Európsky parlament
2019-2024

Výbor pre dopravu a cestovný ruch

2020/0359(COD)

14. 7. 2021

STANOVISKO

Výboru pre dopravu a cestovný ruch

pre Výbor pre priemysel, výskum a energetiku

k návrhu smernice Európskeho parlamentu a Rady o opatreniach na zabezpečenie vysokej spoločnej úrovne kybernetickej bezpečnosti v Únii a o zrušení smernice (EÚ) 2016/1148
(COM(2020)0823 – C9-0422/2020 – 2020/0359(COD))

Spravodajca výboru požiadaného o stanovisko: Jakop G. Dalunde

PA_Legam

STRUČNÉ ODÔVODNENIE

Odvetvie dopravy je čoraz zraniteľnejšie voči kybernetickým bezpečnostným hrozbám a je nimi stále viac zasiahnuté. Doprava má vzhľadom na svoje osobitné črty aj viacero výrazných zraniteľných miest. Hoci pozmeňujúce návrhy v tomto návrhu stanoviska sú všeobecnej povahy, navrhujú sa so zreteľom na tieto osobitosti. Návrhy sú relevantné pre dopravu z týchto dôvodov:

- doprava je často medzinárodným podnikaním, v ktorom mnohé subjekty patria do jurisdikcie viacerých členských štátov. Odvetvie dopravy je preto výrazne ovplyvnené veľkými rozdielmi v povinnostiach v oblasti riadenia a oznamovania kybernetickobezpečnostných rizík medzi členskými štátmi.

- Je závislé od bezpečnej výmeny údajov medzi jednotlivými aktérmi. Vzhľadom na prepojenú povahu logistiky by nedostatočná kybernetická bezpečnosť jedného subjektu mohla ohroziť celý systém a viesť k vážnym dôsledkom pre činnosť iných subjektov.

- Doprava je odvetvím s vysokým podielom ľudskej práce, a preto je obzvlášť citlivá na kybernetickobezpečnostné hrozby zamerané na zamestnancov.

Z týchto dôvodov sa pozmeňujúce návrhy zameriavajú na tieto témy: posúdenie miery rozdielov medzi členskými štátmi, pokiaľ ide o povinnosti v oblasti kybernetickej bezpečnosti, snaha o zosúladenie týchto povinností nelegislatívnymi prostriedkami, podpora odbornej prípravy zamestnancov a vedomostí o rizikách v oblasti kybernetickej bezpečnosti.

Okrem týchto všeobecných otázok treba poznamenať, že odvetvie dopravy čoraz viac využíva diaľkové snímače schopné pripojiť sa na internet pri poskytovaní služieb a že samotné vozidlá sú čoraz viac digitalizované. Hoci tieto zariadenia nie sú nevyhnutne súčasťou širších informačných systémov, môžu si vyžadovať osobitné posúdenia bezpečnosti.

POZMEŇUJÚCE NÁVRHY

Výbor pre dopravu a cestovný ruch vyzýva Výbor pre priemysel, výskum a energetiku, aby ako gestorský výbor vzal do úvahy tieto pozmeňujúce návrhy:

Pozmeňujúci návrh 1

Návrh smernice
Odôvodnenie 3

Text predložený Komisiou	*Pozmeňujúci návrh*
(3) Siete a informačné systémy sa spolu s rýchlou digitálnou transformáciou a prepojenosťou spoločnosti, a to aj pri cezhraničných výmenách, stali bežnou súčasťou každodenného života. Tento vývoj viedol k nárastu kybernetickobezpečnostných hrozieb a prináša nové výzvy, ktoré si vyžadujú prispôsobené, koordinované a inovatívne reakcie vo všetkých členských štátoch. Počet, rozsah, sofistikovanosť, frekvencia a vplyv kybernetickobezpečnostných incidentov sa zvyšujú a pre fungovanie sietí a informačných systémov predstavujú veľkú hrozbu. Vo výsledku môžu takéto incidenty zabraňovať realizácii ekonomických aktivít na vnútornom trhu, spôsobovať finančné straty, narúšať dôveru používateľov a spôsobovať značné škody spoločnosti a hospodárstvu Únie. Pripravenosť a účinnosť v oblasti kybernetickej bezpečnosti sú preto teraz pre riadne fungovanie vnútorného trhu dôležitejšie ako kedykoľvek predtým.	(3) Siete a informačné systémy sa spolu s rýchlou digitálnou transformáciou a prepojenosťou spoločnosti, a to aj pri cezhraničných výmenách, stali bežnou súčasťou každodenného života***, čo prispelo k rastu nových obchodných modelov a služieb, ako sú napríklad tie, ktoré sa týkajú gig ekonomiky, hospodárstva založeného na dopyte a hospodárstva platforiem vrátane cezhraničných výmen a koncepcie „mobilita ako služba“(MaaS)***. Tento vývoj viedol k nárastu kybernetickobezpečnostných hrozieb a prináša nové výzvy, ktoré si vyžadujú prispôsobené, koordinované a inovatívne reakcie vo všetkých členských štátoch. Počet, rozsah, sofistikovanosť, frekvencia a vplyv kybernetickobezpečnostných incidentov sa zvyšujú a pre fungovanie sietí a informačných systémov predstavujú veľkú hrozbu. Vo výsledku môžu takéto incidenty ***poškodiť blaho spoločnosti,*** zabraňovať realizácii ekonomických aktivít na vnútornom trhu, ***ako aj sociálnych činností,*** spôsobovať finančné straty, narúšať dôveru používateľov a ***pracovníkov,*** spôsobovať značné škody spoločnosti a hospodárstvu Únie ***alebo dokonca predstavovať teroristickú hrozbu***. Pripravenosť a účinnosť v oblasti kybernetickej bezpečnosti sú preto teraz pre ***ochranu základných práv a slobôd Únie a pre*** riadne fungovanie vnútorného trhu dôležitejšie ako kedykoľvek predtým. ***Kybernetická bezpečnosť je navyše kľúčovým faktorom, ktorý mnohým kritickým odvetviam, ako je doprava,***

	umožňuje úspešne zvládnuť digitálnu transformáciu a plne využiť hospodárske, sociálne a udržateľné prínosy digitalizácie.

Pozmeňujúci návrh 2

Návrh smernice
Odôvodnenie 9

Text predložený Komisiou	*Pozmeňujúci návrh*
(9) Táto smernica by sa však mala vzťahovať aj na malé subjekty alebo mikrosubjekty spĺňajúce určité kritériá, ktoré sú ukazovateľom kľúčovej úlohy pre hospodárstva alebo spoločnosti členských štátov alebo pre určité odvetvia či druhy služieb. Členské štáty by mali byť zodpovedné za vypracovanie zoznamu takýchto subjektov a mali by ho predložiť Komisii.	(9) Táto smernica by sa však mala vzťahovať aj na malé subjekty alebo mikrosubjekty spĺňajúce určité kritériá, ktoré sú ukazovateľom kľúčovej úlohy pre hospodárstva alebo spoločnosti členských štátov alebo pre určité odvetvia či druhy služieb. Členské štáty by mali byť zodpovedné za vypracovanie zoznamu takýchto subjektov a mali by ho predložiť Komisii. ***Tento postup by sa mal vykonávať s plným vedomím špecifickosti malých a stredných podnikov (MSP) a nemal by predstavovať nadmernú administratívnu záťaž pre MSP.***

Pozmeňujúci návrh 3

Návrh smernice
Odôvodnenie 10

Text predložený Komisiou	*Pozmeňujúci návrh*
(10) Komisia môže v spolupráci so skupinou pre spoluprácu vydať usmernenia o vykonávaní kritérií uplatniteľných na mikropodniky a malé podniky.	(10) Komisia môže v spolupráci so skupinou pre spoluprácu a relevantnými zainteresovanými stranami vydať usmernenia o vykonávaní kritérií uplatniteľných na mikropodniky a malé podniky. ***Komisia by takisto mala zabezpečiť, aby sa všetkým mikropodnikom a malým podnikom, ktoré patria do rozsahu pôsobnosti tejto smernice, poskytli primerané usmernenia. Komisia by v tejto súvislosti mala s podporou členských štátov poskytovať informácie mikropodnikom a malým podnikom. .***

Pozmeňujúci návrh 4

Návrh smernice
Odôvodnenie 12

Text predložený Komisiou	*Pozmeňujúci návrh*
(12) Právne predpisy a nástroje špecifické pre jednotlivé odvetvia môžu prispieť k zabezpečeniu vysokej úrovne kybernetickej bezpečnosti pri plnom zohľadnení špecifík a zložitosti týchto odvetví. Ak sa v právnom akte Únie špecifickom pre určité odvetvia vyžaduje, aby kľúčové alebo dôležité subjekty prijali opatrenia na riadenie kybernetickobezpečnostných rizík, alebo aby oznamovali incidenty alebo závažné kybernetické hrozby a táto povinnosť má mať aspoň rovnocenný účinok ako povinnosti stanovené v tejto smernici, mali by sa uplatňovať dané ustanovenia pre určité odvetvia vrátane ustanovení o dohľade a presadzovaní práva. Komisia môže vydať usmernenia týkajúce sa vykonávania lex specialis. Touto smernicou sa nebráni prijatiu ďalších odvetvových aktov Únie, ktoré sa zaoberajú opatreniami na riadenie kybernetickobezpečnostných rizík a oznamovaním incidentov. Touto smernicou nie sú dotknuté existujúce vykonávacie právomoci, ktoré boli Komisii udelené vo viacerých odvetviach vrátane dopravy a energetiky.	(12) Právne predpisy a nástroje špecifické pre jednotlivé odvetvia môžu prispieť k zabezpečeniu vysokej úrovne kybernetickej bezpečnosti pri plnom zohľadnení špecifík a zložitosti týchto odvetví. Ak sa v právnom akte Únie špecifickom pre určité odvetvia vyžaduje, aby kľúčové alebo dôležité subjekty prijali opatrenia na riadenie kybernetickobezpečnostných rizík, alebo aby oznamovali incidenty alebo závažné kybernetické hrozby a táto povinnosť má mať aspoň rovnocenný účinok ako povinnosti stanovené v tejto smernici, mali by sa uplatňovať dané ustanovenia pre určité odvetvia vrátane ustanovení o dohľade a presadzovaní práva. ***S cieľom predísť právnej neistote pri výklade a uplatňovaní tejto smernice by Komisia mala zabezpečiť súlad medzi touto smernicou a uplatniteľnými odvetvovými právnymi predpismi. Na tento účel by Komisia mala identifikovať duplicitu a nadbytočnosť v príslušných právnych predpisoch, regulačných požiadavkách alebo postupoch s cieľom odstrániť ich.*** Komisia môže vydať usmernenia týkajúce sa vykonávania lex specialis. Touto smernicou sa nebráni prijatiu ďalších odvetvových aktov Únie, ktoré sa zaoberajú opatreniami na riadenie kybernetickobezpečnostných rizík a oznamovaním incidentov. Touto smernicou nie sú dotknuté existujúce vykonávacie právomoci, ktoré boli Komisii udelené vo viacerých odvetviach vrátane dopravy a energetiky.

Pozmeňujúci návrh 5

Návrh smernice
Odôvodnenie 15 a (nové)

Text predložený Komisiou	*Pozmeňujúci návrh*
	(15a) Zvýšená digitalizácia kľúčových hospodárskych odvetví, ako je doprava, by sa mala uskutočňovať bezpečne a budovať s prirodzenou odolnosťou, aby sa zabezpečilo, že celý dodávateľský reťazec bude primerane reagovať na riziká a hrozby. Preto je potrebný koordinovaný prístup, ktorým sa zabezpečí minimálna úroveň bezpečnosti pripojených zariadení, najmä ak sa vyskytujú v odvetviach, ako je doprava, a ak sú súčasťou vozidiel a štandardne zavádzajú šifrovanie medzi koncovými zariadeniami.

Pozmeňujúci návrh 6

Návrh smernice
Odôvodnenie 17

Text predložený Komisiou	*Pozmeňujúci návrh*
(17) Vzhľadom na vznik inovačných technológií a nových obchodných modelov sa očakáva, že sa na trhu objavia nové modely zavádzania cloud computingu a služieb v reakcii na vyvíjajúce sa potreby zákazníkov. V tejto súvislosti sa služby cloud computingu môžu poskytovať vo vysoko distribuovanej forme, ešte bližšie k miestu, kde sa údaje generujú alebo zhromažďujú, čím sa prechádza od tradičného modelu k vysoko distribuovanému modelu („edge computing“).	(17) Vzhľadom na vznik inovačných technológií***, ako je umelá inteligencia,*** a nových obchodných modelov ***a nových modelov flexibilnej a diaľkovej práce*** sa očakáva, že sa na trhu objavia nové modely zavádzania cloud computingu a služieb v reakcii na vyvíjajúce sa potreby zákazníkov ***a podnikov***. V tejto súvislosti sa služby cloud computingu môžu poskytovať vo vysoko distribuovanej forme, ešte bližšie k miestu, kde sa údaje generujú alebo zhromažďujú, čím sa prechádza od tradičného modelu k vysoko distribuovanému modelu („edge computing“).

Pozmeňujúci návrh 7

Návrh smernice
Odôvodnenie 18 a (nové)

Text predložený Komisiou	*Pozmeňujúci návrh*
	(18a) Keďže zavedenie autonómnej mobility prinesie značné výhody, ale bude zahŕňať aj rôzne nové riziká, najmä pokiaľ ide o bezpečnosť cestnej premávky, kybernetickú bezpečnosť, práva duševného vlastníctva, otázky týkajúce sa ochrany údajov a prístupu k údajom, technickú infraštruktúru, normalizáciu a zamestnanosť, je nevyhnutné zabezpečiť, aby právny rámec Únie primerane reagoval na tieto výzvy a účinne riadil všetky riziká spojené s bezpečnosťou sietí a informačných systémov.

Pozmeňujúci návrh 8

Návrh smernice
Odôvodnenie 18 b (nové)

Text predložený Komisiou	*Pozmeňujúci návrh*
	(18b) Pandémia koronavírusu preukázala význam prípravy Únie na digitálne desaťročie a potrebu neustále zlepšovať kybernetickú odolnosť. Cieľom tejto smernice je preto stanoviť minimálne pravidlá týkajúce sa fungovania koordinovaného regulačného rámca s cieľom umožniť digitálnu transformáciu, inovácie v oblasti autonómnej dopravy, logistiky a riadenia dopravy vo všetkých druhoch dopravy a zlepšiť medzi používateľmi, najmä mikropodnikmi, MSP a startupmi, odolnosť proti kybernetickým útokom a schopnosť riešiť slabé miesta.

Pozmeňujúci návrh 9

Návrh smernice
Odôvodnenie 19

Text predložený Komisiou	*Pozmeňujúci návrh*
(19) Poskytovatelia poštových služieb v zmysle smernice Európskeho parlamentu a Rady 97/67/ES[18], ako aj poskytovatelia expresných a kuriérskych doručovacích služieb by mali podliehať tejto smernici, ak zabezpečujú aspoň jeden z krokov v reťazci poštového doručovania, a to najmä vyberanie, triedenie alebo distribúciu vrátane služieb zberu. Dopravné služby, ktoré sa nevykonávajú v spojení s jedným z týchto krokov, by nemali patriť do rozsahu poštových služieb.	(19) Poskytovatelia poštových služieb v zmysle smernice Európskeho parlamentu a Rady 97/67/ES[18], ako aj poskytovatelia expresných a kuriérskych doručovacích služieb by mali podliehať tejto smernici, ak zabezpečujú aspoň jeden z krokov v reťazci poštového doručovania, a to najmä vyberanie, triedenie alebo distribúciu vrátane služieb zberu. Dopravné ***alebo doručovacie*** služby, ktoré sa nevykonávajú v spojení s jedným z týchto krokov, by nemali patriť do rozsahu poštových služieb.
[18] Smernica Európskeho parlamentu a Rady 97/67/ES z 15. decembra 1997 o spoločných pravidlách rozvoja vnútorného trhu poštových služieb Spoločenstva a zlepšovaní kvality služieb (Ú. v. ES L 15, 21.1.1998, s. 14).	[18] Smernica Európskeho parlamentu a Rady 97/67/ES z 15. decembra 1997 o spoločných pravidlách rozvoja vnútorného trhu poštových služieb Spoločenstva a zlepšovaní kvality služieb (Ú. v. ES L 15, 21.1.1998, s. 14).

Pozmeňujúci návrh 10

Návrh smernice
Odôvodnenie 27 a (nové)

Text predložený Komisiou	*Pozmeňujúci návrh*
	(27a) Členské štáty by mali vo svojich vnútroštátnych stratégiách kybernetickej bezpečnosti riešiť osobitné kybernetickobezpečnostné potreby MSP, konkrétne nízku kybernetickú informovanosť, chýbajúcu bezpečnosť IT na diaľku, vysoké náklady na riešenia v oblasti kybernetickej bezpečnosti a zvýšenú mieru ohrozenia. Členské štáty by mali zriadiť kontaktné miesto pre kybernetickú bezpečnosť pre MSP, aby tieto mali prístup k relevantným informáciám, službám a usmerneniam.

Pozmeňujúci návrh 11

Návrh smernice
Odôvodnenie 33

Text predložený Komisiou	*Pozmeňujúci návrh*
(33) Pri vypracúvaní usmerňujúcich dokumentov by skupina pre spoluprácu mala dôsledne: zmapovať vnútroštátne riešenia a skúsenosti, posúdiť vplyv výstupov skupiny pre spoluprácu na vnútroštátne prístupy, diskutovať o výzvach pri vykonávaní a formulovať konkrétne odporúčania, ktorými sa má dosiahnuť lepšie vykonávanie existujúcich pravidiel.	(33) Pri vypracúvaní usmerňujúcich dokumentov by skupina pre spoluprácu mala dôsledne: zmapovať vnútroštátne riešenia a skúsenosti, posúdiť vplyv výstupov skupiny pre spoluprácu na vnútroštátne prístupy, diskutovať o výzvach pri vykonávaní a formulovať konkrétne odporúčania, ktorými sa má dosiahnuť lepšie vykonávanie existujúcich pravidiel, najmä pokiaľ ide o uľahčenie zosúladenia transpozície tejto smernice medzi členskými štátmi. ***Skupina pre spoluprácu by mala zmapovať aj vnútroštátne riešenia s cieľom podporiť kompatibilitu riešení v oblasti kybernetickej bezpečnosti uplatňovaných v každom konkrétnom sektore v celej Európe. Týka sa to najmä odvetví, ktoré majú medzinárodný a cezhraničný charakter, ako je doprava.***

Pozmeňujúci návrh 12

Návrh smernice
Odôvodnenie 34

Text predložený Komisiou	*Pozmeňujúci návrh*
(34) Skupina pre spoluprácu by mala zostať flexibilným fórom a mala by byť schopná reagovať na meniace sa a nové politické priority a výzvy a zároveň zohľadňovať dostupnosť zdrojov. Mala by organizovať pravidelné spoločné stretnutia s príslušnými súkromnými zainteresovanými stranami z celej Únie s cieľom prediskutovať činnosti skupiny a zhromažďovať informácie o nových politických výzvach. S cieľom posilniť spoluprácu na úrovni Únie by skupina mala zvážiť prizývanie orgánov a agentúr Únie zapojených do politiky v oblasti kybernetickej bezpečnosti, ako ***je*** Európske centrum boja proti počítačovej kriminalite	(34) Skupina pre spoluprácu by mala zostať flexibilným fórom a mala by byť schopná reagovať na meniace sa a nové politické priority a výzvy a zároveň zohľadňovať dostupnosť zdrojov. Mala by organizovať pravidelné spoločné stretnutia s príslušnými súkromnými zainteresovanými stranami z celej Únie s cieľom prediskutovať činnosti skupiny a zhromažďovať informácie o nových politických výzvach. S cieľom posilniť spoluprácu na úrovni Únie by skupina mala ***v prípade potreby*** zvážiť prizývanie orgánov a agentúr Únie zapojených do politiky v oblasti kybernetickej bezpečnosti, ako ***sú*** Európske centrum boja

(EC3), Agentúra Európskej únie pre bezpečnosť letectva (EASA) ***a*** Agentúra Európskej únie pre vesmírny program (EUSPA), k účasti na jej práci.	proti počítačovej kriminalite (EC3), ***Európske centrum odvetvových, technologických a výskumných kompetencií v oblasti kybernetickej bezpečnosti, agentúry Európskej únie zodpovedné za bezpečnú dopravu –*** Agentúra Európskej únie pre bezpečnosť letectva (EASA)***, Európska námorná bezpečnostná agentúra (EMSA), Železničná agentúra Európskej únie (ERA) –*** Agentúra Európskej únie pre vesmírny program (EUSPA) ***a akýkoľvek iný orgán a agentúra, ktorých odborné znalosti sú relevantné pre diskusie skupiny***, k účasti na jej práci.

Pozmeňujúci návrh 13

Návrh smernice
Odôvodnenie 37 a (nové)

Text predložený Komisiou	*Pozmeňujúci návrh*
	(37a) Príliš veľké rozdiely v povinnostiach v oblasti riadenia a oznamovania kybernetickobezpečnostných rizík pri transpozícii tejto smernice členskými štátmi by mohli ohroziť celkovú úroveň kybernetickej bezpečnosti v Únii. Agentúra ENISA by preto mala v spolupráci s Komisiou vo svojej dvojročnej správe o stave kybernetickej bezpečnosti v Únii posúdiť rozsah rozdielov v povinnostiach v oblasti riadenia a oznamovania kybernetickobezpečnostných rizík medzi členskými štátmi.

Pozmeňujúci návrh 14

Návrh smernice
Odôvodnenie 46 a (nové)

Text predložený Komisiou	*Pozmeňujúci návrh*
	(46a) V záujme zachovania a ochrany kritických dodávateľských reťazcov by sa pozornosť mala zamerať aj na ochranu

	celého dopravného a logistického reťazca. Dopravný a logistický reťazec pozostáva z veľkého počtu vzájomne prepojených aktérov a systémov, kde sa tovar prepravuje intermodálnym spôsobom leteckou, cestnou, železničnou, vnútrozemskou vodnou a námornou dopravou. Tento proces si vyžaduje rýchlu a spoľahlivú výmenu údajov medzi rôznymi článkami dopravného a logistického reťazca prostredníctvom rôznych rozhraní. Vzhľadom na prepojenosť rôznych článkov reťazca predstavuje nedostatočná kybernetická bezpečnosť riziko ohrozenia fungovania celého reťazca prostredníctvom domino efektov vyvolaných kybernetickým incidentom v jednej alebo viacerých častiach dopravného a logistického reťazca.

Pozmeňujúci návrh 15

Návrh smernice
Odôvodnenie 47

Text predložený Komisiou	*Pozmeňujúci návrh*
(47) Pri posudzovaní rizík v dodávateľskom reťazci by sa vzhľadom na vlastnosti dotknutého odvetvia mali zohľadniť technické a v relevantných prípadoch aj netechnické faktory vrátane tých, ktoré sú vymedzené v odporúčaní (EÚ) 2019/534, v celoeurópskom koordinovanom posúdení rizika bezpečnosti sietí 5G a v súbore nástrojov EÚ pre kybernetickú bezpečnosť 5G, na ktorom sa dohodla skupina pre spoluprácu. Pri určovaní dodávateľských reťazcov, ktoré by mali podliehať koordinovanému posúdeniu rizika, by sa mali zohľadniť tieto kritériá: i) rozsah, v akom kľúčové a dôležité subjekty využívajú konkrétne kritické služby, systémy alebo produkty IKT a spoliehajú sa na ne; ii) relevantnosť konkrétnych kritických služieb, systémov alebo produktov IKT pre vykonávanie kritických alebo citlivých funkcií vrátane	(47) Pri posudzovaní rizík v dodávateľskom reťazci by sa vzhľadom na vlastnosti dotknutého odvetvia mali zohľadniť technické a v relevantných prípadoch aj netechnické faktory vrátane tých, ktoré sú vymedzené v odporúčaní (EÚ) 2019/534, v celoeurópskom koordinovanom posúdení rizika bezpečnosti sietí 5G a v súbore nástrojov EÚ pre kybernetickú bezpečnosť 5G, na ktorom sa dohodla skupina pre spoluprácu. Pri určovaní dodávateľských reťazcov, ktoré by mali podliehať koordinovanému posúdeniu rizika, by sa mali zohľadniť tieto kritériá: i) rozsah, v akom kľúčové a dôležité subjekty využívajú konkrétne kritické služby, systémy alebo produkty IKT a spoliehajú sa na ne; ii) relevantnosť konkrétnych kritických služieb, systémov alebo produktov IKT pre vykonávanie kritických alebo citlivých funkcií vrátane

spracúvania osobných údajov; iii) dostupnosť alternatívnych služieb, systémov alebo produktov IKT; iv) odolnosť celkového dodávateľského reťazca služieb, systémov alebo produktov IKT ***voči*** rušivým udalostiam a v) v prípade vznikajúcich služieb, systémov alebo produktov IKT ich potenciálny budúci význam pre činnosti subjektov.	spracúvania osobných údajov; iii) dostupnosť alternatívnych služieb, systémov alebo produktov IKT; iv) odolnosť celkového dodávateľského reťazca služieb, systémov alebo produktov IKT ***proti*** rušivým udalostiam***; iva) rozsah, v akom sú špecifické kritické služby, systémy alebo produkty IKT, ktoré spotrebitelia priamo používajú, odolné a v súlade s prístupom ústretovým voči zákazníkom;*** a v) v prípade vznikajúcich služieb, systémov alebo produktov IKT ich potenciálny budúci význam pre činnosti subjektov.

Pozmeňujúci návrh 16

Návrh smernice
Odôvodnenie 55

Text predložený Komisiou	*Pozmeňujúci návrh*
(55) V tejto smernici sa stanovuje dvojfázový prístup k oznamovaniu incidentov s cieľom nájsť správnu rovnováhu medzi rýchlym oznamovaním na jednej strane, ktoré pomáha zmierniť potenciálne šírenie incidentov a umožňuje subjektom hľadať podporu, a na druhej strane podávaním podrobných správ, v ktorých sa čerpajú cenné ponaučenia z jednotlivých incidentov a časom sa zlepšuje odolnosť jednotlivých podnikov a celých odvetví voči kybernetickým hrozbám. Ak sa subjekty dozvedia o incidente, malo by sa od nich vyžadovať, aby do ***24*** hodín predložili prvotné oznámenie, po ktorom bude najneskôr do jedného mesiaca nasledovať konečná správa. Prvotné oznámenie by malo obsahovať len informácie, ktoré sú nevyhnutne potrebné na to, aby sa príslušné orgány dozvedeli o incidente a v prípade potreby umožnili subjektu požiadať o pomoc. V takomto oznámení by sa prípadne malo uviesť, či je incident pravdepodobne spôsobený protiprávnym alebo zlomyseľným konaním. Členské štáty by mali zabezpečiť, aby požiadavka	(55) V tejto smernici sa stanovuje dvojfázový prístup k oznamovaniu incidentov s cieľom nájsť správnu rovnováhu medzi rýchlym oznamovaním na jednej strane, ktoré pomáha zmierniť potenciálne šírenie incidentov a umožňuje subjektom hľadať podporu, a na druhej strane podávaním podrobných správ, v ktorých sa čerpajú cenné ponaučenia z jednotlivých incidentov a časom sa zlepšuje odolnosť jednotlivých podnikov a celých odvetví voči kybernetickým hrozbám. Ak sa subjekty dozvedia o incidente, malo by sa od nich vyžadovať, aby do ***36*** hodín predložili prvotné oznámenie, po ktorom bude najneskôr do jedného mesiaca nasledovať konečná správa. Prvotné oznámenie by malo obsahovať len informácie, ktoré sú nevyhnutne potrebné na to, aby sa príslušné orgány dozvedeli o incidente a v prípade potreby umožnili subjektu požiadať o pomoc. V takomto oznámení by sa prípadne malo uviesť, či je incident pravdepodobne spôsobený protiprávnym alebo zlomyseľným konaním. Členské štáty by mali zabezpečiť, aby požiadavka

na predloženie tohto prvotného oznámenia neodklonila zdroje oznamujúceho subjektu od činností súvisiacich s riešením incidentov, ktoré by sa mali uprednostniť. S cieľom zabrániť tomu, aby sa z dôvodu povinností oznamovania incidentov odkláňali zdroje od riešenia reakcie na incidenty alebo aby sa inak ohrozilo úsilie subjektov v tejto súvislosti, by členské štáty mali takisto stanoviť, že v riadne odôvodnených prípadoch a po dohode s príslušnými orgánmi alebo jednotkami CSIRT sa dotknutý subjekt môže odchýliť od lehoty ***24*** hodín pre prvotné oznámenie a od lehoty jedného mesiaca pre záverečnú správu.	na predloženie tohto prvotného oznámenia neodklonila zdroje oznamujúceho subjektu od činností súvisiacich s riešením incidentov, ktoré by sa mali uprednostniť. S cieľom zabrániť tomu, aby sa z dôvodu povinností oznamovania incidentov odkláňali zdroje od riešenia reakcie na incidenty alebo aby sa inak ohrozilo úsilie subjektov v tejto súvislosti, by členské štáty mali takisto stanoviť, že v riadne odôvodnených prípadoch a po dohode s príslušnými orgánmi alebo jednotkami CSIRT sa dotknutý subjekt môže odchýliť od lehoty ***36*** hodín pre prvotné oznámenie a od lehoty jedného mesiaca pre záverečnú správu.

Pozmeňujúci návrh 17

Návrh smernice
Článok 2 – odsek 2 – pododsek 2

Text predložený Komisiou	*Pozmeňujúci návrh*
Členské štáty vypracujú zoznam subjektov identifikovaných podľa písmen b) až f) a predložia ho Komisii do [6 mesiacov po uplynutí lehoty na transpozíciu]. Členské štáty zoznam pravidelne preskúmavajú, a to následne aspoň každé dva roky a v prípade potreby ho aktualizujú.	Členské štáty ***v úzkej spolupráci s príslušnými zainteresovanými stranami odvetvia*** vypracujú zoznam subjektov identifikovaných podľa písmen b) až f) a predložia ho Komisii do [6 mesiacov po uplynutí lehoty na transpozíciu]. Členské štáty zoznam pravidelne preskúmavajú, a to následne aspoň každé dva roky a v prípade potreby ho aktualizujú.

Pozmeňujúci návrh 18

Návrh smernice
Článok 2 – odsek 6

Text predložený Komisiou	*Pozmeňujúci návrh*
6. Ak sa v ustanoveniach právnych aktov Únie špecifických pre určité odvetvie vyžaduje, aby kľúčové alebo dôležité subjekty buď prijali opatrenia na riadenie kybernetickobezpečnostných rizík, alebo aby oznamovali incidenty alebo závažné	6. Ak sa v ustanoveniach právnych aktov Únie špecifických pre určité odvetvie vyžaduje, aby kľúčové alebo dôležité subjekty buď prijali opatrenia na riadenie kybernetickobezpečnostných rizík, alebo aby oznamovali incidenty alebo závažné

kybernetické hrozby, a ak majú tieto požiadavky aspoň rovnocenný účinok ako povinnosti stanovené v tejto smernici, príslušné ustanovenia tejto smernice vrátane ustanovení o dohľade a presadzovaní práva v kapitole VI sa neuplatňujú.	kybernetické hrozby, a ak majú tieto požiadavky aspoň rovnocenný účinok ako povinnosti stanovené v tejto smernici, ***a to aj pokiaľ ide o právomocí, mandát a funkcie príslušných dozorných orgánov,*** príslušné ustanovenia tejto smernice vrátane ustanovení o dohľade a presadzovaní práva v kapitole VI sa neuplatňujú.

Pozmeňujúci návrh 19

Návrh smernice
Článok 5 – odsek 2 – písmeno h

Text predložený Komisiou	*Pozmeňujúci návrh*
h) politiku zameranú na špecifické potreby MSP, najmä tých MSP, ktoré sú vylúčené z rozsahu pôsobnosti tejto smernice, v súvislosti s usmerneniami a podporou pri zlepšovaní ich odolnosti voči kybernetickobezpečnostným hrozbám.	h) politiku zameranú na špecifické potreby MSP, najmä tých MSP, ktoré sú vylúčené z rozsahu pôsobnosti tejto smernice, v súvislosti s usmerneniami***, poskytovaním potrebných a komplexných informácií*** a podporou pri zlepšovaní ich odolnosti voči kybernetickobezpečnostným hrozbám.

Pozmeňujúci návrh 20

Návrh smernice
Článok 12 – odsek 4 – písmeno a

Text predložený Komisiou	*Pozmeňujúci návrh*
a) poskytovanie usmernení príslušným orgánom v súvislosti s transpozíciou a vykonávaním tejto smernice;	a) poskytovanie usmernení príslušným orgánom v súvislosti s transpozíciou a vykonávaním tejto smernice ***s cieľom minimalizovať rozdiely medzi členskými štátmi v oblasti riadenia kybernetickobezpečnostných rizík a noriem oznamovacej povinnosti***;

Pozmeňujúci návrh 21

Návrh smernice
Článok 12 – odsek 4 – písmeno b a (nové)

Text predložený Komisiou	*Pozmeňujúci návrh*
	(ba) zmapovanie vnútroštátnych riešení s cieľom podporiť kompatibilitu riešení v oblasti kybernetickej bezpečnosti uplatňovaných v každom konkrétnom sektore v celej Únii;

Pozmeňujúci návrh 22

Návrh smernice
Článok 15 – odsek 1 – písmeno c a (nové)

Text predložený Komisiou	*Pozmeňujúci návrh*
	ca) miera rozdielnosti v povinnostiach v oblasti riadenia a oznamovania kybernetickobezpečnostných rizík medzi členskými štátmi a rozsah, v akom táto rozdielnosť ovplyvňuje spoločnú úroveň kybernetickej bezpečnosti v Únii.

Pozmeňujúci návrh 23

Návrh smernice
Článok 16 – odsek 1 – bod iii a (nový)

Text predložený Komisiou	*Pozmeňujúci návrh*
	iiia) odporúčania o tom, ako zlepšiť súdržnosť a právnu istotu pri výklade a uplatňovaní tejto smernice a uplatniteľných odvetvových právnych predpisov, s dôrazom na identifikáciu a odstránenie duplicity a nadbytočnosti v príslušných právnych predpisoch, regulačných požiadavkách alebo postupoch;

Pozmeňujúci návrh 24

Návrh smernice
Článok 18 – odsek 2 – písmeno b a (nové)

Text predložený Komisiou	*Pozmeňujúci návrh*
	ba) politiky, programy a postupy na

	zabezpečenie toho, aby zamestnanci mali primerané vedomosti na odhalenie kybernetickobezpečnostných rizík a praktické skúsenosti, ktoré spĺňajú vysoké normy kybernetickej bezpečnosti;

Pozmeňujúci návrh 25

Návrh smernice
Článok 18 – odsek 2 – písmeno e

Text predložený Komisiou	*Pozmeňujúci návrh*
e) bezpečnosť pri nadobúdaní, vývoji a údržbe ***sietí a informačných systémov vrátane riešenia*** zraniteľností a zverejňovania informácií o ***zraniteľnostiach***;	e) bezpečnosť ***sieťových a informačných systémov vrátane mobilných prvkov, ako sú vozidlá a diaľkové snímače,*** pri ***ich*** nadobúdaní, vývoji a údržbe***, ako aj riešení*** zraniteľností a zverejňovania informácií o ***nich***;

Pozmeňujúci návrh 26

Návrh smernice
Článok 18 – odsek 5

Text predložený Komisiou	*Pozmeňujúci návrh*
5. Komisia môže prijať ***vykonávacie*** akty s cieľom stanoviť technické a metodické špecifikácie prvkov uvedených v odseku 2. ***Pri vypracúvaní týchto aktov Komisia postupuje*** v súlade s ***postupom preskúmania, na ktorý sa odkazuje v článku 37 ods. 2,*** a v čo najväčšej možnej miere ***dodržiava*** medzinárodné a európske normy, ako aj príslušné technické špecifikácie.	5. Komisia môže prijať ***delegované*** akty s cieľom stanoviť technické a metodické špecifikácie prvkov uvedených v odseku 2. ***Delegované akty sa prijímajú*** v súlade s ***článkom 36*** a v čo najväčšej možnej miere ***sa dodržiavajú*** medzinárodné a európske normy, ako aj príslušné technické špecifikácie.

Pozmeňujúci návrh 27

Návrh smernice
Článok 18 – odsek 6 a (nový)

Text predložený Komisiou	*Pozmeňujúci návrh*
	6a. S cieľom zabezpečiť účinnú politiku a uľahčiť jej vykonávanie

	Komisia vedie konzultácie so základnými a dôležitými subjektmi, najmä pred prijatím delegovaných aktov uvedených v odsekoch 5 a 6.

Pozmeňujúci návrh 28

Návrh smernice
Článok 20 – odsek 4 – pododsek 1 – písmeno a

Text predložený Komisiou	*Pozmeňujúci návrh*
a) bez zbytočného odkladu a v každom prípade do ***24*** hodín od zistenia incidentu prvotné oznámenie, v ktorom sa prípadne uvedie, či incident pravdepodobne spôsobilo nezákonné alebo zlomyseľné konanie;	a) bez zbytočného odkladu a v každom prípade do ***36*** hodín od zistenia incidentu prvotné oznámenie, v ktorom sa prípadne uvedie, či incident pravdepodobne spôsobilo nezákonné alebo zlomyseľné konanie;

Pozmeňujúci návrh 29

Návrh smernice
Článok 20 – odsek 4 – pododsek 1 – písmeno c – bod iii

Text predložený Komisiou	*Pozmeňujúci návrh*
iii) uplatnené a prebiehajúce zmierňujúce opatrenia.	iii) uplatnené a prebiehajúce zmierňujúce opatrenia ***a ich výsledky***.

Pozmeňujúci návrh 30

Návrh smernice
Článok 20 – odsek 11

Text predložený Komisiou	*Pozmeňujúci návrh*
11. Komisia môže prijať ***vykonávacie*** akty, v ktorých bližšie určí druh informácií, formát a postup oznámenia predkladaného podľa odsekov 1 a 2. Komisia môže prijať aj vykonávacie akty s cieľom ďalej konkretizovať prípady, v ktorých sa incident považuje za závažný, ako sa uvádza v odseku 3. Uvedené vykonávacie akty sa prijmú v súlade s postupom preskúmania, na ktorý sa odkazuje v článku 37 ods. 2.	11. Komisia môže prijať ***delegované*** akty ***v súlade s článkom 36***, v ktorých bližšie určí druh informácií, formát a postup oznámenia predkladaného podľa odsekov 1 a 2 ***tohto článku***. Komisia môže prijať aj vykonávacie akty s cieľom ďalej konkretizovať prípady, v ktorých sa incident považuje za závažný, ako sa uvádza v odseku 3. Uvedené vykonávacie akty sa prijmú v súlade s postupom preskúmania, na ktorý sa odkazuje

v článku 37 ods. 2.

Pozmeňujúci návrh 31

Návrh smernice
Článok 21 – odsek 1

Text predložený Komisiou	*Pozmeňujúci návrh*
1. S cieľom preukázať súlad s určitými požiadavkami článku 18 ***môžu*** členské štáty ***vyžadovať, aby*** kľúčové a dôležité subjekty certifikovali určité produkty IKT, služby IKT a procesy IKT v rámci osobitných európskych systémov certifikácie kybernetickej bezpečnosti prijatých podľa článku 49 nariadenia (EÚ) 2019/881. ***Produkty, služby a procesy, ktoré podliehajú certifikácii, môže vytvoriť kľúčový*** alebo ***dôležitý subjekt alebo sa môžu obstarať od tretích strán***.	1. S cieľom preukázať súlad s určitými požiadavkami článku 18 členské štáty ***podporujú*** kľúčové a dôležité subjekty ***v tom, aby*** certifikovali určité produkty IKT, služby IKT a procesy IKT***, ktoré zabezpečil kľúčový alebo dôležitý subjekt alebo ktoré boli obstarané od tretích strán, a to*** v rámci osobitných európskych systémov certifikácie kybernetickej bezpečnosti prijatých podľa článku 49 nariadenia (EÚ) 2019/881 alebo ***v rámci podobných, medzinárodne uznávaných systémov certifikácie***.

Pozmeňujúci návrh 32

Návrh smernice
Článok 21 – odsek 1 a (nový)

Text predložený Komisiou	*Pozmeňujúci návrh*
	1a. Požiadavkami tejto smernice týkajúcimi sa certifikácie kybernetickej bezpečnosti nie je dotknutý článok 56 ods. 2 a 3 nariadenia (EÚ) 2019/881.

Pozmeňujúci návrh 33

Návrh smernice
Článok 21 – odsek 2

Text predložený Komisiou	*Pozmeňujúci návrh*
2. Komisia je splnomocnená prijímať delegované akty, v ktorých bližšie určí, od ktorých kategórií kľúčových subjektov sa vyžaduje získanie certifikátu a v rámci ktorých konkrétnych európskych systémov certifikácie kybernetickej bezpečnosti	***vypúšťa sa***

podľa odseku 1. Delegované akty sa prijímajú v súlade s článkom 36.

Pozmeňujúci návrh 34

Návrh smernice
Článok 21 – odsek 3

Text predložený Komisiou	*Pozmeňujúci návrh*
3. ***Komisia*** môže požiadať agentúru ENISA, aby vypracovala kandidátsky systém podľa ***článku 48 ods. 2*** nariadenia (EÚ) 2019/881 v prípadoch, keď nie je k dispozícii žiadny európsky systém certifikácie kybernetickej bezpečnosti na účely odseku 2.	3. ***S cieľom zvýšiť celkovú úroveň odolnosti v oblasti kybernetickej bezpečnosti*** môže ***Komisia*** požiadať agentúru ENISA, aby vypracovala kandidátsky systém podľa ***článkov 47 a 48*** nariadenia (EÚ) 2019/881 v prípadoch, keď nie je k dispozícii žiadny európsky systém certifikácie kybernetickej bezpečnosti na účely odseku 2. ***Takéto kandidátske systémy musia spĺňať požiadavky stanovené v článku 56 ods. 2 a článku 56 ods. 3 nariadenia (EÚ) 2019/881.***

POSTUP VÝBORU POŽIADANÉHO O STANOVISKO

Názov	Opatrenia na zabezpečenie vysokej spoločnej úrovne kybernetickej bezpečnosti v Únii a zrušenie smernice (EÚ) 2016/1148
Referenčné čísla	COM(2020)0823 – C9-0422/2020 – 2020/0359(COD)
Gestorský výbor dátum oznámenia na schôdzi	ITRE 21.1.2021
Výbor požiadaný o stanovisko dátum oznámenia na schôdzi	TRAN 21.1.2021
Spravodajca výboru požiadaného o stanovisko dátum vymenovania	Jakop G. Dalunde 3.2.2021
Dátum prijatia	12.7.2021
Výsledok záverečného hlasovania	+: 48 –: 0 0: 1
Poslanci prítomní na záverečnom hlasovaní	Magdalena Adamowicz, Andris Ameriks, Izaskun Bilbao Barandica, Paolo Borchia, Marco Campomenosi, Massimo Casanova, Ciarán Cuffe, Jakop G. Dalunde, Johan Danielsson, Karima Delli, Anna Deparnay-Grunenberg, Gheorghe Falcă, Giuseppe Ferrandino, Mario Furore, Søren Gade, Isabel García Muñoz, Elsi Katainen, Kateřina Konečná, Julie Lechanteux, Peter Lundgren, Benoît Lutgen, Elżbieta Katarzyna Łukacijewska, Marian-Jean Marinescu, Tilly Metz, Cláudia Monteiro de Aguiar, Caroline Nagtegaal, Jan-Christoph Oetjen, Philippe Olivier, João Pimenta Lopes, Rovana Plumb, Dominique Riquet, Dorien Rookmaker, Massimiliano Salini, Sven Schulze, Vera Tax, Barbara Thaler, Henna Virkkunen, Petar Vitanov, Elissavet Vozemberg-Vrionidi, Roberts Zīle, Kosma Złotowski
Náhradníci prítomní na záverečnom hlasovaní	Clare Daly, Nicola Danti, Angel Dzhambazki, Tomasz Frankowski, Michael Gahler, Maria Grapini, Alessandra Moretti, Marianne Vind

ZÁVEREČNÉ HLASOVANIE PODĽA MIEN VO VÝBORE POŽIADANOM O STANOVISKO

48	+
ECR	Angel Dzhambazki, Peter Lundgren, Roberts Zīle, Kosma Złotowski
ID	Paolo Borchia, Marco Campomenosi, Massimo Casanova, Julie Lechanteux, Philippe Olivier
NI	Mario Furore, Dorien Rookmaker
PPE	Magdalena Adamowicz, Gheorghe Falcă, Tomasz Frankowski, Michael Gahler, Elżbieta Katarzyna Łukacijewska, Benoît Lutgen, Marian-Jean Marinescu, Cláudia Monteiro de Aguiar, Massimiliano Salini, Sven Schulze, Barbara Thaler, Henna Virkkunen, Elissavet Vozemberg-Vrionidi
Renew	Izaskun Bilbao Barandica, Nicola Danti, Søren Gade, Elsi Katainen, Caroline Nagtegaal, Jan-Christoph Oetjen, Dominique Riquet
S&D	Andris Ameriks, Johan Danielsson, Giuseppe Ferrandino, Isabel García Muñoz, Maria Grapini, Alessandra Moretti, Rovana Plumb, Vera Tax, Marianne Vind, Petar Vitanov
The Left	Clare Daly, Kateřina Konečná
Verts/ALE	Ciarán Cuffe, Jakop G. Dalunde, Karima Delli, Anna Deparnay-Grunenberg, Tilly Metz

0	-

1	0
The Left	João Pimenta Lopes

Vysvetlenie použitých znakov:
+ : za
- : proti
0 : zdržali sa hlasovania