EIROPAS
KOMISIJA

Briselē, 13.9.2017.
SWD(2017) 501 final

KOMISIJAS DIENESTU DARBA DOKUMENTS

IETEKMES NOVĒRTĒJUMA KOPSAVILKUMS

Pavaddokuments dokumentam

Priekšlikums - EIROPAS PARLAMENTA UN PADOMES REGULA

par ENISA - "ES Kiberdrošības aģentūru" - un Regulas (ES) 526/2013 atcelšanu, un par informācijas un komunikācijas tehnoloģijas kiberdrošības sertifikāciju ("Kiberdrošības akts")

{COM(2017) 477 final}
{SWD(2017) 500 final}
{SWD(2017) 502 final}

A. VAJADZĪBA RĪKOTIES

Kāda ir problēma, un kāpēc tā ir problēma?

Ciparu tehnoloģijas un internets ir ES tautsaimniecības un sabiedrības stūrakmeņi. Tautsaimniecības svarīgākās nozares, kā transports, enerģētika, veselības aprūpe vai finanses, savā pamatdarbībā ir arvien vairāk atkarīgas no tīklu un informācijas sistēmām. Lietu internets savieno priekšmetus un cilvēkus, izmantojot sakaru tīklus. Jaunā situācija rada agrāk nebijušas iespējas – un arī vājās vietas. Kiberdrošības incidenti nudien sazēluši strauji. To sarežģītība, biežums un pamanāmā ietekme augs vēl vairāk – pamatpakalpojumu pieejamībā, demokrātiskajos procesos un citur.

Šajā sakarā ir apzinātas šādas savstarpēji saistītas problēmas:

- kiberdrošības politikas un pieeju nevienādība dalībvalstīs,
- kiberdrošības resursu un pieeju daudzgabalainība ES iestādēs, aģentūrās un struktūrās,
- nepietiekama pilsoņu un uzņēmumu izpratne par kiberapdraudējumu un nepietiekama informācija par nopērkamo IKT produktu un pakalpojumu drošības rekvizītiem – arvien lielākā valstu un nozaru sertifikācijas shēmu daudzveidība to vēl pasliktina.

Šīs problēmas iespaido ES vispārējo kibernoturību un iekšējā tirgus darbības efektivitāti.

Kas būtu jāpanāk?

Iniciatīvas konkrētie politiskie mērķi ir šādi:

1. pastiprināt dalībvalstu un uzņēmumu spējas un gatavību, it sevišķi kritiskās infrastruktūras aspektā,
2. uzlabot sadarbību un koordināciju starp dalībvalstīm un ES iestādēm, aģentūrām un struktūrām,
3. uzlabot ES līmeņa spējas papildināt dalībvalstu rīcību, it īpaši pārrobežu kiberkrīžu gadījumā,
4. uzlabot pilsoņu un uzņēmumu izpratni kiberdrošības jautājumos,
5. uzlabot IKT produktu un pakalpojumu kiberdrošības apliecinājuma vispārējo pārredzamību, lai vairotu uzticēšanos digitālajam vienotajam tirgum un digitālajai inovācijai,
6. nepieļaut ES sertifikācijas shēmu un ar tām saistīto drošības prasību un vērtēšanas kritēriju nevienādību dažādās dalībvalstīs un nozarēs.

Kāda ir ES līmeņa pasākumu pievienotā vērtība?

Tā kā tautsaimniecības un sabiedrības digitalizācijai un savstarpējai savienotībai ir globāls mērogs, arī problēmu loks sniedzas krietni aiz atsevišķas dalībvalsts teritorijas. Tādēļ ir vajadzīgs rīkoties Savienības līmenī. Analizējot attīstības scenārijus pašreizējos apstākļos, šķiet, ka Savienības kolektīvo kibernoturību nevar uzlabot dalībvalstu atsevišķie pasākumi un nevienāda pieeja kiberdrošībai, it īpaši izteiktā pārrobežu dimensija.

B. RISINĀJUMI

Ar kādiem risinājumiem var sasniegt izvirzītos mērķus? Vai kāds no risinājumiem ir vēlamāks par pārējiem?

Šajā ietekmes novērtējumā aplūkots konkrēts politisko risinājumu kopums, kas aptver Eiropas Savienības Tīklu un informācijas drošības aģentūru (*ENISA*) un IKT drošības sertifikāciju.

ENISA pārskatīšana

0 risinājums – pamatscenārijs. Šis risinājums saglabā pašreizējo stāvokli. *ENISA* pilnvaru termiņš tiktu pagarināts; Aģentūras mērķi un uzdevumi lielākoties nemainītos, taču tiktu ņemti vērā uzdevumi, kas *ENISA* tiks uzticēti ar turpmākiem ES tiesību aktiem (piemēram, ar TID direktīvu).

1. risinājums – *ENISA* pilnvaru termiņa notecēšana. (*ENISA* darbības izbeigšanās.) Šis risinājums nozīmētu *ENISA* darbības izbeigšanos tās pilnvaru termiņa beigās (2020. gada jūnijā) un, iespējams, kompetences/darbību pārdali ES un/vai valstu līmenī.

2. risinājums – reformēta *ENISA*. Šis risinājums attīstītu *ENISA* pašreizējās pilnvaras, lai tā varētu pieņemt selektīvas izmaiņas, ievērojot pārmaiņas kiberdrošības ainā. Aģentūra iegūtu pastāvīgas pilnvaras, kas būtu balstītas uz šādiem blokiem: ES politikas izstrādes un īstenošanas atbalste, spēju veidošana, zināšanas un informācija, ar tirgu saistīti uzdevumi, pētniecība un inovācija, operatīvā sadarbība un krīžu pārvarēšana.

3. risinājums – ES kiberdrošības aģentūra ar pilnīgām operatīvajām spējām. Šis risinājums nozīmē, ka *ENISA* tiktu reformēta, apvienojot trīs galvenās funkcijas: 1. politikas izstrādātāja/padomdevēja, 2. informācijas un lietpratības centrs, 3. datorapdraudējumu reaģēšanas vienība (*CERT*). Lielā mērā tas nozīmētu tādas pašas pilnvaru tvēruma izmaiņas kā 2. risinājumā. Tomēr tiktu noteikti papildu uzdevumi reaģēšanā uz incidentiem un krīzes pārvarēšanā, lai Aģentūra aptvertu visu kiberdrošības ciklu un nodarbotos ar kiberincidentu profilaksi, atklāšanu un reaģēšanu uz tiem.

Sertifikācija

0 risinājums – pamatscenārijs. Nedarīt neko. Šajā risinājumā Komisija nemainītu pašreizējo stāvokli un neveiktu nekādas politiskas vai leģislatīvas darbības.

1. risinājums – neleģislatīvi (ieteikumtiesību) pasākumi. Šajā risinājumā Komisija izmantotu nesaistošus politikas līdzekļus (piemēram, skaidrojošus paziņojumus, atbalstu ES mēroga pašregulācijas iniciatīvām un standartizācijai), lai uzlabotu pārredzamību un mazinātu sadrumstalotību.

2. risinājums – ES tiesību akts, kas uz visām dalībvalstīm attiecina *SOG-IS* nolīgumu. Šajā risinājumā Komisija ierosinātu tiesību aktu, kas dalību nolīgumā likumīgi papildinātu ar visām dalībvalstīm.

3. risinājums – vispārējs ES IKT kiberdrošības drošības sertifikācijas satvars. Šajā risinājumā tiktu izveidots Eiropas IKT drošības sertifikācijas satvars (ieskaitot ekspertu grupu no valsts iestāžu pārstāvjiem), iespēju robežās pamatojoties uz pastāvošajām IKT drošības sertificēšanas shēmām. Būtībā tāds satvars ļautu veidot ES sertifikācijas shēmas, kuras akceptētu visās dalībvalstīs.

Vēlamākais risinājums ir apvienot 2. risinājumu *ENISA* jautājumā un 3. risinājumu sertifikācijas jautājumā.

Kā atšķiras ieinteresētās personas? Kuru risinājumu kuras atbalsta?

Lielais vairums visu kategoriju ieinteresēto personu (dalībvalstis, nozares pārstāvji, ES iestādes, pētnieki), kas piedalījās apspriešanā, sliecas uz vēlamākā risinājuma pusi, jo ir par *ENISA* nostiprināšanu un Eiropas IKT drošības sertifikācijas satvara izveidi.

Sevišķi liela ir vienprātība par vajadzību (vismaz) pēc labi funkcionējošas ES aģentūras ar pastāvīgu pilnvarojumu, kurai piešķirti pietiekami resursi un tādas pilnvaras, kas ļauj pretoties tagadējiem un nākamiem izaicinājumiem kiberdrošībai. Plaša ir arī ieinteresēto personu piekrišana brīvprātīga, pielāgojama Eiropas satvara radīšanai.

Nozares pārstāvju vidū sertifikācijas risinājumu atbalsta uzņēmumi, kuriem jau tiek piemērotas sertifikācijas prasības un kuriem varētu būt ieguvums no ES mēroga mehānisma, kas balstītos uz sertifikātu savstarpēju atzīšanu. To atbalsta arī MVU, kas ciestu visvairāk, jo tiem jau tagad ir jāiztur un būtu jāiztur atšķirīgas sertifikācijas procedūras dažādās dalībvalstīs. Dažas dalībvalstis, īpaši tās, kam mazāk resursu, un daži nozares un ES iestāžu pārstāvji pauda pozitīvu viedokli arī par 3. variantu *ENISA* jautājumā.

C. VĒLAMĀKĀ RISINĀJUMA IETEKME

Kādu labumu dos vēlamākais risinājums (ja tāds ir, ja ne – galvenie risinājumi)?

Ar vēlamāko risinājumu ES savā rīcībā iegūtu aģentūru, kas koncentrētos uz dalībvalstu, ES iestāžu un uzņēmumu atbalstīšanu jomās, kur rastos vislielākā pievienotā vērtība. Tās ir: atbalsts TID direktīvas īstenošanā, politikas izstrāde un īstenošana, informācija, zināšanas un izpratne, pētniecība, operatīvā sadarbība un krīžu pārvarēšana, tirgus. *ENISA* īpaši atbalstītu ES politiku IKT drošības sertifikācijas jomā, nodrošinot Eiropas IKT drošības sertificēšanas satvara administratīvo uzturēšanu un tehnisko pārvaldību. Šāds satvars efektīvi ieviestu noteikumu kopumu par ES IKT drošības sertifikācijas pārvaldību, un tas veicinātu dalībvalstīs izdotu sertifikātu savstarpēju atzīšanu. Abu risinājumu apvienojums tiek uzskatīts par visefektīvāku šādu ES noteikto mērķu sasniegšanai: kiberdrošības spēju palielināšana, gatavība, sadarbība, izpratne, pārredzamība, tirgus sadrumstalotības novēršana. Šis risinājums arī vislabāk saskan ar politikas prioritātēm, kas sakņotas kiberdrošības stratēģijā un ar to saistītajā politikā (piem., TID direktīvā), un digitālā vienotā tirgus stratēģiju. Mērķus tas sasniegtu, prātīgi izlietojot resursus.

Kādas ir vēlamākā risinājuma (ja tāds ir; ja nav – galveno risinājumu) izmaksas?

Par spīti jauniegūtiem uzdevumiem, reformēta *ENISA* paliktu dinamiska organizācija. Vajadzīgais ES budžeta finansiālais ieguldījums būtu lielāks nekā tagad, taču joprojām mazāks nekā citām aģentūrām, kuras darbojas kritiski svarīgās jomās.

Eiropas IKT drošības sertificēšanas satvara izveide neprasītu nozarei jaunas sākumizmaksas (arī MVU ne). Gluži otrādi, rastos ievērojami ietaupījumi uzņēmumiem, kuri jau sertificē savu produktu vai vēlas drošības sertificēšanu, kas uzlabotu to spējas konkurēt visā pasaulē. No otras puses, tas nozīmētu zināmas budžeta saistības, kas nodrošinātu satvara uzturēšanu,

kuras galvenokārt rastos reformētas *ENISA* modelī, ciktāl ir runa par tehniskiem un administratīviem uzdevumiem.

Vai tiks ievērojami ietekmēti valstu budžeti un pārvalde?

Nē. Ar *ENISA* stiprināšanu saistītās izmaksas galvenokārt segtu ES budžets, bet dalībvalstis arī turpmāk varētu izdarīt brīvprātīgas finansiālas iemaksas Aģentūrai. Sertifikācijas sakarā valstu budžetu un pārvaldi attiecīgā brīdī galvenokārt ietekmētu sertifikācijas iestādes izveide.

Vai būs arī citāda nozīmīga ietekme?

Nebūs.

Kā ievērota proporcionalitāte?

Vēlamākajā risinājumā ietverti tikai līdzsvaroti pasākumi, kuri tiek uzskatīti par nepieciešamiem, lai visi būtiskie mērķi būtu sasniedzami, neuzliekot pārmērīgu nastu attiecīgajām ieinteresētajām personām. Tādā rakursā šī iniciatīva ir uzskatāma par proporcionalitātes principam atbilstošu.

D. TURPMĀKIE PASĀKUMI

Kad politika tiks pārskatīta?

Pašlaik ierosināts pirmo izvērtēšanu veikt piecus gadus pēc tiesību akta stāšanās spēkā. Pēc tam Komisija par izvērtējumu ziņos Eiropas Parlamentam un Padomei, vajadzības gadījumā pievienojot priekšlikumu to pārskatīt. Tālāk izvērtēšanai būs jānotiek ik pēc pieciem gadiem.