2. točki 4. Direktive 2009/72/EZ
	(b) nafta	— operatori naftovoda
		— operatori proizvodnje nafte, rafinerija i tvornicâ nafte te njezina skladištenja i prijenosa
	(c) plin	— poduzeća za opskrbu kako su definirana člankom 2. točkom 8. Direktive 2009/73/EZ Europskog parlamenta i Vijeća ([2])
		— operatori distribucijskog sustava kako su definirani u članku 2. točki 6. Direktive 2009/73/EZ
		— operatori transportnog sustava kako su definirani u članku 2. točki 4. Direktive 2009/73/EZ
		— operatori sustava skladišta plina kako su definirani u članku 2. točki 10. Direktive 2009/73/EZ
		— operatori terminala za UPP kako su definirani u članku 2. točki 12. Direktive 2009/73/EZ
		— poduzeća za prirodni plin kako su definirana u članku 2. točki 1. Direktive 2009/73/EZ
		— operatori postrojenja za rafiniranje i obradu prirodnog plina
2. Prijevoz	(a) zračni promet	— zračni prijevoznici kako su definirani u članku 3. točki 4. Uredbe (EZ) br. 300/2008 Europskog parlamenta i Vijeća ([3])
		— upravno tijelo zračne luke kako je definirano u članku 2. točki 2. Direktive 2009/12/EZ Europskog parlamenta i Vijeća ([4]), zračna luka kako je definirana u članku 2. točki 1. te Direktive, među ostalim i glavne zračne luke s popisa u 2. odjeljku Priloga II. Uredbi (EU) br. 1315/2013 Europskog parlamenta i Vijeća ([5]) te tijela koja upravljaju pomoćnim objektima u zračnim lukama

Sektor	Podsektor	Vrsta subjekta
		— operatori kontrole upravljanja prometom koji pružaju usluge kontrole zračnog prometa (ATC) kako su definirane u članku 2. točki 1. Uredbe (EZ) br. 549/2004 Europskog parlamenta i Vijeća ([6])
	(b) željeznički prijevoz	— upravitelji infrastrukture kako su definirani u članku 3. točki 2. Direktive 2012/34/EU Europskog parlamenta i Vijeća ([7])
		— željeznički prijevoznici kako su definirani u članku 3. točki 1. Direktive 2012/34/EU, među ostalim i operatori uslužnih objekata kako su definirani u članku 3. točki 12. Direktive 2012/34/EU
	(c) vodni prijevoz	— kompanije za prijevoz putnika unutarnjim plovnim putovima, morem i duž obale te kompanije za prijevoz tereta unutarnjim plovnim putovima, morem i duž obale kako su definirane u Prilogu I. Uredbi (EZ) br. 725/2004 Europskog parlamenta i Vijeća ([8]), ne uključujući pojedinačna plovila kojima upravljaju te kopmanije
		— upravljačka tijela luka kako su definirana u članku 3. točki 1. Direktive 2005/65/EZ Europskog parlamenta i Vijeća ([9]), uključujući njihove luke kako su definirane u članku 2. točki 11. Uredbe (EZ) br. 725/2004 te subjekti koji upravljaju postrojenjima i opremom u lukama
		— služba za nadzor i upravljanje pomorskim prometom kako je definirana u članku 3. točki (o) Direktive 2002/59/EZ Europskog parlamenta i Vijeća ([10])
	(d) cestovni prijevoz	— tijela nadležna za ceste kako su definirana u članku 2. točki 12. Delegirane uredbe Komisije (EU) 2015/962 ([11]) odgovorna za upravljanje prometom
		— operatori inteligentnih prometnih sustava kako su definirani u članku 4. točki 1. Direktive 2010/40/EU Europskog parlamenta i Vijeća ([12])
3. Bankarstvo		kreditne institucije kako su definirane člankom 4. točkom 1. Uredbe (EU) br. 575/2013 Europskog parlamenta i Vijeća ([13])
4. Infrastrukture financijskog tržišta		— operatori mjestâ trgovanja kako su definirana u članku 4. točki 24. Direktive 2014/65/EU Europskog parlamenta i Vijeća ([14])
		— središnje druge ugovorne strane (CCP) kako su definirane u članku 2. točki 1. Uredbe (EU) br. 648/2012 Europskog parlamenta i Vijeća ([15])
5. Zdravstveni sektor	uređenje zdravstvene zaštite (uključujući bolnice i privatne klinike)	pružatelji zdravstvene zaštite kako su definirani u članku 3. točki (g) Direktive 2011/24/EU Europskog parlamenta i Vijeća ([16])

Sektor	Podsektor	Vrsta subjekta
6. Opskrba vodom za piće i njezina distribucija		dobavljači i distributeri vode namijenjene za ljudsku potrošnju kako je definirana u članku 2. stavku 1. točki (a) Direktive Vijeća 98/83/EZ ([17]), ali isključujući distributere kojima distribucija vode za ljudsku potrošnju čini samo dio njihove općenite aktivnosti distribucije druge robe i proizvoda koji se ne smatraju ključnim uslugama
7. Digitalna infrastruktura		— IXP-ovi
		— pružatelj DNS usluga
		— registri naziva TLD-ova

([1]) Direktiva 2009/72/EZ Europskog parlamenta i Vijeća od 13. srpnja 2009. o zajedničkim pravilima za unutarnje tržište električne energije i stavljanju izvan snage Direktive 2003/54/EZ (SL L 211, 14.8.2009., str. 55.).
([2]) Direktiva 2009/73/EZ Europskog parlamenta i Vijeća od 13. srpnja 2009. o zajedničkim pravilima za unutarnje tržište prirodnog plina i stavljanju izvan snage Direktive 2003/55/EZ (SL L 211, 14.8.2009., str. 94.).
([3]) Uredba (EZ) br. 300/2008 Europskog parlamenta i Vijeća od 11. ožujka 2008. o zajedničkim pravilima u području zaštite civilnog zračnog prometa i stavljanju izvan snage Uredbe (EZ) br. 2320/2002 (SL L 97, 9.4.2008., str. 72.).
([4]) Direktiva 2009/12/EZ Europskog parlamenta i Vijeća od 11. ožujka 2009. o naknadama zračnih luka (SL L 70, 14.3.2009., str. 11.).
([5]) Uredba (EU) br. 1315/2013 Europskog parlamenta i Vijeća od 11. prosinca 2013. o smjernicama Unije za razvoj transeuropske prometne mreže i stavljanju izvan snage Odluke br. 661/2010/EU (SL L 348, 20.12.2013., str. 1.).
([6]) Uredba (EZ) br. 549/2004 Europskog parlamenta i Vijeća od 10. ožujka 2004. o utvrđivanju okvira za stvaranje jedinstvenog europskog neba (Okvirna uredba) (SL L 96, 31.3.2004., str. 1.).
([7]) Direktiva 2012/34/EU Europskog parlamenta i Vijeća od 21. studenoga 2012. o uspostavi jedinstvenog Europskog željezničkog prostora (SL L 343, 14.12.2012., str. 32.).
([8]) Uredba (EZ) br. 725/2004 Europskog parlamenta i Vijeća od 31. ožujka 2004. o jačanju sigurnosne zaštite brodova i luka (SL L 129, 29.4.2004., str. 6.).
([9]) Direktiva 2005/65/EZ Europskog parlamenta i Vijeća od 26. listopada 2005. o jačanju sigurnosne zaštite luka (SL L 310, 25.11.2005, str. 28.).
([10]) Direktiva 2002/59/EZ Europskog parlamenta i Vijeća od 27. lipnja 2002. o uspostavi sustava nadzora plovidbe i informacijskog sustava Zajednice i stavljanju izvan snage Direktive Vijeća 93/75/EEZ (SL L 208, 5.8.2002., str. 10.).
([11]) Delegirana uredba Komisije (EU) 2015/962 od 18. prosinca 2014. o dopuni Direktive 2010/40/EU Europskog parlamenta i Vijeća u pogledu pružanja usluga prometnih informacija u cijeloj Europskoj uniji u realnom vremenu (SL L 157, 23.6.2015., str. 21.).
([12]) Direktiva 2010/40/EU Europskog parlamenta i Vijeća od 7. srpnja 2010. o okviru za uvođenje inteligentnih prometnih sustava u cestovnom prometu i za veze s ostalim vrstama prijevoza (SL L 207, 6.8.2010, str. 1.).
([13]) Uredba (EU) br. 575/2013 Europskog parlamenta i Vijeća od 26. lipnja 2013. o bonitetnim zahtjevima za kreditne institucije i investicijska društva i o izmjeni Uredbe (EU) br. 648/2012 (SL L 176, 27.6.2013., str. 1.).
([14]) Direktiva 2014/65/EU Europskog parlamenta i Vijeća od 15. svibnja 2014. o tržištu financijskih instrumenata i izmjeni Direktive 2002/92/EZ i Direktive 2011/61/EU (SL L 173, 12.6.2014., str. 349.).
([15]) Uredba (EU) br. 648/2012 Europskog parlamenta i Vijeća od 4. srpnja 2012. o OTC izvedenicama, središnjoj drugoj ugovornoj strani i trgovinskom repozitoriju (SL L 201, 27.7.2012., str. 1.).
([16]) Direktiva 2011/24/EU Europskog parlamenta i Vijeća od 9. ožujka 2011. o primjeni prava pacijenata u prekograničnoj zdravstvenoj skrbi (SL L 88, 4.4.2011., str. 45.).
([17]) Direktiva Vijeća 98/83/EZ od 3. studenoga 1998. o kvaliteti vode namijenjene za ljudsku potrošnju (SL L 330, 5.12.1998., str. 32.).

PRILOG III.

VRSTE DIGITALNIH USLUGA ZA POTREBE ČLANKA 4. TOČKE 5.

1. Internetsko tržište
2. Internetska tražilica
3. Usluge računalstva u oblaku

ISSN 1977-0847 (elektroničko izdanje)
ISSN 1977-0596 (tiskano izdanje)

Ured za publikacije Europske unije
2985 Luxembourg
LUKSEMBURG

HR