



EIROPAS PARLAMENTS

2009 - 2014

Sesijas dokuments

A7-0224/2013

18.6.2013

*****I**

ZIŅOJUMS

par priekšlikumu Eiropas Parlamenta un Padomes direktīvai par uzbrukumiem informācijas sistēmām un par Padomes Pamatlēmuma 2005/222/TI atcelšanu (COM(2010)0517 – C7-0293/2010 – 2010/0273(COD))

Pilsoņu brīvību, tieslietu un iekšlietu komiteja

Referente: *Monika Hohlmeier*

Izmantoto apzīmējumu skaidrojums

- * Apspriežu procedūra
- *** Piekrišanas procedūra
- ***I Parastā likumdošanas procedūra (pirmais lasījums)
- ***II Parastā likumdošanas procedūra (otrais lasījums)
- ***III Parastā likumdošanas procedūra (trešais lasījums)

(Norādītā procedūra pamatojas uz akta projektā ierosināto juridisko pamatu.)

Grozījumi akta projektā

Izmaiņas, kas ar Parlamenta grozījumiem izdarītas akta projektā, ir iezīmētas ***treknā slīprakstā***. Teksts, kas iezīmēts *parastā slīprakstā*, tehniskajiem dienestiem norāda tās akta projekta daļas, kurās ierosināti labojumi, lai sagatavotu galīgo teksta redakciju (piemēram, nepārprotami kļūdainas teksta daļas vai to izlaidumi kādā no valodām). Šos ierosinātos labojumus apstiprina attiecīgie tehniskie dienesti.

Informācijas bloka, ko ievieto pirms katra grozījuma attiecībā uz spēkā esošu aktu, kuru plānots grozīt ar attiecīgo akta projektu, trešajā un ceturtajā rindā attiecīgi norāda spēkā esošo aktu un tā atbilstīgo teksta vienību. Daļas, kas tiek pārņemtas no tādas spēkā esoša akta teksta vienības, kura netiek grozīta ar attiecīgo akta projektu, bet kuru Parlaments nodomājis grozīt, iezīmē ***treknrakstā***. Iespējamos šādu teksta daļu svītrojumus apzīmē šādi: [...].

SATURA RĀDĪTĀJS

	Lpp.
EIROPAS PARLAMENTA NORMATĪVĀS REZOLŪCIJAS PROJEKTS	5
ĀRLIETU KOMITEJAS SATZINUMS.....	39
RŪPNIECĪBAS, PĒTNIECĪBAS UN ENERĢĒTIKAS KOMITEJAS ATZINUMS	50
PROCEDŪRA.....	66

EIROPAS PARLAMENTA NORMATĪVĀS REZOLŪCIJAS PROJEKTS

par priekšlikumu Eiropas Parlamenta un Padomes direktīvai par uzbrukumiem informācijas sistēmām un par Padomes Pamatlēmuma 2005/222/TI atcelšanu (COM(2010)0517 – C7-0293/2010 – 2010/0273(COD))

(Parastā likumdošanas procedūra: pirmais lasījums)

Eiropas Parlaments,

- ņemot vērā Komisijas priekšlikumu Eiropas Parlamentam un Padomei (COM(2010)0517),
 - ņemot vērā Līguma par Eiropas Savienības darbību 294. panta 2. punktu un 83. panta 1. punktu, saskaņā ar kuriem Komisija tam ir iesniegusi priekšlikumu (C7-0293/2010),
 - ņemot vērā Līguma par Eiropas Savienības darbību 294. panta 3. punktu,
 - ņemot vērā Eiropas Ekonomikas un sociālo lietu komitejas 2011. gada 4. maija atzinumu¹,
 - ņemot vērā ... vēstulē Padomes pārstāvja pausto apņemšanos apstiprināt Eiropas Parlamenta nostāju saskaņā ar Līguma par Eiropas Savienības darbību 294. panta 4. punktu,
 - ņemot vērā Reglamenta 55. pantu,
 - ņemot vērā Pilsoņu brīvību, tieslietu un iekšlietu komitejas ziņojumu un Ārlietu komitejas un Rūpniecības, pētniecības un enerģētikas komitejas atzinumus (A7-0224/2013),
1. pieņem pirmajā lasījumā turpmāk izklāstīto nostāju;
 2. prasa Komisijai priekšlikumu iesniegt vēlreiz, ja tā ir paredzējusi šo priekšlikumu būtiski grozīt vai aizstāt ar citu tekstu;
 3. uzdod priekšsēdētājam nosūtīt Parlamenta nostāju Padomei un Komisijai, kā arī dalībvalstu parlamentiem.

¹ OV C 218, 23.7.2011., 130. lpp.

Grozījums Nr. 129

Direktīvas priekšlikums

-

EIROPAS PARLAMENTA GROZĪJUMI*

Komisijas priekšlikumā

EIROPAS PARLAMENTA UN PADOMES DIREKTĪVA

**par uzbrukumiem informācijas sistēmām un par Padomes Pamatlēmuma 2005/222/TI
aizstāšanu**

EIROPAS PARLAMENTS UN EIROPAS SAVIENĪBAS PADOME,

ņemot vērā Līgumu par Eiropas Savienības darbību un jo īpaši tā 83. panta 1. punktu,

ņemot vērā Eiropas Komisijas priekšlikumu ¹,

pēc leģislatīvā akta projekta nosūtīšanas valstu parlamentiem,

ņemot vērā Eiropas Ekonomikas un sociālo lietu komitejas atzinumu ²,

ņemot vērā Reģionu komitejas atzinumu,

saskaņā ar parasto likumdošanas procedūru,

* Grozījumi: jaunais vai grozītais teksts ir norādīts treknā slīprakstā; svītrojumus apzīmē ar simbolu ■ .

¹ OV C [...], [...], [...]. lpp.

² OVC [...], [...], [...]. lpp.

tā kā:

- (1) Šīs direktīvas mērķis ir tuvināt dalībvalstu *krimināltiesību noteikumus* par uzbrukumiem informācijas sistēmām, *ieviešot minimuma noteikumus attiecībā uz noziedzīgu nodarījumu definēšanu un sankcijām šajā jomā, un* uzlabot sadarbību starp kompetentajām iestādēm, tostarp dalībvalstu policijas un citiem specializētiem tiesībsardzības dienestiem, *kā arī kompetentajām specializētajām Savienības aģentūrām, piemēram, Eurojust, Eiropolu un tā Eiropas kibernetiskās drošības centru un Eiropas Tīklu un informācijas drošības aģentūru (ENISA).*
- (1.a) *Informācijas sistēmas ir būtisks elements Savienības politiskajā, sociālajā un ekonomiskajā mijiedarbībā. Sabiedrība ir ļoti atkarīga no šīm sistēmām, un šī atkarība arvien palielinās. Šo sistēmu netraucēta darbība un drošība Savienībā ir vitāli svarīga iekšējā tirgus un konkurētspējīgas un inovatīvas ekonomikas attīstībai. Informācijas sistēmu pienācīga līmeņa aizsardzības nodrošināšanai būtu jāklūst par daļu no iedarbīgas kompleksas preventīvu pasākumu sistēmas, ar kuriem papildina krimināltiesisku atbildes rīcību uz kibernetiskajiem uzbrukumiem.*

- (2) Uzbrukumi informācijas sistēmām, jo īpaši **uzbrukumi saistībā** ar organizētu noziedzību, kļūst arvien draudīgāki **gan ES, gan pasaules mērogā**, un pieaug bažas par iespējamām teroristiskiem vai politiski motivētiem uzbrukumiem informācijas sistēmām, kas ir dalībvalstu un Savienības kritiskās infrastruktūras sastāvdaļa. Tas apdraud drošākas informācijas sabiedrības un brīvības, drošības un tiesiskuma telpas izveidi, un tāpēc ir jārīkojas Eiropas Savienības līmenī **un jāuzlabo sadarbība un koordinācija starptautiskā līmenī**.
- (2.a) *Savienībā atrodas būtisks skaits kritisko infrastruktūru, kuru sagraušanai vai iznīcināšanai būtu nopietna pārrobežu ietekme. Tā kā Savienībā ir jāpalielina kritiskās infrastruktūras aizsardzības spējas, pasākumi pret kibernetiskiem uzbrukumiem būtu jāpapildina ar nopietniem kriminālsodiem, kas būtu atbilstīgi uzbrukumu smagumam. Kritiskās infrastruktūras var saprast kā objektus, sistēmas vai to daļas, kas ir izvietoti dalībvalstīs un kas ir būtiski, piemēram, svarīgu sabiedrības funkciju uzturēšanai, cilvēku veselības, drošuma, drošības, saimnieciskās vai sociālās labklājības nodrošināšanai – tādi kā spēkstacijas, transporta tīkli vai valdības tīkli –, un kuru darbības pārtraukšana vai kuru iznīcināšana nopietni ietekmētu attiecīgo dalībvalsti, jo būtu traucēta turpmāka šo funkciju izpilde.*

- (3) Ir vērojama tendence, ka plaša mēroga uzbrukumi informācijas sistēmām, kas **bieži var būt** īpaši kritiski svarīgas valstīm vai atsevišķām publiskā vai privātā sektora funkcijām, kļūst aizvien bīstamāki un atkārtojas aizvien biežāk. Līdztekus šai tendencei ir konstatējama arvien sarežģītāku **metožu attīstība, piemēram, tā saukto "robottīklu" ("botnets") izveide un izmantošana, kurā noziedzīgajam nodarījumam ir vairāki posmi un katrs posms atsevišķi var būtiski apdraudēt sabiedrības intereses. Šajā ziņā direktīvā inter alia ir paredzēts ieviest kriminālsankcijas par posmu, kurā "robottīkls" tiek izveidots, proti, kad tiek iegūta ievērojama datoru skaita tāl vadības iespēja, ar mērķtiecīgiem kiberuzbrukumiem inficējot tos ar ļaunprātīgu programmatūru. Vēlākā posmā inficēto datoru tīklu, kas veido "robottīklu", var aktivizēt bez attiecīgo datoru lietotāju ziņas, lai veiktu plaša mēroga kiberuzbrukumu, kurš parasti ir pietiekami spēcīgs, lai radītu nopietnu kaitējumu, kā minēts šajā direktīvā. Dalībvalstis var noteikt, kas ir nopietns kaitējums, saskaņā ar saviem valsts tiesību aktiem un praksi, un tas var ietvert traucējumus sabiedrībai ļoti svarīgos sistēmas pakalpojumos vai lielas finansiālas izmaksas, vai personas datu vai sensitīvas informācijas zaudēšanu.**

- (3.a) *Plaša mēroga uzbrukumi var izraisīt ievērojamu ekonomisku kaitējumu gan informācijas sistēmu darbības un sakaru pārtraukumu, gan komerciāli svarīgas konfidenciālas informācijas vai citu datu zaudēšanas vai izmaiņšanas rezultātā. Īpaša uzmanība būtu jāpievērš novatorisku MVU informētības uzlabošanai par saistītiem draudiem un neaizsargātību, jo tie arvien vairāk ir atkarīgi no informācijas sistēmu pareizas darbības un pieejamības un tiem bieži vien ir ierobežoti resursi informācijas drošībai.***
- (4) Lai nodrošinātu saskaņotu pieeju šīs direktīvas piemērošanai dalībvalstīs, šajā jomā ir svarīgas vienotas definīcijas.
- (5) Ir jāpanāk kopīga pieeja noziedzīgu nodarījumu sastāvdaļām, ieviešot vienotus noziedzīgu nodarījumu sastāvus attiecībā uz nelikumīgu piekļuvi informācijas sistēmai, nelikumīgu iejaukšanos sistēmā, nelikumīgu iejaukšanos datos un nelikumīgu pārtveršanu.
- (5.a) *Pārtveršana ietver, bet neaprobežojas ar saziņas satura noklausīšanos, uzraudzīšanu vai novērošanu, satura datu saņemšanu tiešā veidā, piekļūstot un izmantojot informācijas sistēmu, vai netieši, ar tehniskiem līdzekļiem izmantojot elektroniskas noklausīšanās vai uztveršanas ierīces.***

- (6) Dalībvalstīm būtu jāparedz sodi par uzbrukumiem informācijas sistēmām. Sodiem vajadzētu būt iedarbīgiem, samērīgiem un preventīviem, **un tiem vajadzētu ietvert cietumsodu un/vai naudassodu.**
- (6.a) *Ar šo direktīvu paredz noteikt kriminālsankcijas vismaz tādos gadījumos, kas nav mazsvarīgi. Katra dalībvalsts saskaņā ar saviem tiesību aktiem un praksi var noteikt, kuru pārkāpumu var uzskatīt par mazsvarīgu. Nodarījumu var uzskatīt par mazsvarīgu, piemēram, ja nodarījuma izraisītais kaitējums un/vai risks, ko tas rada publiskām vai privātām interesēm, tādām kā datortīkla vai datorizētu datu integritātei, vai personas neaizskaramībai, tiesībām vai citām interesēm, ir nenozīmīgs vai tāds, ka kriminālsoda piemērošana likumā paredzētajās robežās vai kriminālatbildības piemērošana nav nepieciešama.*
- (6.b) *Kiberuzbrukumu izraisītā apdraudējuma un riska, kā arī informācijas sistēmu saistītās neaizsargātības identifikācija un ziņošana par to ir būtisks elements kiberuzbrukumu efektīvā profilaksē un reaģēšanā uz tiem, kā arī informācijas sistēmu drošības uzlabošanā. Tādēļ varētu būt lietderīgi noteikt stimulus, lai ziņotu par drošības robiem. Dalībvalstīm būtu jātiecas piedāvāt šādas iespējas, lai varētu tiesiski noteikt drošības robus un ziņot par tiem.*

- (7) Ir atbilstīgi noteikt bargākus sodus, ja uzbrukumu informācijas sistēmai ir veikusi noziedzīga organizācija, kā definēts Padomes Pamatlēmumā 2008/841/TI (2008. gada 24. oktobris) par cīņu pret organizēto noziedzību ¹, **vai** ja tas ir plaša mēroga uzbrukums, **kas tādējādi skāris būtisku skaitu informācijas sistēmu vai ir radījis nopietnu kaitējumu, cita starpā, ja uzbrukuma mērķis ir bijis izveidot "robottīklu" vai tas tika izdarīts, izmantojot "robottīklu" un tādējādi radot nopietnu kaitējumu.** Ir atbilstīgi arī noteikt smagākus sodus, ja tāds uzbrukums **ir vērsts pret kritisku infrastruktūru.**
- (7.a) ***Vēl viens nozīmīgs elements integrētā pieejā kibernetizācijas apkarošanai ir efektīvu pasākumu noteikšana pret identitātes zādzību un citiem nodarījumiem saistītā ar identitāti. Apsverot, vai attiecībā uz šādiem noziedzīgiem nodarījumiem ir vajadzīga ES rīcība, varētu arī izvērtēt vajadzību pēc visaptveroša horizontāla ES instrumenta.***
- (8) Padomes 2008. gada 27. un 28. novembra secinājumos ir norādīts, ka dalībvalstīm un Komisijai būtu jāizstrādā jauna stratēģija, ņemot vērā Eiropas Padomes 2001. gada Konvenciju par kibernetizāciju. Šī konvencija ir atsauces tiesiskais regulējums cīņai pret kibernetizāciju, tostarp uzbrukumiem informācijas sistēmām. Šī direktīva ir izstrādāta, pamatojoties uz minēto konvenciju. ***Tāpēc par prioritāti būtu jāuzskatā tas, lai visas dalībvalstis pēc iespējas ātrāk pabeigtu konvencijas ratificēšanas procesu.***

¹ OV L 300, 11.11.2008., 42. lpp.

- (9) Ņemot vērā, ka uzbrukumus ir iespējams veikt dažādos veidos, un to, cik ātri attīstās aparātūra un programmatūra, direktīvā **ir runa** par "rīkiem", ko var izmantot direktīvā uzskaitīto noziedzīgo nodarījumu izdarīšanai. Rīki nozīmē, piemēram, ļaunprātīgu programmatūru, ko izmanto kiberuzbrukumu izdarīšanai, tostarp arī *tādu programmatūru, ar ko ir iespējams izveidot robottīklus. Pat ja ar rīku ir iespējams vai tas pat ir īpaši piemērots minēto nodarījumu veikšanai, tas, iespējams, ir izstrādāts likumīgiem mērķiem. Pamatojoties uz to, ka ir jānovērš kriminālvajāšana gadījumos, kad šādi rīki ir izstrādāti un laisti tirgū likumīgiem mērķiem, piemēram, informācijas tehnoloģiju izstrādājumu izturības vai informācijas sistēmu drošības pārbaudēm, papildus vispārīga nolūka prasībai jābūt izpildītai arī tīša nolūka prasībai, ka šos rīkus iecerēts izmantot, lai veiktu kādu no direktīvā uzskaitītajiem nodarījumiem.*

- (10.a) Nav iecerēts ar šo direktīvu noteikt kriminālatbildību, ja objektīvie kritēriji šajā direktīvā uzskaitītajiem nodarījumiem ir izpildīti, tomēr darbības ir veiktas bez noziedzīga nolūka, piemēram, ja persona nav zinājusi, ka piekļuve bija neatļauta vai ja ir notikusi informācijas sistēmas aizsardzības pilnvarota pārbaude, piemēram, ja uzņēmums vai tirgotājs personai ir uzdevis pārbaudīt savas drošības sistēmas izturību. Saistībā ar šo direktīvu kriminālatbildību neizraisītu līgumā noteiktas saistības vai vienošanās ierobežot piekļuvi informācijas sistēmām, izmantojot lietotāju politiku vai lietošanas noteikumus, kā arī darba strīdi attiecībā uz tiesībām piekļūt un izmantot darba devēja informācijas sistēmas privātiem mērķiem, ja šādās situācijās piekļuvi uzskatītu par neatļautu un tā tādējādi būtu vienīgais pamatojums kriminālvajāšanai. Šī direktīva neietekmē likumīgi garantētās tiesības uz piekļuvi informācijai, kā noteikts valstu un ES tiesību aktos, lai gan tās vienlaicīgi nevar būt par attaisnojumu nelikumīgai un patvaļīgai piekļuvei informācijai.*
- (10.b) Kiberuzbrukumus var atvieglot dažādi apstākļi, piemēram, kad to veicējam saistībā ar viņa darbu ir piekļuve drošības sistēmām, kas ir daļa no skartajām informācijas sistēmām. Šādi apstākļi būtu pienācīgi jāņem vērā kriminālvajāšanā, ievērojot atbilstīgo valstu tiesību aktus.*

- (10.c) *Dalībvalstīm savos valsts tiesību aktos būtu jāparedz atbildību pastiprinoši apstākļi saskaņā ar šo valstu tiesību sistēmā definētiem piemērojamiem noteikumiem par atbildību pastiprinošiem apstākļiem. Tām būtu jānodrošina, ka minētie atbildību pastiprinošie apstākļi būtu zināmi tiesnešiem, lai tie tos ņemtu vērā, nosakot sodu pārkāpējiem. Šādu apstākļu izvērtēšana kopā ar konkrētās lietas citiem faktiem ir tiesneša pilnīgā kompetencē.*
- (10.d) *Šajā direktīvā nereglamentē nosacījumus, kas būtu jāievēro, lai īstenotu jurisdikciju attiecībā uz jebkuru no nodarījumiem, kas uzskaitīti 3.–8. pantā, piemēram, cietušā iesniegts ziņojums tās valsts teritorijā, kur veikts nodarījums, vai kad valsts, kurā noziedzīgais nodarījums tika izdarīts, ir sniegusi oficiālu informāciju, vai tas apstāklis, ka pret likumpārkāpēju nav sāкта tiesvedība valstī, kurā tika izdarīts noziedzīgais nodarījums.*
- (10.e) *Saistībā ar šo direktīvu valstīm un publiskām iestādēm arvien pilnā mērā ir saistoša cilvēktiesību un pamatbrīvību ievērošanas garantēšana saskaņā ar spēkā esošajām starptautiskajām saistībām.*

- (11) Direktīvā ir uzsvērtā tādu tīklu nozīme kā G8 vai Eiropas Padomes kontaktpunktu tīkls, kas ir pastāvīgi pieejami katru dienu divdesmit četras stundas diennaktī. ***Šādiem kontaktpunktiem būtu jāspēj nodrošināt efektīvu palīdzību un tādējādi veicināt, piemēram, esošās atbilstīgās informācijas apmaiņu vai tehnisku konsultāciju vai juridiskas informācijas sniegšanu, lai veiktu izmeklēšanu vai tiesvedību par krimināliem nodarījumiem, kas saistīti ar informācijas sistēmām un saistītiem datiem, kas attiecas uz pieprasītāju dalībvalsti. Lai nodrošinātu tīklu labu darbību, katram kontaktpunktam būtu jāspēj ātri sazināties ar citas valsts kontaktpunktu, tostarp ar apmācīta un sagatavota personāla starpniecību.*** Ņemot vērā, cik ātri ir iespējams veikt plaša mēroga ***kiber***uzbrukumus, dalībvalstīm būtu jāspēj nekavējoties sniegt atbildi uz šī kontaktpunktu tīkla steidzamiem lūgumiem. ***Šādos gadījumos varētu būt lietderīgi, ka informācijas pieprasījumu papildina telefoniska sazināšanās, lai nodrošinātu, ka pieprasījuma saņēmējā dalībvalstī pieprasījumu apstrādās ātri un atbilde tiks sniegta 8 stundu laikā.***

(11.a) *Novēršot un apkarojot uzbrukumus informācijas sistēmām, ļoti nozīmīga ir publisko iestāžu sadarbība ar privāto sektoru un pilsonisko sabiedrību. Ir jāpastiprina un jāuzlabo sadarbība starp pakalpojumu sniedzējiem, ražotājiem, tiesībsardzības struktūrām un tiesu iestādēm, pilnībā ievērojot tiesiskumu. Sadarbība, piemēram, var ietvert pakalpojumu sniedzēju atbalstu, lai palīdzētu saglabāt iespējamus pierādījumus, sniegtu informāciju pārkāpēju identificēšanai un kā pēdējo līdzekli saskaņā ar valstu tiesībām, tostarp valstu tiesību aktiem un praksi, pilnībā vai daļēji izslēgtu informācijas sistēmas vai funkcijas, kuras tiek apdraudētas vai izmantotas nelikumīgiem mērķiem. Dalībvalstīm būtu arī jāapsver iespēja izveidot sadarbības un partnerības tīklus ar pakalpojumu sniedzējiem un ražotājiem, lai apmainītos ar informāciju saistībā ar šīs direktīvas darbības jomā iekļautajiem pārkāpumiem.*

I

(12.a) Ir jāvāc salīdzināmi dati par šajā direktīvā minētajiem nodarījumiem. Atbilstīgi dati būtu jādara pieejami kompetentajām specializētajām aģentūrām, piemēram, Eiropolam un Eiropas Tīklu un informācijas drošības aģentūrai atbilstīgi to uzdevumiem un vajadzībai pēc informācijas, lai panāktu pilnīgāku izpratni par problemātiku saistībā ar kibernetizāciju un tīklu un informācijas drošību Savienības līmenī un tādējādi sekmētu efektīvākas atbildes rīcības sagatavošanu. Dalībvalstīm būtu jāiesniedz Eiropolam un tā Eiropas Kibernetizēgumu centram informācija par nodarījumu veicēju darbības veidu, lai tie veiktu kibernetizācijas izraisīto draudu izvērtējumu un stratēģisku analīzi atbilstīgi Padomes Lēmumam 2009/371/TI. Informācijas sniegšana var sekmēt labāku izpratni par esošajiem un nākotnē gaidāmajiem draudiem un tādējādi var veicināt piemērotāku un mērķtiecīgāku lēmumu pieņemšanu par uzbrukumu informācijas sistēmām apkarošanu un novēršanu.

(12.b) Saskaņā ar šo direktīvu Komisijai ir jāiesniedz ziņojums par direktīvas īstenošanu un jānāk klajā ar visiem vajadzīgajiem leģislatīvo aktu priekšlikumiem, ar kuriem, iespējams, paplašina šīs direktīvas darbības jomu, ņemot vērā norises kibernetizācijas jomā. Šādas norises varētu ietvert tādu tehnoloģiju attīstību, kuras nodrošina, piemēram, efektīvāku izpildi attiecībā uz uzbrukumiem informācijas sistēmām vai kuras veicina šādu uzbrukumu nepieļaušanu vai to seku mazināšanu. Tālab Komisijai būtu arī jāņem vērā pieejamās analīzes un ziņojumi, ko izstrādājuši atbilstīgi dalībnieki un jo īpaši Eiropols un ENISA.

(12.c) Kibernoziegumu efektīvai apkarošanai jāpalielina informācijas sistēmu izturība, veicot piemērotus pasākumus, lai tās efektīvāk aizsargātu pret kiberuzbrukumiem. Dalībvalstīm būtu jāveic vajadzīgie pasākumi kritiskās infrastruktūras aizsardzībai pret kiberuzbrukumiem, kā daļu no tā tām būtu jāuzskata savu informācijas sistēmu un saistītu datu aizsardzība. Svarīga kompleksas pieejas daļa kibernoziēdzības efektīvai apkarošanai ir informācijas sistēmu piemērota līmeņa aizsardzības un drošības nodrošināšana no juridisku personu puses, piemēram, saistībā ar publiski pieejamu elektroniskās saziņas pakalpojumu sniegšanu atbilstīgi spēkā esošajiem ES tiesību aktiem par privāto dzīvi un elektroniskajiem sakariem un datu aizsardzību. Būtu jānodrošina pienācīgs aizsardzības līmenis pret iespējami identificējamiem draudiem un neaizsargātību atbilstoši augstākajam iespējamajam līmenim attiecīgajā nozarē un specifiskām datu apstrādes situācijām. Izmaksām un slogam saistībā ar šādu aizsardzību vajadzētu būt samērīgam ar iespējamo kaitējumu, ko kiberuzbrukums izraisītu iesaistītajām personām. Dalībvalstis tiek mudinātas savos valsts tiesību aktos noteikt atbilstīgus pasākumus, paredzot atbildību gadījumos, kad juridiskā persona nepārprotami nav nodrošinājusi atbilstīga līmeņa aizsardzību pret kiberuzbrukumiem.

- (13) Ievērojami trūkumi un atšķirības dalībvalstu tiesību aktos **un kriminālprocedūrās** saistībā ar uzbrukumiem informācijas sistēmām ■ var kavēt organizētās noziedzības un terorisma apkarošanu un sarežģīt efektīvu policijas un tiesu iestāžu sadarbību.
- Modernās informācijas sistēmas ir starptautiskas, un uz tām neattiecas robežas, bet tas nozīmē, ka uzbrukumiem šādām sistēmām ir **pārrobežu** raksturs, kas vēl vairāk izceļ steidzamo vajadzību tuvināt krimināltiesību aktus šajā jomā. Turklāt koordināciju, saucot pie atbildības saistībā ar uzbrukumiem informācijas sistēmām, būtu jāuzlabo, **atbilstīgi īstenojot un piemērojot** Padomes Pamatlēmumu 2009/948/TI par jurisdikcijas īstenošanas konfliktu novēršanu un atrisināšanu kriminālprocesā.
- Dalībvalstīm sadarbībā ar Eiropas Savienību būtu arī jātiecas uzlabot starptautisku sadarbību saistībā ar informācijas sistēmu, datortīklu un datoru datu drošību. Jebkādos starptautiskos nolīgumos saistībā ar datu apmaiņu būtu pienācīgi jāņem vērā apsvērumi par datu pārsūtīšanas un glabāšanas drošību.***

(13.a) *Lai efektīvi apkarotu kibernoziegumus, ir būtiski uzlabot sadarbību starp kompetentajām tiesībsardzības struktūrām un tiesu iestādēm visā Savienībā. Šajā sakarībā būtu jāveicina pastiprināti centieni, nodrošinot atbilstīgajām iestādēm piemērotu apmācību, lai uzlabotu izpratni par kibernoiedzību un tās ietekmi, un pastiprinot sadarbību un paraugprakses apmaiņu, piemēram, ar kompetentu specializētu ES aģentūru starpniecību. Ar šādām apmācībām būtu inter alia jātiecas uzlabot informētību par atšķirīgajām valstu tiesību sistēmām, iespējamām juridiskām un tehniskām problēmām, ar kurām saskaras kriminālizmeklēšanā, vai kompetenču sadalījumu starp atbilstīgām valstu iestādēm.*

(14) Ņemot vērā to, ka šīs direktīvas mērķus, proti, nodrošināt, ka visās dalībvalstīs par uzbrukumiem informācijas sistēmām soda, piemērojot efektīvus, samērīgus un preventīvus kriminālsodus, un uzlabot un veicināt tiesu iestāžu sadarbību, likvidējot iespējamās sarežģījumus, nevar pietiekami labi sasniegt dalībvalstīs, jo noteikumiem ir jābūt vienotiem un saderīgiem, un to, ka minētos mērķus tādēļ var labāk sasniegt Savienības līmenī, Savienība var pieņemt pasākumus saskaņā ar Līguma par Eiropas Savienību 5. pantā noteikto subsidiaritātes principu. Šajā direktīvā ir paredzēti vienīgi tādi pasākumi, kas ir vajadzīgi šo mērķu sasniegšanai.

I

- (15.a) *Tiesības uz personas datu aizsardzību ir pamattiesības atbilstīgi LESD 16. panta 1. punktam un Pamattiesību hartas 8. pantam. Tāpēc personas datu jebkādā apstrādē saistībā ar šīs direktīvas īstenošanu būtu pilnībā jāievēro atbilstīgi ES tiesību akti datu aizsardzības jomā, kuri pieņemti, pamatojoties uz Līgumiem.*
- (16) Direktīvā ir ievērotas **pamatbrīvības un** pamattiesības un respektēti principi, kuri ir atzīti jo īpaši Eiropas Savienības Pamattiesību hartā **un Eiropas Cilvēktiesību un pamatbrīvību aizsardzības konvencijā**, tostarp personas datu aizsardzība, **tiesības uz privāto dzīvi**, vārda un informācijas brīvība, tiesības uz taisnīgu tiesu, nevainīguma prezumpcija un tiesības uz aizstāvību, kā arī tiesiskuma princips un nodarījuma un soda samērīguma princips krimināltiesībās. Šo tiesību un principu pilnīga ievērošana ir īpašs šīs direktīvas mērķis, un tā ir attiecīgi jāīsteno.
- (17) **Saskaņā ar 3. pantu** Protokolā par Apvienotās Karalistes un Īrijas nostāju saistībā ar brīvības, drošības un tiesiskuma telpu, kas pievienots Līgumam par Eiropas Savienības darbību, Apvienotā Karaliste un Īrija ir informējušas par savu vēlmi piedalīties šīs direktīvas pieņemšanā un piemērošanā ■ .

- (18) Saskaņā ar 1. un 2. pantu Protokolā par Dānijas nostāju, kas pievienots Līgumam par Eiropas Savienības darbību, Dānija nepiedalās šīs direktīvas pieņemšanā, un tādēļ šī direktīva tai nav saistoša un nav jāpiemēro.
- (19) *Šīs direktīvas mērķis ir grozīt un paplašināt Pamatlēmuma 2005/222/TI noteikumus. Tā kā veicamie grozījumi ir būtiski un to skaits ir ievērojams, skaidrības labad attiecībā uz tām dalībvalstīm, kuras piedalās šīs direktīvas pieņemšanā, Pamatlēmums būtu jāaizstāj pilnībā,*

IR PIEŅĒMUŠI ŠO DIREKTĪVU.

1. pants

Priekšmets



Ar šo direktīvu izveido minimuma noteikumus par noziedzīgu nodarījumu un sankciju definēšanu saistībā ar uzbrukumiem informācijas sistēmām. Tās mērķis ir arī veicināt tādu nodarījumu novēršanu un uzlabot tiesu iestāžu un citu kompetento iestāžu sadarbību.

2. pants

Definīcijas

Šajā direktīvā piemēro šādas definīcijas:

- a) "informācijas sistēma" ir jebkura ierīce vai savstarpēji savienotu vai saistītu ierīču kopums, no kurām viena vai vairākas ierīces saskaņā ar programmu veic automātisku datorizētu datu apstrādi, kā arī datorizēti dati, ko minētās ierīces glabā, apstrādā, iegūst vai sūta to darbībai, izmantošanai, aizsardzībai un uzturēšanai;

- b) "datorizēti dati" ir jebkurš fakts, informācijas vai konceptu atveidojums formā, kas ir piemērota apstrādei informācijas sistēmā, tostarp programma, kas piemērota tam, lai informācijas sistēmā izraisītu kādu darbību;
- c) "juridiska persona" ir jebkurš subjekts, kam ir šāds statuss attiecīgos tiesību aktos, izņemot valstis vai citas valsts struktūras, kas īsteno valsts varu, un publisko tiesību starptautiskās organizācijas;
- d) "bez tiesībām" ir **piekļuve, iejaukšanās, pārtveršana vai jebkāda cita šajā direktīvā minēta darbība** bez īpašnieka vai bez sistēmas vai tās daļas cita tiesību subjekta atļaujas vai tāda piekļuve, iejaukšanās, pārtveršana vai jebkāda cita šajā direktīvā minēta darbība, kas nav atļauta saskaņā ar attiecīgās valsts tiesību aktiem.

3. pants

Nelikumīga piekļuve informācijas sistēmām

Dalībvalstis veic vajadzīgos pasākumus, lai nodrošinātu, ka gadījumos, kad noziedzīgu nodarījumu izdara, **pārkāpjot kādu drošības pasākumu** un vismaz gadījumos, kas nav mazsvarīgi, piekļuve bez atļaujas visai informācijas sistēmai vai jebkādai tās daļai, **ja to izdara tīši**, ir sodāma kā noziedzīgs nodarījums.

4. pants

Nelikumīga iejaukšanās sistēmā

Dalībvalstis veic vajadzīgos pasākumus, lai nodrošinātu, ka vismaz gadījumos, kas nav mazsvarīgi, informācijas sistēmas darbības ■ būtiska kavēšana vai pārtraukšana, ievadot, sūtot, bojājot, dzēšot, pasliktinot, grozot, anulējot vai padarot nepieejamus datorizētus datus, ir sodāma kā noziedzīgs nodarījums, ja tas ir darīts **tīši un** bez atļaujas.

5. pants

Nelikumīga iejaukšanās datos

Dalībvalstis veic vajadzīgos pasākumus, lai nodrošinātu, ka vismaz gadījumos, kas nav mazsvarīgi, informācijas sistēmas datorizētu datu ■ dzēšana, bojāšana, pasliktināšana, grozīšana, anulēšana vai padarīšana par nepieejamiem ir sodāma kā noziedzīgs nodarījums, ja tas ir darīts **tīši un** bez atļaujas.

6. pants

Nelikumīga pārtveršana

Dalībvalstis pieņem vajadzīgos pasākumus, lai nodrošinātu, ka **vismaz gadījumos, kas nav mazsvarīgi**, ■ datu pārtveršana, kas ir veikta ar tehnisku līdzekļu palīdzību, kad datorizētus datus pārsūta no informācijas sistēmas vai uz to, vai arī informācijas sistēmā, arī attiecībā uz informācijas sistēmas elektromagnētiskām emisijām, kas satur šādus datorizētus datus, ja attiecīgā pārsūtīšana nav publiska, ir sodāma kā noziedzīgs nodarījums, ja to izdara **tīši un bez atļaujas**.

7. pants

Noziedzīgu nodarījumu izdarīšanas rīki

1. Dalībvalstis veic vajadzīgos **pasākumus**, lai nodrošinātu, ka **vismaz gadījumos, kas nav mazsvarīgi**, turpmāk minēto objektu izstrāde, pārdošana, iepirkšana izmantošanai, imports, ■ izplatīšana vai citāda veida pieejamības nodrošināšana ir sodāma kā noziedzīgs nodarījums, ja to izdara tīši, bez atļaujas un **ar nolūku to izmantot**, lai izdarītu kādu no 3.–6. pantā minētajiem noziedzīgajiem nodarījumiem:
 - a) ■ datorprogramma, kura galvenokārt paredzēta vai pielāgota 3.–6. pantā minēto noziedzīgo nodarījumu izdarīšanai,

- b) datorparole, pieejas kods vai līdzīgi dati, ar kuru palīdzību var piekļūt informācijas sistēmai vai tās daļai.

8. pants

Kūdišana, sekmēšana un atbalstīšana, un mēģinājums

1. Dalībvalstis nodrošina, lai ***kūdišana*** uz kādu no 3.–7. pantā minētajiem nodarījumiem un tādu nodarījumu sekmēšana un atbalstīšana būtu sodāma kā noziedzīgs nodarījums.
2. Dalībvalstis nodrošina, lai mēģinājums izdarīt kādu no ***4. un 5. pantā*** minētajiem ***nodarījumiem*** būtu sodāms kā noziedzīgs nodarījums.

9. pants

Sodi

1. Dalībvalstis veic vajadzīgos pasākumus, lai nodrošinātu, ka par 3.–8. pantā minētajiem noziedzīgajiem nodarījumiem ir paredzēti efektīvi, ***samērīgi*** un preventīvi kriminālsodi.
2. Dalībvalstis veic vajadzīgos pasākumus, lai nodrošinātu, ka par 3.–7. pantā minētajiem nodarījumiem ***vismaz gadījumos, kas nav mazsvarīgi, ir noteikts maksimālais kriminālsods – brīvības atņemšana uz vismaz diviem gadiem.***

3. *Dalībvalstis veic vajadzīgos pasākumus, lai nodrošinātu, ka par 4. un 5. pantā minētajiem nodarījumiem ir noteikts maksimālais kriminālsods – brīvības atņemšana uz vismaz trim gadiem, ja tie izdarīti tīši un ja ir ietekmēts ievērojams skaits informācijas sistēmu, izmantojot rīku, kas minēts 7. panta 1. punktā un kas izstrādāts vai pielāgots galvenokārt šādam mērķim.*
4. *Dalībvalstis veic vajadzīgos pasākumus, lai nodrošinātu, ka par 4. un 5. pantā minētajiem nodarījumiem ir noteikts maksimālais kriminālsods – brīvības atņemšana uz vismaz pieciem gadiem, ja tie*
- a) *ir izdarīti, darbojoties noziedzīgā organizācijā saskaņā ar Pamatlēmumā 2008/841/TI sniegto definīciju, bet neatkarīgi no tajā paredzētās soda pakāpes, vai*
 - b) *izraisa nopietnu kaitējumu, vai*
 - c) *ir izdarīti pret kādu kritiskās infrastruktūras informācijas sistēmu.*

5. *Dalībvalstis veic vajadzīgos pasākumus, lai nodrošinātu, ka gadījumos, kad 4. un 5. pantā minētie nodarījumi ir veikti, ļaunprātīgi izmantojot citu personu personas datus, lai iegūtu trešās puses uzticību, un tādējādi ir nodarīts morālais kaitējums identitātes likumīgajam īpašniekam, to atbilstīgi attiecīgajiem noteikumiem valsts tiesību aktos var uzskatīt par vainu pastiprinošiem apstākļiem, izņemot, ja uz šiem apstākļiem jau attiecas cits nodarījums, par kuru valsts tiesību aktos ir noteikts sods.*

I

11. pants

Juridisko personu atbildība

1. Dalībvalstis veic vajadzīgos pasākumus, lai nodrošinātu, ka juridiskas personas var saukt pie atbildības par 3.–8. pantā minētajiem nodarījumiem, ko to labā, darbojoties individuāli vai kā juridiskas personas struktūras daļa, ir izdarījusi kāda persona, kas veic šās juridiskās personas vadības pienākumus, pamatojoties uz vienu no turpmāk minētā:
- a) pilnvarām pārstāvēt juridisko personu;

- b) pilnvarām pieņemt lēmumus juridiskās personas vārdā;
 - c) pilnvarām veikt juridiskās personas iekšējo kontroli.
2. Katra dalībvalsts veic vajadzīgos pasākumus, lai nodrošinātu, ka juridiskas personas var saukt pie atbildības, ja tādēļ, ka 1. punktā minētā persona nav veikusi uzraudzību vai kontroli, ir bijis iespējams, ka nodarījumu, kas minēts 3.–8. pantā, attiecīgās juridiskās personas labā izdara persona, kas ir tās pakļautībā.
3. Juridiskās personas atbildība saskaņā ar 1. un 2. punktu neizslēdz kriminālvajāšanu pret fiziskām personām, kas ir jebkuru 3.–8. pantā minēto nodarījumu izpildītāji, **kūdtāji** vai līdzdalībnieki.

12. pants

Juridiskām personām piemērojami sodi

1. Dalībvalstis veic vajadzīgos pasākumus, lai nodrošinātu, ka juridiskai personai, kuru sauc pie atbildības saskaņā ar 11. panta 1. punktu, var piemērot efektīvus, samērīgus un preventīvus sodus, kas ietver naudas sodu kā kriminālsodu vai cita veida sodu un var ietvert citus sodus, kas paredz, piemēram,
- a) atņemt tiesības saņemt publiskus līdzekļus vai atbalstu;

- b) uz laiku vai pastāvīgi aizliegt veikt komercdarbību;
 - c) pakļaut tiesas uzraudzībai;
 - d) likvidēt ar tiesas lēmumu;
 - e) uz laiku vai pavisam slēgt uzņēmējdarbības veikšanas vietas, kas izmantotas nodarījuma izdarīšanā.
2. Dalībvalstis veic vajadzīgos pasākumus, lai nodrošinātu, ka juridiskai personai, kuru sauc pie atbildības saskaņā ar 11. panta 2. punktu, ir piemērojami efektīvi, samērīgi un preventīvi sodi vai pasākumi.

13. pants
Jurisdikcija

1. Dalībvalstis nosaka savu jurisdikciju attiecībā uz direktīvas 3.–8. pantā minētajiem nodarījumiem, ja
- a) nodarījums ir pilnīgi vai daļēji izdarīts attiecīgās dalībvalsts teritorijā vai

aa) nodarījumu izdarījis attiecīgās dalībvalsts valstspiederīgais, vismaz gadījumos, kad darbība ir noziedzīgs nodarījums vietā, kur tā ir izdarīta.

■

2. **Dalībvalsts**, nosakot jurisdikciju saskaņā ar 1. punkta a) apakšpunktu, nodrošina, ka tās jurisdikcijā ietilpst gadījumi, kad
- a) likumpārkāpējs izdara nodarījumu, fiziski atrodoties attiecīgās dalībvalsts teritorijā, neatkarīgi no tā, vai nodarījums ir izdarīts pret informācijas sistēmu tās teritorijā, vai
 - b) nodarījums ir izdarīts pret informācijas sistēmu attiecīgās dalībvalsts teritorijā, neatkarīgi no tā, vai likumpārkāpējs izdara nodarījumu, fiziski atrodoties tās teritorijā.

3. *Dalībvalsts informē Komisiju, ja tā pieņem lēmumu noteikt plašāku jurisdikciju par kādu 3.–8. pantā minēto nodarījumu, kas izdarīts ārpus tās teritorijas, piemēram, ja*

- a) *likumpārkāpēja parastā dzīvesvieta ir attiecīgās dalībvalsts teritorijā vai*
- b) *nodarījums ir izdarīts tādas juridiskās personas labā, kas reģistrēta šīs dalībvalsts teritorijā.*

14. pants

Informācijas apmaiņa

1. Lai apmainītos ar informāciju par 3.–8. pantā minētajiem nodarījumiem, ***dalībvalstis nodrošina, ka tām ir valsts operatīvais kontaktpunkts***, un tās izmanto esošo operatīvo kontaktpunktu tīklu, kas ir pastāvīgi pieejams divdesmit četras stundas diennaktī. Dalībvalstis nodrošina arī to, ka ir ieviestas procedūras, lai ***steidzamu lūgumu gadījumā maksimums 8 stundu laikā tās varētu vismaz norādīt, vai uz palīdzības lūgumu tiks sniegta atbilde, kādā veidā tā tiks sniegta, kā arī minēt aptuvenu atbildes sniegšanas laiku.***

2. Dalībvalstis informē Komisiju par to izraudzītajiem kontaktpunktiem informācijas apmaiņai par nodarījumiem, kas minēti 3.–8. pantā. Komisija nosūta šo informāciju citām dalībvalstīm ***un kompetentajām specializētajām ES aģentūrām un struktūrām.***
3. ***Dalībvalstis veic vajadzīgos pasākumus, nodrošinot, ka ir pieejami atbilstīgi ziņošanas kanāli, lai varētu vieglāk un bez kavēšanās ziņot kompetentajām valstu iestādēm par 3.–6. pantā minētajiem nodarījumiem.***

15. pants

Uzraudzība un statistika

1. Dalībvalstis nodrošina tādas sistēmas izveidi, ar kuras palīdzību reģistrē, ģenerē un sniedz statistikas datus par nodarījumiem, kas minēti 3.–7. pantā.
2. Statistikas informācija, kas minēta 1. punktā, aptver vismaz ***pastāvošos datus par 3.–7. pantā minēto nodarījumu skaitu, kas reģistrēts*** dalībvalstīs, un **■** to personu skaitu, pret kurām ***uzsākts kriminālprocess un kas notiesātas*** par 3.–7. pantā minētajiem nodarījumiem.

3. Saskaņā ar šo pantu savāktos datus dalībvalstis nosūta Komisijai. **Komisija nodrošina** šo statistikas ziņojumu konsolidēta pārskata publicēšanu **un iesniegšanu kompetentajām specializētajām ES aģentūrām un struktūrām.**

16. pants

Pamatlēmuma 2005/222/TI aizstāšana

Ar šo **attiecībā uz dalībvalstīm, kuras piedalās šīs direktīvas pieņemšanā, aizstāj** Pamatlēmumu 2005/222/TI, neskarot dalībvalstu pienākumus attiecībā uz **termiņiem pamatlēmuma** transponēšanai valsts tiesību aktos.

Attiecībā uz dalībvalstīm, kuras piedalās šīs direktīvas pieņemšanā, atsaucēs uz Pamatlēmumu **2005/222/TI** uzskata par atsaucēm uz šo direktīvu.

17. pants

Transponēšana

1. Normatīvie un administratīvie akti, kas vajadzīgi, lai izpildītu šīs direktīvas prasības, dalībvalstīs stājas spēkā līdz [divu gadu laikā pēc direktīvas pieņemšanas] **█** .

█

3. *Dalībvalstis Komisijai dara zināmu to noteikumu tekstu, ar kuriem tās savos tiesību aktos transponē pienākumus, kas tām uzlikti saskaņā ar šo direktīvu.*
4. *Kad dalībvalstis pieņem šos pasākumus, tajos ietver atsauci uz šo direktīvu vai šādu atsauci pievieno to oficiālai publikācijai. Dalībvalstis nosaka paņēmienus, kā izdarāma šāda atsauce.*

18. pants

Ziņojumu sniegšana

I

Ne vēlāk kā [ČETRUS GADUS PĒC DIREKTĪVAS PIENĒMŠANAS] Komisija iesniedz Eiropas Parlamentam un Padomei ziņojumu, kurā izvērtēts, cik lielā mērā dalībvalstis ir veikušas vajadzīgos pasākumus, lai panāktu atbilstību šai direktīvai, vajadzības gadījumā ziņojumam pievienojot legīslatīvu aktu priekšlikumus. Šajā sakarībā Komisija ņem vērā arī tehniskās un juridiskās izmaiņas kibernetizācijas jomā, it īpaši attiecībā uz šīs direktīvas darbības jomu.

I

19. pants
Stāšanās spēkā

Šī direktīva stājas spēkā divdesmitajā dienā pēc tās publicēšanas *Eiropas Savienības Oficiālajā Vēstnesī*.

20. pants
Adresāti

Šī direktīva ir adresēta dalībvalstīm saskaņā ar Līgumiem.

I

28.11.2011

ĀRLIETU KOMITEJAS SATZINUMS

Pilsoņu brīvību, tieslietu un iekšlietu komitejai

par priekšlikumu Eiropas Parlamenta un Padomes direktīvai par uzbrukumiem informācijas sistēmām un par Padomes Pamatlēmuma 2005/222/TI atcelšanu (COM(2010)0517 – C7-0293/2010 – 2010/0273(COD))

Atzinumu sagatavoja: *Kristiina Ojula*

ĪSS PAMATOJUMS

Atzinumā stingri atbalstīta nepieciešamība pēc labākas informācijas apmaiņas starp dalībvalstīm attiecībā uz kibernetisko drošību, ņemot vērā arvien pieaugošās bažas par iespējamām kibernetiskām uzbrukumiem. Kibernetiskās drošības jautājums ir steidzami jārisina ES līmenī, un ir nepieciešami saskaņoti dalībvalstu pasākumi.

Atzinumā ir uzsvērtas Komisijas loma pašreizējo iniciatīvu sekmēšanā un koordinēšanā.

Ārlietu komiteja un Drošības un aizsardzības apakškomiteja uzskata, ka ir ļoti svarīgi steidzami rīkoties un pastiprināt atbildes pasākumu, iniciatīvu un programmu koordinēšanu ES līmenī. Ir jāatbalsta spēju attīstīšana un jāpastiprina sadarbība, lai paaugstinātu informācijas drošības līmeni.

Atzinumā atbalstīta ideja izveidot ES kibernetiskās drošības koordinatora amatu, lai veicinātu dažādu Eiropas darbību un iniciatīvu integrēšanu un koordinēšanu ES līmenī un visās ES iestādēs.

GROZĪJUMI

Ārlietu komiteja aicina par jautājumu atbildīgo Pilsoņu brīvību, tieslietu un iekšlietu komiteju ziņojumā iekļaut šādus grozījumus:

Grozījums Nr. 1

Direktīvas priekšlikums 1. apsvērums

Komisijas ierosinātais teksts

(1) Šīs direktīvas uzdevums ir tuvināt dalībvalstu krimināltiesību noteikumus par uzbrukumiem informācijas sistēmām un uzlabot tiesu un citu kompetento iestāžu, tostarp policijas un citu specializētu tiesībsardzības dienestu sadarbību.

Grozījums

(1) Šīs direktīvas uzdevums ir tuvināt dalībvalstu krimināltiesību noteikumus par uzbrukumiem informācijas sistēmām un uzlabot tiesu un citu kompetento iestāžu, tostarp policijas un citu specializētu tiesībsardzības dienestu, ***kā arī Savienības dienestu, sadarbību. Šis mērķis ir daļa no Savienības vispārējās stratēģijas, kuras nolūks ir organizētās noziedzības apkarošana, informācijas tīklu drošības palielināšana, kritiski svarīgas informācijas infrastruktūras aizsardzība un datu aizsardzība.***

Grozījums Nr. 2

Direktīvas priekšlikums 1.a apsvērums (jauns)

Komisijas ierosinātais teksts

Grozījums

(1a) Informācijas sistēmas ir būtisks elements Savienības politiskajā, sociālajā un ekonomiskajā mijiedarbībā. Sabiedrība ir arvien vairāk atkarīga no informācijas sistēmām. Lai gan tās sniedz ievērojamus ieguvumus, tomēr to sarežģītība un neaizsargātība pret dažāda veida datornoziedzīgiem ir saistīta ar daudziem riskiem mūsu drošībai. Tāpēc informācijas sistēmu drošība ir pastāvīgi nozīmīgs jautājums, kam nepieciešami efektīvi dalībvalstu un Savienības atbildes pasākumi.

Grozījums Nr. 3

Direktīvas priekšlikums 2. apsvērums

(2) Uzbrukumi informācijas sistēmām, **jo īpaši organizētas noziedzības aktivitāšu rezultātā**, kļūst arvien draudīgāki, **un** pieaug bažas par iespējamiem teroristiskiem vai politiski motivētiem uzbrukumiem informācijas sistēmām, kas ir dalībvalstu un Savienības īpaši svarīgās infrastruktūras sastāvdaļa. Tas apdraud drošākas informācijas sabiedrības un brīvības, drošības un tiesiskuma telpas izveidi, un tādējādi ir nepieciešama rīcība Eiropas Savienības līmenī.

(2) Uzbrukumi informācijas sistēmām kļūst arvien draudīgāki. **Tos var izraisīt terorisms un organizētā noziedzība, un tos var veikt valstis un privātpersonas.** Pieaug bažas par iespējamiem teroristiskiem vai politiski motivētiem uzbrukumiem informācijas sistēmām, kas ir dalībvalstu un Savienības īpaši svarīgās infrastruktūras sastāvdaļa. **Šādu uzbrukumu risku ievērojami palielina atsevišķu pārkāpumu pārrobežu raksturs, relatīvi nelielais risks un zemās izmaksas izdarītājiem, kā arī potenciāli lielle ieguvumi un nodarītais kaitējums.** Tas apdraud drošākas informācijas sabiedrības un brīvības, drošības un tiesiskuma telpas izveidi, un tādējādi ir nepieciešama rīcība **ne tikai** Eiropas Savienības, **bet arī starptautiskās sabiedrības** līmenī.

Grozījums Nr. 4

Direktīvas priekšlikums 3. apsvērums

(3) Ir vērojama tendence, ka plaša mēroga uzbrukumi informācijas sistēmām, kas ir īpaši svarīgas **valstīm** vai īpašām publiskā vai privātā sektora funkcijām, kļūst aizvien bīstamāki un atkārtojas aizvien biežāk. Šī tendenci pavada aizvien modernāku rīku attīstība, ko noziedznieki var izmantot dažādu kiberuzbrukumu izdarīšanai.

(3) Ir vērojama tendence, ka plaša mēroga uzbrukumi informācijas sistēmām, kas ir īpaši svarīgas **dalībvalstīm, Savienībai** vai īpašām publiskā vai privātā sektora funkcijām, **kā arī Savienības līmenī**, kļūst aizvien bīstamāki un atkārtojas aizvien biežāk. Šo tendenci pavada **datortehnoloģiju strauja attīstība un līdz ar to** aizvien modernāki rīki, ko noziedznieki var izmantot dažāda veida kiberuzbrukumu izdarīšanai, **daži no kuriem var nodarīt ievērojamu ekonomisku un sociālu kaitējumu.**

Grozījums Nr. 5

Direktīvas priekšlikums
4.a apsvērums (jauns)

Komisijas ierosinātais teksts

Grozījums

(4a) Būtu jāveic vispusīgs, ticams un neatkarīgs novērtējums par kopējo draudu līmeni saistībā ar uzbrukumiem informācijas sistēmām. Savienības iestādēm būtu attiecīgi jāpielāgo savs informācijas drošības līmenis.

Grozījums Nr. 6

Direktīvas priekšlikums
4.b apsvērums (jauns)

Komisijas ierosinātais teksts

Grozījums

(4b) Ir nepieciešams īstenot koordinēšanu Savienības līmenī, lai palīdzētu integrēt dažādas iniciatīvas, programmas un darbības.

Grozījums Nr. 7

Direktīvas priekšlikums
6. apsvērums

Komisijas ierosinātais teksts

Grozījums

(6) Dalībvalstīm jāparedz sodi par uzbrukumiem informācijas sistēmām. Šiem sodiem jābūt iedarbīgiem, samērīgiem un tādiem, kas attur no nodarījuma izdarīšanas.

(6) Dalībvalstīm jāparedz sodi par uzbrukumiem informācijas sistēmām, **un tie jāpieņem kā daļa no plašākas valstu stratēģiju sistēmas, kuras mērķis ir nepieļaut un apkarot šādus uzbrukumus.** Šiem sodiem jābūt iedarbīgiem, samērīgiem un tādiem, kas attur no nodarījuma izdarīšanas. **Nemot vērā šo draudu pārrobežu raksturu, dalībvalstīm ir jāsaskaņo paredzētie sodi, tādējādi mazinot pārkāpumu izskatīšanu atšķirības Savienībā.**

Grozījums Nr. 8

**Direktīvas priekšlikums
8.a apsvērums (jauns)**

Komisijas ierosinātais teksts

Grozījums

(8a) Padomei un Komisijai būtu jāaicina tās dalībvalstis, kuras vēl nav ratificējušas Eiropas Padomes Konvenciju par kibernetiskajiem, to izdarīt bez kavēšanās.

Grozījums Nr. 9

**Direktīvas priekšlikums
11.a apsvērums (jauns)**

Komisijas ierosinātais teksts

Grozījums

(11a) Kiberuzbrukumu novēršanai un apkarošanai ļoti nozīmīga ir varasiestāžu sadarbība ar privāto sektoru un pilsonisko sabiedrību. Nepieciešams izveidot pastāvīgu savstarpēju dialogu, ņemot vērā datorsistēmu plašo izmantošanu un vajadzību kopīgi uzņemties atbildību par sistēmu uzticamības un darbības nodrošināšanu. Visām datorsistēmu darbībā ieinteresētajām pusēm ir jābūt labāk informētām, lai veidotu datu drošības mentalitāti.

Grozījums Nr. 10

**Direktīvas priekšlikums
11.b apsvērums (jauns)**

Komisijas ierosinātais teksts

Grozījums

(11b) Ar nesenajām kiberaizsardzības jomas iniciatīvām un projektiem, piemēram, Eiropas Aizsardzības aģentūras (EAA) ietvaros, būtu jāveicina dalībvalstu kiberaizsardzības spēju stiprināšana. Būtu jāparedz ciešāka sadarbība gan ar EAA, gan ar NATO

Kopējās kiberaizsardzības izcilības centru (CCDCOE), it īpaši spēju veidošanas un apmācības jomā.

Grozījums Nr. 11

Direktīvas priekšlikums 12. apsvērums

Komisijas ierosinātais teksts

(12) Ir nepieciešams vākt datus par nodarījumiem, kas minēti šajā direktīvā, lai iegūtu pilnīgāku pārskatu par šo problēmu Savienības līmenī, un tādējādi veicinātu efektīvāku atbildes mehānismu izstrādi. Šie dati turklāt palīdzēs īpašajām aģentūrām, kā Eiropols un Eiropas Tīklu un informācijas drošības aģentūra, labāk novērtēt kibernetizācijas izplatības apjomu un stāvokli tīklu un informācijas drošības jomā Eiropā.

Grozījums

(12) Ir nepieciešams vākt datus par nodarījumiem, kas minēti šajā direktīvā, lai iegūtu pilnīgāku pārskatu par šo problēmu Savienības līmenī, un tādējādi veicinātu efektīvāku atbildes mehānismu izstrādi. ***Dalībvalstīm ar Komisijas un Eiropas Tīklu un informācijas drošības aģentūras atbalstu būtu jāuzlabo apmaiņa ar informāciju par uzbrukumiem informācijas sistēmām.*** Šie dati turklāt palīdzēs īpašajām aģentūrām, kā Eiropols un Eiropas Tīklu un informācijas drošības aģentūra, labāk novērtēt kibernetizācijas izplatības apjomu un ***ietekmi, kā arī*** stāvokli tīklu un informācijas drošības jomā Eiropā. ***Plašākas zināšanas par pašreizējiem un turpmākajiem riskiem ļaus pieņemt efektīvākus lēmumus, kas palīdzētu nepieļaut kibernetizācijas uzbrukumus, aizsargāties pret tiem un mazināt to izraisīto kaitējumu.***

Grozījums Nr. 12

Direktīvas priekšlikums 12.a apsvērums (jauns)

Komisijas ierosinātais teksts

Grozījums

(12a) Informācijas apmaiņai un publiskā un privātā sektora partnerībai (PPP) ir svarīga loma kibernetizācijas uzlabošanā. Tāpēc Komisijai būtu jāizpēta iespēja izveidot sistēmas vai instrumentus, ar kuriem palīdzēt PPP savstarpēji

*sadarboties valstu un Savienības līmenī,
lai ieviestu informācijas kvalitātes
standartus savietojamības jomā un
nodrošinātu pamattiesību ievērošanu,
varas dalījumu un demokrātisku
uzraudzību.*

Grozījums Nr. 13

Direktīvas priekšlikums 13. apsvērums

Komisijas ierosinātais teksts

(13) Ievērojami trūkumi un atšķirības dalībvalstu tiesību aktos uzbrukumu informācijas sistēmām jomā var kavēt organizētās noziedzības un terorisma apkarošanu un sarežģīt efektīvu policijas un tiesu iestāžu sadarbību. Modernās informācijas sistēmas ir starptautiskas un tās nesaista robežas, *tas* nozīmē, ka uzbrukumiem šādām sistēmām ir pārrobežu raksturs, kas vēl vairāk izceļ steidzamo vajadzību tuvināt krimināltiesību aktus šajā jomā. Turklāt, pēc Padomes Pamatlēmuma 2009/948/TI par jurisdikcijas īstenošanas konfliktu novēršanu un atrisināšanu kriminālprocesā pieņemšanas, būtu jāuzlabojas koordinēšanai, saucot pie atbildības saistībā ar uzbrukumiem informācijas sistēmām.

Grozījums

(13) Ievērojami trūkumi un atšķirības dalībvalstu tiesību aktos uzbrukumu informācijas sistēmām jomā var kavēt organizētās noziedzības un terorisma apkarošanu un sarežģīt efektīvu policijas un tiesu iestāžu sadarbību. Modernās informācijas sistēmas ir starptautiskas, un tās nesaista robežas; *kas* nozīmē, ka uzbrukumiem šādām sistēmām ir pārrobežu raksturs, kas vēl vairāk izceļ steidzamo vajadzību ***Savienības līmenī tuvināt*** krimināltiesību aktus šajā jomā. ***Savienībai būtu arī jācenšas veidot plašāku starptautisko sadarbību datu tīklu drošības jomā, cieši sadarbojoties ar citām organizācijām, kurām ir līdzīgi mērķi, piemēram, ANO, NATO, Eiropas Padomi un EDSO, un iesaistot citus starptautisko procesu dalībniekus.*** Turklāt, pēc Padomes Pamatlēmuma 2009/948/TI par jurisdikcijas īstenošanas konfliktu novēršanu un atrisināšanu kriminālprocesā pieņemšanas, būtu jāuzlabojas koordinēšanai, saucot pie atbildības saistībā ar uzbrukumiem informācijas sistēmām.

Grozījums Nr. 14

Direktīvas priekšlikums 16. apsvērums

Komisijas ierosinātais teksts

(16) Direktīvā **ir** ievērotas pamattiesības un Eiropas Savienības Pamattiesību hartā atzītie principi, tostarp personas datu aizsardzība, vārda un informācijas brīvība, tiesības uz taisnīgu tiesu, nevainīguma prezumpcija un tiesības uz aizstāvību, kā arī tiesiskuma princips un nodarījuma un soda samērīguma princips krimināltiesībās. Šo tiesību un principu pilnīga ievērošana ir īpašs šīs direktīvas mērķis un tā ir attiecīgi jāīsteno.

Grozījums

(16) Direktīvā un **tās praktiskajā piemērošanā tiek** ievērotas pamattiesības, **it īpaši tiesības uz privāto dzīvi**, un Eiropas Savienības Pamattiesību hartā atzītie principi, tostarp personas datu aizsardzība, vārda un informācijas brīvība, tiesības uz taisnīgu tiesu, nevainīguma prezumpcija un tiesības uz aizstāvību, kā arī tiesiskuma princips un nodarījuma un soda samērīguma princips krimināltiesībās. Šo tiesību un principu pilnīga ievērošana ir īpašs šīs direktīvas mērķis un tā ir attiecīgi jāīsteno. **Šī direktīva nerada negatīvu ietekmi uz interneta brīvo un atvērto raksturu.**

Grozījums Nr. 15

**Direktīvas priekšlikums
16.a apsvērums (jauns)**

Komisijas ierosinātais teksts

Grozījums

(16a) Padomei un Komisijai sarunās un sadarbībā ar trešām valstīm būtu jāuzstāj uz minimālajām prasībām, kuru mērķis ir nepieļaut un apkarot kibernetizāciju un kibernetizācijas, kā arī minimālajiem informācijas sistēmu drošības standartiem.

Grozījums Nr. 16

**Direktīvas priekšlikums
16.b apsvērums (jauns)**

Komisijas ierosinātais teksts

Grozījums

(16b) Komisijai būtu jāizskata iespējas veicināt un atbalstīt trešo valstu centienus pilnveidot savas kibernetizācijas un kibernetizācijas spējas.

Grozījums Nr. 17

Direktīvas priekšlikums
14. pants – 2.a punkts (jauns)

Komisijas ierosinātais teksts

Grozījums

2.a Komisija palīdz dalībvalstīm veicināt interneta noturību un stabilitāti un veic citas darbības, kuru mērķis ir panākt informācijas drošību.

Grozījums Nr. 18

Direktīvas priekšlikums
14. pants – 2.b punkts (jauns)

Komisijas ierosinātais teksts

Grozījums

2.b Padome precizē Politikas un drošības komitejas un citu tās struktūru lomu saistībā ar rīcību iespējamo kiberuzbrukumu gadījumā.

Grozījums Nr. 19

Direktīvas priekšlikums
14. pants – 2.c punkts (jauns)

Komisijas ierosinātais teksts

Grozījums

2.c Dalībvalstis uzlabo ar kiberdrošību saistītas informācijas apmaiņu. Dalībvalstīm ar Komisijas atbalstu ir jācenšas uzturēt sakarus ar trešām valstīm, jo īpaši tām, no kurām visbiežāk notiek uzbrukumi.

Grozījums Nr. 20

Direktīvas priekšlikums
15. pants – 3. punkts

Komisijas ierosinātais teksts

3. Saskaņā ar šo pantu savāktos datus dalībvalstis nosūta Komisijai. Dalībvalstis nodrošina šo statistikas ziņojumu konsolidēta pārskata publicēšanu.

Grozījums

3. Saskaņā ar šo pantu savāktos datus dalībvalstis nosūta Komisijai. Dalībvalstis nodrošina šo statistikas ziņojumu konsolidēta pārskata **iesniegšanu Eiropas Parlamentam un** publicēšanu.

Grozījums Nr. 21

Direktīvas priekšlikums

15. pants – 3.a punkts (jauns)

Komisijas ierosinātais teksts

Grozījums

3.a Lai veicinātu Savienības iestāžu iniciatīvu, programmu un darbību integrēšanu un koordinēšanu, izveido Savienības kiberdrošības koordinatora amatu.

PROCEDŪRA

Virsraksts	Uzbrukumi informācijas sistēmām un Padomes Pamatlēmuma 2005/222/TI atcelšana
Atsauces	COM(2010)0517 – C7-0293/2010 – 2010/0273(COD)
Atbildīgā komiteja Datums, kad paziņoja plenārsēdē	LIBE 7.10.2010
Komiteja, kurai lūgts sniegt atzinumu Datums, kad paziņoja plenārsēdē	AFET 7.4.2011
Referente Iecelšanas datums	Kristiina Ojuland 29.3.2011
Pieņemšanas datums	22.11.2011
Galīgais balsojums	+: 38 -: 8 0: 0
Komitejas locekļi, kas bija klāt galīgajā balsošanā	Sir Robert Atkins, Frieda Brepoels, Elmar Brok, Marietta Giannakou, Andrzej Grzyb, Takis Hadjigeorgiou, Anna Ibrisagic, Othmar Karas, Ioannis Kasoulides, Tunne Kelam, Evgeni Kirilov, Andrey Kovatchev, Eduard Kukan, Krzysztof Lisek, Sabine Lösing, Ulrike Lunacek, Barry Madlener, Francisco José Millán Mon, Annemie Neyts-Uyttebroeck, Raimon Obiols, Justas Vincas Paleckis, Ioan Mircea Pașcu, Cristian Dan Preda, Libor Rouček, José Ignacio Salafranca Sánchez-Neyra, Jacek Saryusz-Wolski, Werner Schulz, Marek Siwiec, Charles Tannock, Inese Vaidere, Kristian Vigenin, Sir Graham Watson
Aizstājēji, kas bija klāt galīgajā balsošanā	Laima Liucija Andrikienė, Elena Băsescu, Tanja Fajon, Diogo Feio, Monica Luisa Macovei, Emilio Menéndez del Valle, György Schöpflin, Traian Ungureanu, Ivo Vajgl, Renate Weber, Janusz Władysław Zemke
Aizstājēji (187. panta 2. punkts), kas bija klāt galīgajā balsošanā	Luís Paulo Alves, Sylvie Guillaume, Vladimir Urutchev

11.11.2011

RŪPNIECĪBAS, PĒTNIECĪBAS UN ENERĢĒTIKAS KOMITEJAS ATZINUMS

Pilsoņu brīvību, tieslietu un iekšlietu komitejai

par priekšlikumu Eiropas Parlamenta un Padomes direktīvai par uzbrukumiem informācijas sistēmām un par Padomes Pamatlēmuma 2005/222/TI atcelšanu
(COM(2010)0517 – C7-0293/2010 – 2010/0273(COD))

Atzinumu sagatavoja: *Christian Ehler*

GROZĪJUMI

Rūpniecības, pētniecības un enerģētikas komiteja aicina par jautājumu atbildīgo Pilsoņu brīvību, tieslietu un iekšlietu komiteju ziņojumā iekļaut šādus grozījumus:

Grozījums Nr. 1

Direktīvas priekšlikums 1. apsvērums

Komisijas ierosinātais teksts

(1) Šīs direktīvas uzdevums ir tuvināt dalībvalstu krimināltiesību noteikumus par uzbrukumiem informācijas sistēmām un uzlabot tiesu un citu kompetento iestāžu, tostarp policijas un citu specializētu tiesībsardzības dienestu sadarbību.

Grozījums

(1) ***Veidojot daļu no Savienības vispārējās stratēģijas, kuras nolūks ir organizētās noziedzības apkarošana, datortīklu noturības palielināšana, īpaši svarīgas informācijas infrastruktūras aizsardzība un datu aizsardzība, šīs direktīvas uzdevums ir tuvināt dalībvalstu krimināltiesību noteikumus par uzbrukumiem informācijas sistēmām un uzlabot tiesu un citu kompetento iestāžu, tostarp policijas un citu specializētu tiesībsardzības dienestu, Komisijas,***

*Eiropas Tautaslietas, Eiropas Savienības un valstu
datorapdraudējumu reaģēšanas vienību
un Eiropas Tīklu un informācijas
drošības aģentūras sadarbību, lai
nodrošinātu kopēju un vispusīgu
Savienības pieeju.*

Grozījums Nr. 2

Direktīvas priekšlikums 1.a apsvērums (jauns)

Komisijas ierosinātais teksts

Grozījums

*(1a) Informācijas sistēmas ir būtisks
elements Eiropas politiskajā, sociālajā un
ekonomiskajā mijiedarbībā. Sabiedrība ir
ļoti atkarīga no šīm sistēmām, un šī
atkarība arvien palielinās. Šo sistēmu
netraucēta darbība un drošība Eiropā ir
vitāli svarīga iekšējā tirgus un
konkurētspējīgas un inovatīvas
ekonomikas attīstībai. Informācijas
sistēmas sniedz lielus ieguvumus, tomēr
vienlaikus, ņemot vērā to sarežģītību un
neaizsargātību pret dažāda veida
datornoziegumiem, tās ir saistītas ar
daudziem riskiem mūsu drošībai. Tāpēc
informācijas sistēmu drošība ir pastāvīgi
nozīmīgs jautājums, kam nepieciešami
efektīvi dalībvalstu un Savienības atbildes
pasākumi.*

Grozījums Nr. 3

Direktīvas priekšlikums 2. apsvērums

Komisijas ierosinātais teksts

Grozījums

*(2) Uzbrukumi informācijas sistēmām, jo
īpaši organizētas noziedzības **aktivitāšu
rezultātā, kļūst** arvien **draudīgāki**, un
pieaug bažas par iespējamiem
terroristiskiem vai politiski motivētiem
uzbrukumiem informācijas sistēmām, kas*

*(2) Uzbrukumi informācijas sistēmām **var
nākt no dažādiem avotiem, piemēram,
teroristiem**, organizētās noziedzības
**grupām, valstīm vai atsevišķām
privātpersonām**. Tie arvien **vairāk
apdraud informācijas sistēmu darbību***

ir dalībvalstu un Savienības īpaši svarīgās infrastruktūras sastāvdaļa. Tas apdraud drošākas informācijas sabiedrības un brīvības, drošības un tiesiskuma telpas izveidi, un tādējādi ir nepieciešama rīcība Eiropas Savienības līmenī.

gan Savienībā, gan pasaulē, un pieaug bažas par iespējamiem teroristiskiem vai politiski motivētiem uzbrukumiem informācijas sistēmām, kas ir dalībvalstu un Savienības īpaši svarīgās infrastruktūras sastāvdaļa. Šos draudus ievērojami veicina atsevišķu nodarījumu pārrobežu raksturs, relatīvi nelielais risks un izmaksas likumpārkāpējiem un milzīgie ieguvumi, ko ar šādiem uzbrukumiem var gūt, un kaitējums, ko ar tiem var nodarīt. Tas apdraud drošākas informācijas sabiedrības un brīvības, ***demokrātijas***, drošības un tiesiskuma telpas izveidi ***un traucē izveidot Eiropas digitālo iekšējo tirgu***, un tādējādi ir nepieciešama rīcība Eiropas Savienības līmenī, ***kā arī starptautiskā mērogā, piemēram, izmantojot Eiropas Padomes 2001. gada Konvenciju par kibernetiskajiem uzbrukumiem.***

Grozījums Nr. 4

Direktīvas priekšlikums 2.a apsvērums (jauns)

Komisijas ierosinātais teksts

Grozījums

(2a) Nesenie kibernetiskie uzbrukumi Eiropas tīkliem un informācijas sistēmām nodarīja būtisku kaitējumu Savienības ekonomikai un drošībai.

Pamatojums

Atsauce uz 2011. gada martā notikušajiem kibernetiskajiem uzbrukumiem Eiropas iestādēm, kā arī daudzajiem pārkāpumiem pret Eiropas Emisiju tirdzniecības sistēmām, kuru rezultātā tika nozagtas emisiju kvotas miljoniem EUR vērtībā.

Grozījums Nr. 5

Direktīvas priekšlikums 3. apsvērums

Komisijas ierosinātais teksts

(3) Ir vērojama tendence, ka plaša mēroga uzbrukumi informācijas sistēmām, kas ir īpaši svarīgas valstīm vai īpašām publiskā vai privātā sektora funkcijām, kļūst aizvien bīstamāki un atkārtojas aizvien biežāk. Šī tendenci pavada aizvien **modernāku rīku** attīstība, ko noziedznieki var izmantot dažādu kiberuzbrukumu izdarīšanai.

Grozījums

(3) Ir vērojama tendence, ka plaša mēroga uzbrukumi, **tostarp izklaidētie pakalpojumatteices uzbrukumi**, informācijas sistēmām, kas ir īpaši svarīgas **starptautiskajām organizācijām**, valstīm **un Savienībai** vai īpašām publiskā vai privātā sektora funkcijām, kļūst aizvien bīstamāki un atkārtojas aizvien biežāk. **Šādi uzbrukumi var izraisīt ievērojamu ekonomisku kaitējumu gan informācijas sistēmu darbības un sakaru pārtraukumu, gan komerciāli svarīgas konfidencialas informācijas vai citu datu zaudēšanas vai izmaiņšanas rezultātā. Īpaši apdraudēti var būt inovatīvi MVU, kuri ir atkarīgi no informācijas sistēmu pareizas darbības un pieejamības, bet kuriem ir mazākas iespējas novirzīt resursus informācijas drošībai.** Šo tendenci pavada **informācijas tehnoloģiju strauja attīstība un līdz ar to aizvien modernāki rīki**, ko noziedznieki var izmantot dažāda veida kiberuzbrukumu izdarīšanai, **daži no kuriem var nodarīt ievērojamu ekonomisku un sociālu kaitējumu.**

Grozījums Nr. 6

Direktīvas priekšlikums 4. apsvērums

Komisijas ierosinātais teksts

(4) Definīciju, jo īpaši informācijas sistēmu **un** datorizētu datu definīciju, vienotība šajā jomā ir **svarīga**, lai nodrošinātu saskaņotu pieeju šīs direktīvas piemērošanai dalībvalstīs.

Grozījums

(4) Definīciju, jo īpaši informācijas sistēmu, datorizētu datu **un pret informācijas sistēmām un datoru datiem izdarītu kriminālpārkāpumu** definīciju, vienotība šajā jomā ir **būtiska**, lai nodrošinātu saskaņotu **un vienvērtīgu** pieeju šīs direktīvas piemērošanai

dalībvalstīs.

Grozījums Nr. 7

Direktīvas priekšlikums

6. apsvērums

Komisijas ierosinātais teksts

(6) Dalībvalstīm jāparedz sodi par uzbrukumiem informācijas sistēmām. Šiem sodiem jābūt iedarbīgiem, samērīgiem un tādiem, kas attur no nodarījuma izdarīšanas.

Grozījums

(6) ***Papildus dalībvalstu, Savienības un privātā sektora pasākumiem, kuru mērķis ir palielināt informācijas sistēmu drošību un integritāti, novērst uzbrukumus un mazināt to ietekmi, dalībvalstīm jāparedz gan efektīvi pasākumi šādu uzbrukumu nepieļaušanai, gan saskaņoti sodi, kurus piemēro par uzbrukumiem informācijas sistēmām un kuri būtu jāpieņem kā daļa no plašākas valsts stratēģijas, kas vērsta uz šādu uzbrukumu nepieļaušanu un apkarošanu. Šiem sodiem jābūt iedarbīgiem, samērīgiem un tādiem, kas attur no nodarījuma izdarīšanas. Dalībvalstīs paredzēto sankciju un sodu konverģence ir nepieciešama, jo draudiem bieži vien ir pārrobežu raksturs, un tās mērķis ir mazināt atšķirības starp dalībvalstīm, kad nākas saskarties ar Savienībā veiktiem nodarījumiem.***

Grozījums Nr. 8

Direktīvas priekšlikums

6.a apsvērums (jauns)

Komisijas ierosinātais teksts

Grozījums

(6a) ***Dalībvalstīm, Savienībai un privātajam sektoram sadarbībā ar Eiropas Tīklu un informācijas drošības aģentūru būtu jāveic pasākumi, lai palielinātu informācijas sistēmu drošību un integritāti, novērstu uzbrukumus un mazinātu uzbrukumu ietekmi.***

Grozījums Nr. 9

Direktīvas priekšlikums 8. apsvērums

Komisijas ierosinātais teksts

(8) Padomes 2008. gada 27.–28. novembra secinājumos ir norādīts, ka dalībvalstīm un Komisijai būtu jāizstrādā jauna stratēģija, ņemot vērā 2001. gada Eiropas Padomes konvenciju par kibernetizāciju. Šī konvencija ir atsauces tiesiskais regulējums kibernetizācijas, tostarp uzbrukumu informācijas sistēmām, apkarošanai. **Šī direktīva ir izstrādāta, pamatojoties uz minēto konvenciju.**

Grozījums

(8) Padomes 2008. gada 27. un 28. novembra secinājumos ir norādīts, ka dalībvalstīm un Komisijai būtu jāizstrādā jauna stratēģija, ņemot vērā 2001. gada Eiropas Padomes konvenciju par kibernetizāciju. **Padomei un Komisijai būtu jānodrošina dalībvalstis, kuras vēl nav ratificējušas šo konvenciju, to izdarīt pēc iespējas drīzāk.** Šī konvencija ir atsauces tiesiskais regulējums kibernetizācijas, tostarp uzbrukumu informācijas sistēmām, apkarošanai. **Šajā direktīvā ir ņemti vērā minētās konvencijas attiecīgi noteikumi.**

Grozījums Nr. 10

Direktīvas priekšlikums 10. apsvērums

Komisijas ierosinātais teksts

(10) Direktīva nav domāta, lai paredzētu kriminālatbildību gadījumos, kad **nodarījumi ir izdarīti** bez krimināla nolūka, piemēram, **atļautu testēšana** vai informācijas sistēmas **aizsardzība**.

Grozījums

(10) **Direktīva neattiecas uz rīcību, kas veikta, lai nodrošinātu informācijas sistēmu drošību, piemēram, informācijas sistēmas noturību pret šajā direktīvā definētajām noziedzīgajām darbībām, vai lai sistēmas atbrīvotu no rīkiem, kas izmantoti šādām darbībām vai paredzēti tām.** Direktīva nav **arī** domāta, lai paredzētu kriminālatbildību gadījumos, kad **šajā direktīvā uzskaitīto noziegumu objektīvie kritēriji ir izpildīti, tomēr darbība ir izdarīta bez noziedzīga nodoma,** piemēram, **lai veiktu atļautu testēšanu vai aizsargātu** informācijas sistēmas.

Pamatojums

Ņemot vērā dažkārt neskaidro robežu starp ļaunprātīgu un neļāunprātīgu piekļuvi (piemēram, automātiskas atjaunināšanas gadījumos utt.), grozījuma mērķis ir precizēt, ka, piemēram,

pretvīrusu programmatūras vai vīrusu noņemšanas rīku darbība un inficētu ierīču karantīna ir pilnībā ārpus šīs direktīvas darbības jomas.

Grozījums Nr. 11

Direktīvas priekšlikums

11. apsvērums

Komisijas ierosinātais teksts

(11) Direktīvā uzsvērtā tādu informācijas apmaiņas tīklu nozīme kā G8 vai Eiropas Padomes kontaktpunktu tīkls, kas ir pieejami divdesmit četras stundas diennaktī un septiņas dienas nedēļā, lai nodrošinātu tūlītēju palīdzību ar informācijas sistēmām saistītu noziedzīgu nodarījumu izmeklēšanai vai tiesvedībai, vai noziedzīga nodarījuma pierādījumu vākšanai **elektroniskā formā**. Ņemot vērā, cik ātri iespējams veikt plaša mēroga uzbrukumus, dalībvalstīm būtu jāspēj nekavējoties sniegt atbildi uz šī kontaktpunktu tīkla steidzamiem lūgumiem. Šādam atbalstam būtu jāietver šādu pasākumu *atvieglošanu* vai *tiešu veikšanu*: **tehnisku konsultāciju** sniegšana, datu saglabāšana, pierādījumu vākšana, juridiskas informācijas sniegšana un aizdomās turēto atrašanās vietas noteikšana.

Grozījums

(11) Direktīvā uzsvērtā tādu informācijas apmaiņas tīklu nozīme kā G8 vai Eiropas Padomes kontaktpunktu tīkls, kas ir pieejami divdesmit četras stundas diennaktī un septiņas dienas nedēļā, lai nodrošinātu tūlītēju palīdzību ar informācijas sistēmām saistītu noziedzīgu nodarījumu izmeklēšanai vai tiesvedībai, vai noziedzīga nodarījuma **vai tā izdarīšanas nodoma** pierādījumu vākšanai. Ņemot vērā, cik ātri iespējams veikt plaša mēroga uzbrukumus, dalībvalstīm, **Savienībai un Eiropas Tīklu un informācijas drošības aģentūrai** būtu jāspēj nekavējoties **un efektīvi** sniegt atbildi uz šī kontaktpunktu tīkla steidzamiem lūgumiem. Šādam atbalstam būtu jāietver šādu pasākumu *atvieglošana* vai *tieša veikšana*: **tehniskas palīdzības** sniegšana, **tostarp par informācijas sistēmas funkcionalitātes atjaunošanu**, datu saglabāšana **saskaņā ar personas datu aizsardzības principiem**, pierādījumu vākšana, juridiskas informācijas sniegšana, **apdraudētās un/vai iegūtās informācijas identificēšana** un aizdomās turēto atrašanās vietas noteikšana **un identificēšana**.

Grozījums Nr. 12

Direktīvas priekšlikums

11.a apsvērums (jauns)

Komisijas ierosinātais teksts

Grozījums

(11a) Publisko iestāžu sadarbība ar

privāto sektoru un pilsonisko sabiedrību ir ļoti nozīmīga, novēršot un apkarojot uzbrukumus informācijas sistēmām. Ar šiem partneriem būtu jāizveido pastāvīgs dialogs, ņemot vērā plašo apjomu, kādā tie izmanto informācijas sistēmas, un kopīgu atbildību par šo sistēmu stabilu un pienācīgu darbību. Veidojot IT drošības kultūru, ir svarīgi uzlabot visu ieinteresēto pušu informētību par informācijas sistēmu izmantošanu.

Grozījums Nr. 13

Direktīvas priekšlikums 12. apsvērums

Komisijas ierosinātais teksts

(12) Ir nepieciešams vākt datus par nodarījumiem, kas minēti šajā direktīvā, lai iegūtu pilnīgāku pārskatu par šo problēmu Savienības līmenī, un tādējādi veicinātu efektīvāku atbildes mehānismu izstrādi. Šie dati turklāt palīdzēs *īpašajām* aģentūrām, kā Eiropols un Eiropas Tīklu un informācijas drošības aģentūra, labāk novērtēt kibernetizācijas izplatības apjomu un stāvokli tīklu un informācijas drošības jomā **Eiropā**.

Grozījums

(12) Ir nepieciešams vākt datus par nodarījumiem, kas minēti šajā direktīvā, lai iegūtu pilnīgāku pārskatu par šo problēmu Savienības līmenī, un tādējādi veicinātu efektīvāku atbildes mehānismu izstrādi. ***Dalībvalstīm ar Komisijas un Eiropas Tīklu un informācijas drošības aģentūras atbalstu ir jāuzlabo apmaiņa ar informāciju par uzbrukumiem informācijas sistēmām.*** Šie dati turklāt palīdzēs *specializētām struktūrām un aģentūrām, piemēram, dalībvalstu CERT vienībām un tādām* aģentūrām kā Eiropols un Eiropas Tīklu un informācijas drošības aģentūra, labāk novērtēt kibernetizācijas izplatības apjomu un stāvokli tīklu un informācijas drošības jomā ***Savienībā un palīdzēt dalībvalstīm pieņemt lēmumus par atbildes pasākumiem informācijas drošības incidentu gadījumā. Labākas zināšanas par pašreizējiem un turpmākajiem riskiem palīdzēs pieņemt atbilstošākus lēmumus, lai nepieļautu, novērstu vai ierobežotu kaitējumu, ko izraisa uzbrukumi informācijas sistēmām.***

Grozījums Nr. 14

Direktīvas priekšlikums 12.a apsvērums (jauns)

Komisijas ierosinātais teksts

Grozījums

(12a) Lai gan šai direktīvai ir jāatbilst stingrām prasībām attiecībā uz tiesisko noteiktību un krimināllikuma paredzamību, saskaņā ar šīs direktīvas noteikumiem par datu vākšanu, informācijas apmaiņu un Komisijas pienākumu regulāri ziņot par direktīvas piemērošanu un iesniegt vajadzīgos priekšlikumus ir arī jānodrošina elastīgs mehānisms, kas ļautu pielāgoties turpmākām norisēm, kā rezultātā šīs direktīvas darbības joma, iespējams, varētu kļūt plašāka. Šādas turpmākas norises ietver tādu tehnoloģiju attīstību, kuras nodrošina, piemēram, efektīvāku izpildi attiecībā uz uzbrukumiem informācijas sistēmām vai kuras veicina šādu uzbrukumu nepieļaušanu vai to seku mazināšanu.

Pamatojums

Sodu ieviešana ir atzinīgi vērtējama, tomēr vispusīga Savienības pieeja kibernetizācijas apkarošanai būtu jāīsteno, pievēršot uzmanību ne tikai tiesību aktu efektīvas izpildes nodrošināšanai, bet arī šādu noziedzīgu darbību nepieļaušanai paredzētu stratēģiju un instrumentu izstrādei.

Grozījums Nr. 15

Direktīvas priekšlikums 12.b apsvērums (jauns)

Komisijas ierosinātais teksts

Grozījums

(12b) Eiropas Tīklu un informācijas drošības aģentūrai būtu jāuzņemas stratēģiska loma koordinēt dalībvalstu un Savienības iestāžu centienus. Piemēram, Aģentūrai var uzdot uzraudzīt šo savstarpējo informācijas apmaiņu,

uzņemoties vienota kontaktpunkta un Savienības kiberdrošības incidentu reģistrētāja lomu. Tai var uzdot arī apkopot Savienības līmenī statistikas datus par šajā direktīvā minētajiem nodarījumiem un izmantot tos par pamatu ziņojumu sagatavošanai par informācijas sistēmu un datoru datu drošības stāvokli visā Savienībā.

Grozījums Nr. 16

Direktīvas priekšlikums 13. apsvērums

Komisijas ierosinātais teksts

(13) Ievērojami trūkumi un atšķirības dalībvalstu tiesību aktos uzbrukumu informācijas sistēmām jomā var kavēt organizētās noziedzības un terorisma apkarošanu un sarežģīt efektīvu policijas un tiesu iestāžu sadarbību. Modernās informācijas sistēmas ir starptautiskas un tās nesaista robežas, tas nozīmē, ka uzbrukumiem šādām sistēmām ir pārrobežu raksturs, kas vēl vairāk izceļ steidzamo vajadzību tuvināt krimināltiesību aktus šajā jomā. Turklāt, pēc Padomes Pamatlēmuma 2009/948/TI par jurisdikcijas īstenošanas konfliktu novēršanu un atrisināšanu kriminālprocesā pieņemšanas, būtu jāuzlabojas koordinēšanai, saucot pie atbildības saistībā ar uzbrukumiem informācijas sistēmām.

Grozījums

(13) Ievērojami trūkumi un atšķirības dalībvalstu tiesību aktos uzbrukumu informācijas sistēmām jomā var kavēt organizētās noziedzības un terorisma apkarošanu un sarežģīt efektīvu policijas un tiesu iestāžu sadarbību. Modernās informācijas sistēmas ir starptautiskas un tās nesaista robežas, tas nozīmē, ka uzbrukumiem šādām sistēmām ir pārrobežu raksturs, kas vēl vairāk izceļ steidzamo vajadzību ***rīkoties Savienības līmenī, lai tuvinātu valstu*** krimināltiesību aktus šajā jomā. ***Tāpat Savienībai būtu jācenšas panākt ciešāku starptautisko sadarbību tīklu un informācijas sistēmu drošības jomā, iesaistot visus attiecīgos starptautisko procesu dalībniekus.*** Turklāt, pēc Padomes Pamatlēmuma 2009/948/TI par jurisdikcijas īstenošanas konfliktu novēršanu un atrisināšanu kriminālprocesā pieņemšanas, būtu jāuzlabojas koordinēšanai, saucot pie atbildības saistībā ar uzbrukumiem informācijas sistēmām.

Grozījums Nr. 17

Direktīvas priekšlikums 1. pants – 1. punkts

Komisijas ierosinātais teksts

Ar šo direktīvu definē noziedzīgus nodarījumus uzbrukumu informācijas sistēmām jomā un izveido minimuma noteikumus attiecībā uz sodiem par šiem nodarījumiem. Tās mērķis ir arī ieviest vienotus noteikumus šādu uzbrukumu novēršanai un uzlabot sadarbību šajā jautājumā krimināltiesību jomā Eiropā.

Grozījums

Ar šo direktīvu definē noziedzīgus nodarījumus uzbrukumu informācijas sistēmām jomā un izveido **saskaņotus** minimuma noteikumus attiecībā uz sodiem par šiem nodarījumiem. Tās mērķis ir arī ieviest vienotus noteikumus šādu uzbrukumu novēršanai **un apkarošanai** un uzlabot sadarbību šajā jautājumā Eiropā, **it īpaši krimināltiesību jomā**.

Grozījums Nr. 18

Direktīvas priekšlikums
2. pants – d apakšpunkts

Komisijas ierosinātais teksts

d) „bez tiesībām” ir piekļuve vai iejaukšanās bez īpašnieka vai bez sistēmas vai tās daļas cita tiesību subjekta atļaujas, vai tāda piekļuve vai iejaukšanās, kas nav atļauta saskaņā ar attiecīgās valsts tiesību aktiem.

Grozījums

d) „bez tiesībām” ir piekļuve vai iejaukšanās bez īpašnieka vai bez sistēmas vai tās daļas cita tiesību subjekta atļaujas, vai tāda piekļuve vai iejaukšanās, kas nav atļauta saskaņā ar attiecīgiem valsts **vai Savienības** tiesību aktiem.

Grozījums Nr. 19

Direktīvas priekšlikums
7. pants – b apakšpunkts

Komisijas ierosinātais teksts

b) datorparole, pieejas kods vai līdzīgi dati, ar kuru palīdzību var piekļūt informācijas sistēmai vai tās daļai.

Grozījums

b) datorparole, pieejas kods, **digitāla vai fiziska drošības marķierierīce** vai līdzīgi dati, ar kuru palīdzību var piekļūt informācijas sistēmai vai tās daļai.

Grozījums Nr. 20

Direktīvas priekšlikums
8. pants – 1.a punkts (jauns)

Komisijas ierosinātais teksts

Grozījums

1.a Dalībvalstis nodrošina, ka identifikācijas datu neatļauta nosūtīšana citām personām ar mērķi veikt kādu no 3.–7. pantā minētajām darbībām ir uzskatāma par noziedzīgu nodarījumu.

Grozījums Nr. 21

Direktīvas priekšlikums 8. pants – 1.b punkts (jauns)

Komisijas ierosinātais teksts

Grozījums

1.b Dalībvalstis nodrošina, ka gadījumā, ja kādu no 3.–7. pantā minētajiem nodarījumiem veic persona, kurai amata pienākumu dēļ ir piekļuve informācijas sistēmu drošības sistēmām, to uzskata par atbildību pastiprinošu apstākli un par noziedzīgu nodarījumu.

Grozījums Nr. 22

Direktīvas priekšlikums 10. pants – 2. punkts

Komisijas ierosinātais teksts

Grozījums

2. Dalībvalstis veic nepieciešamos pasākumus, lai nodrošinātu, ka par 3.–6. pantā minētajiem nodarījumiem paredzētais maksimālais kriminālsods ir brīvības atņemšana uz vismaz pieciem gadiem, ja tie izdarīti, izmantojot rīku, kas domāts tādu uzbrukumu sākšanai, kas ietekmē ievērojamu skaitu informācijas sistēmu, vai rada ievērojamu kaitējumu, piemēram, sistēmas pakalpojumu pārtraukumu, finansiālas izmaksas vai personas datu zudumu.

2. Dalībvalstis veic nepieciešamos pasākumus, lai nodrošinātu, ka par 3.–6. pantā minētajiem nodarījumiem paredzētais maksimālais kriminālsods ir brīvības atņemšana uz vismaz pieciem gadiem, ja tie izdarīti, izmantojot rīku, kas domāts tādu uzbrukumu sākšanai, kas ietekmē ievērojamu skaitu informācijas sistēmu, vai rada ievērojamu kaitējumu, piemēram, sistēmas pakalpojumu pārtraukumu, finansiālas izmaksas vai personas datu ***vai jutīgas informācijas*** zudumu.

Grozījums Nr. 23

Direktīvas priekšlikums

13. pants – 1. punkts – c apakšpunkts

Komisijas ierosinātais teksts

c) nodarījums ir izdarīts par labu juridiskai personai, ***kuras galvenais birojs ir*** attiecīgās dalībvalsts teritorijā.

Grozījums

c) nodarījums ir izdarīts par labu juridiskai personai, ***kura reģistrēta*** attiecīgās dalībvalsts teritorijā.

Grozījums Nr. 24

Direktīvas priekšlikums

14. pants – 1. punkts

Komisijas ierosinātais teksts

1. Lai apmainītos ar informāciju par 3.–8. pantā minētajiem nodarījumiem, saskaņā ar datu aizsardzības noteikumiem dalībvalstis izmanto ***pastāvošo*** operatīvo kontaktpunktu tīklu, kas ir pieejams divdesmit četras stundas diennaktī un septiņas dienas nedēļā. Dalībvalstis nodrošina, ka ir ieviestas procedūras, lai tās varētu atbildēt uz steidzamiem lūgumiem maksimums astoņu stundu laikā. ***Šādā atbildē vismaz norāda, vai, kādā veidā un kad tiks sniegta palīdzības lūguma risinājums.***

Grozījums

1. Lai apmainītos ar informāciju par 3.–8. pantā minētajiem nodarījumiem, saskaņā ar datu aizsardzības noteikumiem dalībvalstis ***nodrošina, ka tām ir valsts operatīvais kontaktpunkts, un*** izmanto operatīvo kontaktpunktu tīklu, kas ir pieejams divdesmit četras stundas diennaktī un septiņas dienas nedēļā, ***un nosūta šādu informāciju arī Komisijai un Eiropas Tīklu un informācijas drošības aģentūrai.*** Dalībvalstis ***arī*** nodrošina, ka ir ieviestas procedūras, lai tās varētu atbildēt uz steidzamiem lūgumiem maksimums astoņu stundu laikā. ***Šāda atbilde ir efektīva, un tā attiecīgos gadījumos ietver šādu pasākumu veicināšanu vai tiešu īstenošanu: tehnisku konsultāciju sniegšana, tostarp par informācijas sistēmas funkcionalitātes atjaunošanu, datu saglabāšana saskaņā ar personas datu aizsardzības principiem, pierādījumu vākšana, juridiskas informācijas sniegšana un aizdomās turēto atrašanās vietas noteikšana un identifikēšana. Kontaktpunkti norāda veidu un termiņus, kādos sniegs atbildes uz palīdzības pieprasījumiem.***

Grozījums Nr. 25

Direktīvas priekšlikums

14. pants – 2. punkts

Komisijas ierosinātais teksts

2. Dalībvalstis informē Komisiju par to nozīmētajiem kontaktpunktiem informācijas apmaiņai par nodarījumiem, kas minēti 3.–8. pantā. Komisija nosūta šo informāciju citām dalībvalstīm.

Grozījums

2. Dalībvalstis informē Komisiju, ***Eiropas Tīklu un informācijas drošības aģentūru*** par to nozīmētajiem kontaktpunktiem informācijas apmaiņai par nodarījumiem, kas minēti 3.–8. pantā. Komisija nosūta šo informāciju citām dalībvalstīm.

Grozījums Nr. 26

Direktīvas priekšlikums

15. pants – 3. punkts

Komisijas ierosinātais teksts

3. Saskaņā ar šo pantu savāktos datus dalībvalstis nosūta Komisijai. ***Dalībvalstis*** nodrošina šo statistikas ziņojumu konsolidēta pārskata publicēšanu.

Grozījums

3. Saskaņā ar šo pantu savāktos datus dalībvalstis nosūta Komisijai, ***Eiropolam un Eiropas Tīklu un informācijas drošības aģentūrai un arī*** nodrošina šo statistikas ziņojumu ***periodiska*** konsolidēta pārskata publicēšanu.

Grozījums Nr. 27

Direktīvas priekšlikums

18. pants – 1. punkts

Komisijas ierosinātais teksts

1. [ČETRUS GADUS PĒC PIENĒMŠANAS] un turpmāk ik pēc trīs gadiem Komisija iesniedz Eiropas Parlamentam un Padomei ziņojumu par šīs direktīvas piemērošanu dalībvalstīs, tostarp visus vajadzīgos priekšlikumus.

Grozījums

1. [ČETRUS GADUS PĒC PIENĒMŠANAS] un turpmāk ik pēc trīs gadiem Komisija ***pēc apspriešanās ar visām attiecīgajām ieinteresētajām personām*** iesniedz Eiropas Parlamentam un Padomei ziņojumu par šīs direktīvas piemērošanu dalībvalstīs, tostarp visus vajadzīgos priekšlikumus. ***Katrā ziņojumā identificē un saistībā ar ikvienu vajadzīgo priekšlikumu ņem vērā tehniskos***

*risinājumus, kas ļauj Savienībā
nodrošināt efektīvāku izpildi attiecībā uz
uzbrukumiem informācijas sistēmām,
tostarp tehniskos risinājumus, kuri varētu
novērst šādus uzbrukumus vai mazināt to
sekas.*

Grozījums Nr. 28

Direktīvas priekšlikums 18. pants – 2. punkts

Komisijas ierosinātais teksts

2. Dalībvalstis nosūta Komisijai visu informāciju, kas ir vajadzīga, lai sagatavotu 1. punktā minēto ziņojumu. Šajā informācijā ietver sīku aprakstu par leģislatīvajiem un citiem pasākumiem, kas pieņemti īstenojot šo direktīvu.

Grozījums

2. Dalībvalstis ***un Eiropas Tīklu un informācijas drošības aģentūra*** nosūta Komisijai visu informāciju, kas ir vajadzīga, lai sagatavotu 1. punktā minēto ziņojumu. Šajā informācijā ietver sīku aprakstu par leģislatīvajiem un citiem pasākumiem, kas pieņemti īstenojot šo direktīvu.

PROCEDŪRA

Virsraksts	Uzbrukumi informācijas sistēmām un Padomes Pamatlēmuma 2005/222/TI atcelšana	
Atsauces	COM(2010)0517 – C7-0293/2010 – 2010/0273(COD)	
Atbildīgā komiteja Datums, kad paziņoja plenārsēdē	LIBE 7.10.2010	
Komitejas, kurām ir lūgts sniegt atzinumu Datums, kad paziņoja plenārsēdē	ITRE 7.10.2010	
Referents Iecelšanas datums	Christian Ehler 24.11.2010	
Izskatīšana komitejā	13.4.2011	6.10.2011
Pieņemšanas datums	10.11.2011	
Galīgais balsojums	+: 49 -: 0 0: 1	
Komitejas locekļi, kas bija klāt galīgajā balsošanā	Ivo Belet, Bendt Bendtsen, Maria Da Graça Carvalho, Giles Chichester, Pilar del Castillo Vera, Christian Ehler, Ioan Enciu, Adam Gierek, Norbert Glante, Robert Goebbels, Fiona Hall, Jacky Hénin, Kent Johansson, Romana Jordan Cizelj, Lena Kolarska-Bobińska, Béla Kovács, Philippe Lamberts, Bogdan Kazimierz Marcinkiewicz, Marisa Matias, Judith A. Merkies, Angelika Niebler, Jaroslav Paška, Aldo Patriciello, Anni Podimata, Miloslav Ransdorf, Herbert Reul, Michèle Rivasi, Jens Rohde, Paul Rübig, Amalia Sartori, Francisco Sosa Wagner, Konrad Szymański, Michael Theurer, Ioannis A. Tsoukalas, Claude Turmes, Niki Tzavela, Marita Ulvskog, Vladimir Urutchev, Adina-Ioana Vălean	
Aizstājēji, kas bija klāt galīgajā balsošanā	Antonio Cancian, Jolanta Emilia Hibner, Yannick Jadot, Ivailo Kalfin, Bernd Lange, Werner Langen, Markus Pieper, Mario Pirillo, Hannes Swoboda, Silvia-Adriana Țicău	
Aizstājēji (187. panta 2. punkts), kas bija klāt galīgajā balsošanā	Eider Gardiazábal Rubial	

PROCEDŪRA

Virsraksts	Uzbrukumi informācijas sistēmām un Padomes Pamatlēmuma 2005/222/TI atcelšana			
Atsauces	COM(2010)0517 – C7-0293/2010 – 2010/0273(COD)			
Datums, kad to iesniedza EP	30.9.2010			
Atbildīgā komiteja Datums, kad paziņoja plenārsēdē	LIBE 7.10.2010			
Komitejas, kurām lūgts sniegt atzinumu Datums, kad paziņoja plenārsēdē	AFET 7.4.2011	BUDG 7.10.2010	ITRE 7.10.2010	
Atzinumu nesniedza Lēmuma datums	BUDG 20.10.2010			
Referents(-i) Iecelšanas datums	Monika Hohlmeier 9.12.2010			
Izskatīšana komitejā	3.2.2011	25.5.2011	12.1.2012	28.2.2012
	27.3.2012	21.6.2012	6.6.2013	
Pieņemšanas datums	6.6.2013			
Galīgais balsojums	+: –: 0:	36 8 0		
Komitejas locekļi, kas bija klāt galīgajā balsošanā	Jan Philipp Albrecht, Emine Bozkurt, Arkadiusz Tomasz Bratkowski, Philip Claeys, Carlos Coelho, Ioan Enciu, Frank Engel, Cornelia Ernst, Kinga Gál, Kinga Göncz, Sylvie Guillaume, Sophia in 't Veld, Lívia Járóka, Teresa Jiménez-Becerril Barrio, Juan Fernando López Aguilar, Baroness Sarah Ludford, Monica Luisa Macovei, Svetoslav Hristov Malinov, Véronique Mathieu Houillon, Nuno Melo, Roberta Metsola, Antigoni Papadopolou, Georgios Papanikolaou, Jacek Protasiewicz, Carmen Romero López, Birgit Sippel, Csaba Sógor, Rui Tavares, Nils Torvalds, Wim van de Camp, Axel Voss, Josef Weidenholzer, Cecilia Wikström, Tatjana Ždanoka, Auke Zijlstra			
Aizstājēji, kas bija klāt galīgajā balsošanā	Dimitrios Droutsas, Mariya Gabriel, Evelyne Gebhardt, Stanimir Ilchev, Franziska Keller, Jean Lambert, Jan Mulder			
Aizstājēji (187. panta 2. punkts), kas bija klāt galīgajā balsošanā	Jens Nilsson, Sabine Verheyen			
Iesniegšanas datums	19.6.2013			