EIROPAS
KOMISIJA

Briselē, 4.10.2017.
COM(2017) 476 final

NOTE
This language version reflects the corrections done to the original EN version transmitted under COM(2017) 476 final of 13.9.2017 and retransmitted (with corrections) under COM(2017) 476 final/2 of 4.10.2017

KOMISIJAS PAZIŅOJUMS EIROPAS PARLAMENTAM UN PADOMEI

TID direktīvas potenciāla maksimāla izmantošana - kā efektīvi īstenot Direktīvu (ES) 2016/1148 par pasākumiem nolūkā panākt vienādi augsta līmeņa tīklu un informācijas sistēmu drošību visā Savienībā

Ievads

Direktīva (ES) 2016/1148 par tīklu un informācijas sistēmu drošību visā Savienībā[1] (turpmāk — "TID direktīva" vai "Direktīva"), kas pieņemta 2016. gada 6. jūlijā, ir pirmais ES horizontālais leģislatīvais akts, kurā iztirzāta kiberdrošības problemātika, un ir īsts pavērsiens kiberdrošības izturētspējas un sadarbības jomā Eiropā.

Direktīvai ir trīs galvenie mērķi:

- uzlabot valstu kiberdrošības spējas,
- iedibināt sadarbību ES mērogā un
- iedibināt risku pārvaldības un incidentu ziņošanas kultūru nozīmīgāko ekonomikas dalībnieku, īpaši pamatpakalpojumu sniedzēju (PS), kas nodrošina saimnieciskām un sabiedriskām norisēm nepieciešamos pakalpojumus, un digitālo pakalpojumu sniedzēju (DPS) vidū.

TID direktīva ir viens no pamata elementiem ES pretpasākumos arvien pieaugošajiem kiberdraudiem un problemātikai, kas pavada saimnieciskās un sabiedriskās dzīves digitalizāciju, un tās ieviešana tādējādi ir būtiska daļa no kiberdrošības paketes, ar ko nāca klajā 2017. gada 13. septembrī. Tomēr, kamēr TID direktīva vēl nav pilnībā transponēta visās ES dalībvalstīs, ES pretpasākumi nav pietiekami iedarbīgi. Tas tika atzīts par kritisku punktu arī Komisijas 2016. gada paziņojumā par Eiropas Kiberizturētspējas sistēmas nostiprināšanu[2].

TID direktīvas novitāte un tas, cik steidzami nepieciešami pretpasākumi strauji mainīgu kiberdraudu apstākļos, nozīmē, ka īpaša uzmanība jāvelta problēmām, ar ko sastopas visi aktori, kuru uzdevums ir savlaicīga un veiksmīga direktīvas transponēšana. Ņemot vērā transponēšanas termiņu (2018. gada 9. maijs) un termiņu pamatpakalpojumu sniedzēju identifikācijai (2018. gada 9. novembris), Komisija atbalsta dalībvalstu transponēšanas procesu un darbu sadarbības grupā.

Šī paziņojuma un tā pielikuma pamatā ir Komisijas sagatavošanās darbs un analīze, kas saistīta ar TID direktīvas līdzšinējo ieviešanu, Eiropas Savienības Tīklu un informācijas drošības aģentūras (ENISA) sniegto informāciju un pārrunām, kas notikušas ar dalībvalstīm direktīvas transponēšanas periodā, jo īpaši sadarbības grupā[3]. Šis paziņojums papildina līdzšinējos nozīmīgos centienus, konkrētāk:

- sadarbības grupas intensīvo darbu; sadarbības grupa ir vienojusies par darba plānu, kurā galvenā uzmanība pievērsta TID direktīvas transponēšanai un jo īpaši jautājumam par pamatpakalpojumu sniedzēju identifikāciju un to pienākumiem saistībā ar drošības prasībām un ziņošanu par incidentiem. Lai gan direktīva pieļauj,

[1] Eiropas Parlamenta un Padomes 2016. gada 6. jūlija Direktīva (ES) 2016/1148 par pasākumiem nolūkā panākt vienādi augsta līmeņa tīklu un informācijas sistēmu drošību visā Savienībā. Direktīva stājās spēkā 2016. gada 8. augustā.
[2] COM(2016) 410 *final*.
[3] dalībvalstu stratēģiskās sadarbības mehānismu saskaņā ar TID direktīvas 11. pantu.

ka, transponējot noteikumus par pamatpakalpojumu sniedzējiem, dalībvalstīm ir rīcības brīvība, dalībvalstis ir atzinušas, ka šajā sakarā svarīga ir saskaņota pieeja[4].

- datordrošības incidentu reaģēšanas vienību (*CSIRT*) tīkla izveide un tā ātra darbība saskaņā ar direktīvas 12. panta 1. punktu. Kopš tā laika šis tīkls ir sācis likt pamatus strukturētai operatīvajai sadarbībai Eiropas mērogā.

Gan rīcībpolitikas, gan operatīvajā līmenī, kuru šīs abas struktūras pārstāv, pilnīga dalībvalstu iesaiste ir būtiski svarīga, lai sasniegtu mērķi — vienādi augstu tīklu un informācijas sistēmu drošību Savienības līmenī.

Šis paziņojums un tā pielikums stiprinās šos centienus, apkopojot un salīdzinot direktīvas ieviešanai būtisku labāko praksi dalībvalstīs, sniedzot turpmākas vadlīnijas, kā būtu ieviešama direktīva, un sīkāk skaidrojot atsevišķus noteikumus. Virsmērķis ir palīdzēt dalībvalstīm panākt efektīvu un saskaņotu TID direktīvas ieviešanu visā ES.

Šo paziņojumu papildinās arī sagatavošanā esošā Komisijas Īstenošanas regula par tādu elementu un parametru precizēšanu, kas saistīti ar drošības prasībām un incidentu paziņošanas pienākumu digitālo pakalpojumu sniedzējiem saskaņā ar TID direktīvas 16. panta 8. punktu. Īstenošanas regula atvieglos Direktīvas ieviešanu saistībā ar digitālo pakalpojumu sniedzēju pienākumiem.[5].

Šajā paziņojumā izklāstīti galvenie secinājumi par to jautājumu analīzi, kas tiek uzskatīti par būtiskiem atskaites punktiem un iespējamu iedvesmas avotu, ja runājam par transponēšanu valstu tiesību aktos. Galvenā uzmanība pievērsta noteikumiem, kas attiecas uz dalībvalstu spējām un pienākumiem attiecībā uz direktīvas darbības jomā ietilpstošajiem subjektiem. Pielikumā sniegts sīkāks to jomu apskats, kurās Komisijas ieskatā būtu visvērtīgāk sniegt praktiskas transponēšanas vadlīnijas ar atsevišķu direktīvas noteikumu skaidrojumu un interpretāciju un iepazīstināt ar labo praksi un uzkrāto pieredzi līdzšinējā darbā ar direktīvu.

Virzība uz TID direktīvas efektīvu ieviešanu

TID direktīvas mērķis ir nodrošināt vienādi augsta līmeņa tīklu un informācijas sistēmu drošību ES ietvaros. Tas nozīmē, ka jāpalielina mūsu sabiedrībai un ekonomikai vitāli nepieciešamā interneta un privāto tīklu, un informācijas sistēmu drošība. Pirmais svarīgais elements šajā sakarā ir dalībvalstu gatavība, kas būtu jānodrošina ar valstu kiberdrošības stratēģiju ieviešanu, kā noteikts direktīvā, un ar CSIRT un valstu kompetento iestāžu darbu.

Valstu stratēģiju vispusīgums

[4] Sadarbības grupa šobrīd strādā pie vadlīniju dokumentiem, cita starpā par: kritērijiem, pēc kā nosaka pamatpakalpojuma sniedzēja svarīgumu saskaņā ar direktīvas 5. panta 2. punktu; apstākļiem, kādos pamatpakalpojumu sniedzējiem ir pienākums paziņot par incidentiem saskaņā ar direktīvas 14. panta 7. punktu; un drošības prasībām pamatpakalpojumu sniedzējiem saskaņā ar 14. panta 1. punktu un 14. panta 2. punktu;

[5] Īstenošanas regulas projekta sabiedriskā apspriešana: https://ec.europa.eu/info/law/better-regulation/have-your-say_en

Ir svarīgi, lai dalībvalstis izmantotu TID direktīvas transponēšanu kā iespēju izvērtēt savas nacionālās kiberdrošības stratēģijas, ņemot vērā to neaptvertās jomas, labo praksi un jaunos uzdevumus, kas iztirzāti pielikumā.

Lai gan direktīvā saprotamu iemeslu dēļ galvenā uzmanība pievērsta kritiski svarīgiem uzņēmumiem un pakalpojumiem, galvenais uzdevums ir visaptveroši un konsekventi nodrošināt ekonomikas un sabiedrības kiberdrošību kopumā, ņemot vērā arvien pieaugošo paļaušanos uz IKT. Tādējādi visaptverošu valstu stratēģiju pieņemšana, kas pārsniedz minimālās TID direktīvas prasības (t.i., aptverot vairāk nozaru un pakalpojumu, nekā uzskaitīts attiecīgi direktīvas II un III pielikumā), palielinātu vispārējo tīklu un informācijas sistēmu drošības līmeni.

Tā kā kiberdrošība joprojām ir relatīvi jauna un strauji augoša sabiedriskās kārtības joma, vairumā gadījumu nepieciešamas jaunas investīcijas, pat ja kopējā situācija valsts budžetā liek samazināt izdevumus un taupīt. Tāpēc direktīvas mērķus nebūs iespējams sasniegt, ja netiks pieņemti vērienīgi lēmumi par to, kā nodrošināt finanšu resursus un cilvēkresursus, kas ir nepieciešami efektīvai valstu stratēģiju ieviešanai, tostarp valstu kompetento iestāžu un CSIRT pietiekamam nodrošinājumam ar resursiem.

Īstenošanas un izpildes efektivitāte

Nepieciešamība izraudzīties attiecīgas valstu kompetentās iestādes un vienotos kontaktpunktus ir noteikta direktīvas 8. pantā, un tā ir svarīgs elements, lai nodrošinātu efektīvu TID direktīvas ieviešanu un pārrobežu sadarbību. Šajā jomā dalībvalstīs ir izveidojušās gan centralizētākas, gan decentralizētākas pieejas. Ja dalībvalstis pieņem decentralizētāku pieeju attiecībā uz valsts kompetento iestāžu izraudzīšanos, nozīmīga kļūst spēcīgas sadarbības iedibināšana starp vairākām iestādēm un vienoto kontaktpunktu (*skatīt 1. tabulu pielikuma 3.2. iedaļā*). Tas palielinās ieviešanas efektivitāti un atvieglos piemērošanu.

Iepriekš gūtā pieredze par informācijas kritiskās infrastruktūras aizsardzību (IKIA) varētu palīdzēt izveidot optimālu pārvaldības modeli dalībvalstīs, kas nodrošinātu gan efektīvu TID direktīvas ieviešanu nozarēs, gan vienotu horizontālu pieeju (*skatīt pielikuma 3.1. iedaļu*).

Valstu CSIRT spēju stiprināšana

Bez efektīvi strādājošiem un ar atbilstošiem resursiem nodrošinātiem valstu CSIRT visā ES, kā noteikts TID direktīvas 9. pantā, ES arī turpmāk būs pārāk ievainojama pret pārrobežu kiberdraudiem. Dalībvalstis tādēļ varētu apsvērt CSIRT darbības jomas paplašināšanu, tajā ietverot ne tikai tās nozares un pakalpojumus, kas iekļauti direktīvas darbības jomā (*skatīt pielikuma 3.3. iedaļu*). Tas ļautu valstu CSIRT nodrošināt operatīvu atbalstu tādu kiberincidentu gadījumā, kuri notiek uzņēmumos un organizācijās, kas neietilpst direktīvas darbības jomā, bet arī ir svarīgi sabiedrībai un ekonomikai. Turklāt dalībvalstis varētu pilnībā

izmantot papildu finansējuma iespējas, kuras piedāvā Eiropas infrastruktūras savienošanas (*CEF*) Kiberdrošības digitālo pakalpojumu infrastruktūras (*DSI*) programma, kas paredzēta, lai stiprinātu valstu CSIRT spējas un sadarbību to starpā (*skatīt pielikuma 3.5. iedaļu*).

PS identifikācijas procesa konsekvence

Saskaņā ar TID direktīvas 5. pantu dalībvalstīm ir pienākums līdz 2018. gada 9. novembrim identificēt vienības, kas tiks uzskatītas par pamatpakalpojumu sniedzējiem. Sakarā ar šo uzdevumu dalībvalstis varētu apsvērt šajā paziņojumā iekļauti definīciju un vadlīniju konsekventu izmantošanu, lai nodrošinātu, ka vienāda veida vienības, kam ir līdzīgas lomas iekšējā tirgū, konsekventi tiktu identificētas kā pamatpakalpojumu sniedzēji citās dalībvalstīs. Dalībvalstis arī varētu paplašināt TID direktīvas darbības jomu, iekļaujot tajā valsts pārvaldes iestādes, ņemot vērā to lomu sabiedrībā un ekonomikā kopumā (*skatīt pielikuma 2.1. un 4.1.3. iedaļu*).

Valstu pieeju maksimāla saskaņošana pamatpakalpojumu sniedzēju identificēšanā, īpaši ievērojot sadarbības grupas izstrādātās vadlīnijas (*skatīt pielikuma 4.1.2. iedaļu*), būtu ļoti noderīga, jo tā novestu pie direktīvas noteikumu saskaņotākas piemērošanas un tādējādi samazinātu tirgus sadrumstalotības risku. Ja pamatpakalpojumu sniedzēji sniedz pakalpojumus divās vai vairākās dalībvalstīs, ir svarīgi panākt vienošanos starp dalībvalstīm 5. panta 4. punkta apspriešanās procesa kontekstā par konsekventu vienību identificēšanu, (*skatīt pielikuma 4.1.7. iedaļu*), jo tas ļautu izvairīties no tā, ka vienai vienībai piemēro atšķirīgu regulējumu dažādu dalībvalstu jurisdikcijās.

Informācijas par PS identificēšanu iesniegšana Komisijai

Saskaņā ar 5. panta 7. punktu dalībvalstīm ir pienākums sniegt Komisijai informāciju par valstu pasākumiem, kas ļauj identificēt PS, pamatpakalpojumu sarakstu, identificēto PS skaitu un šo pakalpojumu sniedzēju nozīmīgumu nozarē. Turklāt dalībvalstīm ir pienākums informēt par robežvērtībām, ja tādas pastāv, kas tiek izmantotas identifikācijas procesā, lai noteiktu attiecīgo piedāvājuma līmeni vai konkrēta pakalpojumu sniedzēja nozīmīgumu pietiekama piegādes līmeņa uzturēšanai. Dalībvalstis varētu arī apsvērt identificēto pamatpakalpojumu sniedzēju sarakstu iesniegšanu Komisijai (ja nepieciešams — konfidenciāli), jo tas palīdzētu uzlabot Komisijas vērtējuma precizitāti un kvalitāti (*skatīt pielikuma 4.1.5. un 4.1.6. iedaļu*).
Saskaņotas pieejas prasībām PS par drošību un incidentu paziņošanu

Kas attiecas uz pienākumiem par drošības prasībām un incidentu paziņošanu pamatpakalpojumu sniedzējiem (14. panta 1. punkts, 2. punkts un 3. punkts), vienota pieeja drošības prasībām un incidentu paziņošanai nolūkā palīdzēt PS panākt atbilstību vairākās ES dalībvalstīs, veicinātu vienota tirgus efektu lielākajā iespējamajā mērā. Šeit svarīgs ir darbs pie vadlīniju dokumenta sadarbības grupā (*skatīt pielikuma 4.2. un 4.3. iedaļu*).

Ir ļoti iespējams, ka liela mēroga kiberincidenta gadījumā, kas skar vairākas dalībvalstis, par incidentu obligāti ziņos PS un DPS saskaņā ar 14. panta 3. punktu un 16. panta 3. punktu, vai cits subjekts, kas nav direktīvas darbības jomā, brīvprātīgi saskaņā ar 20. panta 1. punktu.

Saskaņā ar Komisijas Ieteikumu par koordinētu reaģēšanu uz plašapmēra kiberdrošības incidentiem un krīzēm dalībvalstīm būtu jāapsver savu nacionālo pieeju saskaņošana tā, lai tās varētu pēc iespējas drīzāk, pamatojoties uz šādiem paziņojumiem, sniegt attiecīgu informāciju citu iesaistīto dalībvalstu kompetentajām iestādēm vai CSIRT. Precīza un praktiski izmantojama informācija ir svarīga, lai samazinātu inficēšanās gadījumu skaitu vai novērstu ievainojamības, pirms tās tikušas ļaunprātīgi izmantotas.

Sadarbības garā un nolūkā panākt vislabākos rezultātus no TID direktīvas, Komisija plāno Eiropas infrastruktūras savienošanas instrumenta ietvaros paplašināt atbalstu visām ieinteresētajām personām saskaņā ar šiem tiesību aktiem. Līdz šim galvenā uzmanība bija pievērsta CSIRT spēju veidošanai un tādas platformas radīšanai, kas ir pamatā ātrai un efektīvai operatīvajai sadarbībai, tādējādi stiprinot CSIRT tīklu, bet tagad Komisija pētīs, kā finansēšana Eiropas infrastruktūras savienošanas instrumenta ietvaros varētu dot labumu valstu kompetentajām iestādēm, kā arī pamatpakalpojumu sniedzējiem un digitālo pakalpojumu sniedzējiem.

Secinājumi

Ņemot vērā, ka tuvojas TID direktīvas transponēšanas termiņš valstu tiesību aktos (2018. gada 9. maijs) un termiņš pamatpakalpojumu sniedzēju identificēšanai (2018. gada 9. novembris), dalībvalstīm būtu jāveic piemēroti pasākumi, lai nodrošinātu, ka TID direktīvas noteikumi un sadarbības modeļi ir vislabākie iespējamie ES mēroga instrumenti, ar kuriem var sasniegt vienādi augsta līmeņa tīklu un informācijas sistēmu drošību visā Savienībā. Komisija aicina dalībvalstis šajā procesā apsvērt attiecīgo informāciju, vadlīnijas un ieteikumus, kas ietvertas šajā paziņojumā.

Šo paziņojumu vēlāk var papildināt ar citiem pasākumiem, tostarp tiem, kas izriet no sadarbības grupas darba.