EURÓPSKY PARLAMENT 2009 - 2014

Výbor pre občianske slobody, spravodlivosť a vnútorné veci

2013/0027(COD)

15.1.2014

STANOVISKO

Výboru pre občianske slobody, spravodlivosť a vnútorné veci

pre Výbor pre vnútorný trh a ochranu spotrebiteľa

k návrhu smernice Európskeho parlamentu a Rady o opatreniach na zabezpečenie vysokej úrovne sieťovej a informačnej bezpečnosti v Únii (COM(2013)0048 – C7-0035/2013 – 2013/0027(COD))

Spravodajca výboru požiadaného o stanovisko: Carl Schlyter

PA_Legam

STRUČNÉ ODÔVODNENIE

Cieľom návrhu je dosiahnuť vysokú úroveň sieťovej a informačnej bezpečnosti v Únii. Spravodajca súhlasí s cieľmi, ktoré sú predmetom návrhu, a odporúča zmeny, ktorými sa zvýši právna istota a posilnia sa záruky a ochrana osôb a ich súkromia. Cieľom je zabezpečiť jednotlivcom kontrolu nad ich osobnými údajmi, zaistiť, aby dôverovali digitálnemu prostrediu, vytvoriť kultúru riadenia rizík a zlepšiť výmenu informácií medzi súkromnými a verejnými subjektmi.

Navrhované zmeny sa týkajú lepšieho odkazovania na právne predpisy v oblasti ochrany údajov, vyjasnenia, že súčasťou „kritickej infraštruktúry“ by nemali byť sociálne siete a obchody s aplikáciami (pozri zmenený zoznam v prílohe II), a zabezpečenia dodržiavania proporcionality tým, že sa zvýrazňuje civilný rozmer: väčšina narušení a bežných zlyhaní systémov nie je totiž spôsobená úmyselnými kybernetickými útokmi teroristov, zločincov alebo zahraničných špiónov, ale je dôsledkom neúmyselných ľudských chýb a prirodzených príčin. Je mimoriadne dôležité, aby EÚ rozlišovala medzi uplatňovaním navrhovaných právnych predpisov a akoukoľvek militarizáciou tejto otázky a aby vzala do úvahy rámec globálneho digitálneho trhu a vylúčila ciele bezpečnostného priemyslu a priemyslu v oblasti dozoru a sledovania.

Veľmi dôležitou otázkou, ktorá nie je naďalej vyriešená, je vzťah medzi navrhovaným systémom a systémom oznamovania, navrhnutým vo všeobecnom nariadení o ochrane údajov, a ich účinná koexistencia. Ide o jeden z dôvodov prečo zdôrazňujeme skutočnosť, že akýkoľvek právny predpis EÚ v oblasti kybernetickej bezpečnosti by mal byť prijatý až po prijatí všeobecného nariadenia o ochrane údajov, a nie predtým. Zvážiť by sa navyše mali reálne finančné a administratívne dôsledky vrátane celkových spoločenských nákladov, a nielen náklady na vykonanie oznámenia. Softvérové spoločnosti, ktoré vykonávajú programovanie nedbanlivým spôsobom a šetria náklady tým, že vystavujú svojich zákazníkov riziku, nemôžu byť vo všetkých prípadoch chránení ustanoveniami v podmienkach používania, ktoré ich zbavujú akejkoľvek zodpovednosti za nefungovanie ich softvéru. Aby zabezpečili primeranú úroveň bezpečnosti, nato potrebujú motiváciu. Vyjasniť by sa napokon mali základné pojmy, ktoré by sa nemali ponechať členským štátom na voľný výklad (napríklad pojmy „verejné správy“ a „významný vplyv“ a presné vymedzenie pojmu „kybernetická kriminalita“).

POZMEŇUJÚCE NÁVRHY

Výbor pre občianske slobody, spravodlivosť a vnútorné veci vyzýva Výbor pre vnútorný trh a ochranu spotrebiteľa, aby ako gestorský výbor zaradil do svojej správy tieto pozmeňujúce návrhy:

Pozmeňujúci návrh 1

Návrh smernice
Odôvodnenie 1

Text predložený Komisiou	*Pozmeňujúci návrh*
(1) Siete a informačné systémy a služby hrajú v spoločnosti základnú úlohu. Ich spoľahlivosť a bezpečnosť sú nevyhnutné pre ekonomické činnosti ***a*** sociálne zabezpečenie ***a najmä pre fungovanie vnútorného trhu***.	(1) Siete a informačné systémy a služby hrajú v spoločnosti základnú úlohu. Ich spoľahlivosť a bezpečnosť sú nevyhnutné pre ekonomické činnosti***,*** sociálne zabezpečenie ***a komunikáciu a styky medzi osobami, organizáciami občianskej spoločnosti a podnikmi, ako aj pre ochranu a rešpektovanie súkromia a osobných údajov***.

Pozmeňujúci návrh 2

Návrh smernice
Odôvodnenie 2

Text predložený Komisiou	*Pozmeňujúci návrh*
(2) Rozsah a frekvencia úmyselných alebo náhodných bezpečnostných incidentov sa zvyšuje a predstavuje významnú hrozbu pre fungovanie sietí a informačných systémov. Takéto incidenty môžu zabraňovať napredovaniu ekonomických činností, spôsobovať značné finančné straty, narúšať dôveru používateľa a spôsobovať značné škody v hospodárstve Únie.	(2) Rozsah a frekvencia úmyselných alebo náhodných bezpečnostných incidentov sa zvyšuje a predstavuje významnú hrozbu pre fungovanie sietí a informačných systémov. Takéto incidenty môžu zabraňovať napredovaniu ekonomických činností, spôsobovať značné finančné straty, narúšať dôveru používateľa a spôsobovať značné škody v hospodárstve Únie. ***Čoraz viac sa uznáva skutočnosť, že systémy kontroly sú zraniteľné voči počítačovým útokom z rôznych zdrojov vrátane nepriateľských vlád, teroristických skupín a iných zlomyseľných votrelcov. Inteligentné útoky a koordinované útoky by mohli mať vážne dôsledky pre stabilitu, výkonnosť a hospodárnosť infraštruktúry.***

Pozmeňujúci návrh 3

Návrh smernice
Odôvodnenie 3

Text predložený Komisiou	*Pozmeňujúci návrh*
(3) Digitálne informačné systémy, a najmä internet, ako komunikačné nástroje bez hraníc hrajú významnú úlohu pri uľahčení pohybu tovaru, služieb a osôb cez hranice. Z dôvodu tohto nadnárodného charakteru môže vážne narušenie týchto systémov v jednom členskom štáte ovplyvniť aj ďalšie členské štáty a Úniu ako celok. Preto je na riadne fungovanie vnútorného trhu nevyhnutná odolnosť a stabilita sietí a informačných systémov.	(3) Digitálne informačné systémy, a najmä internet, ako komunikačné nástroje bez hraníc hrajú významnú úlohu pri uľahčení pohybu tovaru, služieb a osôb cez hranice. Z dôvodu tohto nadnárodného charakteru môže vážne narušenie týchto systémov v jednom členskom štáte ovplyvniť aj ďalšie členské štáty a Úniu ako celok. Preto je na riadne fungovanie vnútorného trhu ***a komunikácie a stykov medzi osobami, organizáciami občianskej spoločnosti a podnikmi*** nevyhnutná odolnosť a stabilita sietí a informačných systémov.

Pozmeňujúci návrh 4

Návrh smernice
Odôvodnenie 3 a (nové)

Text predložený Komisiou	*Pozmeňujúci návrh*
	(3a) Keďže k poruchám systémov naďalej väčšinou dochádza z neúmyselných dôvodov – ide napríklad o prirodzené príčiny alebo ľudskú chybu, infraštruktúra by mala byť odolná voči úmyselným i neúmyselným narušeniam a prevádzkovatelia kritickej infraštruktúry by mali navrhovať také systémy, ktoré by boli odolné a fungovali by aj vtedy, ak by zlyhali ostatné systémy mimo ich kontroly.

Pozmeňujúci návrh 5

Návrh smernice
Odôvodnenie 6 a (nové)

Text predložený Komisiou	*Pozmeňujúci návrh*
	(6a) Je životne dôležité uznávať neistotu, ktorá je bytostne vlastná zložitým systémom, o ktoré sa opierame. To si

	vyžaduje lepšie spoločné chápanie toho, čo je kriticky dôležité, medzi tými, ktorí organizáciu chránia, a tými, ktorí určujú jej strategické smerovanie.

Pozmeňujúci návrh 6

Návrh smernice
Odôvodnenie 8

Text predložený Komisiou	*Pozmeňujúci návrh*
(8) Ustanovenia tejto smernice by sa mali uplatňovať bez toho, aby bola dotknutá možnosť členských štátov prijať potrebné opatrenia na zabezpečenie ochrany svojich základných bezpečnostných záujmov, chrániť verejný poriadok a verejnú bezpečnosť a povoliť vyšetrovanie a odhaľovanie trestných činov, ako aj prenasledovanie ich páchateľov. V súlade s článkom 346 ZFEÚ žiaden členský štát nie je povinný poskytovať informácie, ktorých sprístupnenie odporuje podľa jeho názoru základným záujmom jeho bezpečnosti.	(8) Ustanovenia tejto smernice by sa mali uplatňovať bez toho, aby bola dotknutá možnosť členských štátov prijať potrebné opatrenia na zabezpečenie ochrany svojich základných bezpečnostných záujmov, chrániť verejný poriadok a verejnú bezpečnosť a povoliť vyšetrovanie a odhaľovanie trestných činov, ako aj prenasledovanie ich páchateľov ***pod podmienkou, že by ich nemali používať ako zámienku na nesplnenie svojich všeobecnejších povinností týkajúcich sa dodržiavania ochrany súkromia a osobných údajov***. V súlade s článkom 346 ZFEÚ žiaden členský štát nie je povinný poskytovať informácie, ktorých sprístupnenie odporuje podľa jeho názoru základným záujmom jeho bezpečnosti.

Pozmeňujúci návrh 7

Návrh smernice
Odôvodnenie 9

Text predložený Komisiou	*Pozmeňujúci návrh*
(9) S cieľom dosiahnuť a udržiavať spoločnú vysokú úroveň bezpečnosti sietí a informačných systémov by mal mať každý členský štát vnútroštátnu stratégiu pre bezpečnosť sietí a informácií, v ktorej by boli vymedzené strategické ciele a konkrétne opatrenia, ktoré sa majú v rámci tejto politiky vykonať. Na vnútroštátnej	(9) S cieľom dosiahnuť a udržiavať spoločnú vysokú úroveň bezpečnosti sietí a informačných systémov by mal mať každý členský štát vnútroštátnu stratégiu pre bezpečnosť sietí a informácií, v ktorej by boli vymedzené strategické ciele a konkrétne opatrenia, ktoré sa majú v rámci tejto politiky vykonať. Na vnútroštátnej

úrovni je treba vytvoriť plány spolupráce v oblasti bezpečnosti sietí a informácií, ktoré by boli v súlade so základnými požiadavkami, s cieľom dosiahnuť úroveň možností reakcie, ktoré v prípade incidentov umožnia účinnú a efektívnu spoluprácu ako na vnútroštátnej úrovni, tak aj na úrovni Únie.

úrovni je treba vytvoriť plány spolupráce v oblasti bezpečnosti sietí a informácií, ktoré by boli v súlade so základnými požiadavkami, s cieľom dosiahnuť úroveň možností reakcie, ktoré v prípade incidentov umožnia účinnú a efektívnu spoluprácu ako na vnútroštátnej úrovni, tak aj na úrovni Únie***, pričom je nutné rešpektovať a chrániť súkromie a osobné údaje***.

Pozmeňujúci návrh 8

Návrh smernice
Odôvodnenie 10

Text predložený Komisiou	*Pozmeňujúci návrh*
(10) S cieľom umožniť účinné vykonávanie ustanovení prijatých podľa tejto smernice by sa mal v každom členskom štáte zriadiť alebo určiť orgán, ktorý bude zodpovedný za koordináciu otázok v oblasti bezpečnosti sietí a informácií a ktorý bude pôsobiť ako ústredný bod pre cezhraničnú spoluprácu na úrovni Únie. Tieto orgány by mali dostať primerané technické, finančné a ľudské zdroje, aby mohli efektívnym a účinným spôsobom vykonávať úlohy, ktoré im budú pridelené, a tak dosahovať ciele tejto smernice.	(10) S cieľom umožniť účinné vykonávanie ustanovení prijatých podľa tejto smernice by sa mal v každom členskom štáte zriadiť alebo určiť ***príslušný vnútroštátny*** orgán ***podliehajúci civilnej kontrole s plnohodnotným demokratickým dohľadom nad transparentnosťou jeho činností***, ktorý bude zodpovedný za koordináciu otázok v oblasti bezpečnosti sietí a informácií a ktorý bude pôsobiť ako ústredný bod pre cezhraničnú spoluprácu na úrovni Únie. Tieto orgány by mali dostať primerané technické, finančné a ľudské zdroje, aby mohli efektívnym a účinným spôsobom vykonávať úlohy, ktoré im budú pridelené, a tak dosahovať ciele tejto smernice.

Pozmeňujúci návrh 9

Návrh smernice
Odôvodnenie 14 a (nové)

Text predložený Komisiou	*Pozmeňujúci návrh*
	(14a) Viacero odvetví používa vo svojom počítačovom prostredí tzv. cloudové služby, napríklad IT služby prevádzkujúce

	kriticky dôležitú infraštruktúru. Dostatočné bezpečnostné opatrenia musia zaistiť dôvernosť, integritu a dostupnosť údajov v cloude. S prevádzkovaním hostiteľských infraštruktúrnych služieb a uchovávaním citlivých údajov v cloudovom prostredí súvisia požiadavky na bezpečnosť a odolnosť, ktoré súčasné cloudové služby nedokážu riešiť. Preto je potrebné zabezpečiť, aby cloudové počítačové prostredie dokázalo zabezpečiť odbornú ochranu citlivých údajov kriticky dôležitej infraštruktúry.

Pozmeňujúci návrh 10

Návrh smernice
Odôvodnenie 15

Text predložený Komisiou	*Pozmeňujúci návrh*
(15) Keďže väčšinu sietí a informačných systémov prevádzkujú súkromní operátori, je nevyhnutná spolupráca medzi verejným a súkromným sektorom. Účastníci trhu by mali byť povzbudzovaní, aby sa s cieľom zabezpečiť bezpečnosť sietí a informácií snažili aj o vytvorenie svojich vlastných neformálnych mechanizmov spolupráce. Mali by spolupracovať aj s verejným sektorom a vymieňať si informácie a osvedčené postupy ***výmenou za*** prevádzkovú podporu v prípade incidentov.	(15) Keďže väčšinu sietí a informačných systémov prevádzkujú súkromní operátori, je nevyhnutná spolupráca medzi verejným a súkromným sektorom. Účastníci trhu by mali byť povzbudzovaní, aby sa s cieľom zabezpečiť bezpečnosť sietí a informácií snažili aj o vytvorenie svojich vlastných neformálnych mechanizmov spolupráce. Mali by spolupracovať aj s verejným sektorom a vymieňať si ***navzájom*** informácie a osvedčené postupy***, ako aj vzájomnú*** prevádzkovú podporu ***podľa potreby*** v prípade incidentov.

Pozmeňujúci návrh 11

Návrh smernice
Odôvodnenie 15 a (nové)

Text predložený Komisiou	*Pozmeňujúci návrh*
	(15a) Už existujúce vnútroštátne mechanizmy spolupráce medzi verejnými a súkromnými subjektmi by sa mali v rámci možnosti dodržiavať v plnej miere

	a v súlade so smernicou 95/46/ES a ustanovenia uvedené v tejto smernici by nemali takéto zavedené systémy spolupráce oslabovať.

Pozmeňujúci návrh 12

Návrh smernice
Odôvodnenie 16

Text predložený Komisiou	*Pozmeňujúci návrh*
(16) S cieľom zabezpečiť transparentnosť a riadne informovať občanov EÚ a účastníkov trhu, príslušné orgány by mali zriadiť spoločnú internetovú stránku, na ktorej by uverejňovali informácie o incidentoch a rizikách, ktoré nemajú dôverný charakter.	(16) S cieľom zabezpečiť transparentnosť a riadne informovať občanov EÚ a účastníkov trhu, príslušné orgány by mali zriadiť spoločnú internetovú stránku, na ktorej by ***urýchlene*** uverejňovali ***komplexné*** informácie o incidentoch a rizikách, ktoré nemajú dôverný charakter.

Pozmeňujúci návrh 13

Návrh smernice
Odôvodnenie 21

Text predložený Komisiou	*Pozmeňujúci návrh*
(21) Vzhľadom na globálny charakter problémov bezpečnosti sietí a informácií je potrebná užšia medzinárodná spolupráca s cieľom zlepšiť bezpečnostné normy a výmenu informácií a presadzovať spoločný globálny prístup k otázke bezpečnosti sietí a informácií.	(21) Vzhľadom na globálny charakter problémov bezpečnosti sietí a informácií je potrebná užšia medzinárodná spolupráca s cieľom zlepšiť bezpečnostné normy a výmenu informácií a presadzovať spoločný globálny prístup k otázke bezpečnosti sietí a informácií***, pričom štáty, s ktorými sa táto spolupráca plánuje, musia mať k dispozícii nástroje na kontrolu a ochranu osobných údajov zaručujúce rovnakú bezpečnosť ako nástroje EÚ***.

Pozmeňujúci návrh 14

Návrh smernice
Odôvodnenie 22

Text predložený Komisiou	*Pozmeňujúci návrh*
(22) Zodpovednosť za zabezpečenie bezpečnosti sietí a informácií spočíva vo veľkej miere na verejnej správe a ***účastníkoch trhu***. Kultúra riadenia rizika vrátane hodnotenia rizika a vykonávania bezpečnostných opatrení, ktoré ***sú primerané rizikám***, by sa mala podporovať a rozvíjať prostredníctvom vhodných právnych požiadaviek a dobrovoľných priemyselných postupov. Vytvorenie rovnakých podmienok pre všetkých je tiež nevyhnutné na účinné fungovanie siete spolupráce v záujme zabezpečenia účinnej spolupráce všetkých členských štátov.	(22) Zodpovednosť za zabezpečenie bezpečnosti sietí a informácií spočíva vo veľkej miere na verejnej správe a ***podnikoch***. Kultúra riadenia rizika vrátane hodnotenia rizika a vykonávania bezpečnostných opatrení, ktoré ***sa snažia predvídať zámerné aj náhodné bezpečnostné incidenty***, by sa mala podporovať a rozvíjať prostredníctvom vhodných právnych požiadaviek a dobrovoľných priemyselných postupov. ***Ak takáto kultúra riadenia rizika už existuje, a najmä ak sa opiera o dobrovoľné postupy, mala by sa podporovať, posilňovať a spoločne využívať.*** Vytvorenie rovnakých podmienok pre všetkých je tiež nevyhnutné na účinné fungovanie siete spolupráce v záujme zabezpečenia účinnej spolupráce všetkých členských štátov.

Pozmeňujúci návrh 15

Návrh smernice
Odôvodnenie 22 a (nové)

Text predložený Komisiou	*Pozmeňujúci návrh*
	(22a) Orgány verejnej správy a súkromné podniky vrátane poskytovateľov sieťových služieb aj informácií a súborov by mali ochranu svojich informačných systémov a údajov, ktoré obsahujú, považovať za súčasť svojej povinnosti riadnej starostlivosti. Je vhodné zaistiť primeranú úroveň ochrany pred hrozbami a zraniteľnými prvkami, ktoré možno identifikovať. Náklady a poplatky spojené s touto ochranou by mali odrážať prípadnú škodu spôsobenú počítačovým útokom dotknutým osobám.

Pozmeňujúci návrh 16

Návrh smernice
Odôvodnenie 26 a (nové)

Text predložený Komisiou	*Pozmeňujúci návrh*
	(26a) Deti sú vystavené internetu a iným moderným technológiám, ako aj súvisiacim hrozbám, už vo veľmi ranej etape svojho života. Náležitá správa internetového priestoru, ktorý bude vhodný pre deti, je kľúčová pre zmierňovanie škôd a zabezpečenie toho, aby sa neohrozila ochrana detí a ich práv.

Pozmeňujúci návrh 17

Návrh smernice
Odôvodnenie 28

Text predložený Komisiou	*Pozmeňujúci návrh*
(28) Príslušné orgány by mali venovať náležitú pozornosť zachovaniu neformálnych a dôveryhodných kanálov na výmenu informácií medzi účastníkmi trhu a verejným a súkromným sektorom. Pri uverejňovaní incidentov oznámených príslušným orgánom by sa ***mala v primeranej miere udržiavať rovnováha medzi záujmom*** verejnosti ***mať*** informácie o hrozbách ***a možnými rizikami poškodenia obchodu a dobrej povesti verejných správ a účastníkov trhu, ktorí incidenty oznámia. Pri vykonávaní povinnosti oznamovania by príslušné orgány mali venovať osobitnú pozornosť potrebe, aby sa pred zavedením príslušných bezpečnostných opatrení zachovali informácie o zraniteľných miestach výrobku v prísnej tajnosti.***	(28) Príslušné orgány by mali venovať náležitú pozornosť zachovaniu neformálnych a dôveryhodných kanálov na výmenu informácií medzi účastníkmi trhu a verejným a súkromným sektorom. Pri uverejňovaní incidentov oznámených príslušným orgánom by sa ***mal záujem*** verejnosti ***o*** informácie o hrozbách ***uprednostňovať pred krátkodobými hospodárskymi úvahami***.

Pozmeňujúci návrh 18

Návrh smernice

Odôvodnenie 29 a (nové)

Text predložený Komisiou	*Pozmeňujúci návrh*
	(29a) Podvodné využívanie internetu umožňuje organizovanému zločinu rozširovať svoju činnosť na internete na účely prania špinavých peňazí, falšovania a iných výrobkov a služieb porušujúcich práva duševného vlastníctva, ako aj experimentovať s novou trestnou činnosťou, čím sa odhaľuje jeho hrozivá schopnosť prispôsobovať sa moderným technológiám.

Pozmeňujúci návrh 19

Návrh smernice
Odôvodnenie 30 a (nové)

Text predložený Komisiou	*Pozmeňujúci návrh*
	(30a) Počítačová kriminalita vytvára čoraz významnejšie hospodárske a sociálne škody s dôsledkami pre milióny spotrebiteľov a spôsobuje ročné straty v odhadovanej výške 290 miliárd EUR[4a];
	[4a] Podľa správy spoločnosti Norton o počítačovej kriminalite za rok 2012 (Norton Cybercrime Report 2012).

Pozmeňujúci návrh 20

Návrh smernice
Odôvodnenie 33

Text predložený Komisiou	*Pozmeňujúci návrh*
(33) Komisia by mala robiť pravidelné preskúmanie tejto smernice, najmä s ohľadom na stanovenie potreby zmeny na základe meniacich sa technologických a trhových podmienok.	(33) Komisia by mala robiť pravidelné preskúmanie tejto smernice, najmä s ohľadom na stanovenie potreby zmeny na základe meniacich sa technologických a trhových podmienok ***a povinností v oblasti čo najvyššej úrovne bezpečnosti a integrity***

sietí a informácií a ochrany súkromia a osobných údajov.

Pozmeňujúci návrh 21

Návrh smernice
Odôvodnenie 39

Text predložený Komisiou	*Pozmeňujúci návrh*
(39) Pri výmene informácii o rizikách a incidentoch v rámci siete spolupráce a dodržiavaní požiadaviek oznamovať incidenty vnútroštátnym príslušným orgánom sa môže vyžadovať spracovanie osobných údajov. ***Takéto*** spracovanie osobných údajov ***je*** potrebné v záujme plnenia cieľov verejného záujmu, ktoré sú sledované v tejto smernici, ***a tým je*** v súlade s článkom 7 smernice 95/46/ES legitímne. ***Nepredstavuje v súvislosti s týmito legitímnymi cieľmi neprimeraný a neúnosný zásah, ktorý by narušil samotnú podstatu*** práva na ochranu osobných údajov, ktoré je zaručené v článku 8 Charty základných práv. Pri uplatňovaní tejto smernice by sa malo primerane uplatňovať nariadenie Európskeho parlamentu a Rady (ES) č. 1049/2001 z 30. mája 2001 o prístupe verejnosti k dokumentom Európskeho parlamentu, Rady a Komisie[31]. V prípade spracúvania údajov inštitúciami a orgánmi Únie, takéto spracúvanie by na účely uplatňovania tejto smernice malo byť v súlade s nariadením Európskeho parlamentu a Rady (ES) č. 45/2001 z 18. decembra 2000 o ochrane jednotlivcov so zreteľom na spracovanie osobných údajov inštitúciami a orgánmi Spoločenstva a o voľnom pohybe takýchto údajov.	(39) Pri výmene informácii o rizikách a incidentoch v rámci siete spolupráce a dodržiavaní požiadaviek oznamovať incidenty vnútroštátnym príslušným orgánom sa môže vyžadovať spracovanie osobných údajov. ***Ak je*** takéto spracovanie osobných údajov potrebné v záujme plnenia cieľov verejného záujmu, ktoré sú sledované v tejto smernici, ***môže byť*** v súlade s článkom 7 smernice 95/46/ES legitímne. ***Neoslobodzuje však príslušné orgány od povinnosti primerane konať spôsobom, ktorý pravdepodobne neohrozí*** práva na ochranu osobných údajov, ktoré je zaručené v článku 8 Charty základných práv. Pri uplatňovaní tejto smernice by sa malo primerane uplatňovať nariadenie Európskeho parlamentu a Rady (ES) č. 1049/2001 z 30. mája 2001 o prístupe verejnosti k dokumentom Európskeho parlamentu, Rady a Komisie[31]. V prípade spracúvania údajov inštitúciami a orgánmi Únie, takéto spracúvanie by na účely uplatňovania tejto smernice malo byť v súlade s nariadením Európskeho parlamentu a Rady (ES) č. 45/2001 z 18. decembra 2000 o ochrane jednotlivcov so zreteľom na spracovanie osobných údajov inštitúciami a orgánmi Spoločenstva a o voľnom pohybe takýchto údajov.
[31] Ú. v. ES L 145, 31.5.2001, s. 43.	[31] Ú. v. EÚ L 145, 31.05.01, s. 43.

Pozmeňujúci návrh 22

Návrh smernice
Odôvodnenie 41 a (nové)

Text predložený Komisiou	*Pozmeňujúci návrh*
	(41a) V prípade akýchkoľvek opatrení by sa mali chrániť základné ľudské práva, najmä práva uvedené v Európskom dohovore o ochrane ľudských práv (článok 8 – rešpektovanie súkromného života), a je nutné dodržiavať zásadu proporcionality.

Pozmeňujúci návrh 23

Návrh smernice
Článok 1 – odsek 5

Text predložený Komisiou	*Pozmeňujúci návrh*
5. Táto smernica ***sa nedotýka ani smernice*** Európskeho parlamentu a Rady 95/46/EHS z 24. októbra 1995 o ochrane fyzických osôb pri spracovaní osobných údajov a voľnom pohybe týchto údajov, ***ani smernice*** Európskeho parlamentu a Rady 2002/58/ES z 12. júla 2002 ***týkajúcej*** sa spracovávania osobných údajov a ochrany súkromia v sektore elektronických komunikácií***, ani nariadenia*** Európskeho parlamentu a Rady o ochrane jednotlivcov so zreteľom na spracovanie osobných údajov a o voľnom pohybe takýchto údajov.	5. Táto smernica ***v plnej miere zohľadňuje smernicu*** Európskeho parlamentu a Rady 95/46/EHS z 24. októbra 1995 o ochrane fyzických osôb pri spracovaní osobných údajov a voľnom pohybe týchto údajov, ***smernicu*** Európskeho parlamentu a Rady 2002/58/ES z 12. júla 2002 ***týkajúcu*** sa spracovávania osobných údajov a ochrany súkromia v sektore elektronických komunikácií ***a nariadenie*** Európskeho parlamentu a Rady ***(ES) č. 45/2001 z 18. decembra 2000*** o ochrane jednotlivcov so zreteľom na spracovanie osobných údajov inštitúciami a orgánmi spoločenstva a o voľnom pohybe takýchto údajov.

Pozmeňujúci návrh 24

Návrh smernice
Článok 2

Text predložený Komisiou	*Pozmeňujúci návrh*
Členským štátom sa nebude brániť v prijímaní alebo zachovaní ustanovení, ktoré zabezpečujú vyššiu úroveň bezpečnosti, bez toho, aby boli dotknuté ich povinnosti v súlade s právom Únie.	Členským štátom sa nebude brániť v prijímaní alebo zachovaní ustanovení, ktoré zabezpečujú vyššiu úroveň bezpečnosti, bez toho, aby boli dotknuté ich povinnosti v súlade s právom Únie***, pričom však tieto ustanovenia musia spĺňať spoločné minimálne očakávania, ktoré sa vzťahujú na tento prípad a sú uvedené v tejto smernici***.

Pozmeňujúci návrh 25

Návrh smernice
Článok 3 – bod 2

Text predložený Komisiou	*Pozmeňujúci návrh*
(2) „bezpečnosť“ znamená schopnosť siete alebo informačného systému odolávať ***na určitom stupni spoľahlivosti*** náhodným udalostiam alebo zlomyseľnému konaniu, ktoré ohrozuje dostupnosť, pravosť, integritu a dôvernosť uchovávaných alebo prenášaných údajov alebo súvisiacich služieb poskytovaných prostredníctvom tejto siete a informačného systému alebo prístupných prostredníctvom tejto siete a informačného systému;	(2) „bezpečnosť“ znamená schopnosť siete alebo informačného systému odolávať náhodným udalostiam alebo zlomyseľnému konaniu, ktoré ohrozuje dostupnosť, pravosť, integritu a dôvernosť uchovávaných alebo prenášaných údajov alebo súvisiacich služieb poskytovaných prostredníctvom tejto siete a informačného systému alebo prístupných prostredníctvom tejto siete a informačného systému;

Pozmeňujúci návrh 26

Návrh smernice
Článok 3 – odsek 2 – písmeno a (nové)

Text predložený Komisiou	*Pozmeňujúci návrh*
	„kybernetická odolnosť“ znamená schopnosť sieťového a informačného systému odolať a nadobudnúť plnú prevádzkovú kapacitu po incidentoch, medzi ktoré okrem iného patria technické poruchy, výpadky elektrickej energie

	alebo bezpečnostné incidenty;

Pozmeňujúci návrh 27

Návrh smernice
Článok 3 – odsek 4

Text predložený Komisiou	*Pozmeňujúci návrh*
„incident“ znamená každú okolnosť alebo udalosť, ktorá má konkrétny nepriaznivý vplyv na bezpečnosť;	„incident“ znamená každú okolnosť alebo udalosť, ktorá má konkrétny nepriaznivý vplyv na bezpečnosť ***a poskytovanie základných služieb***;

Pozmeňujúci návrh 28

Návrh smernice
Článok 3 – bod 8 – písmeno b

Text predložený Komisiou	*Pozmeňujúci návrh*
b) prevádzkovateľ kritickej infraštruktúry, ktorá má zásadný význam z hľadiska zachovania dôležitých ***ekonomických a spoločenských*** činností v oblasti energetiky, dopravy, bankovníctva, burzy cenných papierov a zdravotníctva, ktorých neúplný zoznam je uvedený v prílohe II,	b) prevádzkovateľ kritickej infraštruktúry, ktorá má zásadný význam z hľadiska zachovania dôležitých ***spoločenských a ekonomických*** činností v oblasti energetiky, dopravy, bankovníctva, burzy cenných papierov***, potravinového dodávateľského reťazca*** a zdravotníctva, ktorých neúplný zoznam je uvedený v prílohe II,

Pozmeňujúci návrh 29

Návrh smernice
Článok 5 – odsek 2 – písmeno a

Text predložený Komisiou	*Pozmeňujúci návrh*
a) ***plán na*** hodnotenie rizika na účely identifikácie rizík a hodnotenia vplyvu potenciálnych incidentov;	a) ***rámec riadenia rizika zahŕňajúci prinajmenšom pravidelné*** hodnotenie rizika na účely identifikácie rizík a hodnotenia vplyvu potenciálnych incidentov***, ako aj opatrenia na ochranu bezpečnosti a integrity informácií vrátane***

včasného varovania;

Odôvodnenie

Plán na hodnotenie nestačí a nezahŕňa ďalšie opatrenia potrebné na riadenie rizika v oblasti bezpečnosti sietí a informácií. Európsky dozorný úradník pre ochranu údajov odporúča zavedenie rámca riadenia rizika zahŕňajúceho hodnotenie rizika.

Pozmeňujúci návrh 30

Návrh smernice
Článok 5 – odsek 3

Text predložený Komisiou	*Pozmeňujúci návrh*
3. Vnútroštátna stratégia pre bezpečnosť sietí a informácií a vnútroštátny plán spolupráce v oblasti bezpečnosti sietí a informácií sa oznamujú Komisii do jedného mesiaca po ich prijatí.	3. Vnútroštátna stratégia pre bezpečnosť sietí a informácií a vnútroštátny plán spolupráce v oblasti bezpečnosti sietí a informácií sa oznamujú Komisii***, Európskemu parlamentu, Rade, európskemu dozornému úradníkovi pre ochranu údajov*** do jedného mesiaca po ich prijatí***, čo nesmie byť neskôr ako 12 mesiacov od nadobudnutia účinnosti tejto smernice***.

Pozmeňujúci návrh 31

Návrh smernice
Článok 5 – odsek 3 a (nový)

Text predložený Komisiou	*Pozmeňujúci návrh*
	3a. Komisia zosumarizuje stratégie pre bezpečnosť sietí a informácií všetkých členských štátov a postúpi ich všetkým členským štátom v organizovanej podobe.

Odôvodnenie

Pre členské štáty bude užitočné vidieť plány ostatných. Pomôže im to určiť vlastný prístup, a môžu sa dokonca objaviť príležitosti na výmenu osvedčených postupov.

Pozmeňujúci návrh 32

Návrh smernice
Článok 5 – odsek 3 b (nový)

Text predložený Komisiou	*Pozmeňujúci návrh*
	3b. Do šiestich mesiacov od prijatia tejto smernice Komisia vytvorí usmernenia ku štruktúre stratégie pre bezpečnosť sietí a informácií. Zámerom bude pomôcť členským štátom pripraviť a schváliť dokumenty s približne rovnakou štruktúrou.

Odôvodnenie

Organizovanie a sumarizovanie na úrovni EÚ môže byť efektívnejšie, ak bude 28 dokumentov, z ktorých vychádza, dodržiavať určitú všeobecnú štruktúru. Hoci usmernenia Komisie nebudú záväzné, aj tak povedú k tomu, že budú motivovať členské štáty, aby sa pri príprave vlastných vnútroštátnych stratégií pridržiavali tohto odporúčaného modelu/štruktúry.

Pozmeňujúci návrh 33

Návrh smernice
Článok 6 – odsek 1

Text predložený Komisiou	*Pozmeňujúci návrh*
1. Každý členský štát určí príslušný vnútroštátny orgán pre oblasť bezpečnosti sietí a informačných systémov (ďalej len „príslušný orgán“).	1. Každý členský štát určí príslušný ***civilný*** vnútroštátny orgán pre oblasť bezpečnosti sietí a informačných systémov (ďalej len „príslušný orgán“).

Pozmeňujúci návrh 34

Návrh smernice
Článok 6 – odsek 5

Text predložený Komisiou	*Pozmeňujúci návrh*
5. ***V prípade potreby sa*** príslušné orgány radia s príslušnými vnútroštátnymi orgánmi presadzovania práva a orgánmi na ochranu údajov a ***spolupracujú s nimi***.	5. Príslušné orgány ***sa*** radia s príslušnými vnútroštátnymi orgánmi presadzovania práva a orgánmi na ochranu údajov a ***úzko s nimi spolupracujú vždy, keď je to potrebné, a so zreteľom na zásadu***

proporcionality.

Pozmeňujúci návrh 35

Návrh smernice
Článok 6 – odsek 5 (nový)

Text predložený Komisiou	*Pozmeňujúci návrh*
	5a. Pokiaľ ide o zhromažďovanie, spracovanie a výmenu informácií, príslušné orgány dodržiavajú požiadavky týkajúce sa ochrany osobných údajov uvedené v článku 17 smernice 95/46/ES.

Pozmeňujúci návrh 36

Návrh smernice
Článok 7 – odsek 1

Text predložený Komisiou	*Pozmeňujúci návrh*
1. Každý členský štát zostaví ***tím*** reakcie na núdzové počítačové situácie (ďalej len „CERT“), ktorý bude zodpovedný za riešenie incidentov a rizík podľa presne stanoveného postupu v súlade s požiadavkami stanovenými v bode 1 prílohy I. Tím CERT ***môže*** byť vytvorený v rámci príslušného orgánu.	1. Každý členský štát zostaví ***tímy*** reakcie na núdzové počítačové situácie (ďalej len „CERT“), ktorý bude zodpovedný za riešenie incidentov a rizík podľa presne stanoveného postupu v súlade s požiadavkami stanovenými v bode 1 prílohy I. Tím CERT ***je v náležitých prípadoch*** vytvorený v rámci príslušného orgánu.

Pozmeňujúci návrh 37

Návrh smernice
Článok 8 – odsek 2

Text predložený Komisiou	*Pozmeňujúci návrh*
2. Sieť spolupráce zabezpečí medzi Komisiou a príslušnými orgánmi stálu komunikáciu. Na požiadanie pomáha v sieti spolupráce aj Európska agentúra pre bezpečnosť sietí a informácií (ďalej len „ENISA“) tým, že poskytuje ***svoje odborné***	2. Sieť spolupráce zabezpečí medzi Komisiou a príslušnými orgánmi stálu komunikáciu. Na požiadanie pomáha v sieti spolupráce aj Európska agentúra pre bezpečnosť sietí a informácií (ďalej len „ENISA“) tým, že poskytuje ***technologicky***

znalosti a poradenstvo.	***neutrálne*** poradenstvo ***s vhodnými opatreniami pre verejný aj súkromný sektor***.

Pozmeňujúci návrh 38

Návrh smernice
Článok 9 – odsek 2 – písmeno b a (nové)

Text predložený Komisiou	*Pozmeňujúci návrh*
	ba) kritériá zapojenia členských štátov do bezpečného systému výmeny informácií s cieľom zabezpečiť, aby bola všetkými účastníkmi vo všetkých fázach spracovania zaistená vysoká úroveň bezpečnosti a odolnosti, a to aj na základe príslušných opatrení v oblasti dôvernosti a bezpečnosti podľa článkov 16 a 17 smernice 95/46/ES a článkov 21 a 22 nariadenia (ES) č. 45/2001.

Pozmeňujúci návrh 39

Návrh smernice
Článok 9 – odsek 3

Text predložený Komisiou	*Pozmeňujúci návrh*
3. Komisia prijme prostredníctvom vykonávacích aktov rozhodnutia o prístupe členských štátov k tejto bezpečnej infraštruktúre, v súlade s kritériami uvedenými v odsekoch 2 a 3. Tieto vykonávacie akty sa prijmú v súlade s postupom preskúmania uvedeným v článku 19 ods. 3.	***vypúšťa sa***

Pozmeňujúci návrh 40

Návrh smernice
Článok 12 – odsek 2 – písmeno a – zarážka 2

Text predložený Komisiou	*Pozmeňujúci návrh*
– vymedzenie ***postupov a*** kritérií na hodnotenie rizika a incidentov prostredníctvom siete spolupráce;	– vymedzenie kritérií na hodnotenie rizika a incidentov prostredníctvom siete spolupráce;

Pozmeňujúci návrh 41

Návrh smernice
Článok 13

Text predložený Komisiou	*Pozmeňujúci návrh*
Bez toho, aby bola dotknutá možnosť neformálne spolupracovať na medzinárodnej úrovni v rámci siete spolupráce, Únia môže uzatvárať medzinárodné dohody s tretími krajinami alebo medzinárodnými organizáciami, a tým umožniť ich účasť na niektorých činnostiach siete spolupráce a takúto účasť zorganizovať. ***V takýchto dohodách sa berie do úvahy potreba zabezpečenia primeranej*** ochrany osobných údajov, ktoré sú zasielané v rámci siete spolupráce.	Bez toho, aby bola dotknutá možnosť neformálne spolupracovať na medzinárodnej úrovni v rámci siete spolupráce, Únia môže uzatvárať medzinárodné dohody s tretími krajinami alebo medzinárodnými organizáciami, a tým umožniť ich účasť na niektorých činnostiach siete spolupráce a takúto účasť zorganizovať. ***Takéto dohody sa uzavrú iba vtedy, ak možno zabezpečiť úroveň*** ochrany osobných údajov, ktoré sú zasielané v rámci siete spolupráce***, ktorá je primeraná a porovnateľná s úrovňou ochrany Únie*** .

Pozmeňujúci návrh 42

Návrh smernice
Článok 14 – odsek 1

Text predložený Komisiou	*Pozmeňujúci návrh*
1. Členské štáty zabezpečia, aby verejná správa a účastníci trhu prijali primerané technické a organizačné opatrenia na riadenie rizík spojených s bezpečnosťou sietí a informačných systémov, ktoré riadia a využívajú vo svojej prevádzke. S ohľadom na najnovší technologický vývoj tieto opatrenia zaručujú takú úroveň bezpečnosti, ktorá zodpovedá miere daného rizika. Opatrenia sa prijímajú	1. Členské štáty zabezpečia, aby verejná správa a účastníci trhu prijali primerané technické a organizačné opatrenia na ***odhaľovanie, účinné*** riadenie ***a obmedzovanie*** rizík spojených s bezpečnosťou sietí a informačných systémov, ktoré riadia a využívajú vo svojej prevádzke. S ohľadom na najnovší technologický vývoj tieto opatrenia zaručujú takú úroveň bezpečnosti, ktorá

najmä s cieľom zabrániť a minimalizovať vplyv incidentov ovplyvňujúcich ich siete a informačný systém na základné služby, ktoré poskytujú, a tak zabezpečiť kontinuitu služieb podporovaných týmito sieťami a informačnými systémami.

zodpovedá ***a je primeraná*** miere daného rizika. Opatrenia sa prijímajú najmä s cieľom zabrániť a minimalizovať vplyv incidentov ovplyvňujúcich ich siete a informačný systém na základné služby, ktoré poskytujú, a tak zabezpečiť kontinuitu služieb ***a bezpečnosť údajov*** podporovaných týmito sieťami a informačnými systémami.

Pozmeňujúci návrh 43

Návrh smernice
Článok 14 – odsek 2 – písmeno a (nové)

Pozmeňujúci návrh

a) Výrobcovia komerčného softvéru sú v prípade hrubej nedbalosti v oblasti bezpečnosti a zabezpečenia zodpovední napriek doložkám o vzdaní sa zodpovednosti uvedeným v súhlasoch používateľov.

Odôvodnenie

V dohode o udelení licencie sa výrobcovia komerčného softvéru zriekajú zodpovednosti za akúkoľvek škodu, ktorá môže vzniknúť kvôli nedostatočnému zabezpečeniu a nekvalitnému programovaniu. Aby sa výrobcovia softvéru motivovali k investovaniu do bezpečnostných opatrení, je nutná iná kultúra. Možno to dosiahnuť len vtedy, ak budú výrobcovia softvéru zodpovedať za akékoľvek bezpečnostné nedostatky.

Pozmeňujúci návrh 44

Návrh smernice
Článok 14 – odsek 3

Text predložený Komisiou	*Pozmeňujúci návrh*
3. Požiadavky uvedené v odsekoch 1 a 2 sa týkajú všetkých účastníkov trhu, ktorí poskytujú služby v rámci Európskej únie.	3. Požiadavky uvedené v odsekoch 1 a 2 sa týkajú všetkých účastníkov trhu ***a výrobcov softvéru***, ktorí poskytujú služby v rámci Európskej únie.

Pozmeňujúci návrh 45

Návrh smernice
Článok 14 – odsek 6

Text predložený Komisiou	*Pozmeňujúci návrh*
6. Na základe delegovaných aktov prijatých podľa odseku 5 môžu príslušné orgány prijať usmernenia a v prípade potreby vydať pokyny týkajúce sa okolností, za akých sa vyžaduje od verejnej správy a účastníkov trhu, aby oznamovali incidenty.	***vypúšťa sa***

Pozmeňujúci návrh 46

Návrh smernice
Článok 15 – odsek 1

Text predložený Komisiou	*Pozmeňujúci návrh*
1. Členské štáty zabezpečia, aby príslušné orgány mali ***všetky*** právomoci potrebné na vyšetrovanie prípadov, ak verejná správa alebo účastníci trhu nedodržiavajú svoje povinnosti podľa článku 14, a ich dôsledkov na bezpečnosť sietí a informačných systémov.	1. Členské štáty zabezpečia, aby príslušné orgány mali právomoci potrebné na vyšetrovanie prípadov, ak verejná správa alebo účastníci trhu nedodržiavajú svoje povinnosti podľa článku 14, a ich dôsledkov na bezpečnosť sietí a informačných systémov.

Pozmeňujúci návrh 47

Návrh smernice
Článok 15 – odsek 5

Text predložený Komisiou	*Pozmeňujúci návrh*
5. Príslušné orgány úzko spolupracujú s orgánmi na ochranu osobných údajov pri riešení incidentov, ktoré majú za následok porušenie ochrany osobných údajov.	5. ***Bez toho, aby to malo vplyv na príslušnú právnu úpravu ochrany údajov, a na základe plnohodnotných konzultácií s príslušnými kontrolórmi alebo spracovateľmi údajov,*** príslušné orgány ***a jednotné kontaktné miesta*** úzko spolupracujú s orgánmi na ochranu osobných údajov pri riešení incidentov,

ktoré majú za následok porušenie ochrany osobných údajov.

Pozmeňujúci návrh 48

Návrh smernice
Článok 19 a (nový)

Text predložený Komisiou	*Pozmeňujúci návrh*
	Článok 19a
	Ochrana a spracovanie osobných údajov
	1. Akékoľvek spracovanie osobných údajov v členských štátoch v zmysle tejto smernice sa uskutoční v súlade so smernicou 95/46/ES a so smernicou 2002/58/ES.
	2. Akékoľvek spracovanie osobných údajov Komisiou a agentúrou ENISA v zmysle tejto smernice sa uskutoční v súlade s nariadením (ES) č. 45/2001.
	3. Akékoľvek spracovanie osobných údajov Centrom boja proti kybernetickej kriminalite v rámci Europolu na účely tejto smernice sa uskutoční v súlade s rozhodnutím 2009/371/SVV.
	4. Spracovanie osobných údajov je korektné a striktne sa obmedzuje na minimum údajov potrebných na účely, na ktoré sa spracúvajú. Uchovávajú sa vo forme, ktorá umožňuje identifikáciu dotknutých osôb len počas časového obdobia, ktoré je nevyhnutné na účely, na ktoré sa osobné údaje spracúvajú.
	5. Oznamovanie incidentov uvedené v článku 14 sa nedotýka ustanovení a povinností týkajúcich sa oznamovania porušení ochrany osobných údajov uvedené v článku 4 smernice 2002/58/ES a v nariadení (EÚ) č. 611/2013.
	6. Odkazy na smernicu 95/46/ES sa vykladajú ako odkazy na nariadenie Európskeho parlamentu a Rady o ochrane fyzických osôb pri spracúvaní

	osobných údajov a voľnom pohybe týchto údajov (všeobecné nariadenie o ochrane údajov), len čo nadobudne účinnosť.

Pozmeňujúci návrh 49

Návrh smernice
Článok 20 – odsek 1

Text predložený Komisiou	*Pozmeňujúci návrh*
Komisia pravidelne skúma funkčnosť tejto smernice a podáva správu Európskemu parlamentu a Rade. Prvá správa sa predkladá najneskôr ***tri*** roky po dátume transpozície, na ktorú sa odkazuje v článku 21. Na tento účel môže Komisia požadovať od členských štátov, aby bez zbytočného odkladu poskytli informácie.	Komisia pravidelne skúma funkčnosť tejto smernice a podáva správu Európskemu parlamentu a Rade. Prvá správa sa predkladá najneskôr ***dva*** roky po dátume transpozície, na ktorú sa odkazuje v článku 21. Na tento účel môže Komisia požadovať od členských štátov, aby bez zbytočného odkladu poskytli informácie.

Pozmeňujúci návrh 50

Návrh smernice
Príloha 1 – odsek 1 – bod 1 – písmeno b

Text predložený Komisiou	*Pozmeňujúci návrh*
b) Tím CERT vykonáva a riadi bezpečnostné opatrenia s cieľom zabezpečiť dôvernosť, integritu, dostupnosť a pravosť informácií, ktoré získava a spracováva.	b) Tím CERT vykonáva a riadi bezpečnostné opatrenia s cieľom zabezpečiť dôvernosť, integritu, dostupnosť a pravosť informácií, ktoré získava a spracováva***, a to v súlade s požiadavkami v oblasti ochrany údajov***.

Pozmeňujúci návrh 51

Návrh smernice
Príloha 2 – odsek 1

Text predložený Komisiou	*Pozmeňujúci návrh*
Zoznam účastníkov trhu uvedených v článku 3 ods. 8 písm. a)	Zoznam účastníkov trhu uvedených v článku 3 ods. 8 písm. a)

1. platformy elektronického obchodu;	1. platformy elektronického obchodu;
2. internetové platobné portály;	2. internetové platobné portály;
3. sociálne siete;	
4. vyhľadávače;	***3***. vyhľadávače;
5. služby cloud computing;	***4.*** služby cloud computing***, ktoré uchovávajú údaje o kritickej infraštruktúre Európskej únie***
6. obchody s aplikáciami;	

Pozmeňujúci návrh 52

Návrh smernice
Príloha 2 – odsek 2 – bod 5 a (nový)

Text predložený Komisiou	*Pozmeňujúci návrh*
	5a. Potravinový dodávateľský reťazec

POSTUP

Názov	Vysoká úroveň bezpečnosti sietí a informácií v Únii			
Referenčné čísla	COM(2013)0048 – C7-0035/2013 – 2013/0027(COD)			
Gestorský výbor dátum oznámenia na schôdzi	IMCO 15.4.2013			
Výbor, ktorý predložil stanovisko dátum oznámenia na schôdzi	LIBE 15.4.2013			
Postup pridružených výborov - dátum oznámenia na schôdzi	12.9.2013			
Spravodajca výboru požiadaného o stanovisko dátum vymenovania	Carl Schlyter 7.3.2013			
Prerokovanie vo výbore	25.4.2013	18.9.2013	4.11.2013	13.1.2014
Dátum prijatia	13.1.2014			
Výsledok záverečného hlasovania:	+: –: 0:	36 6 0		
Poslanci prítomní na záverečnom hlasovaní	Jan Philipp Albrecht, Roberta Angelilli, Edit Bauer, Rita Borsellino, Arkadiusz Tomasz Bratkowski, Philip Claeys, Frank Engel, Cornelia Ernst, Tanja Fajon, Monika Flašíková Beňová, Kinga Gál, Kinga Göncz, Salvatore Iacolino, Sophia in ‘t Veld, Timothy Kirkhope, Juan Fernando López Aguilar, Baroness Sarah Ludford, Monica Luisa Macovei, Svetoslav Hristov Malinov, Véronique Mathieu Houillon, Anthea McIntyre, Nuno Melo, Roberta Metsola, Claude Moraes, Jacek Protasiewicz, Carmen Romero López, Birgit Sippel, Csaba Sógor, Renate Sommer, Axel Voss, Renate Weber, Josef Weidenholzer, Cecilia Wikström, Tatjana Ždanoka, Auke Zijlstra			
Náhradníci prítomní na záverečnom hlasovaní	Monika Hohlmeier, Jean Lambert, Ulrike Lunacek, Jan Mulder, Carl Schlyter, Marco Scurria			
Náhradníčka (čl. 187 ods. 2) prítomná na záverečnom hlasovaní	Katarína Neveďalová			