POZMEŇUJÚCE NÁVRHY 001-280
predložené Výbor pre priemysel, výskum a energetiku

Správa
Bart Groothuis **A9-0313/2021**
Vysoká spoločná úroveň kybernetickej bezpečnosti v Únii

Návrh smernice (COM(2020)0823 – C9-0422/2020 – 2020/0359(COD))

Pozmeňujúci návrh 1

Návrh smernice
Názov

Text predložený Komisiou	*Pozmeňujúci návrh*
Návrh	Návrh
SMERNICA EURÓPSKEHO PARLAMENTU A RADY	SMERNICA EURÓPSKEHO PARLAMENTU A RADY
o opatreniach na zabezpečenie vysokej spoločnej úrovne kybernetickej bezpečnosti v Únii ***a o zrušení smernice*** (EÚ) 2016/1148	o opatreniach na zabezpečenie vysokej spoločnej úrovne kybernetickej bezpečnosti v Únii ***(smernica NIS 2), ktorou sa zrušuje smernica*** (EÚ) 2016/1148

Pozmeňujúci návrh 2

Návrh smernice
Odôvodnenie 1

Text predložený Komisiou	*Pozmeňujúci návrh*
(1) Cieľom smernice Európskeho parlamentu a Rady (EÚ) 2016/1148[11] bolo budovať kybernetickobezpečnostné kapacity v celej Únii, zmierňovať hrozby	(1) Cieľom smernice Európskeho parlamentu a Rady (EÚ) 2016/1148[11]***, bežne označovanej ako „smernica NIS“,*** bolo budovať kybernetickobezpečnostné

pre siete a informačné systémy používané na poskytovanie základných služieb v kľúčových odvetviach a zabezpečiť kontinuitu takýchto služieb pri riešení kybernetickobezpečnostných incidentov, a tým prispievať k ***efektívnemu fungovaniu spoločnosti*** a hospodárstva ***Únie***.	kapacity v celej Únii, zmierňovať hrozby pre siete a informačné systémy používané na poskytovanie základných služieb v kľúčových odvetviach a zabezpečiť kontinuitu takýchto služieb pri riešení kybernetickobezpečnostných incidentov, a tým prispievať k ***bezpečnosti Únie*** a ***účinnému fungovaniu jej*** hospodárstva ***a spoločnosti***.
[11] Smernica Európskeho parlamentu a Rady (EÚ) 2016/1148 zo 6. júla 2016 o opatreniach na zabezpečenie vysokej spoločnej úrovne bezpečnosti sietí a informačných systémov v Únii (Ú. v. EÚ L 194/1, 19.7.2016, s. 1).	[11] Smernica Európskeho parlamentu a Rady (EÚ) 2016/1148 zo 6. júla 2016 o opatreniach na zabezpečenie vysokej spoločnej úrovne bezpečnosti sietí a informačných systémov v Únii (Ú. v. EÚ L 194/1, 19.7.2016, s. 1). 1).

Pozmeňujúci návrh 3

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. 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.

	Kybernetická bezpečnosť je navyše kľúčovým faktorom, ktorý mnohým kritickým odvetviam umožňuje úspešne zvládnuť digitálnu transformáciu a plne využívať hospodárske, sociálne a udržateľné prínosy digitalizácie.

Pozmeňujúci návrh 4

Návrh smernice
Odôvodnenie 3 a (nové)

Text predložený Komisiou	*Pozmeňujúci návrh*
	(3a) Kybernetickobezpečnostné incidenty a krízy veľkého rozsahu na úrovni Únie si z dôvodu vysokého stupňa previazanosti odvetví a krajín vyžadujú koordinované opatrenia na zabezpečenie rýchlej a účinnej reakcie. Dostupnosť kyberneticky odolných sietí a informačných systémov a dostupnosť, dôvernosť a integrita údajov sú nevyhnutné pre bezpečnosť Únie v rámci jej hraníc, ako aj za jej hranicami, keďže kybernetické hrozby by mohli pochádzať z územia mimo Únie. Ambícia Únie získať významnejšiu geopolitickú úlohu spočíva taktiež v dôveryhodnej kybernetickej obrane a odrádzaní od kybernetických útokov vrátane schopnosti včas a účinne identifikovať zlomyseľné konanie a primerane naň reagovať.

Pozmeňujúci návrh 5

Návrh smernice
Odôvodnenie 5

Text predložený Komisiou	*Pozmeňujúci návrh*
(5) Všetky tieto rozdiely spôsobujú fragmentáciu vnútorného trhu a môžu mať škodlivý vplyv na jeho fungovanie, a to najmä pokiaľ ide o cezhraničné poskytovanie služieb a úroveň kybernetickobezpečnostnej odolnosti v dôsledku uplatňovania rôznych noriem. Cieľom tejto smernice je odstrániť takéto veľké rozdiely medzi členskými štátmi, a	(5) Všetky tieto rozdiely spôsobujú fragmentáciu vnútorného trhu a môžu mať škodlivý vplyv na jeho fungovanie, a to najmä pokiaľ ide o cezhraničné poskytovanie služieb a úroveň kybernetickobezpečnostnej odolnosti v dôsledku uplatňovania rôznych noriem. ***Tieto rozdiely by v konečnom dôsledku mohli viesť k väčšej zraniteľnosti***

to najmä stanovením minimálnych pravidiel týkajúcich sa fungovania koordinovaného regulačného rámca, stanovením mechanizmov účinnej spolupráce medzi zodpovednými orgánmi v každom členskom štáte, aktualizáciou zoznamu odvetví a činností podliehajúcich povinnostiam v oblasti kybernetickej bezpečnosti a poskytnutím účinných nápravných opatrení a sankcií, ktoré sú nevyhnutné na účinné presadzovanie týchto povinností. Smernica (EÚ) 2016/1148 by sa preto mala zrušiť a nahradiť touto smernicou.	***niektorých členských štátov voči kybernetickobezpečnostným hrozbám s možnými účinkami presahovania v celej Únii.*** Cieľom tejto smernice je odstrániť takéto veľké rozdiely medzi členskými štátmi, a to najmä stanovením minimálnych pravidiel týkajúcich sa fungovania koordinovaného regulačného rámca, stanovením mechanizmov účinnej spolupráce medzi zodpovednými orgánmi v každom členskom štáte, aktualizáciou zoznamu odvetví a činností podliehajúcich povinnostiam v oblasti kybernetickej bezpečnosti a poskytnutím účinných nápravných opatrení a sankcií, ktoré sú nevyhnutné na účinné presadzovanie týchto povinností. Smernica (EÚ) 2016/1148 by sa preto mala zrušiť a nahradiť touto smernicou ***(smernicou NIS 2)***.

Pozmeňujúci návrh 6

Návrh smernice
Odôvodnenie 6

Text predložený Komisiou	*Pozmeňujúci návrh*
(6) Táto smernica neovplyvňuje možnosť členských štátov prijať potrebné opatrenia na zaručenie ochrany základných záujmov vlastnej bezpečnosti, chrániť verejný poriadok a verejnú bezpečnosť a umožniť vyšetrovanie a odhaľovanie trestných činov, ako aj stíhanie ich páchateľov, a to v súlade s právom Únie. V súlade s článkom 346 ZFEÚ nemá byť žiaden členský štát povinný poskytovať informácie, ktorých sprístupnenie by odporovalo základným záujmom jeho verejnej bezpečnosti. V tejto súvislosti sú relevantné pravidlá Únie a členských štátov na ochranu utajovaných skutočností, dohody o zachovaní mlčanlivosti a neformálne dohody o zachovaní mlčanlivosti, ako napríklad semaforový protokol[14].	(6) Táto smernica neovplyvňuje možnosť členských štátov prijať potrebné opatrenia na zaručenie ochrany základných záujmov vlastnej bezpečnosti, chrániť verejný poriadok a verejnú bezpečnosť a umožniť ***prevenciu,*** vyšetrovanie a odhaľovanie trestných činov, ako aj stíhanie ich páchateľov, a to v súlade s právom Únie. V súlade s článkom 346 ZFEÚ nemá byť žiaden členský štát povinný poskytovať informácie, ktorých sprístupnenie by odporovalo základným záujmom jeho verejnej bezpečnosti. V tejto súvislosti sú relevantné pravidlá Únie a členských štátov na ochranu utajovaných skutočností, dohody o zachovaní mlčanlivosti a neformálne dohody o zachovaní mlčanlivosti, ako napríklad semaforový protokol[14].
_____	_____

[14] Semaforový protokol (Traffic Light Protocol, TLP) slúži pri sprístupňovaní informácií na informovanie príjemcov o akýchkoľvek obmedzeniach pri ďalšom šírení týchto informácií. Používa sa takmer vo všetkých komunitách jednotiek CSIRT a v niektorých strediskách pre výmenu a analýzu informácií (ISAC).

[14] Semaforový protokol (Traffic Light Protocol, TLP) slúži pri sprístupňovaní informácií na informovanie príjemcov o akýchkoľvek obmedzeniach pri ďalšom šírení týchto informácií. Používa sa takmer vo všetkých komunitách jednotiek CSIRT a v niektorých strediskách pre výmenu a analýzu informácií (ISAC).

Pozmeňujúci návrh 7

Návrh smernice
Odôvodnenie 7

Text predložený Komisiou	*Pozmeňujúci návrh*
(7) Zrušením smernice (EÚ) 2016/1148 by sa rozsah uplatňovania podľa odvetví mal rozšíriť na väčšiu časť hospodárstva vzhľadom na úvahy uvedené v odôvodneniach 4 až 6. Odvetvia, na ktoré sa vzťahuje smernica (EÚ) 2016/1148, by sa preto mali rozšíriť tak, aby boli komplexne pokryté odvetvia a služby, ktoré majú zásadný význam pre kľúčové spoločenské a hospodárske činnosti v rámci vnútorného trhu. ***Pravidlá*** by sa nemali líšiť podľa toho, či sú subjekty prevádzkovateľmi základných služieb alebo poskytovateľmi digitálnych služieb. Takéto rozlišovanie sa ukázalo ako zastarané, pretože neodráža skutočný význam odvetví alebo služieb pre spoločenské a hospodárske činnosti na vnútornom trhu.	(7) Zrušením smernice (EÚ) 2016/1148 by sa rozsah uplatňovania podľa odvetví mal rozšíriť na väčšiu časť hospodárstva vzhľadom na úvahy uvedené v odôvodneniach 4 až 6. Odvetvia, na ktoré sa vzťahuje smernica (EÚ) 2016/1148, by sa preto mali rozšíriť tak, aby boli komplexne pokryté odvetvia a služby, ktoré majú zásadný význam pre kľúčové spoločenské a hospodárske činnosti v rámci vnútorného trhu. ***Požiadavky na riadenie rizík a oznamovacie povinnosti*** by sa nemali líšiť podľa toho, či sú subjekty prevádzkovateľmi základných služieb alebo poskytovateľmi digitálnych služieb. Takéto rozlišovanie sa ukázalo ako zastarané, pretože neodráža skutočný význam odvetví alebo služieb pre spoločenské a hospodárske činnosti na vnútornom trhu.

Pozmeňujúci návrh 8

Návrh smernice
Odôvodnenie 8

Text predložený Komisiou	*Pozmeňujúci návrh*
(8) V súlade so smernicou (EÚ) 2016/1148 boli členské štáty zodpovedné za určenie tých subjektov, ktoré spĺňajú kritériá, aby mohli pôsobiť ako prevádzkovatelia základných služieb	(8) V súlade so smernicou (EÚ) 2016/1148 boli členské štáty zodpovedné za určenie tých subjektov, ktoré spĺňajú kritériá, aby mohli pôsobiť ako prevádzkovatelia základných služieb

(„proces identifikácie“). S cieľom odstrániť v tejto súvislosti veľké rozdiely medzi členskými štátmi a zabezpečiť právnu istotu, pokiaľ ide o požiadavky na riadenie rizík a oznamovacie povinnosti pre všetky príslušné subjekty, by sa malo stanoviť jednotné kritérium, ktorým sa určia subjekty, ktoré patria do rozsahu pôsobnosti tejto smernice. Toto kritérium by malo spočívať v uplatňovaní pravidla obmedzenia veľkosti, podľa ktorého všetky stredné a veľké podniky, ako sú vymedzené v odporúčaní Komisie 2003/361/ES[15], ktoré pôsobia v rámci takých odvetví alebo poskytujú taký druh služieb, na ktoré sa vzťahuje táto smernica, patria do rozsahu jej pôsobnosti. ***Od členských štátov by sa nemalo vyžadovať, aby zostavili zoznam subjektov, ktoré spĺňajú toto všeobecne uplatniteľné kritérium týkajúce sa veľkosti.***

(„proces identifikácie“). S cieľom odstrániť v tejto súvislosti veľké rozdiely medzi členskými štátmi a zabezpečiť právnu istotu, pokiaľ ide o požiadavky na riadenie rizík a oznamovacie povinnosti pre všetky príslušné subjekty, by sa malo stanoviť jednotné kritérium, ktorým sa určia subjekty, ktoré patria do rozsahu pôsobnosti tejto smernice. Toto kritérium by malo spočívať v uplatňovaní pravidla obmedzenia veľkosti, podľa ktorého všetky stredné a veľké podniky, ako sú vymedzené v odporúčaní Komisie 2003/361/ES[15], ktoré pôsobia v rámci takých odvetví alebo poskytujú taký druh služieb, na ktoré sa vzťahuje táto smernica, patria do rozsahu jej pôsobnosti.

---

[15] Odporúčanie Komisie 2003/361/ES zo 6. mája 2003 o vymedzení pojmov mikropodnik, malý a stredný podnik (Ú. v. EÚ L 124, 20.5.2003, s. 36).

[15] Odporúčanie Komisie 2003/361/ES zo 6. mája 2003 o vymedzení pojmov mikropodnik, malý a stredný podnik (Ú. v. EÚ L 124, 20.5.2003, s. 36).

Pozmeňujúci návrh 9

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.

Pozmeňujúci návrh 10

Návrh smernice
Odôvodnenie 9 a (nové)

Text predložený Komisiou	*Pozmeňujúci návrh*
	(9a) Členské štáty by mali vypracovať zoznam všetkých kľúčových a dôležitých subjektov. Tento zoznam by mal zahŕňať subjekty, ktoré spĺňajú všeobecne uplatniteľné kritériá týkajúce sa veľkosti, ako aj malé podniky a mikropodniky, ktoré spĺňajú určité kritériá, ktoré sú ukazovateľom ich kľúčovej úlohy pre hospodárstva alebo spoločnosti členských štátov. Na to, aby jednotky pre riešenie počítačových bezpečnostných incidentov (CSIRT) a príslušné orgány poskytovali pomoc a varovali subjekty pred kybernetickými incidentmi, ktoré by ich mohli ovplyvniť, je dôležité, aby tieto orgány mali správne kontaktné údaje týchto subjektov. Kľúčové a dôležité subjekty by preto mali príslušným orgánom predkladať aspoň tieto informácie: názov subjektu, adresu a aktuálne kontaktné údaje vrátane e-mailových adries, rozsahov IP adries, telefónnych čísel, ako aj príslušné odvetvie(-ia) a pododvetvie(-ia) uvedené v prílohách I a II. Subjekty by mali príslušným orgánom oznamovať akékoľvek zmeny týchto informácií. Členské štáty by mali bez zbytočného odkladu zabezpečiť, aby sa tieto informácie mohli ľahko poskytovať prostredníctvom jednotného kontaktného miesta. Na tento účel by agentúra ENISA v spolupráci so skupinou pre spoluprácu mala bez zbytočného odkladu vydať usmernenia a vzory týkajúce sa oznamovacích povinností. Členské štáty by mali Komisii a skupine pre spoluprácu oznámiť počet kľúčových a dôležitých subjektov. Členské štáty by tiež mali na účely preskúmania uvedeného v tejto smernici oznámiť Komisii názvy malých podnikov a mikropodnikov, ktoré boli identifikované ako kľúčové a dôležité subjekty, aby Komisia mohla posúdiť

	súlad medzi prístupmi členských štátov. S týmito informáciami by sa malo zaobchádzať ako s prísne dôvernými.

Pozmeňujúci návrh 11

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 ***by mala*** v spolupráci so skupinou pre spoluprácu ***a príslušnými 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 mikropodnikom a malým podnikom informácie.***

Pozmeňujúci návrh 12

Návrh smernice
Odôvodnenie 10 a (nové)

Text predložený Komisiou	*Pozmeňujúci návrh*
	(10a) Komisia by takisto mala vydať usmernenia na podporu členských štátov pri správnom vykonávaní ustanovení týkajúcich sa rozsahu pôsobnosti a na hodnotenie primeranosti povinností stanovených v tejto smernici, najmä pokiaľ ide o subjekty s komplexnými obchodnými modelmi alebo prevádzkovým prostredím, pričom subjekt môže súčasne spĺňať kritériá určené pre kľúčové aj dôležité subjekty, alebo môže súčasne vykonávať činnosti, z ktorých niektoré patria do rozsahu pôsobnosti tejto smernice a niektoré nie.

Pozmeňujúci návrh 13

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. ***Právne akty Únie špecifické pre jednotlivé odvetvia, ktoré vyžadujú, aby kľúčové alebo dôležité subjekty prijali opatrenia na riadenie kybernetickobezpečnostných rizík alebo aby oznamovali závažné incidenty, by mali byť, ak je to možné, v súlade s príslušnou terminológiou a odkazovať na vymedzenie pojmov stanovených v tejto smernici.*** 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***,*** a ***ak majú tieto požiadavky*** aspoň rovnocenný účinok ako povinnosti stanovené v tejto smernici ***a vzťahujú sa na všetky bezpečnostné aspekty operácií a služieb poskytovaných kľúčovými a dôležitými subjektmi,*** mali by sa uplatňovať dané ustanovenia pre určité odvetvia vrátane ustanovení o dohľade a presadzovaní práva. Komisia ***by mala*** vydať ***komplexné*** usmernenia týkajúce sa vykonávania lex specialis ***s prihliadnutím na príslušné stanoviská, odborné znalosti a najlepšie postupy agentúry ENISA a skupiny pre spoluprácu***. Touto smernicou sa nebráni prijatiu ďalších odvetvových aktov Únie, ktoré sa zaoberajú opatreniami na riadenie kybernetickobezpečnostných rizík a oznamovaním incidentov ***a ktoré riadne zohľadnia potrebu komplexného a súdržného rámca pre kybernetickú bezpečnosť***. Touto smernicou nie sú dotknuté existujúce vykonávacie právomoci, ktoré boli Komisii udelené vo viacerých odvetviach vrátane dopravy a energetiky.

Pozmeňujúci návrh 14

Návrh smernice
Odôvodnenie 14

Text predložený Komisiou	*Pozmeňujúci návrh*
(14) Vzhľadom na prepojenia medzi kybernetickou bezpečnosťou a fyzickou bezpečnosťou subjektov by sa mal zabezpečiť jednotný prístup medzi smernicou Európskeho parlamentu a Rady (EÚ) XXX/XXX[17] a touto smernicou. Na dosiahnutie tohto cieľa by členské štáty mali zabezpečiť, aby sa kritické subjekty (a rovnocenné subjekty) podľa smernice (EÚ) XXX/XXX považovali za kľúčové subjekty podľa tejto smernice. Členské štáty by tiež mali zabezpečiť, aby ich stratégie kybernetickej bezpečnosti poskytovali politický rámec pre posilnenú koordináciu medzi ***príslušným orgánom*** podľa tejto smernice a príslušným orgánom podľa smernice (EÚ) XXX/XXX v kontexte zdieľania informácií o incidentoch a kybernetických hrozbách, ako aj vykonávania úloh dohľadu. Orgány, na ktoré sa obe smernice vzťahujú, by mali spolupracovať a vymieňať si informácie, najmä pokiaľ ide o identifikáciu kritických subjektov, kybernetické hrozby, kybernetickobezpečnostné riziká, incidenty ovplyvňujúce kritické subjekty, ako aj o kybernetickobezpečnostných opatreniach prijatých kritickými subjektmi. Príslušné orgány podľa tejto smernice by na žiadosť príslušných orgánov podľa smernice (EÚ) XXX/XXX mali byť oprávnené vykonávať svoje právomoci v oblasti dohľadu a presadzovania práva vo vzťahu ku kľúčovému subjektu identifikovanému ako kritický subjekt. Na tento účel by oba orgány mali spolupracovať a vymieňať si informácie.	(14) Vzhľadom na prepojenia medzi kybernetickou bezpečnosťou a fyzickou bezpečnosťou subjektov by sa mal zabezpečiť jednotný prístup medzi smernicou Európskeho parlamentu a Rady (EÚ) XXX/XXX[17] a touto smernicou. Na dosiahnutie tohto cieľa by členské štáty mali zabezpečiť, aby sa kritické subjekty (a rovnocenné subjekty) podľa smernice (EÚ) XXX/XXX považovali za kľúčové subjekty podľa tejto smernice. Členské štáty by tiež mali zabezpečiť, aby ich stratégie kybernetickej bezpečnosti poskytovali politický rámec pre posilnenú koordináciu medzi ***príslušnými orgánmi v rámci členských štátov a medzi členskými štátmi*** podľa tejto smernice a príslušným orgánom podľa smernice (EÚ) XXX/XXX v kontexte zdieľania informácií o incidentoch a kybernetických hrozbách, ako aj vykonávania úloh dohľadu. Orgány, na ktoré sa obe smernice vzťahujú, by mali spolupracovať a vymieňať si informácie ***bez zbytočného odkladu***, najmä pokiaľ ide o identifikáciu kritických subjektov, kybernetické hrozby, kybernetickobezpečnostné riziká, incidenty ovplyvňujúce kritické subjekty, ako aj o kybernetickobezpečnostných opatreniach prijatých kritickými subjektmi. Príslušné orgány podľa tejto smernice by na žiadosť príslušných orgánov podľa smernice (EÚ) XXX/XXX mali byť oprávnené vykonávať svoje právomoci v oblasti dohľadu a presadzovania práva vo vzťahu ku kľúčovému subjektu identifikovanému ako kritický subjekt. Na tento účel by oba orgány mali spolupracovať a vymieňať si informácie ***pokiaľ možno v reálnom čase***.
[17] [vložte celý názov a odkaz na	[17] [vložte celý názov a odkaz na

uverejnenie v ú. v., keď budú známe]	uverejnenie v ú. v., keď budú známe]

Pozmeňujúci návrh 15

Návrh smernice
Odôvodnenie 15

Text predložený Komisiou	*Pozmeňujúci návrh*
(15) Potvrdenie a udržanie spoľahlivého, odolného a bezpečného systému doménových mien (DNS) je kľúčovým faktorom zachovania integrity internetu a je nevyhnutné pre jeho nepretržité a stabilné fungovanie, od ktorého závisí digitálne hospodárstvo a spoločnosť. Táto smernica by sa preto mala vzťahovať na ***všetkých poskytovateľov služieb DNS v rozlišovacom reťazci DNS vrátane prevádzkovateľov koreňových menných serverov, menných serverov domén najvyššej úrovne (TLD), autoritatívnych menných serverov pre doménové mená a rekurzívne resolvery***.	(15) Potvrdenie a udržanie spoľahlivého, odolného a bezpečného systému doménových mien (DNS) je kľúčovým faktorom zachovania integrity internetu a je nevyhnutné pre jeho nepretržité a stabilné fungovanie, od ktorého závisí digitálne hospodárstvo a spoločnosť. Táto smernica by sa preto mala vzťahovať na ***menné servery domén najvyššej úrovne (TLD), verejne dostupné služby rekurzívneho rozlišovania doménových mien pre koncových používateľov internetu a služby autoritatívneho rozlišovania doménových mien. Táto smernica sa nevzťahuje na koreňové menné servery***.

Pozmeňujúci návrh 16

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***, pri zohľadnení stupňa ich závislosti od sietí a informačných systémov***. Dopravné 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 17

Návrh smernice
Odôvodnenie 20

Text predložený Komisiou	*Pozmeňujúci návrh*
(20) Táto rastúca previazanosť je výsledkom čoraz väčšej cezhraničnej a previazanej siete poskytovania služieb s využitím kľúčových infraštruktúr v celej Únii v odvetviach energetiky, dopravy, digitálnej infraštruktúry, pitnej a odpadovej vody, zdravia, určitých aspektov verejnej správy, ako aj kozmického priestoru, pokiaľ ide o poskytovanie určitých služieb v závislosti od pozemných infraštruktúr, ktoré vlastnia, spravujú a prevádzkujú členské štáty alebo súkromné strany, a preto sa nevzťahujú na infraštruktúry vlastnené, spravované alebo prevádzkované Úniou alebo v jej mene ako súčasť jej vesmírnych programov. Táto previazanosť znamená, že akékoľvek narušenie, dokonca aj také, ktoré sa pôvodne obmedzovalo na jeden subjekt alebo jedno odvetvie, môže mať širšie kaskádovité účinky, čo môže viesť k ďalekosiahlym a dlhotrvajúcim negatívnym vplyvom na poskytovanie služieb na celom vnútornom trhu. ***Pandémia ochorenia*** COVID-19 ***ukázala*** zraniteľnosť našich čoraz previazanejších spoločností voči rizikám s nízkou pravdepodobnosťou.	(20) Táto rastúca previazanosť je výsledkom čoraz väčšej cezhraničnej a previazanej siete poskytovania služieb s využitím kľúčových infraštruktúr v celej Únii v odvetviach energetiky, dopravy, digitálnej infraštruktúry, pitnej a odpadovej vody, zdravia, určitých aspektov verejnej správy, ako aj kozmického priestoru, pokiaľ ide o poskytovanie určitých služieb v závislosti od pozemných infraštruktúr, ktoré vlastnia, spravujú a prevádzkujú členské štáty alebo súkromné strany, a preto sa nevzťahujú na infraštruktúry vlastnené, spravované alebo prevádzkované Úniou alebo v jej mene ako súčasť jej vesmírnych programov. Táto previazanosť znamená, že akékoľvek narušenie, dokonca aj také, ktoré sa pôvodne obmedzovalo na jeden subjekt alebo jedno odvetvie, môže mať širšie kaskádovité účinky, čo môže viesť k ďalekosiahlym a dlhotrvajúcim negatívnym vplyvom na poskytovanie služieb na celom vnútornom trhu. ***Intenzívnejšie útoky na siete a informačné systémy počas pandémie*** COVID-19 ***ukázali*** zraniteľnosť našich čoraz previazanejších spoločností voči rizikám s nízkou pravdepodobnosťou.

Pozmeňujúci návrh 18

Návrh smernice
Odôvodnenie 24

Text predložený Komisiou	*Pozmeňujúci návrh*
(24) Členské štáty by mali mať primerané vybavenie, pokiaľ ide o technické a organizačné kapacity, aby mohli predchádzať incidentom a rizikám v oblasti sietí a informačných systémov, odhaľovať ich, reagovať na ne a zmierňovať ich. Členské štáty by preto mali ***zabezpečiť, aby mali dobre fungujúce jednotky CSIRT, známe aj ako jednotky reakcie na núdzové počítačové situácie (ďalej len „jednotky CERT“), ktoré budú dodržiavať*** základné požiadavky s cieľom zaručiť účinné a zlučiteľné kapacity na riešenie incidentov a rizík a zabezpečiť účinnú spoluprácu na úrovni Únie. S cieľom posilniť dôverný vzťah medzi subjektmi a jednotkami CSIRT v prípadoch, keď je jednotka CSIRT súčasťou príslušného orgánu, by členské štáty mali zvážiť funkčné oddelenie operačných úloh poskytovaných jednotkami CSIRT, najmä pokiaľ ide o zdieľanie informácií a podporu subjektov, od činností dohľadu príslušných orgánov.	(24) Členské štáty by mali mať primerané vybavenie, pokiaľ ide o technické a organizačné kapacity, aby mohli predchádzať incidentom a rizikám v oblasti sietí a informačných systémov, odhaľovať ich, reagovať na ne a zmierňovať ich. Členské štáty by preto mali ***určiť jednu alebo viac jednotiek CSIRT podľa tejto smernice a zabezpečiť, aby dobre fungovali a dodržiavali*** základné požiadavky s cieľom zaručiť účinné a zlučiteľné kapacity na riešenie incidentov a rizík a zabezpečiť účinnú spoluprácu na úrovni Únie***. Členské štáty môžu ako jednotky CSIRT určiť existujúce jednotky reakcie na núdzové počítačové situácie (CERT).*** S cieľom posilniť dôverný vzťah medzi subjektmi a jednotkami CSIRT v prípadoch, keď je jednotka CSIRT súčasťou príslušného orgánu, by členské štáty mali zvážiť funkčné oddelenie operačných úloh poskytovaných jednotkami CSIRT, najmä pokiaľ ide o zdieľanie informácií a podporu subjektov, od činností dohľadu príslušných orgánov.

Pozmeňujúci návrh 19

Návrh smernice
Odôvodnenie 25

Text predložený Komisiou	*Pozmeňujúci návrh*
(25) Pokiaľ ide o osobné údaje, jednotky CSIRT by mali mať možnosť vykonávať v súlade s nariadením Európskeho parlamentu a Rady (EÚ) 2016/679[19] v mene subjektu a na jeho žiadosť podľa tejto smernice proaktívnu kontrolu sietí a informačných systémov používaných na poskytovanie jeho služieb. Členské štáty by sa mali zamerať na zabezpečenie rovnakej úrovne technických kapacít pre všetky odvetvové jednotky CSIRT.	(25) Pokiaľ ide o osobné údaje, jednotky CSIRT by mali mať možnosť vykonávať v súlade s nariadením Európskeho parlamentu a Rady (EÚ) 2016/679[19] v mene subjektu a na jeho žiadosť podľa tejto smernice ***alebo v prípade vážnej hrozby pre národnú bezpečnosť*** proaktívnu kontrolu sietí a informačných systémov používaných na poskytovanie jeho služieb. Členské štáty by sa mali zamerať na zabezpečenie rovnakej úrovne

Členské štáty môžu pri tvorbe vnútroštátnych jednotiek CSIRT požiadať o pomoc Agentúru Európskej únie pre kybernetickú bezpečnosť (ENISA).	technických kapacít pre všetky odvetvové jednotky CSIRT. Členské štáty môžu pri tvorbe vnútroštátnych jednotiek CSIRT požiadať o pomoc Agentúru Európskej únie pre kybernetickú bezpečnosť (ENISA).
[19] Nariadenie Európskeho parlamentu a Rady (EÚ) 2016/679 z 27. apríla 2016 o ochrane fyzických osôb pri spracúvaní osobných údajov a o voľnom pohybe takýchto údajov, ktorým sa zrušuje smernica 95/46/ES (všeobecné nariadenie o ochrane údajov) (Ú. v. EÚ L 119, 4.5.2016, s. 1).	[19] Nariadenie Európskeho parlamentu a Rady (EÚ) 2016/679 z 27. apríla 2016 o ochrane fyzických osôb pri spracúvaní osobných údajov a o voľnom pohybe takýchto údajov, ktorým sa zrušuje smernica 95/46/ES (všeobecné nariadenie o ochrane údajov) (Ú. v. EÚ L 119, 4.5.2016, s. 1).

Pozmeňujúci návrh 20

Návrh smernice
Odôvodnenie 25 a (nové)

Text predložený Komisiou	*Pozmeňujúci návrh*
	(25a) Jednotky CSIRT by mali byť na žiadosť subjektu schopné nepretržite objavovať, spravovať a monitorovať všetky aktíva orientované na internet, a to na pracoviskách, ako aj mimo nich, aby pochopili ich celkové organizačné riziko pre novoobjavené ohrozenie dodávateľského reťazca alebo kritické zraniteľnosti. Informácie o tom, či subjekt prevádzkuje privilegované rozhranie správy, ovplyvňujú rýchlosť vykonávania zmierňujúcich opatrení.

Pozmeňujúci návrh 21

Návrh smernice
Odôvodnenie 26

Text predložený Komisiou	*Pozmeňujúci návrh*
(26) Vzhľadom na význam medzinárodnej spolupráce v oblasti kybernetickej bezpečnosti by sa malo jednotkám CSIRT umožniť, aby sa okrem siete jednotiek CSIRT zriadenej podľa tejto smernice	(26) Vzhľadom na význam medzinárodnej spolupráce v oblasti kybernetickej bezpečnosti by sa malo jednotkám CSIRT umožniť, aby sa okrem siete jednotiek CSIRT zriadenej podľa tejto smernice

mohli stať súčasťou sietí medzinárodnej spolupráce.	mohli stať súčasťou sietí medzinárodnej spolupráce***, a to aj s jednotkami CSIRT z tretích krajín, ak je výmena informácií vzájomná a prispieva k bezpečnosti občanov a subjektov, s cieľom prispieť k rozvoju noriem Únie, ktoré môžu formovať prostredie kybernetickej bezpečnosti na medzinárodnej úrovni. Členské štáty by mohli preskúmať aj možnosť zintenzívnenia spolupráce s podobne zmýšľajúcimi partnerskými krajinami a medzinárodnými organizáciami, a to s cieľom zabezpečiť multilaterálne dohody o kybernetických normách, zodpovednom správaní štátnych a neštátnych subjektov v kybernetickom priestore a účinnej globálnej digitálnej správe a tiež vytvoriť otvorený, slobodný, stabilný a bezpečný kybernetický priestor na základe medzinárodného práva.***

Pozmeňujúci návrh 22

Návrh smernice
Odôvodnenie 26 a (nové)

Text predložený Komisiou	*Pozmeňujúci návrh*
	(26a) Politiky kybernetickej hygieny poskytujú základy pre ochranu infraštruktúry sietí a informačných systémov, hardvéru, softvéru a bezpečnosti online aplikácií a obchodných údajov alebo údajov koncových používateľov, na ktoré sa subjekty spoliehajú. Politiky kybernetickej hygieny zahŕňajúce spoločný základný súbor postupov, okrem iného aktualizácie softvéru a hardvéru, zmeny hesiel, riadenie nových inštalácií, obmedzenie prístupových účtov na úrovni správcu a zálohovanie údajov, umožňujú proaktívny rámec pripravenosti a celkovej bezpečnosti a ochrany v prípade incidentov alebo hrozieb. Agentúra ENISA by mala monitorovať a posudzovať politiky kybernetickej hygieny členských štátov a preskúmať celoúnijné

systémy s cieľom umožniť cezhraničné kontroly, ktoré zabezpečujú rovnocennosť nezávisle od požiadaviek členských štátov.

Pozmeňujúci návrh 23

Návrh smernice
Odôvodnenie 26 b (nové)

Text predložený Komisiou	*Pozmeňujúci návrh*
	(26b) Využívanie umelej inteligencie v kybernetickej bezpečnosti má potenciál zlepšiť odhaľovanie a zastaviť útoky na siete a informačné systémy, čo umožňuje presmerovanie zdrojov na sofistikovanejšie útoky. Členské štáty by preto mali vo svojich vnútroštátnych stratégiách podporovať využívanie (polo)automatizovaných nástrojov v oblasti kybernetickej bezpečnosti a zdieľanie údajov potrebných pre vyvíjanie a zlepšovanie automatizovaných nástrojov v oblasti kybernetickej bezpečnosti. S cieľom zmierniť riziká neoprávneného zasahovania do práv a slobôd jednotlivcov, ktoré môžu systémy založené na umelej inteligencii predstavovať, sa uplatňujú požiadavky na špecificky navrhnutú a štandardnú ochranu údajov stanovenú v článku 25 nariadenia (EÚ) 2016/679. Takéto riziká by mohli byť ďalej zmiernené začlenením vhodných záruk, ako je pseudonymizácia, šifrovanie, presnosť údajov a minimalizácia údajov.

Pozmeňujúci návrh 24

Návrh smernice
Odôvodnenie 26 c (nové)

Text predložený Komisiou	*Pozmeňujúci návrh*
	(26c) Nástroje a aplikácie kybernetickej bezpečnosti s otvoreným zdrojovým kódom môžu prispieť k vyššej miere transparentnosti a môžu mať pozitívny vplyv na efektívnosť priemyselných inovácií. Otvorené normy uľahčujú

interoperabilitu medzi bezpečnostnými nástrojmi, čo je v prospech bezpečnosti zainteresovaných strán z oblasti priemyslu. Nástroje a aplikácie kybernetickej bezpečnosti s otvoreným zdrojovým kódom môžu mobilizovať širšiu komunitu vývojárov a umožniť subjektom uplatňovať diverzifikáciu predajcov a otvorené bezpečnostné stratégie. Otvorená bezpečnosť môže viesť k transparentnejšiemu procesu overovania nástrojov súvisiacich s kybernetickou bezpečnosťou a ku komunitnému procesu objavovania zraniteľností. Členské štáty by preto mali podporovať používanie softvéru s otvoreným zdrojovým kódom a otvorených noriem uplatňovaním politík týkajúcich sa využívania otvorených údajov a otvoreného zdroja ako súčasť bezpečnosti prostredníctvom transparentnosti. Politiky podporujúce používanie a udržateľné využívanie nástrojov kybernetickej bezpečnosti s otvoreným zdrojovým kódom majú osobitný význam pre malé a stredné podniky (MSP), ktoré čelia značným nákladom na vykonávanie, ktoré by sa mohli minimalizovať znížením potreby špecifických aplikácií alebo nástrojov.

Pozmeňujúci návrh 25

Návrh smernice
Odôvodnenie 26 d (nové)

Text predložený Komisiou	*Pozmeňujúci návrh*
	(26d) Verejno-súkromné partnerstvá v oblasti kybernetickej bezpečnosti môžu poskytnúť vhodný rámec pre výmenu znalostí, výmenu najlepších postupov a vytvorenie spoločnej úrovne porozumenia medzi všetkými zainteresovanými stranami. Členské štáty by mali v rámci svojich národných stratégií kybernetickej bezpečnosti prijať politiky na podporu vytvárania verejno-súkromných partnerstiev špecificky zameraných na kybernetickú bezpečnosť. Tieto politiky by

	mali okrem iného spresniť rozsah a zapojené zainteresované strany, model riadenia, dostupné možnosti financovania a interakciu medzi zúčastnenými zainteresovanými stranami. Verejno-súkromné partnerstvá môžu využívať odborné znalosti subjektov súkromného sektora na podporu príslušných orgánov členských štátov pri rozvoji špičkových služieb a procesov, okrem iného vrátane výmeny informácií, včasného varovania, cvičení zameraných na kybernetickú hrozbu a incidenty, krízového riadenia a plánovania odolnosti.

Pozmeňujúci návrh 26

Návrh smernice
Odôvodnenie 27

Text predložený Komisiou	*Pozmeňujúci návrh*
(27) V súlade s prílohou k odporúčaniu Komisie (EÚ) 2017/1548 o koordinovanej reakcii na kybernetické incidenty a krízy veľkého rozsahu (ďalej len „koncepcia“)[20] by incident veľkého rozsahu mal znamenať incident s významným dosahom na najmenej dva členské štáty alebo ktorý svojím narušením presahuje schopnosť členského štátu reagovať naň. Incidenty veľkého rozsahu sa v závislosti od svojej príčiny a dosahu môžu vystupňovať a naplno prepuknúť v krízu, ktorá neumožňuje riadne fungovanie vnútorného trhu. Vzhľadom na široký rozsah a vo väčšine prípadov cezhraničný charakter takýchto incidentov by členské štáty a príslušné inštitúcie, orgány a agentúry Únie mali spolupracovať na technickej, prevádzkovej a politickej úrovni s cieľom riadne koordinovať reakciu v celej Únii.	(27) V súlade s prílohou k odporúčaniu Komisie (EÚ) 2017/1548 o koordinovanej reakcii na kybernetické incidenty a krízy veľkého rozsahu (ďalej len „koncepcia“)[20] by incident veľkého rozsahu mal znamenať incident s významným dosahom na najmenej dva členské štáty alebo ktorý svojím narušením presahuje schopnosť členského štátu reagovať naň. Incidenty veľkého rozsahu sa v závislosti od svojej príčiny a dosahu môžu vystupňovať a naplno prepuknúť v krízu, ktorá neumožňuje riadne fungovanie vnútorného trhu ***alebo predstavuje vážne rizika pre verejnú bezpečnosť a ochranu subjektov alebo občanov v niekoľkých členských štátoch alebo v Únii ako celku***. Vzhľadom na široký rozsah a vo väčšine prípadov cezhraničný charakter takýchto incidentov by členské štáty a príslušné inštitúcie, orgány a agentúry Únie mali spolupracovať na technickej, prevádzkovej a politickej úrovni s cieľom riadne koordinovať reakciu v celej Únii.
[20] Odporúčanie Komisie (EÚ) 2017/1584 z	[20] Odporúčanie Komisie (EÚ) 2017/1584 z

13. septembra 2017 o koordinovanej reakcii na kybernetické incidenty a krízy veľkého rozsahu (Ú. v. EÚ L 239, 19.9.2017, s. 36).	13. septembra 2017 o koordinovanej reakcii na kybernetické incidenty a krízy veľkého rozsahu (Ú. v. EÚ L 239, 19.9.2017, s. 36).

Pozmeňujúci návrh 27

Návrh smernice
Odôvodnenie 27 a (nové)

Text predložený Komisiou	*Pozmeňujúci návrh*
	(27a) Členské štáty by sa mali v rámci svojich národných stratégií kybernetickej bezpečnosti zamerať na osobitné potreby MSP v oblasti kybernetickej bezpečnosti. MSP predstavujú v kontexte Únie veľký percentuálny podiel priemyselného a obchodného trhu a v prepojenejšom svete majú často problém prispôsobiť sa novým obchodným postupom a orientovať sa v digitálnom prostredí, v ktorom zamestnanci pracujú z domu a obchodné činnosti sa čoraz častejšie vykonávajú online. Niektoré MSP čelia osobitným výzvam v oblasti kybernetickej bezpečnosti, ako je nízke povedomie o kybernetickej bezpečnosti, nedostatočná bezpečnosť IT na diaľku, vysoké náklady na riešenia v oblasti kybernetickej bezpečnosti a zvýšená úroveň hrozieb, ako je napríklad ransomware, v súvislosti s ktorými by mali dostať usmernenia a podporu. Členské štáty by mali mať pre MSP zriadené jednotné kontaktné miesto pre kybernetickú bezpečnosť, ktoré poskytuje usmernenia a podporu pre MSP, alebo ich nasmeruje na príslušné subjekty poskytujúce usmernenia a podporu v otázkach súvisiacich s kybernetickou bezpečnosťou. Členské štáty sa nabádajú, aby malým podnikom a mikropodnikom, ktoré nemajú tieto kapacity, ponúkali aj služby, ako je konfigurácia webových stránok a protokolovanie.

Pozmeňujúci návrh 28

Návrh smernice
Odôvodnenie 27 b (nové)

Text predložený Komisiou	*Pozmeňujúci návrh*
	(27b) Členské štáty by mali v rámci svojich národných stratégií kybernetickej bezpečnosti prijať politiky na podporu aktívnej kybernetickej obrany. Aktívna kybernetická obrana je proaktívna prevencia, odhaľovanie, monitorovanie, analýza a zmierňovanie narušení bezpečnosti siete v kombinácii s využitím kapacít nasadených v zasiahnutej sieti a mimo nej. Schopnosť rýchlo a automaticky zdieľať a pochopiť informácie a analýzy týkajúce sa hrozieb, varovaní pred kybernetickou činnosťou a opatrení reakcie je zásadne dôležitá pre umožnenie jednotného úsilia o úspešné odhaľovanie, prevenciu a riešenie útokov proti sieťam a informačným systémom. Aktívna kybernetická obrana je založená na obrannej stratégii, ktorá vylučuje ofenzívne opatrenia proti kritickej civilnej infraštruktúre.

Pozmeňujúci návrh 29

Návrh smernice
Odôvodnenie 28

Text predložený Komisiou	*Pozmeňujúci návrh*
(28) Keďže využívanie zraniteľností v sieťach a informačných systémoch môže spôsobiť značné narušenie a škody, rýchla identifikácia a náprava týchto zraniteľností je dôležitým faktorom pri znižovaní kybernetickobezpečnostného rizika. Subjekty, ktoré takéto systémy vyvíjajú, by preto mali zaviesť vhodné postupy na riešenie zistených zraniteľností. Keďže zraniteľnosti často odhaľujú a oznamujú (zverejňujú) tretie strany (oznamujúce subjekty), výrobca alebo poskytovateľ produktov alebo služieb IKT by mal zaviesť aj potrebné postupy na získavanie informácií o zraniteľnosti od tretích strán.	(28) Keďže využívanie zraniteľností v sieťach a informačných systémoch môže spôsobiť značné narušenie a škody, rýchla identifikácia a náprava týchto zraniteľností je dôležitým faktorom pri znižovaní kybernetickobezpečnostného rizika. Subjekty, ktoré takéto systémy vyvíjajú, by preto mali zaviesť vhodné postupy na riešenie zistených zraniteľností. Keďže zraniteľnosti často odhaľujú a oznamujú (zverejňujú) tretie strany (oznamujúce subjekty), výrobca alebo poskytovateľ produktov alebo služieb IKT by mal zaviesť aj potrebné postupy na získavanie informácií o zraniteľnosti od tretích strán.

V tejto súvislosti sa v medzinárodnej norme ISO/IEC 30111 poskytujú usmernenia na riešenie zraniteľností a v medzinárodnej norme ISO/IEC 29417 zasa usmernenia na zverejňovanie informácií o zraniteľnosti. ***Pokiaľ ide o*** zverejňovanie informácií o zraniteľnosti***,*** obzvlášť ***dôležitá je koordinácia*** medzi oznamujúcimi subjektmi a výrobcami alebo poskytovateľmi produktov alebo služieb IKT. Koordinované zverejňovanie informácií o zraniteľnosti sa riadi štruktúrovaným procesom, v rámci ktorého sa zraniteľnosti hlásia organizáciám takým spôsobom, ktorým sa danej organizácii umožňuje diagnostikovať zraniteľnosť a zabezpečiť jej nápravu pred tým, ako sa podrobné informácie o zraniteľnosti poskytnú tretím stranám alebo verejnosti. Koordinované zverejňovanie informácií o zraniteľnosti by malo zahŕňať aj koordináciu medzi oznamujúcim subjektom a organizáciou, pokiaľ ide o načasovanie nápravy a zverejnenie zraniteľností.	V tejto súvislosti sa v medzinárodnej norme ISO/IEC 30111 poskytujú usmernenia na riešenie zraniteľností a v medzinárodnej norme ISO/IEC 29417 zasa usmernenia na zverejňovanie informácií o zraniteľnosti. ***Na uľahčenie dobrovoľného rámca pre*** zverejňovanie informácií o zraniteľnosti ***je*** obzvlášť ***dôležité posilnenie koordinácie*** medzi oznamujúcimi subjektmi a výrobcami alebo poskytovateľmi produktov alebo služieb IKT. Koordinované zverejňovanie informácií o zraniteľnosti sa riadi štruktúrovaným procesom, v rámci ktorého sa zraniteľnosti hlásia organizáciám takým spôsobom, ktorým sa danej organizácii umožňuje diagnostikovať zraniteľnosť a zabezpečiť jej nápravu pred tým, ako sa podrobné informácie o zraniteľnosti poskytnú tretím stranám alebo verejnosti. Koordinované zverejňovanie informácií o zraniteľnosti by malo zahŕňať aj koordináciu medzi oznamujúcim subjektom a organizáciou, pokiaľ ide o načasovanie nápravy a zverejnenie zraniteľností.

Pozmeňujúci návrh 30

Návrh smernice
Odôvodnenie 28 a (nové)

Text predložený Komisiou	*Pozmeňujúci návrh*
	(28a) Komisia, agentúra ENISA a členské štáty by mali naďalej podporovať medzinárodné zosúladenie s normami a existujúcimi najlepšími odvetvovými postupmi v oblasti riadenia rizík, napríklad v oblastiach posudzovania bezpečnosti dodávateľského reťazca, zdieľania informácií a zverejňovania informácií o zraniteľnosti.

Pozmeňujúci návrh 31

Návrh smernice
Odôvodnenie 29

Text predložený Komisiou	*Pozmeňujúci návrh*
(29) Členské štáty by preto mali prijať opatrenia na uľahčenie koordinovaného zverejňovania informácií o zraniteľnostiach zavedením príslušnej vnútroštátnej politiky. V tejto ***súvislosti*** by členské štáty mali ***určiť jednotku CSIRT, ktorá by prevzala úlohu „koordinátora“***, ***ktorý by v prípade potreby pôsobil ako sprostredkovateľ medzi oznamujúcimi subjektmi a výrobcami alebo poskytovateľmi produktov alebo služieb IKT***. ***Úlohy koordinátora jednotiek CSIRT by mali zahŕňať najmä identifikáciu*** a ***kontaktovanie dotknutých subjektov, podporu oznamujúcich subjektov***, ***rokovania o harmonograme zverejňovania informácií a riadenie koordinovaného zverejňovania informácií o*** zraniteľnosti, ***ktoré majú vplyv na viaceré organizácie (zverejňovanie informácií o zraniteľnosti viacerých strán)***. ***Ak majú zraniteľnosti vplyv na viacerých výrobcov alebo poskytovateľov produktov alebo služieb IKT usadených vo viac ako jednom členskom štáte, určené jednotky CSIRT*** z ***každého dotknutého členského štátu by mali spolupracovať v rámci siete jednotiek CSIRT***.	(29) Členské štáty ***v spolupráci s agentúrou ENISA*** by preto mali prijať opatrenia na uľahčenie koordinovaného zverejňovania informácií o zraniteľnostiach zavedením príslušnej vnútroštátnej politiky. V ***rámci*** tejto ***vnútroštátnej politiky*** by členské štáty mali ***riešiť problémy***, ***s ktorými sa stretávajú výskumní pracovníci zaoberajúci sa zraniteľnosťami***. ***Subjekty*** a ***fyzické osoby***, ***ktoré skúmajú*** zraniteľnosti, ***môžu byť v niektorých členských štátoch vystavení trestnej a občianskoprávnej zodpovednosti***. ***Členské štáty sa preto nabádajú, aby vydali usmernenia, pokiaľ ide o nestíhanie výskumu v oblasti bezpečnosti informácií a vyňatie týchto činností z občianskoprávnej zodpovednosti***.

Pozmeňujúci návrh 32

Návrh smernice
Odôvodnenie 29 a (nové)

Text predložený Komisiou	*Pozmeňujúci návrh*
	(29a) Členské štáty by mali určiť jednotku CSIRT, ktorá by prevzala úlohu „koordinátora“, ktorý by v prípade potreby pôsobil ako sprostredkovateľ medzi oznamujúcimi subjektmi a výrobcami alebo poskytovateľmi produktov alebo služieb IKT, v prípade ktorých je pravdepodobné, že budú dotknuté zraniteľnosťami. Úlohy koordinátora jednotiek CSIRT by mali

	zahŕňať najmä identifikáciu a kontaktovanie dotknutých subjektov, podporu oznamujúcich subjektov, rokovania o harmonograme zverejňovania informácií a riadenie zraniteľností, ktoré majú vplyv na viaceré organizácie (zverejňovanie informácií o zraniteľnosti viacerých strán). Ak majú zraniteľnosti vplyv na viacerých výrobcov alebo poskytovateľov produktov alebo služieb IKT usadených vo viac ako jednom členskom štáte, určené jednotky CSIRT z každého dotknutého členského štátu by mali spolupracovať v rámci siete jednotiek CSIRT.

Pozmeňujúci návrh 33

Návrh smernice
Odôvodnenie 30

Text predložený Komisiou	*Pozmeňujúci návrh*
(30) Prístup k správnym a včasným informáciám o zraniteľnostiach ovplyvňujúcich produkty a služby IKT prispieva k lepšiemu riadeniu kybernetickobezpečnostných rizík. ***V tejto súvislosti sú*** zdroje verejne dostupných informácií o zraniteľnostiach dôležitým nástrojom pre subjekty a ich používateľov, ale aj pre príslušné vnútroštátne orgány a jednotky CSIRT. Agentúra ENISA by preto mala zriadiť ***register*** zraniteľností, v ***ktorom*** by kľúčové a dôležité subjekty a ich dodávatelia, ako aj subjekty, ktoré nepatria do rozsahu pôsobnosti tejto smernice, mohli dobrovoľne zverejňovať zraniteľnosti a poskytovať o nich informácie, ktoré používateľom umožnia prijať vhodné zmierňujúce opatrenia.	(30) Prístup k správnym a včasným informáciám o zraniteľnostiach ovplyvňujúcich produkty a služby IKT prispieva k lepšiemu riadeniu kybernetickobezpečnostných rizík. Zdroje verejne dostupných informácií o zraniteľnostiach ***sú*** dôležitým nástrojom pre subjekty a ich používateľov, ale aj pre príslušné vnútroštátne orgány a jednotky CSIRT. Agentúra ENISA by preto mala zriadiť ***databázu*** zraniteľností, v ***ktorej*** by kľúčové a dôležité subjekty a ich dodávatelia, ako aj subjekty, ktoré nepatria do rozsahu pôsobnosti tejto smernice, mohli dobrovoľne zverejňovať zraniteľnosti a poskytovať o nich informácie, ktoré používateľom umožnia prijať vhodné zmierňujúce opatrenia. ***Cieľom tejto databázy je riešiť jedinečné výzvy, ktoré predstavujú kybernetickobezpečnostné riziká pre európske subjekty. Agentúra ENISA by okrem toho mala zaviesť zodpovedný postup, pokiaľ ide o proces uverejňovania, s cieľom poskytnúť subjektom čas na prijatie opatrení na***

	zmiernenie ich zraniteľností, a zaviesť najmodernejšie kybernetickobezpečnostné opatrenia, ako aj strojovo čitateľné súbory údajov a zodpovedajúce rozhrania (API). S cieľom podporiť kultúru zverejňovania informácií o zraniteľnostiach by zverejnenie nemalo spôsobiť ujmu oznamujúcemu subjektu.

Pozmeňujúci návrh 34

Návrh smernice
Odôvodnenie 31

Text predložený Komisiou	*Pozmeňujúci návrh*
(31) ***Hoci podobné registre alebo databázy zraniteľností existujú, ich hostiteľmi a správcami sú subjekty, ktoré nie sú usadené v Únii. Európsky*** register zraniteľností***, ktorý vedie agentúra ENISA, by zabezpečil lepšiu transparentnosť, pokiaľ ide o proces uverejňovania pred tým***, ***ako je daná zraniteľnosť oficiálne oznámená, ako aj odolnosť v prípade narušenia alebo prerušenia poskytovania podobných služieb.*** Agentúra ENISA ***by mala*** preskúmať možnosť uzatvorenia dohôd o štruktúrovanej spolupráci s podobnými registrami v jurisdikciách tretích krajín ***s cieľom zabrániť duplicite úsilia a usilovať sa v čo najväčšej možnej miere o komplementaritu***.	(31) ***Európska databáza*** zraniteľností ***spravovaná agentúrou ENISA by mala využívať'*** register ***spoločných*** zraniteľností ***a expozícií (Common Vulnerabilities and Exposures – CVE) prostredníctvom použitia svojho rámca pre identifikáciu***, ***sledovanie a hodnotenie zraniteľností. S cieľom zabrániť duplicite úsilia a usilovať sa o komplementaritu by*** agentúra ENISA ***mala navyše*** preskúmať možnosť uzatvorenia dohôd o štruktúrovanej spolupráci s ***inými*** podobnými registrami ***alebo databázami*** v jurisdikciách tretích krajín.

Pozmeňujúci návrh 35

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	(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.

konkrétne odporúčania, ktorými sa má dosiahnuť lepšie vykonávanie existujúcich pravidiel***, najmä pokiaľ ide o uľahčenie zosúladenia pri transpozícii 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 odvetví v celej Únii. Týka sa to najmä odvetví, ktoré majú medzinárodný a cezhraničný charakter.***

Pozmeňujúci návrh 36

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 (EC3)***, Agentúra Európskej únie pre bezpečnosť letectva (EASA) a Agentúra Európskej únie pre vesmírny program (EUSPA), k účasti na jej práci.	(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 ***príslušných*** orgánov a agentúr Únie zapojených do politiky v oblasti kybernetickej bezpečnosti, ako je ***Europol***, Agentúra Európskej únie pre bezpečnosť letectva (EASA) a Agentúra Európskej únie pre vesmírny program (EUSPA), k účasti na jej práci.

Pozmeňujúci návrh 37

Návrh smernice
Odôvodnenie 35

Text predložený Komisiou	*Pozmeňujúci návrh*
(35) Príslušné orgány a jednotky CSIRT	(35) Príslušné orgány a jednotky CSIRT

by mali mať možnosť zúčastňovať sa na výmenných programoch pre úradníkov z iných členských štátov s cieľom zlepšovať spoluprácu. Príslušné orgány by mali prijať potrebné opatrenia, ktoré úradníkom z iných členských štátov umožnia zohrávať účinnú úlohu v činnostiach hostiteľského príslušného orgánu.	by mali mať možnosť zúčastňovať sa na výmenných programoch pre úradníkov z iných členských štátov ***v rámci štruktúrovaných pravidiel a mechanizmov podporujúcich rozsah pôsobnosti a prípadne požadovanú bezpečnostnú previerku úradníkov zúčastňujúcich sa na takýchto výmenných programoch*** s cieľom zlepšovať spoluprácu ***a posilniť dôveru medzi členskými štátmi***. Príslušné orgány by mali prijať potrebné opatrenia, ktoré úradníkom z iných členských štátov umožnia zohrávať účinnú úlohu v činnostiach hostiteľského príslušného orgánu ***alebo jednotky CSIRT***.

Pozmeňujúci návrh 38

Návrh smernice
Odôvodnenie 36

Text predložený Komisiou	*Pozmeňujúci návrh*
(36) Únia by v prípade potreby mala v súlade s článkom 218 ZFEÚ uzatvárať medzinárodné dohody s tretími krajinami alebo medzinárodnými organizáciami, ktorými môže povoľovať a organizovať ich účasť na niektorých činnostiach skupiny pre spoluprácu a siete jednotiek CSIRT. Takýmito dohodami by sa ***mala*** zabezpečiť primeraná ochrana údajov.	(36) Únia by v prípade potreby mala v súlade s článkom 218 ZFEÚ uzatvárať medzinárodné dohody s tretími krajinami alebo medzinárodnými organizáciami, ktorými môže povoľovať a organizovať ich účasť na niektorých činnostiach skupiny pre spoluprácu a siete jednotiek CSIRT. Takýmito dohodami by sa ***mali*** zabezpečiť ***záujmy Únie a*** primeraná ochrana údajov. ***Tým sa nevylučuje právo členských štátov spolupracovať s podobne zmýšľajúcimi tretími krajinami v oblasti riadenia zraniteľností a riadenia rizík kybernetickej bezpečnosti s cieľom uľahčiť podávanie správ a všeobecné zdieľanie informácií v súlade s právom Únie.***

Pozmeňujúci návrh 39

Návrh smernice
Odôvodnenie 38

Text predložený Komisiou	*Pozmeňujúci návrh*
(38) Na účely tejto smernice by sa pojem „riziko“ mal vzťahovať na potenciál straty alebo narušenia v dôsledku kybernetickobezpečnostného incidentu a mal by sa vyjadriť ako kombinácia rozsahu takejto straty alebo narušenia a pravdepodobnosti výskytu daného incidentu.	***vypúšťa sa***

Pozmeňujúci návrh 40

Návrh smernice
Odôvodnenie 39

Text predložený Komisiou	*Pozmeňujúci návrh*
(39) Na účely tejto smernice by sa pojem „udalosti odvrátené v poslednej chvíli“ mal vzťahovať na udalosť, ktorá by mohla spôsobiť škodu, ale úspešne sa zabránilo jej prejaveniu v plnej miere.	***vypúšťa sa***

Pozmeňujúci návrh 41

Návrh smernice
Odôvodnenie 40

Text predložený Komisiou	*Pozmeňujúci návrh*
(40) Opatrenia na riadenie rizika by mali zahŕňať opatrenia na identifikáciu ***rizika*** incidentov, opatrenia na predchádzanie incidentom ***a*** ich odhaľovanie a ***zvládanie***, ako aj opatrenia na zmiernenie ich vplyvu. Bezpečnosť sietí a informačných systémov by mala zahŕňať bezpečnosť uchovávaných, prenášaných a spracúvaných údajov.	(40) Opatrenia na riadenie rizika by mali zahŕňať opatrenia na identifikáciu ***všetkých rizík*** incidentov, opatrenia na predchádzanie incidentom***,*** ich odhaľovanie***, reakciu na ne*** a ***zotavenie sa z nich***, ako aj opatrenia na zmiernenie ich vplyvu. Bezpečnosť sietí a informačných systémov by mala zahŕňať bezpečnosť uchovávaných, prenášaných a spracúvaných údajov. ***Tieto systémy by mali zabezpečovať systémovú analýzu, pri ktorej sa rozčlenia rôzne procesy a interakcie medzi subsystémami a zohľadní sa ľudský faktor, s cieľom získať úplný obraz o bezpečnosti informačného systému.***

Pozmeňujúci návrh 42

Návrh smernice
Odôvodnenie 41

Text predložený Komisiou	*Pozmeňujúci návrh*
(41) S cieľom vyhnúť sa neprimeranému finančnému a administratívnemu zaťaženiu kľúčových a dôležitých subjektov by požiadavky na riadenie kybernetickobezpečnostných rizík mali byť primerané riziku, ktorým čelí daná sieť a daný informačný systém, berúc pritom do úvahy najnovší technický vývoj v oblasti takýchto opatrení.	(41) S cieľom vyhnúť sa neprimeranému finančnému a administratívnemu zaťaženiu kľúčových a dôležitých subjektov by požiadavky na riadenie kybernetickobezpečnostných rizík mali byť primerané riziku, ktorým čelí daná sieť a daný informačný systém, berúc pritom do úvahy najnovší technický vývoj v oblasti takýchto opatrení ***a európske alebo medzinárodné normy, ako sú ISO 31000 a ISA/IEC 27005***.

Pozmeňujúci návrh 43

Návrh smernice
Odôvodnenie 43

Text predložený Komisiou	*Pozmeňujúci návrh*
(43) Riešenie kybernetickobezpečnostných rizík vyplývajúcich z dodávateľského reťazca subjektu a jeho vzťahu s dodávateľmi je obzvlášť dôležité vzhľadom na výskyt incidentov, keď sa subjekty stali obeťami ***kybernetických útokov*** a keď aktéri s nekalými úmyslami dokázali ohroziť bezpečnosť sietí a informačných systémov subjektu využívaním zraniteľností a zasiahnuť tak produkty a služby tretích strán. Subjekty by preto mali posúdiť a zohľadniť celkovú kvalitu produktov a postupy svojich dodávateľov a poskytovateľov služieb v oblasti kybernetickej bezpečnosti vrátane ich bezpečných vývojových postupov.	(43) Riešenie kybernetickobezpečnostných rizík vyplývajúcich z dodávateľského reťazca subjektu a jeho vzťahu s dodávateľmi***, ako sú poskytovatelia služieb ukladania a spracúvania dát alebo riadených bezpečnostných služieb,*** je obzvlášť dôležité vzhľadom na výskyt incidentov, keď sa subjekty stali obeťami ***útokov na siete a informačné systémy*** a keď aktéri s nekalými úmyslami dokázali ohroziť bezpečnosť sietí a informačných systémov subjektu využívaním zraniteľností a zasiahnuť tak produkty a služby tretích strán. Subjekty by preto mali posúdiť a zohľadniť celkovú kvalitu ***a odolnosť*** produktov a ***služieb, kybernetickobezpečnostné opatrenia, ktoré zahŕňajú, a*** postupy svojich dodávateľov a poskytovateľov služieb v oblasti kybernetickej bezpečnosti vrátane ich bezpečných vývojových postupov. ***Subjekty by sa mali nabádať najmä k***

	tomu, aby začlenili kybernetickobezpečnostné opatrenia do zmluvných dohôd so svojimi dodávateľmi a poskytovateľmi služieb prvej úrovne. Subjekty by mohli zohľadniť kybernetickobezpečnostné riziká, ktoré vyplývajú zo strany dodávateľov a poskytovateľov služieb ďalších úrovní.

Pozmeňujúci návrh 44

Návrh smernice
Odôvodnenie 44

Text predložený Komisiou	*Pozmeňujúci návrh*
(44) Spomedzi poskytovateľov služieb zohrávajú poskytovatelia riadených bezpečnostných služieb (MSSP) osobitne dôležitú úlohu v pomoci subjektom v ich úsilí o odhaľovanie incidentov ***a*** reakciu na ne, a to v takých oblastiach, ako je reakcia na incidenty, penetračné testovanie, bezpečnostné audity a poradenstvo. Avšak aj samotní poskytovatelia MSSP boli cieľom kybernetických útokov a ich úzke zapojenie do činnosti prevádzkovateľov predstavuje osobitné kybernetickobezpečnostné riziko. Subjekty by preto mali výberu poskytovateľa MSSP venovať zvýšenú pozornosť.	(44) Spomedzi poskytovateľov služieb zohrávajú poskytovatelia riadených bezpečnostných služieb (MSSP) osobitne dôležitú úlohu v pomoci subjektom v ich úsilí o ***prevenciu,*** odhaľovanie incidentov***,*** reakciu na ne ***alebo zotavenie sa z nich***, a to v takých oblastiach, ako je reakcia na incidenty, penetračné testovanie, bezpečnostné audity a poradenstvo. Avšak aj samotní poskytovatelia MSSP boli cieľom kybernetických útokov a ich úzke zapojenie do činnosti prevádzkovateľov predstavuje osobitné kybernetickobezpečnostné riziko. Subjekty by preto mali výberu poskytovateľa MSSP venovať zvýšenú pozornosť.

Pozmeňujúci návrh 45

Návrh smernice
Odôvodnenie 45

Text predložený Komisiou	*Pozmeňujúci návrh*
(45) Subjekty by mali riešiť aj kybernetickobezpečnostné riziká vyplývajúce z ich interakcií a vzťahov s inými zainteresovanými stranami v rámci širšieho ekosystému. Predovšetkým by mali prijať vhodné opatrenia, aby sa ich spolupráca s akademickými a výskumnými inštitúciami uskutočňovala v súlade s ich politikami v oblasti kybernetickej	(45) Subjekty by mali riešiť aj kybernetickobezpečnostné riziká vyplývajúce z ich interakcií a vzťahov s inými zainteresovanými stranami v rámci širšieho ekosystému***, a to aj s cieľom bojovať proti priemyselnej špionáži a chrániť obchodné tajomstvo***. Predovšetkým by mali prijať vhodné opatrenia, aby sa ich spolupráca s

bezpečnosti a aby sa riadila osvedčenými postupmi, pokiaľ ide o bezpečný prístup k informáciám a ich šírenie vo všeobecnosti, a najmä o ochranu duševného vlastníctva. Podobne by subjekty, ktoré závisia od služieb v oblasti transformácie údajov a analýzy údajov od tretích strán, mali prijať všetky vhodné kybernetickobezpečnostné opatrenia, a to vzhľadom na význam a hodnotu údajov pre činnosti subjektov.	akademickými a výskumnými inštitúciami uskutočňovala v súlade s ich politikami v oblasti kybernetickej bezpečnosti a aby sa riadila osvedčenými postupmi, pokiaľ ide o bezpečný prístup k informáciám a ich šírenie vo všeobecnosti, a najmä o ochranu duševného vlastníctva. Podobne by subjekty, ktoré závisia od služieb v oblasti transformácie údajov a analýzy údajov od tretích strán, mali prijať všetky vhodné kybernetickobezpečnostné opatrenia, a to vzhľadom na význam a hodnotu údajov pre činnosti subjektov.

Pozmeňujúci návrh 46

Návrh smernice
Odôvodnenie 45 a (nové)

Text predložený Komisiou	*Pozmeňujúci návrh*
	(45a) Subjekty by mali prijať širokú škálu základných postupov v oblasti kybernetickej hygieny, ako sú architektúra nulovej dôvery, aktualizácie softvéru, konfigurácia zariadení, segmentácia siete, správa identity a prístupu alebo informovanosť používateľov, a organizovať školenia pre svojich zamestnancov zamerané na kybernetické hrozby pre podnikové e-maily, phishing alebo techniky sociálneho inžinierstva. Okrem toho by subjekty mali vyhodnotiť vlastné spôsobilosti v oblasti kybernetickej bezpečnosti a prípadne sa usilovať o integráciu technológií posilňujúcich kybernetickú bezpečnosť a využívajúcich umelú inteligenciu alebo systémy strojového učenia s cieľom automatizovať svoje spôsobilosti a ochranu sieťovej architektúry.

Pozmeňujúci návrh 47

Návrh smernice
Odôvodnenie 46

Text predložený Komisiou	*Pozmeňujúci návrh*
(46) V záujme ďalšieho riešenia rizík kľúčového dodávateľského reťazca a pomoci subjektom pôsobiacim v odvetviach, na ktoré sa vzťahuje táto smernica, pri náležitom riadení kybernetickobezpečnostných rizík súvisiacich s dodávateľským reťazcom a dodávateľmi, by skupina pre spoluprácu, do ktorej sú zapojené príslušné vnútroštátne orgány, mala v spolupráci s Komisiou a agentúrou ENISA vykonať koordinované ***odvetvové*** posúdenia rizík dodávateľského reťazca, ktoré sa už vykonali v prípade sietí 5G v nadväznosti na odporúčanie (EÚ) 2019/534 o kybernetickej bezpečnosti sietí 5G[21] s cieľom identifikovať za každé odvetvie kritické služby, systémy alebo produkty IKT, relevantné hrozby a zraniteľnosti.	(46) V záujme ďalšieho riešenia rizík kľúčového dodávateľského reťazca a pomoci subjektom pôsobiacim v odvetviach, na ktoré sa vzťahuje táto smernica, pri náležitom riadení kybernetickobezpečnostných rizík súvisiacich s dodávateľským reťazcom a dodávateľmi, by skupina pre spoluprácu, do ktorej sú zapojené príslušné vnútroštátne orgány, mala v spolupráci s Komisiou a agentúrou ENISA vykonať koordinované posúdenia rizík dodávateľského reťazca, ktoré sa už vykonali v prípade sietí 5G v nadväznosti na odporúčanie (EÚ) 2019/534 o kybernetickej bezpečnosti sietí 5G[21] s cieľom identifikovať za každé odvetvie kritické služby, systémy alebo produkty IKT ***a IKS***, relevantné hrozby a zraniteľnosti. ***Takéto posúdenia rizík by mali určiť opatrenia, plány zmierňovania a najlepšie postupy vo vzťahu ku kritickým závislostiam, potenciálnym jediným bodom zlyhania, hrozbám, zraniteľnostiam a ďalším rizikám spojeným s dodávateľským reťazcom a mali by preskúmať spôsoby, ako ďalej podporovať ich širšie prijatie subjektmi. Potenciálne netechnické rizikové faktory, ako je neprimeraný vplyv tretej krajiny na dodávateľov a poskytovateľov služieb, najmä v prípade alternatívnych modelov riadenia, zahŕňajú skryté zraniteľnosti alebo zadné vrátka a potenciálne systémové narušenie dodávok, najmä v prípade odkázanosti na určitého dodávateľa technológie alebo závislosti od poskytovateľa.***
[21] Odporúčanie Komisie (EÚ) 2019/534 z 26. marca 2019 Kybernetická bezpečnosť sietí 5G (Ú. v. EÚ L 88, 29.3.2019, s. 42).	[21] Odporúčanie Komisie (EÚ) 2019/534 z 26. marca 2019 Kybernetická bezpečnosť sietí 5G (Ú. v. EÚ L 88, 29.3.2019, s. 42).

Pozmeňujúci návrh 48

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 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.	(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 ***počas celého ich životného cyklu*** voči rušivým udalostiam a v) v prípade vznikajúcich služieb, systémov alebo produktov IKT ich potenciálny budúci význam pre činnosti subjektov. ***Okrem toho by sa osobitný dôraz mal klásť na služby, systémy alebo produkty IKT, na ktoré sa vzťahujú osobitné požiadavky, ktoré pochádzajú z tretích krajín.***

Pozmeňujúci návrh 49

Návrh smernice
Odôvodnenie 47 a (nové)

Text predložený Komisiou	*Pozmeňujúci návrh*
	(47a) Skupina zainteresovaných strán pre

certifikáciu kybernetickej bezpečnosti zriadená podľa článku 22 nariadenia Európskeho parlamentu a Rady (EÚ) 2019/881[1a] by mala vydať stanovisko k posúdeniam bezpečnostných rizík konkrétnych kritických služieb, systémov alebo produktov IKT a IKS v rámci dodávateľského reťazca. Skupina pre spoluprácu a agentúra ENISA by mali toto stanovisko zohľadniť.

[1a] Nariadenie Európskeho parlamentu a Rady (EÚ) 2019/881 zo 17. apríla 2019 o agentúre ENISA (Agentúra Európskej únie pre kybernetickú bezpečnosť) a o certifikácii kybernetickej bezpečnosti informačných a komunikačných technológií a o zrušení nariadenia (EÚ) č. 526/2013 (akt o kybernetickej bezpečnosti) (Ú. v. EÚ L 151, 7.6.2019, s. 15).

Pozmeňujúci návrh 50

Návrh smernice
Odôvodnenie 50

Text predložený Komisiou	*Pozmeňujúci návrh*
(50) Vzhľadom na rastúci význam interpersonálnych komunikačných služieb nezávislých od číslovania je potrebné zabezpečiť, aby takéto služby tiež podliehali príslušným bezpečnostným požiadavkám vzhľadom na ich špecifický charakter a hospodársky význam. Poskytovatelia takýchto služieb by preto mali takisto zabezpečiť takú úroveň bezpečnosti sietí a informačných systémov, ktorá zodpovedá miere daného rizika. Vzhľadom na to, že poskytovatelia interpersonálnych komunikačných služieb nezávislých od číslovania obyčajne nevykonávajú samotnú kontrolu nad prenosom signálov v sieťach, stupeň rizika sa v prípade takýchto služieb môže v niektorých aspektoch považovať za nižší ako v prípade tradičných elektronických komunikačných služieb. To isté platí pre	(50) Vzhľadom na rastúci význam interpersonálnych komunikačných služieb nezávislých od číslovania je potrebné zabezpečiť, aby takéto služby tiež podliehali príslušným bezpečnostným požiadavkám vzhľadom na ich špecifický charakter a hospodársky význam. Poskytovatelia takýchto služieb by preto mali takisto zabezpečiť takú úroveň bezpečnosti sietí a informačných systémov, ktorá zodpovedá miere daného rizika. Vzhľadom na to, že poskytovatelia interpersonálnych komunikačných služieb nezávislých od číslovania obyčajne nevykonávajú samotnú kontrolu nad prenosom signálov v sieťach, stupeň rizika ***pre bezpečnosť siete*** sa v prípade takýchto služieb môže v niektorých aspektoch považovať za nižší ako v prípade tradičných elektronických komunikačných

interpersonálne komunikačné služby, ktoré využívajú čísla a ktoré nevykonávajú skutočnú kontrolu nad prenosom signálu.

služieb. To isté platí pre interpersonálne komunikačné služby, ktoré využívajú čísla a ktoré nevykonávajú skutočnú kontrolu nad prenosom signálu. ***Keďže však priestor na útoky sa naďalej rozširuje, interpersonálne komunikačné služby nezávislé od číslovania, okrem iného vrátane sociálnych médií pre zasielanie správ, sa stávajú populárnymi vektormi útokov. Aktéri s nekalými úmyslami využívajú platformy na komunikáciu s obeťami a ich nalákanie na otvorenie napadnutých webových stránok, čím sa zvyšuje pravdepodobnosť incidentov zahŕňajúcich zneužívanie údajov, čo má následne vplyv na bezpečnosť informačných systémov.***

Pozmeňujúci návrh 51

Návrh smernice
Odôvodnenie 51

Text predložený Komisiou	*Pozmeňujúci návrh*
(51) Vnútorný trh je viac než kedykoľvek predtým závislý od fungovania internetu. Služby prakticky všetkých kľúčových a dôležitých subjektov sú závislé od služieb poskytovaných cez internet. V záujme zabezpečenia bezproblémového poskytovania služieb kľúčovými a dôležitými subjektmi je dôležité, aby verejné elektronické komunikačné siete, ako sú napríklad internetové chrbticové siete alebo podmorské komunikačné káble, mali zavedené vhodné kybernetickobezpečnostné opatrenia a aby oznamovali incidenty, ktoré sa ich týkajú.	(51) Vnútorný trh je viac než kedykoľvek predtým závislý od fungovania internetu. Služby prakticky všetkých kľúčových a dôležitých subjektov sú závislé od služieb poskytovaných cez internet. V záujme zabezpečenia bezproblémového poskytovania služieb kľúčovými a dôležitými subjektmi je dôležité, aby ***všetky*** verejné elektronické komunikačné siete, ako sú napríklad internetové chrbticové siete alebo podmorské komunikačné káble, mali zavedené vhodné kybernetickobezpečnostné opatrenia a aby oznamovali ***závažné*** incidenty, ktoré sa ich týkajú. ***Členské štáty by mali zabezpečiť zachovanie integrity a dostupnosti týchto verejných elektronických komunikačných sietí a mali by zvážiť ich ochranu pred sabotážou a špionážou zásadného bezpečnostného záujmu. Informácie o incidentoch, napríklad týkajúcich sa podmorských komunikačných káblov, by sa mali aktívne zdieľať medzi členskými štátmi.***

Pozmeňujúci návrh 52

Návrh smernice
Odôvodnenie 52

Text predložený Komisiou	*Pozmeňujúci návrh*
(52) V prípade potreby by subjekty mali informovať príjemcov svojich služieb o konkrétnych a významných hrozbách a o opatreniach, ktoré môžu prijať na zmiernenie vyplývajúceho rizika. ***Požiadavka informovať týchto príjemcov o takýchto hrozbách*** by ***nemala subjekty zbaviť'*** povinnosti na vlastné náklady prijať vhodné a okamžité opatrenia na prevenciu alebo odstránenie akýchkoľvek kybernetických hrozieb a obnovenie bežnej úrovne bezpečnosti služby. Takéto informácie o bezpečnostných hrozbách by sa mali príjemcom poskytovať bezplatne.	(52) V prípade potreby by subjekty mali informovať príjemcov svojich služieb o konkrétnych a významných hrozbách a o opatreniach, ktoré môžu prijať na zmiernenie vyplývajúceho rizika. ***Subjekty*** by ***tým nemali byť zbavené*** povinnosti na vlastné náklady prijať vhodné a okamžité opatrenia na prevenciu alebo odstránenie akýchkoľvek kybernetických hrozieb a obnovenie bežnej úrovne bezpečnosti služby. Takéto informácie o bezpečnostných hrozbách by sa mali príjemcom poskytovať bezplatne ***a mali by byť formulované v ľahko zrozumiteľnom jazyku***.

Pozmeňujúci návrh 53

Návrh smernice
Odôvodnenie 53

Text predložený Komisiou	*Pozmeňujúci návrh*
(53) Poskytovatelia verejných elektronických komunikačných sietí alebo verejne dostupných elektronických komunikačných služieb by mali ***predovšetkým*** informovať príjemcov služieb o konkrétnych a významných kybernetických hrozbách a o opatreniach, ktoré môžu prijať na ochranu bezpečnosti svojej komunikácie, napríklad použitím určitých typov softvéru alebo ***šifrovacích*** technológií.	(53) Poskytovatelia verejných elektronických komunikačných sietí alebo verejne dostupných elektronických komunikačných služieb by mali ***zaviesť bezpečnosť už v štádiu návrhu a bezpečnosť ako štandard a*** informovať príjemcov služieb o konkrétnych a významných kybernetických hrozbách a o opatreniach, ktoré môžu prijať na ochranu bezpečnosti ***svojich zariadení a*** svojej komunikácie, napríklad použitím určitých typov ***šifrovacieho*** softvéru alebo ***iných bezpečnostných*** technológií ***zameraných na dáta***.

Pozmeňujúci návrh 54

Návrh smernice
Odôvodnenie 54

Text predložený Komisiou	*Pozmeňujúci návrh*
(54) S cieľom zaistiť bezpečnosť elektronických komunikačných sietí a služieb by sa malo podporovať používanie šifrovania, a ***najmä šifrovania medzi koncovými bodmi***, a v prípade potreby by malo byť povinné pre poskytovateľov takýchto služieb a sietí v súlade so zásadami štandardnej a špecificky navrhnutej bezpečnosti a ochrany súkromia na účely článku 18. Používanie šifrovania medzi koncovými bodmi by sa malo zosúladiť s právomocami členských štátov na zabezpečenie ochrany ich základných bezpečnostných záujmov a verejnej bezpečnosti a na umožnenie vyšetrovania, odhaľovania a stíhania trestných činov v súlade s právom Únie. ***Riešenia na účely zákonného prístupu*** k ***informáciám v koncovej šifrovanej komunikácii by mali zachovať účinnosť*** šifrovania ***pri ochrane súkromia a bezpečnosti komunikácií a zároveň poskytovať*** účinnú ***reakciu na trestnú činnosť***.	(54) S cieľom zaistiť bezpečnosť elektronických komunikačných sietí a služieb by sa malo podporovať používanie šifrovania ***a ďalšíchbezpečnostných technológií zameraných na dáta***, ***ako je tokenizácia, segmentácia, regulácia prístupu, označovanie, anotovanie, silná správa identity*** a ***prístupu a automatizované rozhodnutia o prístupe***, a v prípade potreby by malo byť povinné pre poskytovateľov takýchto služieb a sietí v súlade so zásadami štandardnej a špecificky navrhnutej bezpečnosti a ochrany súkromia na účely článku 18. Používanie šifrovania medzi koncovými bodmi by sa malo zosúladiť s právomocami členských štátov na zabezpečenie ochrany ich základných bezpečnostných záujmov a verejnej bezpečnosti a na umožnenie vyšetrovania, odhaľovania a stíhania trestných činov v súlade s právom Únie. ***Nemalo by to však viesť*** k ***úsiliu o oslabenie*** šifrovania ***medzi koncovými bodmi, ktoré je zásadnou technológiou pre*** účinnú ***ochranu údajov a súkromia***.

Pozmeňujúci návrh 55

Návrh smernice
Odôvodnenie 54 a (nové)

Text predložený Komisiou	*Pozmeňujúci návrh*
	(54a) S cieľom zaistiť bezpečnosť a zabrániť zneužívaniu elektronických komunikačných sietí a služieb a manipulácii s nimi by sa malo podporovať používanie interoperabilných noriem bezpečného smerovania, aby sa zabezpečila integrita a spoľahlivosť funkcií smerovania v rámci celého ekosystému poskytovateľov internetu.

Pozmeňujúci návrh 56

Návrh smernice
Odôvodnenie 54 b (nové)

Text predložený Komisiou	*Pozmeňujúci návrh*
	(54b) V záujme zabezpečenia funkčnosti a integrity internetu a obmedzenia bezpečnostných problémov týkajúcich sa DNS by sa mali príslušné zainteresované strany vrátane podnikov, poskytovateľov internetových služieb a predajcov prehliadačov v Únii nabádať k tomu, aby prijali stratégiu diverzifikácie rozlišovania DNS. Členské štáty by navyše mali podporovať rozvoj a používanie verejnej a bezpečnej európskej služby resolverov DNS.

Pozmeňujúci návrh 57

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***	(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 predložili prvotné oznámenie, po ktorom bude najneskôr do jedného mesiaca ***od predloženia prvotného oznámenia nasledovať komplexná správa***. ***Harmonogram*** prvotného oznámenia incidentov by ***nemal subjektom brániť v tom***, aby ***incidenty oznamovali skôr,*** aby ***mali možnosť rýchlo požiadať o podporu jednotky CSIRT s cieľom umožniť zmiernenie oznámeného incidentu a***

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***.

prípadne obmedziť jeho šírenie. Jednotky CSIRT môžu požiadať o priebežnú správu o relevantných aktualizáciách stavu, pričom zohľadnia reakciu oznamujúceho subjektu na incident a ***jeho úsilie o nápravu***.

Pozmeňujúci návrh 58

Návrh smernice
Odôvodnenie 55 a (nové)

Text predložený Komisiou	*Pozmeňujúci návrh*
	(55a) Závažný incident môže mať vplyv na dôvernosť, integritu alebo dostupnosť služby. Kľúčové a dôležité subjekty by mali jednotkám CSIRT oznamovať závažné incidenty, ktoré majú vplyv na dostupnosť ich služby, do 24 hodín od zistenia incidentu. Jednotkám CSIRT by mali oznamovať závažné incidenty, ktoré narúšajú dôvernosť a integritu ich služieb, do 72 hodín od zistenia incidentu. Rozlišovanie medzi typmi incidentov nie je založené na závažnosti incidentu, ale na ťažkostiach oznamujúceho subjektu pri posudzovaní incidentu, jeho závažnosti a schopnosti oznamovať informácie, ktoré môžu byť pre jednotku CSIRT užitočné. Prvotné oznámenie by malo obsahovať informácie, ktoré sú potrebné na to, aby sa jednotka CSIRT dozvedela o incidente, a na základe ktorých môže subjekt v prípade potreby požiadať o pomoc. 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 ďalej 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 jednotkami CSIRT sa dotknutý subjekt môže odchýliť od lehoty pre prvotné oznámenie a od lehoty pre komplexnú správu.

Pozmeňujúci návrh 59

Návrh smernice
Odôvodnenie 59

Text predložený Komisiou	*Pozmeňujúci návrh*
(59) Udržiavanie presných ***a*** úplných databáz ***doménových mien a registračných údajov*** (tzv. údajov WHOIS) ***a poskytovanie zákonného prístupu k takýmto údajom*** je nevyhnutné na zaistenie bezpečnosti, stability a odolnosti DNS, čo zase prispieva k vysokej spoločnej úrovni kybernetickej bezpečnosti v ***Únii***. Ak spracúvanie zahŕňa osobné údaje, takéto spracúvanie musí byť v súlade s právnymi predpismi Únie o ochrane údajov.	(59) Udržiavanie presných***, overených a*** úplných databáz ***údajov o registrácii doménových mien*** (tzv. údajov WHOIS) je nevyhnutné na zaistenie bezpečnosti, stability a odolnosti DNS, čo zase prispieva k vysokej spoločnej úrovni kybernetickej bezpečnosti v ***Únii a k boju proti nezákonným činnostiam. Od správcov TLD a subjektov poskytujúcich služby registrácie doménových mien by sa preto malo vyžadovať, aby zhromažďovali údaje o registrácii doménových mien, ktoré by mali zahŕňať aspoň meno držiteľov domény, ich fyzickú a e-mailovú adresu, ako aj ich telefónne číslo. V praxi nemusia byť zhromaždené údaje vždy úplne presné, správcovia TLD a subjekty poskytujúce služby registrácie doménových mien by však mali prijať a zaviesť primerané postupy na overenie toho, či fyzické alebo právnické osoby žiadajúce alebo vlastniace doménové meno poskytli kontaktné údaje, na ktorých ich možno zastihnúť a očakávať od nich odpoveď. Pri použití prístupu***

„najlepšieho úsilia“ by tieto overovacie procesy mali odrážať súčasné najlepšie postupy používané v tomto odvetví. Tieto najlepšie postupy pri overovacom procese by mali odrážať pokrok dosiahnutý v procese elektronickej identifikácie. Správcovia TLD a subjekty poskytujúce služby registrácie doménových mien by mali svoje politiky a postupy zverejňovať na zabezpečenie integrity a dostupnosti údajov o registrácii doménových mien. Ak spracúvanie zahŕňa osobné údaje, takéto spracúvanie musí byť v súlade s právnymi predpismi Únie o ochrane údajov.

Pozmeňujúci návrh 60

Návrh smernice
Odôvodnenie 60

Text predložený Komisiou	*Pozmeňujúci návrh*
(60) Dostupnosť a včasná prístupnosť ***týchto údajov*** pre ***orgány verejnej moci*** vrátane ***príslušných orgánov*** podľa práva Únie alebo vnútroštátneho práva na predchádzanie trestným činom, ich vyšetrovanie alebo stíhanie***, pre*** jednotky CERT***,*** jednotky CSIRT, a ***pokiaľ ide*** o ***údaje ich klientov pre poskytovateľov elektronických komunikačných sietí*** a ***služieb*** a ***poskytovateľov kybernetickobezpečnostných technológií a*** služieb ***konajúcich v mene týchto klientov, je nevyhnutná na predchádzanie zneužívaniu systému doménových mien a boj proti tomuto zneužívaniu***, ***najmä*** na ***predchádzanie kybernetickobezpečnostným incidentom, ich odhaľovanie*** a ***reakciu na ne***. ***Takýto prístup by mal byť v súlade s právnymi predpismi Únie o ochrane údajov, pokiaľ ide o osobné údaje.***	(60) Dostupnosť a včasná prístupnosť ***údajov o registrácii doménových mien pre oprávnených záujemcov o prístup je nevyhnutná na účely kybernetickej bezpečnosti a*** pre ***boj proti nezákonným činnostiam v online ekosystéme. Od správcov TLD a subjektov poskytujúcich služby registrácie doménových mien by sa preto malo vyžadovať, aby oprávneným záujemcom o prístup umožnili zákonný prístup k špecifickým registračným údajom o doménových menách vrátane osobných údajov v súlade s právnymi predpismi Únie o ochrane údajov. Oprávnení záujemcovia o prístup by mali predložiť riadne odôvodnenú žiadosť o prístup k registračným údajom o doménových menách na základe práva Únie alebo vnútroštátneho práva a môžu zahŕňať príslušné orgány*** podľa práva Únie alebo vnútroštátneho práva na predchádzanie trestným činom, ich vyšetrovanie alebo stíhanie ***a vnútroštátne*** jednotky CERT ***alebo*** jednotky CSIRT***. Členské štáty by mali zabezpečiť, aby správcovia TLD a subjekty, ktoré poskytujú služby registrácie doménových***

	mien, bez zbytočného odkladu a v každom prípade do 72 hodín reagovali na žiadosti oprávnených záujemcov o prístup týkajúcich sa zverejnenia registračných údajov o doménových menách. Správcovia TLD a subjekty, ktoré poskytujú služby registrácie doménových mien, by mali stanoviť politiky a postupy uverejňovania a sprístupňovania registračných údajov vrátane dohôd o úrovni poskytovaných služieb na vybavovanie žiadostí o prístup od oprávnených záujemcov o prístup. Postup týkajúci sa udelenia prístupu môže zahŕňať aj použitie rozhrania, portálu alebo iných technických nástrojov na zabezpečenie účinného systému na podávanie žiadostí o registračné údaje a prístup k nim. S cieľom podporovať harmonizované postupy na celom vnútornom trhu môže Komisia prijať usmernenia o takýchto postupoch bez toho, aby boli dotknuté právomoci Európskeho výboru pre ochranu údajov.

Pozmeňujúci návrh 61

Návrh smernice
Odôvodnenie 61

Text predložený Komisiou	*Pozmeňujúci návrh*
(61) S cieľom zabezpečiť dostupnosť presných a úplných údajov o registrácii doménových mien by mali správcovia TLD a subjekty poskytujúce služby registrácie doménových mien pre TLD (tzv. registrátori) zhromažďovať registračné údaje o menách domén a zaručovať ich integritu a dostupnosť. Správcovia TLD a subjekty poskytujúce služby registrácie doménových mien pre TLD by mali najmä stanoviť politiky a postupy na zhromažďovanie a uchovávanie presných a úplných registračných údajov, ako aj na predchádzanie nepresným registračným údajom a ich opravu v súlade s pravidlami	***vypúšťa sa***

Únie v oblasti ochrany údajov.

Pozmeňujúci návrh 62

Návrh smernice
Odôvodnenie 62

Text predložený Komisiou	*Pozmeňujúci návrh*
(62) ***Správcovia*** TLD a ***subjekty***, ktoré ***pre nich*** poskytujú služby registrácie doménových mien, by ***mali zverejňovať'*** registračné údaje o doménových menách, ktoré ***nepatria do rozsahu pôsobnosti pravidiel Únie v oblasti ochrany údajov, ako sú údaje, ktoré sa týkajú*** právnických osôb[25]***.*** Správcovia TLD a subjekty ***poskytujúce služby registrácie doménových mien pre TLD by tiež*** mali ***oprávneným záujemcom o prístup umožniť zákonný prístup k špecifickým registračným údajom o doménových menách týkajúcim sa fyzických osôb v súlade s právnymi predpismi Únie o ochrane údajov. Členské štáty by mali zabezpečiť***, ***aby správcovia TLD*** a ***subjekty, ktoré pre nich poskytujú služby registrácie doménových mien***, ***bezodkladne reagovali na žiadosti oprávnených záujemcov o prístup týkajúcich*** sa ***zverejnenia registračných údajov o doménových menách. Správcovia TLD a subjekty***, ***ktoré pre nich poskytujú služby registrácie doménových mien***, ***by mali stanoviť politiky a postupy uverejňovania a sprístupňovania registračných údajov vrátane dohôd o úrovni poskytovaných služieb na vybavovanie žiadostí o prístup od oprávnených záujemcov o prístup. Postup týkajúci sa udelenia prístupu môže zahŕňať aj použitie rozhrania, portálu alebo iného technického nástroja na zabezpečenie účinného systému na podávanie žiadostí o registračné údaje a prístup k nim. S cieľom podporovať harmonizované postupy na celom vnútornom trhu môže Komisia prijať usmernenia o takýchto postupoch bez***	(62) ***Od správcov*** TLD a ***subjektov***, ktoré poskytujú služby registrácie doménových mien, by ***sa malo vyžadovať', aby zverejnili*** registračné údaje o doménových menách, ktoré ***neobsahujú osobné údaje. Malo by sa rozlišovať' medzi fyzickými a právnickými osobami[25]. V prípade*** právnických osôb ***by*** správcovia TLD a subjekty mali ***zverejňovať' aspoň meno držiteľa domény***, ***jeho fyzickú*** a ***e-mailovú adresu***, ***ako aj jeho telefónne číslo. Od právnickej osoby by*** sa ***malo vyžadovať'***, ***aby buď' poskytla všeobecnú e-mailovú adresu***, ***ktorá*** sa môže ***zverejniť'***, alebo ***poskytla súhlas s uverejnením osobnej e-mailovej adresy. Právnická osoba by mala byť' schopná preukázať' takýto súhlas*** na ***žiadosť' správcov TLD a subjektov poskytujúcich služby registrácie doménových mien***.

toho, aby boli dotknuté právomoci Európskeho výboru pre ochranu údajov.

---

[25] Odôvodnenie 14 nariadenia Európskeho parlamentu a Rady (EÚ) 2016/679: „Toto nariadenie sa nevzťahuje na spracúvanie osobných údajov, ktoré sa týka právnických osôb, a najmä podnikov založených ako právnické osoby vrátane názvu, formy a kontaktných údajov právnickej osoby.“

---

[25] Odôvodnenie 14 nariadenia Európskeho parlamentu a Rady (EÚ) 2016/679: „Toto nariadenie sa nevzťahuje na spracúvanie osobných údajov, ktoré sa týka právnických osôb, a najmä podnikov založených ako právnické osoby vrátane názvu, formy a kontaktných údajov právnickej osoby.“

Pozmeňujúci návrh 63

Návrh smernice
Odôvodnenie 63

Text predložený Komisiou	*Pozmeňujúci návrh*
(63) Všetky kľúčové a dôležité subjekty podľa tejto smernice by mali patriť do jurisdikcie členského štátu, v ktorom poskytujú svoje služby. Ak subjekt poskytuje služby vo viac ako jednom členskom štáte, mal by patriť do samostatnej a súbežnej jurisdikcie každého z týchto členských štátov. Príslušné orgány týchto členských štátov by mali spolupracovať, vzájomne si pomáhať a v prípade potreby vykonávať spoločné opatrenia dohľadu.	(63) Všetky kľúčové a dôležité subjekty podľa tejto smernice by mali patriť do jurisdikcie členského štátu, v ktorom poskytujú svoje služby ***alebo vykonávajú svoje činnosti***. Ak subjekt poskytuje služby vo viac ako jednom členskom štáte, mal by patriť do samostatnej a súbežnej jurisdikcie každého z týchto členských štátov. Príslušné orgány týchto členských štátov by mali spolupracovať, vzájomne si pomáhať a v prípade potreby vykonávať spoločné opatrenia dohľadu.

Pozmeňujúci návrh 64

Návrh smernice
Odôvodnenie 64

Text predložený Komisiou	*Pozmeňujúci návrh*
(64) S cieľom zohľadniť cezhraničný charakter služieb a operácií poskytovateľov služieb DNS, správcov mien TLD, poskytovateľov sietí na sprístupňovanie obsahu, poskytovateľov služieb cloud computingu, poskytovateľov služieb dátového centra a poskytovateľov digitálnych služieb by mal mať právomoc	(64) S cieľom zohľadniť cezhraničný charakter služieb a operácií poskytovateľov služieb DNS, správcov mien TLD, poskytovateľov sietí na sprístupňovanie obsahu, poskytovateľov služieb cloud computingu, poskytovateľov služieb dátového centra a poskytovateľov digitálnych služieb by mal mať právomoc

nad týmito subjektmi len jeden členský štát. Právomoc by sa mala udeliť členskému štátu, v ktorom má príslušný subjekt hlavné miesto podnikateľskej činnosti v Únii. Kritérium miesta podnikateľskej činnosti na účely tejto smernice zahŕňa účinné vykonávanie činnosti prostredníctvom stabilných dojednaní. Právna forma takýchto dojednaní, či už ide o pobočku alebo dcérsku spoločnosť s právnou subjektivitou, nie je v tomto ohľade určujúcim faktorom. Spĺňanie tohto kritéria by nemalo závisieť od toho, či sa sieť a informačné systémy fyzicky nachádzajú na danom mieste; samotná prítomnosť a používanie takýchto systémov nepredstavuje hlavné miesto podnikateľskej činnosti, a preto nejde o rozhodujúce kritériá na určenie hlavného miesta podnikateľskej činnosti. Hlavným miestom podnikateľskej činnosti by malo byť miesto v Únii, kde sa prijímajú rozhodnutia týkajúce sa opatrení na riadenie kybernetickobezpečnostných rizík. Zvyčajne zodpovedá miestu ústredia spoločností v Únii. Ak sa takéto rozhodnutia neprijímajú v Únii, ***predpokladá*** sa, že hlavné miesto podnikateľskej činnosti ***by malo byť'*** v členských štátoch, v ktorých majú subjekty miesto podnikateľskej činnosti s najvyšším počtom zamestnancov v Únii. Ak služby vykonáva skupina podnikov, hlavné miesto podnikateľskej činnosti riadiaceho podniku by sa malo považovať za hlavné miesto podnikateľskej činnosti skupiny podnikov.	nad týmito subjektmi len jeden členský štát. Právomoc by sa mala udeliť členskému štátu, v ktorom má príslušný subjekt hlavné miesto podnikateľskej činnosti v Únii. Kritérium miesta podnikateľskej činnosti na účely tejto smernice zahŕňa účinné vykonávanie činnosti prostredníctvom stabilných dojednaní. Právna forma takýchto dojednaní, či už ide o pobočku alebo dcérsku spoločnosť s právnou subjektivitou, nie je v tomto ohľade určujúcim faktorom. Spĺňanie tohto kritéria by nemalo závisieť od toho, či sa sieť a informačné systémy fyzicky nachádzajú na danom mieste; samotná prítomnosť a používanie takýchto systémov nepredstavuje hlavné miesto podnikateľskej činnosti, a preto nejde o rozhodujúce kritériá na určenie hlavného miesta podnikateľskej činnosti. Hlavným miestom podnikateľskej činnosti by malo byť miesto v Únii, kde sa prijímajú rozhodnutia týkajúce sa opatrení na riadenie kybernetickobezpečnostných rizík. Zvyčajne zodpovedá miestu ústredia spoločností v Únii. Ak sa takéto rozhodnutia neprijímajú v Únii, ***malo by*** sa ***predpokladať'***, že hlavné miesto podnikateľskej činnosti ***je*** v členských štátoch, v ktorých majú subjekty ***buď'*** miesto podnikateľskej činnosti s najvyšším počtom zamestnancov v Únii***, alebo miesto podnikateľskej činnosti, kde sa vykonávajú kybernetickobezpečnostné operácie***. Ak služby vykonáva skupina podnikov, hlavné miesto podnikateľskej činnosti riadiaceho podniku by sa malo považovať za hlavné miesto podnikateľskej činnosti skupiny podnikov.

Pozmeňujúci návrh 65

Návrh smernice
Odôvodnenie 65 a (nové)

Text predložený Komisiou	*Pozmeňujúci návrh*
	(65a) Agentúra ENISA by mala vytvoriť

	a viesť register obsahujúci informácie o kľúčových a dôležitých subjektoch, ktoré zahŕňajú poskytovateľov služieb DNS, správcov mien TLD a poskytovateľov služieb cloud computingu, služieb dátových centier, sietí na sprístupňovania obsahu, online trhov, online vyhľadávačov a platforiem sociálnych sietí. Tieto kľúčové a dôležité subjekty by mali agentúre ENISA poskytovať svoje názvy, adresy a aktuálne kontaktné údaje. Akékoľvek zmeny týchto údajov by mali agentúre ENISA oznámiť bezodkladne a v každom prípade do dvoch týždňov odo dňa nadobudnutia účinnosti zmeny. Agentúra ENISA by mala postúpiť tieto informácie príslušnému jednotnému kontaktnému miestu. Od kľúčových a dôležitých subjektov predkladajúcich svoje informácie agentúre ENISA sa preto nevyžaduje, aby osobitne informovali príslušný orgán v rámci členského štátu. Agentúra ENISA by mala vytvoriť jednoduchý, verejne dostupný program aplikácií, ktorý by tieto subjekty mohli používať na aktualizáciu svojich informácií. Okrem toho by agentúra ENISA mala zaviesť príslušné protokoly pre klasifikáciu a riadenie informácií s cieľom zaistiť bezpečnosť a dôvernosť zverejnených informácií a obmedziť prístup, uchovávanie a prenos takýchto informácií na predpokladaných používateľov.

Pozmeňujúci návrh 66

Návrh smernice
Odôvodnenie 66

Text predložený Komisiou	*Pozmeňujúci návrh*
(66) Ak sa informácie, ktoré sa považujú za utajované ***podľa vnútroštátneho práva*** alebo ***práva*** Únie, vymieňajú, oznamujú alebo inak zdieľajú podľa ustanovení tejto smernice, mali by sa uplatňovať zodpovedajúce osobitné pravidlá zaobchádzania s utajovanými	(66) Ak sa informácie, ktoré sa považujú za utajované ***v súlade s vnútroštátnym právom*** alebo ***právom*** Únie, vymieňajú, oznamujú alebo inak zdieľajú podľa ustanovení tejto smernice, mali by sa uplatňovať zodpovedajúce osobitné pravidlá zaobchádzania s utajovanými

skutočnosťami.	skutočnosťami. ***Okrem toho by agentúra ENISA mala mať zavedenú infraštruktúru, postupy a pravidlá pre zaobchádzanie s citlivými a utajovanými skutočnosťami v súlade s platnými bezpečnostnými predpismi na ochranu utajovaných skutočností EÚ.***

Pozmeňujúci návrh 67

Návrh smernice
Odôvodnenie 68

Text predložený Komisiou	*Pozmeňujúci návrh*
(68) ***Subjekty by sa*** mali nabádať, aby kolektívne využívali svoje individuálne znalosti a praktické skúsenosti na strategickej, taktickej a operačnej úrovni s cieľom zlepšiť svoje schopnosti primerane posudzovať kybernetické hrozby, monitorovať ich, brániť sa proti nim a reagovať na ne. Preto treba umožniť, aby sa na úrovni Únie vytvorili mechanizmy dohôd o dobrovoľnom zdieľaní informácií. Na tento účel by členské štáty mali aktívne podporovať a podnecovať aj príslušné subjekty, na ktoré sa nevzťahuje rozsah pôsobnosti tejto smernice, aby sa na takýchto mechanizmoch zdieľania informácií zúčastňovali. Tieto mechanizmy by sa mali vykonávať v plnom súlade s pravidlami Únie týkajúcimi sa hospodárskej súťaže, ako aj právnymi predpismi Únie v oblasti ochrany údajov.	(68) ***Členské štáty by*** mali nabádať ***a podporovať subjekty***, aby kolektívne využívali svoje individuálne znalosti a praktické skúsenosti na strategickej, taktickej a operačnej úrovni s cieľom zlepšiť svoje schopnosti primerane posudzovať kybernetické hrozby, monitorovať ich, brániť sa proti nim a reagovať na ne. Preto treba umožniť, aby sa na úrovni Únie vytvorili mechanizmy dohôd o dobrovoľnom zdieľaní informácií. Na tento účel by členské štáty mali aktívne podporovať a podnecovať aj príslušné subjekty, na ktoré sa nevzťahuje rozsah pôsobnosti tejto smernice***, ako sú subjekty zamerané na služby a výskum v oblasti kybernetickej bezpečnosti***, aby sa na takýchto mechanizmoch zdieľania informácií zúčastňovali. Tieto mechanizmy by sa mali vykonávať v plnom súlade s pravidlami Únie týkajúcimi sa hospodárskej súťaže, ako aj právnymi predpismi Únie v oblasti ochrany údajov.

Pozmeňujúci návrh 68

Návrh smernice
Odôvodnenie 69

Text predložený Komisiou	*Pozmeňujúci návrh*
(69) Spracúvanie osobných údajov v rozsahu, ktorý je nevyhnutne potrebný a primeraný na účely zaistenia bezpečnosti	(69) Spracúvanie osobných údajov v rozsahu, ktorý je nevyhnutne potrebný a primeraný na účely zaistenia bezpečnosti

sietí a ***informácií*** subjektmi, ***orgánmi verejnej moci***, ***jednotkami CERT***, ***jednotkami CSIRT*** a ***poskytovateľmi bezpečnostných technológií*** a ***služieb***, ***by malo predstavovať oprávnený záujem dotknutého prevádzkovateľa***, ako sa uvádza v ***nariadení*** (EÚ) 2016/679. ***To by malo zahŕňať*** opatrenia týkajúce sa prevencie, odhaľovania a analýzy incidentov a reakcie na ne, opatrenia na zvýšenie informovanosti o konkrétnych kybernetických hrozbách, výmenu informácií v kontexte nápravy zraniteľnosti a koordinovaného zverejňovania, ako aj dobrovoľnú výmenu informácií o týchto incidentoch, ako aj o kybernetických hrozbách a zraniteľnostiach, ukazovatele kompromitácie, taktiky, techniky a postupy, kybernetickobezpečnostné varovania a konfiguračné nástroje***.*** ***Takéto opatrenia*** si ***môžu vyžadovať*** spracovanie ***týchto druhov*** osobných údajov***:*** IP adresy, jednotné vyhľadávače prostriedkov (URL), doménové mená ***a*** e-mailové adresy.	sietí a ***informácií kľúčovými a dôležitými*** subjektmi, ***jednotkami CSIRT a poskytovateľmi bezpečnostných technológií a služieb***, ***je nevyhnutné na splnenie ich zákonných povinností stanovených v tejto smernici. Takéto spracúvanie osobných údajov môže byť potrebné aj na účely oprávnených záujmov***, ***ktoré sledujú kľúčové*** a ***dôležité subjekty. Ak sa v tejto smernici vyžaduje spracúvanie osobných údajov na účely kybernetickej bezpečnosti sietí*** a ***informácií v súlade s ustanoveniami článkov 18***, ***20 a 23 smernice, toto spracúvanie sa považuje za nevyhnutné na splnenie zákonnej povinnosti***, ako sa uvádza v ***článku 6 ods. 1 písm. c) nariadenia*** (EÚ) 2016/679. ***Na účely článkov 26 a 27 tejto smernice sa spracúvanie, ako sa uvádza v článku 6 ods. 1 písm. f) nariadenia (EÚ) 2016/679, považuje za nevyhnutné na účely oprávnených záujmov, ktoré sledujú kľúčové a dôležité subjekty.*** Opatrenia týkajúce sa prevencie, odhaľovania***, identifikácie, obmedzovania následkov*** a analýzy incidentov a reakcie na ne, opatrenia na zvýšenie informovanosti o konkrétnych kybernetických hrozbách, výmenu informácií v kontexte nápravy zraniteľnosti a koordinovaného zverejňovania, ako aj dobrovoľnú výmenu informácií o týchto incidentoch, ako aj o kybernetických hrozbách a zraniteľnostiach, ukazovatele kompromitácie, taktiky, techniky a postupy, kybernetickobezpečnostné varovania a konfiguračné nástroje si ***vyžadujú*** spracovanie ***určitých kategórií*** osobných údajov***, ako sú*** IP adresy, jednotné vyhľadávače prostriedkov (URL), doménové mená***,*** e-mailové adresy***, časové pečiatky, informácie súvisiace s operačným systémom alebo prehliadačom, súbory cookie alebo iné informácie označujúce modus operandi***.

Pozmeňujúci návrh 69

Návrh smernice
Odôvodnenie 71

Text predložený Komisiou	*Pozmeňujúci návrh*
(71) Aby bolo presadzovanie povinností účinné, mal by sa stanoviť minimálny zoznam správnych sankcií za porušenie povinností v oblasti riadenia kybernetickobezpečnostných rizík a oznamovania stanovených v tejto smernici, ktorým sa stanoví jasný a konzistentný rámec pre takéto sankcie v celej Únii. Náležitá pozornosť by sa mala venovať povahe, závažnosti a trvaniu porušenia, skutočnej spôsobenej škode alebo vzniknutým stratám ***alebo potenciálnym škodám či stratám, ktoré mohli vzniknúť***, úmyselnému alebo nedbanlivostnému charakteru porušenia, opatreniam prijatým na zabránenie alebo zmiernenie vzniknutej škody a/alebo strát, miere zodpovednosti alebo akémukoľvek relevantnému predchádzajúcemu porušeniu, miere spolupráce s príslušným orgánom a akýmkoľvek ďalším priťažujúcim alebo poľahčujúcim faktorom. ***Ukladanie sankcií*** vrátane správnych pokút by malo podliehať primeraným procesným zárukám v súlade so všeobecnými zásadami práva Únie a Charty základných práv Európskej únie vrátane účinnej súdnej ochrany ***a*** riadneho procesu.	(71) Aby bolo presadzovanie povinností účinné, mal by sa stanoviť minimálny zoznam správnych sankcií za porušenie povinností v oblasti riadenia kybernetickobezpečnostných rizík a oznamovania stanovených v tejto smernici, ktorým sa stanoví jasný a konzistentný rámec pre takéto sankcie v celej Únii. Náležitá pozornosť by sa mala venovať povahe, závažnosti a trvaniu porušenia, skutočnej spôsobenej škode alebo vzniknutým stratám, úmyselnému alebo nedbanlivostnému charakteru porušenia, opatreniam prijatým na zabránenie alebo zmiernenie vzniknutej škody a/alebo strát, miere zodpovednosti alebo akémukoľvek relevantnému predchádzajúcemu porušeniu, miere spolupráce s príslušným orgánom a akýmkoľvek ďalším priťažujúcim alebo poľahčujúcim faktorom. ***Sankcie*** vrátane správnych pokút by ***mali byť primerané a ich ukladanie by*** malo podliehať primeraným procesným zárukám v súlade so všeobecnými zásadami práva Únie a Charty základných práv Európskej únie ***(ďalej len „charta“)*** vrátane účinnej súdnej ochrany***, riadneho procesu, prezumpcie neviny*** a ***práva na obhajobu***.

Pozmeňujúci návrh 70

Návrh smernice
Odôvodnenie 72

Text predložený Komisiou	*Pozmeňujúci návrh*
(72) S cieľom zabezpečiť účinné presadzovanie povinností stanovených v tejto smernici by mal mať každý príslušný orgán právomoc uložiť správne pokuty alebo požiadať o ich uloženie.	(72) S cieľom zabezpečiť účinné presadzovanie povinností stanovených v tejto smernici by mal mať každý príslušný orgán právomoc uložiť správne pokuty alebo požiadať o ich uloženie***, ak bolo porušenie úmyselné, z nedbanlivosti alebo ak dotknutý subjekt dostal oznámenie o***

nedodržaní povinností.

Pozmeňujúci návrh 71

Návrh smernice
Odôvodnenie 76

Text predložený Komisiou	*Pozmeňujúci návrh*
(76) S cieľom ďalej posilniť účinnosť a odrádzajúci účinok sankcií za porušenie povinností stanovených podľa tejto smernice by príslušné orgány mali byť oprávnené uplatňovať ***sankcie pozostávajúce z pozastavenia*** certifikácie alebo povolenia časti alebo všetkých služieb, ktoré poskytuje kľúčový subjekt, a ***uloženia*** dočasného zákazu fyzickej osobe vykonávať riadiace funkcie. Takéto ***sankcie*** by sa vzhľadom na svoju závažnosť a vplyv na činnosti subjektov a v konečnom dôsledku na ich spotrebiteľov mali uplatňovať len úmerne k závažnosti porušenia a s prihliadnutím na osobitné okolnosti každého prípadu vrátane úmyselného alebo nedbanlivostného charakteru porušenia, opatrení prijatých na zabránenie alebo zmiernenie vzniknutej škody a/alebo strát. Takéto ***sankcie*** by sa mali uplatňovať len ako ultima ratio, čo znamená až po vyčerpaní ostatných príslušných opatrení na presadzovanie povinností stanovených v tejto smernici, a len na obdobie, kým subjekty, na ktoré sa vzťahujú, neprijmú potrebné opatrenia na nápravu nedostatkov alebo na splnenie požiadaviek príslušného orgánu, v prípade ktorých sa takéto ***sankcie*** uplatnili. Ukladanie takýchto ***sankcií by malo*** podliehať primeraným procesným zárukám v súlade so všeobecnými zásadami práva Únie a Charty ***základných práv Európskej únie*** vrátane účinnej súdnej ochrany, riadneho procesu, prezumpcie neviny a práva na obhajobu.	(76) S cieľom ďalej posilniť účinnosť a odrádzajúci účinok sankcií za porušenie povinností stanovených podľa tejto smernice by príslušné orgány mali byť oprávnené uplatňovať ***dočasné pozastavenie*** certifikácie alebo povolenia časti alebo všetkých ***relevantných*** služieb, ktoré poskytuje kľúčový subjekt, a ***požadovať uloženie*** dočasného zákazu fyzickej osobe vykonávať riadiace funkcie ***na úrovni výkonného riaditeľa alebo právneho zástupcu. Členské štáty by mali vypracovať osobitné postupy a pravidlá týkajúce sa dočasného zákazu vykonávania riadiacich funkcií fyzickou osobou na úrovni výkonného riaditeľa alebo právneho zástupcu v subjektoch verejnej správy. Pri vypracúvaní takýchto postupov a pravidiel by členské štáty mali zohľadniť osobitosti svojich príslušných úrovní a systémov riadenia v rámci svojich subjektov verejnej správy.*** Takéto ***dočasné pozastavenia alebo zákazy*** by sa vzhľadom na svoju závažnosť a vplyv na činnosti subjektov a v konečnom dôsledku na ich spotrebiteľov mali uplatňovať len úmerne k závažnosti porušenia a s prihliadnutím na osobitné okolnosti každého prípadu vrátane úmyselného alebo nedbanlivostného charakteru porušenia, opatrení prijatých na zabránenie alebo zmiernenie vzniknutej škody a/alebo strát. Takéto ***dočasné pozastavenia alebo zákazy*** by sa mali uplatňovať len ako ultima ratio, čo znamená až po vyčerpaní ostatných príslušných opatrení na presadzovanie povinností stanovených v tejto smernici, a len na obdobie, kým subjekty, na ktoré sa vzťahujú, neprijmú potrebné opatrenia na nápravu nedostatkov alebo na splnenie

požiadaviek príslušného orgánu, v prípade ktorých sa takéto ***dočasné pozastavenia alebo zákazy*** uplatnili. Ukladanie takýchto ***dočasných pozastavení alebo zákazov musí*** podliehať primeraným procesným zárukám v súlade so všeobecnými zásadami práva Únie a charty vrátane účinnej súdnej ochrany, riadneho procesu, prezumpcie neviny a práva na obhajobu.

Pozmeňujúci návrh 72

Návrh smernice
Odôvodnenie 79

Text predložený Komisiou	*Pozmeňujúci návrh*
(79) Mal by sa zaviesť mechanizmus partnerského preskúmania, ktorý odborníkom určeným členskými štátmi umožní posúdiť vykonávanie politík v oblasti kybernetickej bezpečnosti vrátane úrovne schopností a dostupných zdrojov členských štátov.	(79) Mal by sa zaviesť mechanizmus partnerského preskúmania, ktorý ***nezávislým*** odborníkom určeným členskými štátmi umožní posúdiť vykonávanie politík v oblasti kybernetickej bezpečnosti vrátane úrovne schopností a dostupných zdrojov členských štátov. ***Partnerské preskúmania môžu poskytnúť cenné poznatky a odporúčania, ktoré posilnia celkové kybernetickobezpečnostné schopnosti. Môžu najmä prispieť k uľahčeniu transferu technológií, nástrojov, opatrení a procesov medzi členskými štátmi zapojenými do partnerského preskúmania, vytvoriť funkčný spôsob výmeny najlepších postupov medzi členskými štátmi s rôznymi úrovňami vyspelosti v oblasti kybernetickej bezpečnosti a umožniť zavedenie vysokej spoločnej úrovne kybernetickej bezpečnosti v celej Únii. Partnerskému preskúmaniu by malo predchádzať sebahodnotenie členského štátu, ktorý je predmetom preskúmania, ktoré by sa vzťahovalo na skúmané aspekty a akékoľvek ďalšie cielené otázky, ktoré členskému štátu zapojenému do partnerského preskúmania oznámia určení experti pred začatím procesu. Komisia by v spolupráci s agentúrou ENISA a skupinou pre spoluprácu mala***

	vypracovať vzory pre sebahodnotenie skúmaných aspektov s cieľom zjednodušiť proces a zabrániť procesným nezrovnalostiam a oneskoreniam, ktoré by členské štáty zapojené do partnerského preskúmania mali vyplniť a poskytnúť určeným expertom vykonávajúcim partnerské preskúmanie pred začatím procesu partnerského preskúmania.

Pozmeňujúci návrh 73

Návrh smernice
Odôvodnenie 80

Text predložený Komisiou	*Pozmeňujúci návrh*
(80) S cieľom zohľadniť nové kybernetické hrozby, technologický vývoj alebo odvetvové špecifiká by sa mala na Komisiu delegovať právomoc prijímať akty v súlade s článkom 290 ZFEÚ, pokiaľ ide o prvky týkajúce sa opatrení na riadenie rizík, ktoré sa vyžadujú v tejto smernici. Komisia by mala byť splnomocnená prijímať aj delegované akty, v ktorých stanoví, od ktorých kategórií kľúčových subjektov sa vyžaduje získanie certifikátu a v rámci ktorých konkrétnych európskych systémov certifikácie kybernetickej bezpečnosti. Je osobitne dôležité, aby Komisia počas prípravných prác uskutočnila príslušné konzultácie, a to aj na úrovni expertov, a aby tieto konzultácie vykonávala v súlade so zásadami stanovenými v Medziinštitucionálnej dohode z 13. apríla 2016 o lepšej tvorbe práva[26]. Predovšetkým, v záujme rovnakého zastúpenia pri príprave delegovaných aktov, sa všetky dokumenty doručujú Európskemu parlamentu a Rade v rovnakom čase ako expertom z členských štátov, a experti Európskeho parlamentu a Rady majú systematický prístup na zasadnutia skupín expertov Komisie, ktoré sa zaoberajú prípravou delegovaných aktov.	(80) S cieľom zohľadniť nové kybernetické hrozby, technologický vývoj alebo odvetvové špecifiká by sa mala na Komisiu delegovať právomoc prijímať akty v súlade s článkom 290 ZFEÚ, pokiaľ ide o prvky týkajúce sa opatrení na riadenie ***kybernetickobezpečnostných*** rizík ***a oznamovacích povinností***, ktoré sa vyžadujú v tejto smernici. Komisia by mala byť splnomocnená prijímať aj delegované akty, v ktorých stanoví, od ktorých kategórií kľúčových ***a dôležitých*** subjektov sa vyžaduje získanie certifikátu a v rámci ktorých konkrétnych európskych systémov certifikácie kybernetickej bezpečnosti. Je osobitne dôležité, aby Komisia počas prípravných prác uskutočnila príslušné konzultácie, a to aj na úrovni expertov, a aby tieto konzultácie vykonávala v súlade so zásadami stanovenými v Medziinštitucionálnej dohode z 13. apríla 2016 o lepšej tvorbe práva. Predovšetkým, v záujme rovnakého zastúpenia pri príprave delegovaných aktov, sa všetky dokumenty doručujú Európskemu parlamentu a Rade v rovnakom čase ako expertom z členských štátov, a experti Európskeho parlamentu a Rady majú systematický prístup na zasadnutia skupín expertov Komisie, ktoré sa zaoberajú prípravou delegovaných aktov.

[26] Ú. v. EÚ L 123, 12.5.2016, s. 1.

[26] Ú. v. EÚ L 123, 12.5.2016, s. 1.

Pozmeňujúci návrh 74

Návrh smernice
Odôvodnenie 81

Text predložený Komisiou	*Pozmeňujúci návrh*
(81) S cieľom zabezpečiť jednotné podmienky vykonávania príslušných ustanovení tejto smernice týkajúcich sa procedurálnych opatrení potrebných na fungovanie skupiny pre spoluprácu***, technických prvkov týkajúcich sa opatrení na riadenie rizík alebo druhu informácií, formátu*** a postupu oznamovania incidentov by sa mali na Komisiu preniesť vykonávacie právomoci. Uvedené právomoci by sa mali vykonávať v súlade s nariadením Európskeho parlamentu a Rady (EÚ) č. 182/2011[27].	(81) S cieľom zabezpečiť jednotné podmienky vykonávania príslušných ustanovení tejto smernice týkajúcich sa procedurálnych opatrení potrebných na fungovanie skupiny pre spoluprácu a postupu oznamovania incidentov by sa mali na Komisiu preniesť vykonávacie právomoci. Uvedené právomoci by sa mali vykonávať v súlade s nariadením Európskeho parlamentu a Rady (EÚ) č. 182/2011[27].

[27] Nariadenie Európskeho parlamentu a Rady (EÚ) č. 182/2011 zo 16. februára 2011, ktorým sa ustanovujú pravidlá a všeobecné zásady mechanizmu, na základe ktorého členské štáty kontrolujú vykonávanie vykonávacích právomocí Komisie (Ú. v. EÚ L 55, 28.2.2011, s. 13).

[27] Nariadenie Európskeho parlamentu a Rady (EÚ) č. 182/2011 zo 16. februára 2011, ktorým sa ustanovujú pravidlá a všeobecné zásady mechanizmu, na základe ktorého členské štáty kontrolujú vykonávanie vykonávacích právomocí Komisie (Ú. v. EÚ L 55, 28.2.2011, s. 13).

Pozmeňujúci návrh 75

Návrh smernice
Odôvodnenie 82

Text predložený Komisiou	*Pozmeňujúci návrh*
(82) Komisia by mala túto smernicu pravidelne preskúmavať a radiť sa pritom so zainteresovanými subjektmi najmä s cieľom určiť, či ***ju treba zmeniť na základe zmien*** spoločenských, politických, technologických alebo trhových podmienok.	(82) Komisia by mala túto smernicu pravidelne preskúmavať a radiť sa pritom so zainteresovanými subjektmi najmä s cieľom určiť, či ***je vhodné navrhnúť zmeny vzhľadom na zmeny*** spoločenských, politických, technologických alebo trhových podmienok. ***V rámci týchto preskúmaní by Komisia mala posúdiť relevantnosť***

odvetví, pododvetví a typov subjektov uvedených v prílohách pre fungovanie hospodárstva a spoločnosti v súvislosti s kybernetickou bezpečnosťou. Komisia by mala okrem iného posúdiť, či by sa za kľúčové subjekty podľa tejto smernice mali určiť poskytovatelia digitálnych služieb, ktorí sú klasifikovaní ako veľmi veľké online platformy v zmysle článku 25 nariadenia (EÚ) XXXX/XXXX [jednotný trh s digitálnymi službami (akt o digitálnych službách) alebo ako strážcovia v zmysle vymedzenia v článku 2 bode 1 nariadenia (EÚ) XXXX/XXXX [súťažeschopné a spravodlivé trhy digitálneho sektora (akt o digitálnych trhoch)]. Okrem toho by Komisia mala posúdiť, či je vhodné zmeniť prílohu I k smernici Európskeho parlamentu a Rady 2020/1828[1a] doplnením odkazu na túto smernicu.

[1a] Smernica Európskeho parlamentu a Rady (EÚ) 2020/1828 z 25. novembra 2020 o žalobách v zastúpení na ochranu kolektívnych záujmov spotrebiteľov a o zrušení smernice 2009/22/ES (Ú. v. EÚ L 409, 4.12.2020, s. 1).

Pozmeňujúci návrh 76
Návrh smernice
Odôvodnenie 82 a (nové)

Text predložený Komisiou	*Pozmeňujúci návrh*
	(82a) V tejto smernici sa stanovujú požiadavky na kybernetickú bezpečnosť pre členské štáty, ako aj pre kľúčové a dôležité subjekty usadené v Únii. Tieto požiadavky na kybernetickú bezpečnosť by mali uplatňovať aj inštitúcie, orgány, úrady a agentúry Únie na základe legislatívneho aktu Únie.

Pozmeňujúci návrh 77

Návrh smernice
Odôvodnenie 82 b (nové)

Text predložený Komisiou	*Pozmeňujúci návrh*
	(82b) Táto smernica vytvára nové úlohy pre agentúru ENISA, čím sa posilňuje jej úloha, a môže viesť tiež k tomu, že agentúra ENISA bude musieť vykonávať svoje existujúce úlohy podľa nariadenia (EÚ) 2019/881 s vyššími štandardmi ako predtým. S cieľom zabezpečiť, aby agentúra ENISA mala potrebné finančné a ľudské zdroje na vykonávanie existujúcich a nových činností v rámci svojich úloh, ako aj na splnenie akýchkoľvek vyšších štandardov vyplývajúcich z jej posilnenej úlohy, jej rozpočet by sa mal zodpovedajúcim spôsobom zvýšiť. Aby sa zabezpečilo efektívne využívanie zdrojov, agentúre ENISA by sa mala navyše poskytnúť väčšia flexibilita, pokiaľ ide o spôsob, akým môže interne prideľovať zdroje, aby mohla účinne vykonávať svoje úlohy a plniť očakávania.

Pozmeňujúci návrh 78

Návrh smernice
Odôvodnenie 84

Text predložený Komisiou	*Pozmeňujúci návrh*
(84) V tejto smernici sa dodržiavajú základné práva a zásady uznané Chartou ***základných práv Európskej únie***, najmä právo na rešpektovanie súkromného života a komunikácie, ochrana osobných údajov, sloboda podnikania, právo vlastniť majetok, právo na účinný prostriedok nápravy pred súdom a právo na vypočutie. Táto smernica by sa mala vykonávať v súlade s uvedenými právami a zásadami**,**	(84) V tejto smernici sa dodržiavajú základné práva a zásady uznané chartou, najmä právo na rešpektovanie súkromného života a komunikácie, ochrana osobných údajov, sloboda podnikania, právo vlastniť majetok, právo na účinný prostriedok nápravy pred súdom a právo na vypočutie**.** ***Patrí sem aj právo príjemcov služieb poskytovaných kľúčovými a dôležitými subjektmi na účinný prostriedok nápravy pred súdom***. Táto smernica by sa mala vykonávať v súlade s uvedenými právami a zásadami**.**

Pozmeňujúci návrh 79

Návrh smernice
Článok 1 – odsek 2 – písmeno c a (nové)

Text predložený Komisiou	*Pozmeňujúci návrh*
	ca) stanovujú povinnosti členských štátov týkajúce sa dohľadu a presadzovania práva.

Pozmeňujúci návrh 80

Návrh smernice
Článok 2 – odsek 1

Text predložený Komisiou	*Pozmeňujúci návrh*
1. Táto smernica sa uplatňuje na verejné a súkromné subjekty, a to typu, ktorý sa v prílohe I označuje ako kľúčové subjekty a v prílohe II ako dôležité subjekty. Táto smernica sa neuplatňuje na ***subjekty, ktoré*** v zmysle ***odporúčania*** Komisie 2003/361/ES[28] ***spĺňajú kritériá mikropodniku alebo malého podniku***.	1. Táto smernica sa uplatňuje na verejné a súkromné ***kľúčové a dôležité*** subjekty, a to typu, ktorý sa v prílohe I označuje ako kľúčové subjekty a v prílohe II ako dôležité subjekty***, ktoré poskytujú svoje služby alebo vykonávajú svoju činnosť v rámci Únie***. Táto smernica sa neuplatňuje na ***malé podniky ani mikropodniky*** v zmysle ***článku 2 bodov 2 a 3 prílohy k odporúčaniu*** Komisie 2003/361/ES[28]***. Článok 3 bod 4 prílohy k uvedenému odporúčaniu sa neuplatňuje.***
[28] Odporúčanie Komisie 2003/361/ES zo 6. mája 2003 o vymedzení pojmov mikropodnik, malý a stredný podnik (Ú. v. EÚ L 124, 20.5.2003, s. 36).	[28] Odporúčanie Komisie 2003/361/ES zo 6. mája 2003 o vymedzení pojmov mikropodnik, malý a stredný podnik (Ú. v. EÚ L 124, 20.5.2003, s. 36).

Pozmeňujúci návrh 81

Návrh smernice
Článok 2 – odsek 2 – pododsek 1 – úvodná časť

Text predložený Komisiou	*Pozmeňujúci návrh*
Táto smernica sa ***však*** bez ohľadu na ich veľkosť uplatňuje aj na ***subjekty uvedené v prílohe I a II***, keď:	Táto smernica sa bez ohľadu na ich veľkosť uplatňuje aj na ***kľúčové a dôležité subjekty***, keď:

Pozmeňujúci návrh 82

Návrh smernice
Článok 2 – odsek 2 – pododsek 1 – písmeno d

Text predložený Komisiou	*Pozmeňujúci návrh*
d) ***potenciálne*** narušenie služby poskytovanej subjektom by mohlo mať vplyv na ochranu verejnosti, verejnú bezpečnosť alebo verejné zdravie;	d) narušenie služby poskytovanej subjektom by mohlo mať vplyv na ochranu verejnosti, verejnú bezpečnosť alebo verejné zdravie;

Pozmeňujúci návrh 83

Návrh smernice
Článok 2 – odsek 2 – pododsek 1 – písmeno e

Text predložený Komisiou	*Pozmeňujúci návrh*
e) ***potenciálne*** narušenie služby poskytovanej subjektom by mohlo vyvolať systémové riziká, najmä v odvetviach, v ktorých by takéto narušenie mohlo mať cezhraničný vplyv;	e) narušenie služby poskytovanej subjektom by mohlo vyvolať systémové riziká, najmä v odvetviach, v ktorých by takéto narušenie mohlo mať cezhraničný vplyv;

Pozmeňujúci návrh 84

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.	***vypúšťa sa***

Pozmeňujúci návrh 85

Návrh smernice
Článok 2 – odsek 2 a (nový)

Text predložený Komisiou	*Pozmeňujúci návrh*
	2a. Do ... [6 mesiacov po uplynutí lehoty na transpozíciu] členské štáty vypracujú zoznam kľúčových a dôležitých subjektov vrátane subjektov uvedených v odseku 1 a

subjektov identifikovaných podľa odseku 2 písm. b) až f) a článku 24 ods. 1. Členské štáty uvedený zoznam pravidelne preskúmavajú a v prípade potreby aktualizujú, a to následne aspoň každé dva roky.

Pozmeňujúci návrh 86

Návrh smernice
Článok 2 – odsek 2 b (nový)

Text predložený Komisiou	*Pozmeňujúci návrh*
	2b. Členské štáty zabezpečia, aby kľúčové a dôležité subjekty predkladali príslušným orgánom aspoň tieto informácie:
	a) názov subjektu;
	b) adresu a aktuálne kontaktné údaje vrátane e-mailových adries, rozsahov IP adries, telefónnych čísel; a
	c) príslušné odvetvie(-ia) a pododvetvie(-ia) uvedené v prílohách I a II.
	Kľúčové a dôležité subjekty bezodkladne oznámia všetky zmeny údajov, ktoré predložili podľa prvého pododseku, a v každom prípade do dvoch týždňov odo dňa, keď zmena nadobudla účinnosť. Na tento účel Komisia s pomocou agentúry ENISA bez zbytočného odkladu vydá usmernenia a vzory týkajúce sa povinností uvedených v tomto odseku.

Pozmeňujúci návrh 87

Návrh smernice
Článok 2 – odsek 2 c (nový)

Text predložený Komisiou	*Pozmeňujúci návrh*
	2c. Členské štáty do ... [6 mesiacov po uplynutí lehoty na transpozíciu] a následne každé dva roky oznámia:
	a) Komisii a skupine pre spoluprácu počet všetkých kľúčových a dôležitých

subjektov identifikovaných pre každé odvetvie a pododvetvie uvedené v prílohách I a II, a

b) Komisii názvy subjektov identifikovaných podľa odseku 2 písm. b) až f).

Pozmeňujúci návrh 88

Návrh smernice
Článok 2 – odsek 4

Text predložený Komisiou	*Pozmeňujúci návrh*
4. Táto smernica sa uplatňuje bez toho, aby boli dotknuté smernica Rady 2008/114/ES[30] a smernice Európskeho parlamentu a Rady 2011/93/EÚ[31] ***a*** 2013/40/EÚ[32].	4. Táto smernica sa uplatňuje bez toho, aby boli dotknuté smernica Rady 2008/114/ES[30] a smernice Európskeho parlamentu a Rady 2011/93/EÚ[31]**,** 2013/40/EÚ[32] ***a 2002/58/EC[32a]***.
[30] Smernica Rady 2008/114/ES z 8. decembra 2008 o identifikácii a označení európskych kritických infraštruktúr a zhodnotení potreby zlepšiť ich ochranu (Ú. v. EÚ L 345, 23.12.2008, s. 75).	[30] Smernica Rady 2008/114/ES z 8. decembra 2008 o identifikácii a označení európskych kritických infraštruktúr a zhodnotení potreby zlepšiť ich ochranu (Ú. v. EÚ L 345, 23.12.2008, s. 75).
[31] Smernica Európskeho parlamentu a Rady 2011/93/EÚ z 13. decembra 2011 o boji proti sexuálnemu zneužívaniu a sexuálnemu vykorisťovaniu detí a proti detskej pornografii, ktorou sa nahrádza rámcové rozhodnutie Rady 2004/68/SVV (Ú. v. EÚ L 335, 17.12.2011, s. 1).	[31] Smernica Európskeho parlamentu a Rady 2011/93/EÚ z 13. decembra 2011 o boji proti sexuálnemu zneužívaniu a sexuálnemu vykorisťovaniu detí a proti detskej pornografii, ktorou sa nahrádza rámcové rozhodnutie Rady 2004/68/SVV (Ú. v. EÚ L 335, 17.12.2011, s. 1).
[32] Smernica Európskeho parlamentu a Rady 2013/40/EÚ z 12. augusta 2013 o útokoch na informačné systémy, ktorou sa nahrádza rámcové rozhodnutie Rady 2005/222/SVV (Ú. v. EÚ L 218, 14.8.2013, s. 8).	[32] Smernica Európskeho parlamentu a Rady 2013/40/EÚ z 12. augusta 2013 o útokoch na informačné systémy, ktorou sa nahrádza rámcové rozhodnutie Rady 2005/222/SVV (Ú. v. EÚ L 218, 14.8.2013, s. 8).
	[32a] Smernica Európskeho parlamentu a Rady 2002/58/ES z 12. júla 2002, týkajúca sa spracovávania osobných údajov a ochrany súkromia v sektore elektronických komunikácií (smernica o súkromí a elektronických komunikáciách) (Ú. v. ES L 201, 31.7.2002, s. 37).

Pozmeňujúci návrh 89

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 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.	6. Ak sa v ustanoveniach právnych aktov Únie špecifických pre určité odvetvie vyžaduje, aby kľúčové alebo dôležité subjekty prijali opatrenia na riadenie kybernetickobezpečnostných rizík alebo oznamovali incidenty, 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. ***Komisia bez zbytočného odkladu vydá usmernenia týkajúce sa vykonávania právnych aktov Únie špecifických pre určité odvetvie s cieľom zabezpečiť, aby uvedené akty spĺňali požiadavky na kybernetickú bezpečnosť stanovené v tejto smernici a aby nedochádzalo k prekrývaniu alebo právnej neistote. Pri príprave týchto usmernení Komisia zohľadňuje najlepšie postupy a odborné znalosti agentúry ENISA a skupiny pre spoluprácu.***

Pozmeňujúci návrh 90

Návrh smernice
Článok 2 – odsek 6 a (nový)

Text predložený Komisiou	*Pozmeňujúci návrh*
	6a. Kľúčové a dôležité subjekty, jednotky CSIRT a poskytovatelia bezpečnostných technológií a služieb spracúvajú osobné údaje v rozsahu, ktorý je nevyhnutne potrebný a primeraný na účely kybernetickej bezpečnosti a bezpečnosti sietí a informácií, s cieľom splniť povinnosti stanovené v tejto smernici. Uvedené spracúvanie osobných údajov podľa tejto smernice sa vykonáva v súlade s nariadením (EÚ) 2016/679,

najmä s jeho článkom 6.

Pozmeňujúci návrh 91

Návrh smernice
Článok 2 – odsek 6 b (nový)

Text predložený Komisiou	*Pozmeňujúci návrh*
	6b. Spracúvanie osobných údajov podľa tejto smernice poskytovateľmi verejných elektronických komunikačných sietí alebo poskytovateľmi verejne dostupných elektronických komunikácií uvedenými v prílohe I bode 8 sa vykonáva v súlade so smernicou 2002/58/ES.

Pozmeňujúci návrh 92

Návrh smernice
Článok 4 – odsek 1 – bod 4 a (nový)

Text predložený Komisiou	*Pozmeňujúci návrh*
	(4a) „udalosť odvrátená v poslednej chvíli“ je udalosť, ktorá mohla ohroziť dostupnosť, pravosť, integritu alebo dôvernosť údajov alebo ktorá mohla spôsobiť škodu, ale jej negatívnemu vplyvu sa úspešne zabránilo;

Pozmeňujúci návrh 93

Návrh smernice
Článok 4 – odsek 1 – bod 6

Text predložený Komisiou	*Pozmeňujúci návrh*
(6) „riešenie incidentov“ sú všetky kroky a postupy zamerané na odhaľovanie, analýzu a obmedzovanie následkov incidentu a reakcie naň;	(6) „riešenie incidentov“ sú všetky kroky a postupy zamerané na ***prevenciu,*** odhaľovanie, analýzu a obmedzovanie následkov incidentu a reakcie naň;

Pozmeňujúci návrh 94

Návrh smernice
Článok 4 – odsek 1 – bod 7 a (nový)

Text predložený Komisiou	*Pozmeňujúci návrh*
	(7a) „riziko“ je potenciál straty alebo narušenia v dôsledku incidentu a má sa vyjadriť ako kombinácia rozsahu takejto straty alebo narušenia a pravdepodobnosti výskytu daného incidentu;

Pozmeňujúci návrh 95

Návrh smernice
Článok 4 – odsek 1 – bod 11

Text predložený Komisiou	*Pozmeňujúci návrh*
(11) „technická špecifikácia“ je technická špecifikácia v zmysle článku 2 ***bodu 4*** nariadenia (EÚ) č. ***1025***/***2012***;	(11) „technická špecifikácia“ je technická špecifikácia v zmysle ***vymedzenia v*** článku 2 ***bode 20*** nariadenia (EÚ) ***2019***/***881***;

Pozmeňujúci návrh 96

Návrh smernice
Článok 4 – odsek 1 – bod 13

Text predložený Komisiou	*Pozmeňujúci návrh*
(13) „systém doménových mien (DNS)“ je hierarchický distribuovaný systém pomenovaní, ktorý umožňuje ***koncovým používateľom dostať sa*** k službám a zdrojom ***na internete***;	(13) „systém doménových mien (DNS)“ je hierarchický distribuovaný systém pomenovaní, ktorý umožňuje ***identifikáciu internetových služieb a zdrojov a ktorý umožňuje, aby zariadenia koncových používateľov využívali služby smerovania internetu a pripojenia na účely prístupu*** k ***týmto*** službám a zdrojom;

Pozmeňujúci návrh 97

Návrh smernice
Článok 4 – odsek 1 – bod 14

Text predložený Komisiou	*Pozmeňujúci návrh*
(14) „poskytovateľ služieb DNS“ je subjekt, ktorý ***koncovým používateľom internetu a iným poskytovateľom služieb DNS*** poskytuje ***služby rekurzívneho alebo autoritatívneho rozlišovania doménových***	(14) „poskytovateľ služieb DNS“ je subjekt, ktorý poskytuje***:***

mien;

Pozmeňujúci návrh 98

Návrh smernice
Článok 4 – odsek 1 – bod 14 – písmeno a (nové)

Text predložený Komisiou	*Pozmeňujúci návrh*
	a) koncovým používateľom internetu otvorené a verejné služby rekurzívneho rozlišovania doménových mien; alebo

Pozmeňujúci návrh 99

Návrh smernice
Článok 4 – odsek 1 – bod 14 – písmeno b (nové)

Text predložený Komisiou	*Pozmeňujúci návrh*
	b) služby autoritatívneho rozlišovania doménových mien ako službu, ktorú môžu obstarať subjekty, ktoré sú tretími stranami;

Pozmeňujúci návrh 100

Návrh smernice
Článok 4 – odsek 1 – bod 15

Text predložený Komisiou	*Pozmeňujúci návrh*
(15) „správca mien domény najvyššej úrovne“ je subjekt, ktorému bola udelená osobitná doména najvyššej úrovne (TLD) a ktorý je zodpovedný za správu TLD vrátane registrácie doménových mien v rámci TLD a za technickú prevádzku TLD vrátane prevádzky menných serverov, údržby databáz a distribúcie zónových súborov TLD v rámci menných serverov;	(15) „správca mien domény najvyššej úrovne“ je subjekt, ktorému bola udelená osobitná doména najvyššej úrovne (TLD) a ktorý je zodpovedný za správu TLD vrátane registrácie doménových mien v rámci TLD a za technickú prevádzku TLD vrátane prevádzky menných serverov, údržby databáz a distribúcie zónových súborov TLD v rámci menných serverov***, bez ohľadu na to, či ktorúkoľvek z týchto operácií vykonáva subjekt alebo sa vykonáva externe***;

Pozmeňujúci návrh 101

Návrh smernice
Článok 4 – odsek 1 – bod 15 a (nový)

Text predložený Komisiou	*Pozmeňujúci návrh*
	(15a) „služby registrácie doménových mien“ sú služby poskytované správcami a registrátormi doménových mien, poskytovateľmi služieb registrácie v oblasti služieb ochrany súkromia alebo proxy, sprostredkovateľmi alebo ďalšími predajcami domén a akékoľvek ďalšie služby, ktoré súvisia s registráciou doménových mien;

Pozmeňujúci návrh 102

Návrh smernice
Článok 4 – odsek 1 – bod 23 a (nový)

Text predložený Komisiou	*Pozmeňujúci návrh*
	(23a) „verejná elektronická komunikačná sieť“ je verejná elektronická komunikačná sieť v zmysle vymedzenia v článku 2 bode 8 smernice (EÚ) 2018/1972;

Pozmeňujúci návrh 103

Návrh smernice
Článok 4 – odsek 1 – bod 23 b (nový)

Text predložený Komisiou	*Pozmeňujúci návrh*
	(23b) „elektronická komunikačná služba“ je elektronická komunikačná služba v zmysle vymedzenia v článku 2 bode 4 smernice (EÚ) 2018/1972;

Pozmeňujúci návrh 104

Návrh smernice
Článok 5 – odsek 1 – úvodná časť

Text predložený Komisiou	*Pozmeňujúci návrh*
1. Každý členský štát prijme národnú stratégiu kybernetickej bezpečnosti,	1. Každý členský štát prijme národnú stratégiu kybernetickej bezpečnosti,

v ktorej sa vymedzia strategické ciele a vhodné politické a regulačné opatrenia na dosiahnutie a zachovanie vysokej úrovne kybernetickej bezpečnosti. Národná stratégia kybernetickej bezpečnosti sietí obsahuje najmä tieto prvky:	v ktorej sa vymedzia strategické ciele***,*** ***požadované technické, organizačné*** a ***finančné zdroje na dosiahnutie týchto cieľov, ako aj*** vhodné politické a regulačné opatrenia na dosiahnutie a zachovanie vysokej úrovne kybernetickej bezpečnosti. Národná stratégia kybernetickej bezpečnosti sietí obsahuje najmä tieto prvky:

Pozmeňujúci návrh 105

Návrh smernice
Článok 5 – odsek 1 – písmeno a

Text predložený Komisiou	*Pozmeňujúci návrh*
a) vymedzenie cieľov a priorít stratégie členského štátu v oblasti kybernetickej bezpečnosti;	*(Netýka sa slovenskej verzie.)*

Pozmeňujúci návrh 106

Návrh smernice
Článok 5 – odsek 1 – písmeno b

Text predložený Komisiou	*Pozmeňujúci návrh*
b) riadiaci rámec na dosiahnutie týchto cieľov a priorít vrátane politík uvedených v odseku 2***, ako aj úloh a zodpovedností vládnych orgánov, inštitúcií a ďalších relevantných aktérov***;	b) riadiaci rámec na dosiahnutie týchto cieľov a priorít vrátane politík uvedených v odseku 2;

Pozmeňujúci návrh 107

Návrh smernice
Článok 5 – odsek 1 – písmeno b a (nové)

Text predložený Komisiou	*Pozmeňujúci návrh*
	ba) rámec na prideľovanie úloh a povinností verejných orgánov a subjektov, ako aj iných relevantných aktérov, ktorým sa podporuje spolupráca a koordinácia na vnútroštátnej úrovni medzi príslušnými orgánmi určenými podľa článku 7 ods. 1 a článku 8 ods. 1, jednotným kontaktným miestom určeným podľa článku 8 ods. 3 a

	jednotkami CSIRT určenými podľa článku 9;

Pozmeňujúci návrh 108

Návrh smernice
Článok 5 – odsek 1 – písmeno e

Text predložený Komisiou	*Pozmeňujúci návrh*
e) zoznam rôznych orgánov a aktérov zapojených do vykonávania národnej stratégie kybernetickej bezpečnosti;	e) zoznam rôznych orgánov a aktérov zapojených do vykonávania národnej stratégie kybernetickej bezpečnosti ***vrátane jednotného kontaktného miesta pre kybernetickú bezpečnosť pre MSP, ktoré poskytuje podporu pri vykonávaní osobitných opatrení v oblasti kybernetickej bezpečnosti;***

Pozmeňujúci návrh 109

Návrh smernice
Článok 5 – odsek 1 – písmeno f

Text predložený Komisiou	*Pozmeňujúci návrh*
f) politický rámec pre posilnenú koordináciu medzi príslušnými orgánmi podľa tejto smernice a smernice Európskeho parlamentu a Rady (EÚ) XXXX/XXXX[38] [smernica o odolnosti kritických subjektov] na účely výmeny informácií o incidentoch a kybernetických hrozbách a vykonávania úloh dohľadu.	f) politický rámec pre posilnenú koordináciu medzi príslušnými orgánmi podľa tejto smernice a smernice Európskeho parlamentu a Rady (EÚ) XXXX/XXXX[38] [smernica o odolnosti kritických subjektov] ***v rámci jednotlivých členských štátov aj medzi členskými štátmi*** na účely výmeny informácií o incidentoch a kybernetických hrozbách a vykonávania úloh dohľadu.
[38] [vložte celý názov a odkaz na uverejnenie v ú. v., keď budú známe]	[38] [vložte celý názov a odkaz na uverejnenie v ú. v., keď budú známe]

Pozmeňujúci návrh 110

Návrh smernice
Článok 5 – odsek 1 – písmeno f a (nové)

Text predložený Komisiou	*Pozmeňujúci návrh*
	fa) posúdenie všeobecnej úrovne informovanosti občanov o kybernetickej bezpečnosti.

Pozmeňujúci návrh 111

Návrh smernice
Článok 5 – odsek 2 – písmeno -a (nové)

Text predložený Komisiou	*Pozmeňujúci návrh*
	-a) politiku zameranú na kybernetickú bezpečnosť pre každý sektor, na ktorý sa vzťahuje táto smernica;

Pozmeňujúci návrh 112

Návrh smernice
Článok 5 – odsek 2 – písmeno b

Text predložený Komisiou	*Pozmeňujúci návrh*
b) usmernenia týkajúce sa zahrnutia a špecifikácie požiadaviek týkajúcich sa kybernetickej bezpečnosti produktov a služieb IKT vo verejnom obstarávaní;	b) usmernenia týkajúce sa zahrnutia a špecifikácie požiadaviek týkajúcich sa kybernetickej bezpečnosti produktov a služieb IKT vo verejnom obstarávaní ***vrátane požiadaviek na šifrovanie a využívania produktov kybernetickej bezpečnosti s otvoreným zdrojovým kódom***;

Pozmeňujúci návrh 113

Návrh smernice
Článok 5 – odsek 2 – písmeno d

Text predložený Komisiou	*Pozmeňujúci návrh*
d) politiku súvisiacu s udržaním všeobecnej dostupnosti a integrity verejného jadra otvoreného internetu;	d) politiku súvisiacu s udržaním všeobecnej dostupnosti a integrity verejného jadra otvoreného internetu ***vrátane kybernetickej bezpečnosti podmorských komunikačných káblov***;

Pozmeňujúci návrh 114

Návrh smernice
Článok 5 – odsek 2 – písmeno d a (nové)

Text predložený Komisiou	*Pozmeňujúci návrh*
	da) politiku na presadzovanie a podporu rozvoja vznikajúcich technológií, ako je umelá inteligencia, a ich integrácie do nástrojov a aplikácií na posilnenie kybernetickej bezpečnosti;

Pozmeňujúci návrh 115

Návrh smernice
Článok 5 – odsek 2 – písmeno d b (nové)

Text predložený Komisiou	*Pozmeňujúci návrh*
	db) politiku na podporu integrácie nástrojov a aplikácií s otvoreným zdrojovým kódom;

Pozmeňujúci návrh 116

Návrh smernice
Článok 5– odsek 2 – písmeno f

Text predložený Komisiou	*Pozmeňujúci návrh*
f) politiku podporovania akademických a výskumných inštitúcií pri vývoji nástrojov kybernetickej bezpečnosti a bezpečnej sieťovej infraštruktúry;	f) politiku podporovania akademických a výskumných inštitúcií pri vývoji***, zlepšovaní a zavádzaní*** nástrojov kybernetickej bezpečnosti a bezpečnej sieťovej infraštruktúry;

Pozmeňujúci návrh 117

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 ***podporu kybernetickej bezpečnosti pre*** MSP ***vrátane*** tých MSP, ktoré sú vylúčené z rozsahu pôsobnosti tejto smernice, ***na riešenie ich osobitných potrieb a na poskytovanie ľahko prístupných usmernení a podpory vrátane usmernení***

na riešenie výziev súvisiacich s dodávateľským reťazcom, ktorým MSP čelia;

Pozmeňujúci návrh 118

Návrh smernice
Článok 5 – odsek 2 – písmeno h a (nové)

Text predložený Komisiou	*Pozmeňujúci návrh*
	ha) politiku na podporu kybernetickej hygieny, ktorá zahŕňa základný súbor postupov a kontrol a zvyšuje všeobecnú informovanosť občanov o kybernetickobezpečnostných hrozbách a najlepších postupoch;

Pozmeňujúci návrh 119

Návrh smernice
Článok 5 – odsek 2 – písmeno h b (nové)

Text predložený Komisiou	*Pozmeňujúci návrh*
	hb) politiku na podporu aktívnej kybernetickej obrany;

Pozmeňujúci návrh 120

Návrh smernice
Článok 5 – odsek 2 – písmeno h c (nové)

Text predložený Komisiou	*Pozmeňujúci návrh*
	hc) politiku, ktorá orgánom pomôže rozvíjať kompetencie a chápanie bezpečnostných aspektov potrebných na navrhovanie, budovanie a riadenie pripojených miest;

Pozmeňujúci návrh 121

Návrh smernice
Článok 5 – odsek 2 – písmeno h d (nové)

Text predložený Komisiou	*Pozmeňujúci návrh*
	hd) politiku osobitne zameranú na riešenie ransomvérovej hrozby a narušenie obchodného modelu založeného na ransomvéri;

Pozmeňujúci návrh 122

Návrh smernice
Článok 5 – odsek 2 – písmeno h e (nové)

Text predložený Komisiou	*Pozmeňujúci návrh*
	he) politiku vrátane príslušných postupov a rámcov riadenia na podporu a presadzovanie vytvárania verejno-súkromných partnerstiev v oblasti kybernetickej bezpečnosti.

Pozmeňujúci návrh 123

Návrh smernice
Článok 5 – odsek 3

Text predložený Komisiou	*Pozmeňujúci návrh*
3. Členské štáty oznámia Komisii svoje národné stratégie kybernetickej bezpečnosti do troch mesiacov od ich prijatia. Z oznámenia môžu vylúčiť špecifické informácie, a to v takom prípade a takom rozsahu, v akom je to ***nevyhnutne*** potrebné na zachovanie národnej bezpečnosti.	3. Členské štáty oznámia Komisii svoje národné stratégie kybernetickej bezpečnosti do troch mesiacov od ich prijatia. Z oznámenia môžu vylúčiť špecifické informácie, a to v takom prípade a takom rozsahu, v akom je to potrebné na zachovanie národnej bezpečnosti.

Pozmeňujúci návrh 124

Návrh smernice
Článok 5 – odsek 4

Text predložený Komisiou	*Pozmeňujúci návrh*
4. Členské štáty posúdia svoje národné stratégie kybernetickej bezpečnosti aspoň každé štyri roky na základe kľúčových ukazovateľov výkonnosti a v prípade potreby ich zmenia. Agentúra Európskej	4. Členské štáty posúdia svoje národné stratégie kybernetickej bezpečnosti aspoň každé štyri roky na základe kľúčových ukazovateľov výkonnosti a v prípade potreby ich zmenia. Agentúra Európskej

únie pre kybernetickú bezpečnosť (ENISA) členským štátom na ich žiadosť pomáha pri vypracúvaní národnej stratégie a kľúčových ukazovateľov výkonnosti na posúdenie stratégie.	únie pre kybernetickú bezpečnosť (ENISA) členským štátom na ich žiadosť pomáha pri vypracúvaní národnej stratégie a kľúčových ukazovateľov výkonnosti na posúdenie stratégie. ***Agentúra ENISA poskytne členským štátom usmernenia s cieľom zosúladiť už vypracované vnútroštátne stratégie v oblasti kybernetickej bezpečnosti s požiadavkami a povinnosťami stanovenými v tejto smernici.***

Pozmeňujúci návrh 125

Návrh smernice
Článok 6 – nadpis

Text predložený Komisiou	*Pozmeňujúci návrh*
Koordinované zverejňovanie informácií o zraniteľnosti a ***európsky register*** zraniteľností	Koordinované zverejňovanie informácií o zraniteľnosti a ***európska databáza*** zraniteľností

Pozmeňujúci návrh 126

Návrh smernice
Článok 6 – odsek 1

Text predložený Komisiou	*Pozmeňujúci návrh*
1. Každý členský štát určí jednu zo svojich jednotiek CSIRT v zmysle článku 9 za koordinátora na účely koordinovaného zverejňovania informácií o zraniteľnosti. Určená jednotka CSIRT koná ako dôveryhodný sprostredkovateľ, ktorý ***v prípade potreby*** uľahčuje interakciu medzi oznamujúcim subjektom a výrobcom alebo poskytovateľom produktov IKT alebo služieb IKT. Ak sa oznámená zraniteľnosť týka viacerých výrobcov alebo poskytovateľov produktov IKT alebo služieb IKT v celej Únii, určená jednotka CSIRT každého dotknutého členského štátu spolupracuje so sieťou jednotiek CSIRT.	1. Každý členský štát určí jednu zo svojich jednotiek CSIRT v zmysle článku 9 za koordinátora na účely koordinovaného zverejňovania informácií o zraniteľnosti. Určená jednotka CSIRT koná ako dôveryhodný sprostredkovateľ, ktorý ***na žiadosť oznamujúceho subjektu*** uľahčuje interakciu medzi oznamujúcim subjektom a výrobcom alebo poskytovateľom produktov IKT alebo služieb IKT. Ak sa oznámená zraniteľnosť týka viacerých výrobcov alebo poskytovateľov produktov IKT alebo služieb IKT v celej Únii, určená jednotka CSIRT každého dotknutého členského štátu spolupracuje so sieťou jednotiek CSIRT.

Pozmeňujúci návrh 127

Návrh smernice
Článok 6 – odsek 2

Text predložený Komisiou	*Pozmeňujúci návrh*
2. Agentúra ENISA vytvorí a vedie ***európsky register*** zraniteľností. Na tento účel agentúra ENISA zriadi a udržiava vhodné informačné systémy, politiky a postupy, najmä s cieľom umožniť dôležitým a kľúčovým subjektom a ich dodávateľom sietí a informačných systémov zverejňovať a registrovať zraniteľnosti v produktoch IKT alebo službách IKT***, ako aj poskytovať*** prístup k informáciám o ***zraniteľnosti*** nachádzajúcich sa v ***registri všetkým zainteresovaným stranám. Register*** obsahuje najmä informácie opisujúce zraniteľnosť, zasiahnuté produkty IKT alebo služby IKT a závažnosť zraniteľnosti z hľadiska okolností, za ktorých ju možno zneužiť, dostupnosť súvisiacich bezpečnostných záplat ***a v*** prípade, že žiadne nie sú k dispozícii, usmernenie pre používateľov zraniteľných produktov a služieb o tom, ako možno zmierniť riziká vyplývajúce zo zverejnených zraniteľností.	2. Agentúra ENISA vytvorí a vedie ***európsku databázu*** zraniteľností ***s využitím globálneho registra spoločných zraniteľností a expozícií (CVE)***. Na tento účel agentúra ENISA zriadi a udržiava vhodné informačné systémy, politiky a postupy ***a prijme potrebné technické a organizačné opatrenia na zaistenie bezpečnosti a integrity databázy,*** najmä s cieľom umožniť dôležitým a kľúčovým subjektom a ich dodávateľom sietí a informačných systémov***, ako aj subjektom, ktoré nepatria do rozsahu pôsobnosti tejto smernice, a ich dodávateľom*** zverejňovať a registrovať zraniteľnosti v produktoch IKT alebo službách IKT***. Všetkým zainteresovaným stranám sa poskytne*** prístup k informáciám o ***zraniteľnostiach*** nachádzajúcich sa v ***databáze, pri ktorých sú k dispozícii bezpečnostné záplaty alebo zmierňujúce opatrenia. Databáza*** obsahuje najmä informácie opisujúce zraniteľnosť, zasiahnuté produkty IKT alebo služby IKT a závažnosť zraniteľnosti z hľadiska okolností, za ktorých ju možno zneužiť, ***a*** dostupnosť súvisiacich bezpečnostných záplat***. V*** prípade, že žiadne nie sú k dispozícii, ***sa do databázy zahrnie*** usmernenie pre používateľov zraniteľných produktov ***IKT*** a služieb ***IKT*** o tom, ako možno zmierniť riziká vyplývajúce zo zverejnených zraniteľností.

Pozmeňujúci návrh 128

Návrh smernice
Článok 7 – odsek 1 a (nový)

Text predložený Komisiou	*Pozmeňujúci návrh*
	1a. Ak členský štát určí viac ako jeden príslušný orgán uvedený v odseku 1, jasne uvedie, ktorý z týchto príslušných orgánov má slúžiť ako koordinátor riadenia

incidentov a kríz veľkého rozsahu.

Pozmeňujúci návrh 129

Návrh smernice
Článok 7 – odsek 2

Text predložený Komisiou	*Pozmeňujúci návrh*
2. Každý členský štát určí kapacity, prostriedky a postupy, ktoré možno použiť v prípade krízy na účely tejto smernice.	2. Každý členský štát určí kapacity, prostriedky a postupy, ktoré možno použiť v prípade krízy na účely tejto smernice.

Pozmeňujúci návrh 130

Návrh smernice
Článok 7 – odsek 4

Text predložený Komisiou	*Pozmeňujúci návrh*
4. Členské štáty oznámia Komisii určenie svojich príslušných orgánov uvedených v odseku 1 a predložia svoje vnútroštátne plány reakcie na kybernetickobezpečnostné incidenty a krízy uvedené v odseku 3 do troch mesiacov od tohto určenia a prijatia týchto plánov. Členské štáty môžu z plánu vylúčiť špecifické informácie, a to v takom prípade a takom rozsahu, v akom je to nevyhnutne potrebné pre ich národnú bezpečnosť.	4. Členské štáty oznámia Komisii určenie svojich príslušných orgánov uvedených v odseku 1 a predložia ***sieti EU-CyCLONe*** svoje vnútroštátne plány reakcie na kybernetickobezpečnostné incidenty a krízy uvedené v odseku 3 do troch mesiacov od tohto určenia a prijatia týchto plánov. Členské štáty môžu z plánu vylúčiť špecifické informácie, a to v takom prípade a takom rozsahu, v akom je to nevyhnutne potrebné pre ich národnú bezpečnosť.

Pozmeňujúci návrh 131

Návrh smernice
Článok 8 – odsek 3

Text predložený Komisiou	*Pozmeňujúci návrh*
3. Každý členský štát určí ***jedno*** vnútroštátne jednotné kontaktné miesto pre kybernetickú bezpečnosť (ďalej len „jednotné kontaktné miesto“). Ak členský štát určí iba jeden príslušný orgán, tento príslušný orgán je aj jednotným kontaktným miestom v danom členskom štáte.	3. Každý členský štát určí ***jeden z príslušných orgánov uvedených v odseku 1 za*** vnútroštátne jednotné kontaktné miesto pre kybernetickú bezpečnosť (ďalej len „jednotné kontaktné miesto“). Ak členský štát určí iba jeden príslušný orgán, tento príslušný orgán je aj jednotným kontaktným miestom v danom členskom štáte.

Pozmeňujúci návrh 132

Návrh smernice
Článok 8 – odsek 4

Text predložený Komisiou	*Pozmeňujúci návrh*
4. Každé jednotné kontaktné miesto vykonáva styčnú funkciu s cieľom zabezpečiť cezhraničnú spoluprácu orgánov daného členského štátu s príslušnými orgánmi v iných členských štátoch, ako aj zabezpečiť medziodvetvovú spoluprácu s inými príslušnými vnútroštátnymi orgánmi v rámci daného členského štátu.	4. Každé jednotné kontaktné miesto vykonáva styčnú funkciu s cieľom zabezpečiť cezhraničnú spoluprácu orgánov daného členského štátu s príslušnými orgánmi v iných členských štátoch, ***Komisiou a agentúrou ENISA,*** ako aj zabezpečiť medziodvetvovú spoluprácu s inými príslušnými vnútroštátnymi orgánmi v rámci daného členského štátu.

Pozmeňujúci návrh 133

Návrh smernice
Článok 9 – odsek 2

Text predložený Komisiou	*Pozmeňujúci návrh*
2. Členské štáty zabezpečia, aby každá jednotka CSIRT mala primerané zdroje na účinné plnenie svojich úloh stanovených v článku 10 ods. 2.	2. Členské štáty zabezpečia, aby každá jednotka CSIRT mala primerané zdroje ***a potrebné technické spôsobilosti*** na účinné plnenie svojich úloh stanovených v článku 10 ods. 2.

Pozmeňujúci návrh 134

Návrh smernice
Článok 9 – odsek 6 a (nový)

Text predložený Komisiou	*Pozmeňujúci návrh*
	6a. Členské štáty zabezpečia možnosť účinnej, efektívnej a bezpečnej výmeny informácií na všetkých stupňoch utajenia medzi ich vlastnými jednotkami CSIRT a jednotkami CSIRT z tretích krajín na rovnakom stupni utajenia.

Pozmeňujúci návrh 135

Návrh smernice
Článok 9 – odsek 6 b (nový)

Text predložený Komisiou	*Pozmeňujúci návrh*
	6b. Bez toho, aby bolo dotknuté právo Únie, najmä nariadenie (EÚ) 2016/679, spolupracujú jednotky CSIRT s jednotkami CSIRT alebo rovnocennými orgánmi v kandidátskych krajinách a ďalších tretích krajinách na západnom Balkáne a krajinách Východného partnerstva a podľa možnosti im poskytujú pomoc v oblasti kybernetickej bezpečnosti.

Pozmeňujúci návrh 136

Návrh smernice
Článok 9 – odsek 7

Text predložený Komisiou	*Pozmeňujúci návrh*
7. Členské štáty bez zbytočného odkladu oznámia Komisii jednotky CSIRT určené v súlade s odsekom 1**,** koordinátora jednotiek CSIRT určeného v súlade s článkom 6 ods. 1 ***a*** ich ***príslušné úlohy stanovené*** vo vzťahu ***k*** subjektom ***uvedeným v prílohách I a II***.	7. Členské štáty bez zbytočného odkladu oznámia Komisii jednotky CSIRT určené v súlade s odsekom 1 ***a*** koordinátora jednotiek CSIRT určeného v súlade s článkom 6 ods. 1 ***vrátane*** ich ***príslušných úloh stanovených*** vo vzťahu ***ku kľúčovým a dôležitým*** subjektom.

Pozmeňujúci návrh 137

Návrh smernice
Článok 10 – nadpis

Text predložený Komisiou	*Pozmeňujúci návrh*
Požiadavky na jednotky CSIRT a ich úlohy	Požiadavky na jednotky CSIRT a ich ***technické spôsobilosti a*** úlohy

Pozmeňujúci návrh 138

Návrh smernice
Článok 10 – odsek 1 – písmeno c

Text predložený Komisiou	*Pozmeňujúci návrh*
c) jednotky CSIRT musia mať zavedený vhodný systém ***riadenia a*** zasielania žiadostí, a to najmä s cieľom	c) jednotky CSIRT musia mať zavedený vhodný systém ***klasifikácie,*** zasielania ***a sledovania*** žiadostí, a to najmä

uľahčiť ich účinné a efektívne odovzdávanie;	s cieľom uľahčiť ich účinné a efektívne odovzdávanie;

Pozmeňujúci návrh 139

Návrh smernice
Článok 10 – odsek 1 – písmeno c a (nové)

Text predložený Komisiou	*Pozmeňujúci návrh*
	ca) jednotky CSIRT musia mať zavedené príslušné kódexy správania, aby sa zabezpečila dôvernosť a dôveryhodnosť ich operácií;

Pozmeňujúci návrh 140

Návrh smernice
Článok 10 – odsek 1 – písmeno d

Text predložený Komisiou	*Pozmeňujúci návrh*
d) jednotky CSIRT musia byť primerane personálne vybavené, aby sa zabezpečila stála dostupnosť ich služieb;	d) jednotky CSIRT musia byť primerane personálne vybavené, aby sa zabezpečila stála dostupnosť ich služieb***, a musia zabezpečiť vhodné rámce odbornej prípravy pre svojich zamestnancov***;

Pozmeňujúci návrh 141

Návrh smernice
Článok 10 – odsek 1 – písmeno e

Text predložený Komisiou	*Pozmeňujúci návrh*
e) jednotky CSIRT musia byť vybavené redundantnými systémami a záložným pracovným priestorom na zabezpečenie kontinuity svojich služieb;	e) jednotky CSIRT musia byť vybavené redundantnými systémami a záložným pracovným priestorom na zabezpečenie kontinuity svojich služieb ***vrátane širokej pripojiteľnosti v sieťach, informačných systémov, služieb a zariadení***;

Pozmeňujúci návrh 142

Návrh smernice
Článok 10 – odsek 1 a (nový)

Text predložený Komisiou	*Pozmeňujúci návrh*
	1a. Jednotky CSIRT musia rozvíjať aspoň tieto technické spôsobilosti:
	a) schopnosť vykonávať monitorovanie sietí a informačných systémov v reálnom alebo takmer reálnom čase a odhaľovať anomálie;
	b) schopnosť podporovať prevenciu a detekciu prienikov;
	c) schopnosť zhromažďovať forenzné údaje a vykonávať komplexné analýzy týchto údajov a reverzné inžinierstvo kybernetických hrozieb;
	d) schopnosť filtrovať škodlivé dátové toky;
	e) schopnosť presadzovať silnú autentifikáciu a oprávnenia na prístup a kontroly prístupu; a
	f) schopnosť analyzovať kybernetické hrozby.

Pozmeňujúci návrh 143

Návrh smernice
Článok 10 – odsek 2 – písmeno a

Text predložený Komisiou	*Pozmeňujúci návrh*
a) monitorujú kybernetické hrozby, zraniteľnosti a incidenty na vnútroštátnej úrovni;	a) monitorujú kybernetické hrozby, zraniteľnosti a incidenty na vnútroštátnej úrovni ***a získavajú spravodajské informácie o hrozbách v reálnom čase***;

Pozmeňujúci návrh 144

Návrh smernice
Článok 10 – odsek 2 – písmeno b

Text predložený Komisiou	*Pozmeňujúci návrh*
b) poskytujú kľúčovým a dôležitým subjektom, ako aj iným relevantným zainteresovaným stranám včasné varovanie, výstrahy, hlásenia a šíria	b) poskytujú kľúčovým a dôležitým subjektom, ako aj iným relevantným zainteresovaným stranám včasné varovanie, výstrahy, hlásenia a šíria

informácie o kybernetických hrozbách, zraniteľnostiach a incidentoch;	informácie o kybernetických hrozbách, zraniteľnostiach a incidentoch ***podľa možnosti v takmer reálnom čase***;

Pozmeňujúci návrh 145

Návrh smernice
Článok 10 – odsek 2 – písmeno c

Text predložený Komisiou	*Pozmeňujúci návrh*
c) reagujú na incidenty;	c) reagujú na incidenty ***a poskytujú pomoc zapojeným subjektom***;

Pozmeňujúci návrh 146

Návrh smernice
Článok 10 – odsek 2 – písmeno e

Text predložený Komisiou	*Pozmeňujúci návrh*
e) na žiadosť subjektu proaktívne kontrolujú siete a informačné systémy používané na poskytovanie jeho služieb;	e) na žiadosť subjektu ***alebo v prípade vážneho ohrozenia národnej bezpečnosti*** proaktívne kontrolujú siete a informačné systémy používané na poskytovanie jeho služieb;

Pozmeňujúci návrh 147

Návrh smernice
Článok 10 – odsek 2 – písmeno f a (nové)

Text predložený Komisiou	*Pozmeňujúci návrh*
	fa) na žiadosť subjektu zabezpečujú umožnenie a konfiguráciu sieťového protokolovania s cieľom chrániť údaje vrátane osobných údajov pred neoprávnenou exfiltráciou;

Pozmeňujúci návrh 148

Návrh smernice
Článok 10 – odsek 2 – písmeno f b (nové)

Text predložený Komisiou	*Pozmeňujúci návrh*
	fb) prispievajú k zavádzaniu zabezpečených nástrojov na výmenu

informácií podľa článku 9 ods. 3.

Pozmeňujúci návrh 149

Návrh smernice
Článok 10 – odsek 4 – úvodná časť

Text predložený Komisiou	*Pozmeňujúci návrh*
4. Jednotky CSIRT v záujme uľahčenia spolupráce podporujú prijímanie a využívanie spoločných alebo normalizovaných postupov, režimov utajenia a taxonómie v súvislosti s týmito prvkami:	4. Jednotky CSIRT v záujme uľahčenia spolupráce podporujú ***automatizáciu výmeny informácií,*** prijímanie a využívanie spoločných alebo normalizovaných postupov, režimov utajenia a taxonómie v súvislosti s týmito prvkami:

Pozmeňujúci návrh 150

Návrh smernice
Článok 11 – odsek 2

Text predložený Komisiou	*Pozmeňujúci návrh*
2. Členské štáty zabezpečia, aby ich ***príslušné orgány alebo*** jednotky CSIRT dostávali oznámenia o incidentoch***, závažných*** kybernetických hrozbách a udalostiach odvrátených v poslednej chvíli ***predkladané podľa tejto smernice. Ak členský štát rozhodne, že jeho jednotky CSIRT nemajú dostávať tieto oznámenia, jednotkám CSIRT sa v rozsahu potrebnom na plnenie ich úloh poskytne prístup k údajom o incidentoch, ktoré oznámili kľúčové alebo dôležité subjekty*** podľa článku ***20***.	2. Členské štáty zabezpečia, aby ich jednotky CSIRT dostávali oznámenia o ***závažných*** incidentoch ***podľa článku 20 a*** kybernetických hrozbách a udalostiach odvrátených v poslednej chvíli podľa článku ***27 prostredníctvom jednotného kontaktného miesta uvedeného v článku 20 ods. 4a***.

Pozmeňujúci návrh 151

Návrh smernice
Článok 11 – odsek 4

Text predložený Komisiou	*Pozmeňujúci návrh*
4. Členské štáty v rozsahu potrebnom na účinné plnenie úloh a povinností stanovených v tejto smernici zabezpečia primeranú spoluprácu medzi príslušnými	4. Členské štáty v rozsahu potrebnom na účinné plnenie úloh a povinností stanovených v tejto smernici zabezpečia primeranú spoluprácu medzi príslušnými

orgánmi ***a*** jednotnými kontaktnými miestami, ako aj orgánmi presadzovania práva, orgánmi na ochranu údajov ***a*** orgánmi zodpovednými za kritickú infraštruktúru podľa smernice (EÚ) XXXX/XXXX [smernica o odolnosti kritických subjektov] a vnútroštátnymi finančnými orgánmi určenými v súlade s nariadením Európskeho parlamentu a Rady (EÚ) XXXX/XXXX[39] [nariadenie DORA] v rámci daného členského štátu.	orgánmi***,*** jednotnými kontaktnými miestami, ***jednotkami CSIRT,*** ako aj orgánmi presadzovania práva, ***národnými regulačnými orgánmi alebo inými príslušnými orgánmi zodpovednými za verejné elektronické komunikačné siete alebo za verejne dostupné elektronické komunikačné služby podľa smernice (EÚ) 2018/1972,*** orgánmi na ochranu údajov***,*** orgánmi zodpovednými za kritickú infraštruktúru podľa smernice (EÚ) XXXX/XXXX [smernica o odolnosti kritických subjektov] a vnútroštátnymi finančnými orgánmi určenými v súlade s nariadením Európskeho parlamentu a Rady (EÚ) XXXX/XXXX[39] [nariadenie DORA] v rámci daného členského štátu ***v súlade s ich príslušnými právomocami***.
[39] [vložte celý názov a odkaz na uverejnenie v ú. v., keď budú známe]	[39] [vložte celý názov a odkaz na uverejnenie v ú. v., keď budú známe]

Pozmeňujúci návrh 152

Návrh smernice
Článok 11 – odsek 5

Text predložený Komisiou	*Pozmeňujúci návrh*
5. Členské štáty zabezpečia, aby ich príslušné orgány pravidelne poskytovali príslušným orgánom určeným podľa smernice (EÚ) XXXX/XXXX [smernica o odolnosti kritických subjektov] informácie o kybernetickobezpečnostných rizikách, kybernetických hrozbách a incidentoch, ktoré zasiahli kľúčové subjekty identifikované ako kritické alebo rovnocenné s kritickými subjektmi podľa smernice (EÚ) XXXX/XXXX [smernica o odolnosti kritických subjektov], ako aj opatrenia prijaté príslušnými orgánmi v reakcii na tieto riziká a incidenty.	5. Členské štáty zabezpečia, aby ich príslušné orgány pravidelne ***a včas*** poskytovali príslušným orgánom určeným podľa smernice (EÚ) XXXX/XXXX [smernica o odolnosti kritických subjektov] informácie o kybernetickobezpečnostných rizikách, kybernetických hrozbách a incidentoch, ktoré zasiahli kľúčové subjekty identifikované ako kritické alebo rovnocenné s kritickými subjektmi podľa smernice (EÚ) XXXX/XXXX [smernica o odolnosti kritických subjektov], ako aj opatrenia prijaté príslušnými orgánmi v reakcii na tieto riziká a incidenty.

Pozmeňujúci návrh 153

Návrh smernice
Článok 12 – odsek 3 – pododsek 1

Text predložený Komisiou	*Pozmeňujúci návrh*
Skupina pre spoluprácu sa skladá zo zástupcov členských štátov, Komisie a agentúry ENISA. Na činnostiach skupiny pre spoluprácu sa ako ***pozorovateľ zúčastňuje*** Európska služba pre vonkajšiu činnosť. Na činnostiach skupiny pre spoluprácu sa môžu zúčastňovať európske orgány dohľadu (ESA) v súlade s článkom 17 ods. 5 písm. c) nariadenia (EÚ) XXXX/XXXX [nariadenie DORA].	Skupina pre spoluprácu sa skladá zo zástupcov členských štátov, Komisie a agentúry ENISA. Na činnostiach skupiny pre spoluprácu sa ako ***pozorovatelia zúčastňujú Európsky parlament a*** Európska služba pre vonkajšiu činnosť. Na činnostiach skupiny pre spoluprácu sa môžu zúčastňovať európske orgány dohľadu (ESA) v súlade s článkom 17 ods. 5 písm. c) nariadenia (EÚ) XXXX/XXXX [nariadenie DORA].

Pozmeňujúci návrh 154

Návrh smernice
Článok 12 – odsek 3 – pododsek 2

Text predložený Komisiou	*Pozmeňujúci návrh*
Vo vhodných prípadoch môže skupina pre spoluprácu prizvať k svojej práci zástupcov príslušných zainteresovaných strán.	Vo vhodných prípadoch môže skupina pre spoluprácu prizvať k svojej práci zástupcov príslušných zainteresovaných strán***, ako sú Európsky výbor pre ochranu údajov a zástupcovia odvetvia***.

Pozmeňujúci návrh 155

Návrh smernice
Článok 12 – odsek 4 – písmeno b

Text predložený Komisiou	*Pozmeňujúci návrh*
b) výmena najlepších postupov a informácií v súvislosti s vykonávaním tejto smernice, a to aj pokiaľ ide o kybernetické hrozby, incidenty, zraniteľnosti, udalosti odvrátené v poslednej chvíli, iniciatívy na zvyšovanie povedomia, odbornú prípravu, cvičenia a zručnosti, budovanie kapacít, ***ako aj*** normy a technické špecifikácie;	b) výmena najlepších postupov a informácií v súvislosti s vykonávaním tejto smernice, a to aj pokiaľ ide o kybernetické hrozby, incidenty, zraniteľnosti, udalosti odvrátené v poslednej chvíli, iniciatívy na zvyšovanie povedomia, odbornú prípravu, cvičenia a zručnosti, budovanie kapacít, normy a technické špecifikácie***, ako aj identifikáciu kľúčových a dôležitých subjektov***;

Pozmeňujúci návrh 156

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 odvetví v celej Únii;

Pozmeňujúci návrh 157

Návrh smernice
Článok 12 – odsek 4 – písmeno c

Text predložený Komisiou	*Pozmeňujúci návrh*
c) vzájomné poradenstvo a spolupráca s Komisiou v súvislosti s novými politickými iniciatívami v oblasti kybernetickej bezpečnosti;	c) vzájomné poradenstvo a spolupráca s Komisiou v súvislosti s novými politickými iniciatívami v oblasti kybernetickej bezpečnosti ***a celkovou súdržnosťou požiadaviek na kybernetickú bezpečnosť špecifických pre jednotlivé odvetvia***;

Pozmeňujúci návrh 158

Návrh smernice
Článok 12– odsek 4 – písmeno f

Text predložený Komisiou	*Pozmeňujúci návrh*
f) prediskutovanie správ o partnerskom preskúmaní uvedených v článku 16 ods. 7;	f) prediskutovanie správ o partnerskom preskúmaní uvedených v článku 16 ods. 7 ***a vypracovanie záverov a odporúčaní***;

Pozmeňujúci návrh 159

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

Text predložený Komisiou	*Pozmeňujúci návrh*
	fa) vykonávanie koordinovaných posúdení bezpečnostných rizík, ktoré sa môžu iniciovať na základe článku 19 ods. 1 v spolupráci s Komisiou a agentúrou

ENISA;

Pozmeňujúci návrh 160

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

Text predložený Komisiou	*Pozmeňujúci návrh*
	ka) predkladanie správ o skúsenostiach získaných na strategickej a operačnej úrovni Komisii na účely preskúmania uvedeného v článku 35;

Pozmeňujúci návrh 161

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

Text predložený Komisiou	*Pozmeňujúci návrh*
	kb) zabezpečenie každoročného posúdenia v spolupráci s agentúrou ENISA, Europolom a vnútroštátnymi orgánmi presadzovania práva, pokiaľ ide o to, ktoré tretie krajiny poskytujú útočisko páchateľom šíriacim ransomvér.

Pozmeňujúci návrh 162

Návrh smernice
Článok 12 – odsek 8

Text predložený Komisiou	*Pozmeňujúci návrh*
8. Skupina pre spoluprácu sa pravidelne a aspoň ***raz*** ročne stretáva so skupinou pre odolnosť kritických subjektov zriadenou podľa smernice (EÚ) XXXX/XXXX [smernica o odolnosti kritických subjektov] s cieľom ***podporovať*** strategickú spoluprácu a výmenu informácií.	8. Skupina pre spoluprácu sa pravidelne a aspoň ***dvakrát*** ročne stretáva so skupinou pre odolnosť kritických subjektov zriadenou podľa smernice (EÚ) XXXX/XXXX [smernica o odolnosti kritických subjektov] s cieľom ***uľahčovať*** strategickú spoluprácu a výmenu informácií.

Pozmeňujúci návrh 163

Návrh smernice
Článok 13 – odsek 3 – písmeno a a (nové)

Text predložený Komisiou	*Pozmeňujúci návrh*
	aa) uľahčovanie výmeny a transferu technológií a príslušných opatrení, politík, najlepších postupov a rámcov medzi jednotkami CSIRT;

Pozmeňujúci návrh 164

Návrh smernice
Článok 13 – odsek 3 – písmeno b a (nové)

Text predložený Komisiou	*Pozmeňujúci návrh*
	ba) zabezpečovanie interoperability, pokiaľ ide o normy výmeny informácií;

Pozmeňujúci návrh 165

Návrh smernice
Článok 14 – odsek 1

Text predložený Komisiou	*Pozmeňujúci návrh*
1. S cieľom podporiť koordinované riadenie kybernetickobezpečnostných incidentov a kríz veľkého rozsahu na operačnej úrovni a zabezpečiť pravidelnú výmenu informácií medzi členskými štátmi a inštitúciami, orgánmi a agentúrami Únie sa týmto zriaďuje Európska sieť styčných organizácií pre kybernetické krízy (EU-CyCLONe).	1. S cieľom podporiť koordinované riadenie kybernetickobezpečnostných incidentov a kríz veľkého rozsahu na operačnej úrovni a zabezpečiť pravidelnú výmenu ***relevantných*** informácií medzi členskými štátmi a inštitúciami, orgánmi a agentúrami Únie sa týmto zriaďuje Európska sieť styčných organizácií pre kybernetické krízy (EU-CyCLONe).

Pozmeňujúci návrh 166

Návrh smernice
Článok 14 – odsek 2

Text predložený Komisiou	*Pozmeňujúci návrh*
2. Sieť EU-CyCLONe tvoria zástupcovia orgánov krízového riadenia členských štátov určených v súlade s článkom 7, Komisia a agentúra ENISA. Agentúra ENISA zabezpečuje sekretariát siete a podporuje bezpečnú výmenu	2. Sieť EU-CyCLONe tvoria zástupcovia orgánov krízového riadenia členských štátov určených v súlade s článkom 7, Komisia a agentúra ENISA. Agentúra ENISA zabezpečuje sekretariát siete ***EU-CyCLONe*** a podporuje bezpečnú

informácií.	výmenu informácií.

Pozmeňujúci návrh 167

Návrh smernice
Článok 14 – odsek 5

Text predložený Komisiou	*Pozmeňujúci návrh*
5. Sieť EU-CyCLONe pravidelne podáva skupine pre spoluprácu správy o ***kybernetických hrozbách,*** incidentoch a trendoch, pričom sa zameriava najmä na ich vplyv na kľúčové a dôležité subjekty.	5. Sieť EU-CyCLONe pravidelne podáva skupine pre spoluprácu správy o incidentoch a ***krízach veľkého rozsahu, ako aj*** trendoch, pričom sa zameriava najmä na ich vplyv na kľúčové a dôležité subjekty.

Pozmeňujúci návrh 168

Návrh smernice
Článok 15 – odsek 1 – úvodná časť

Text predložený Komisiou	*Pozmeňujúci návrh*
1. Agentúra ENISA v spolupráci s Komisiou vydáva každé dva roky správu o stave kybernetickej bezpečnosti v Únii. Správa obsahuje najmä posúdenie týchto aspektov:	1. Agentúra ENISA v spolupráci s Komisiou vydáva každé dva roky správu o stave kybernetickej bezpečnosti v Únii ***a predkladá a prezentuje ju Európskemu parlamentu***. Správa ***sa dodáva v strojovo čitateľnom formáte a*** obsahuje najmä posúdenie týchto aspektov:

Pozmeňujúci návrh 169

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

Text predložený Komisiou	*Pozmeňujúci návrh*
	aa) všeobecná úroveň informovanosti o kybernetickej bezpečnosti a hygiene medzi občanmi a subjektmi vrátane MSP, ako aj všeobecná úroveň bezpečnosti pripojených zariadení;

Pozmeňujúci návrh 170

Návrh smernice
Článok 15 – odsek 1 – písmeno c

Text predložený Komisiou	*Pozmeňujúci návrh*
c) index kybernetickej bezpečnosti poskytujúci súhrnné posúdenie úrovne vyspelosti kybernetickobezpečnostných schopností.	c) index kybernetickej bezpečnosti poskytujúci súhrnné posúdenie úrovne vyspelosti kybernetickobezpečnostných schopností ***v celej Únii vrátane zosúladenia národných stratégií kybernetickej bezpečnosti členských štátov***;

Pozmeňujúci návrh 171

Návrh smernice
Článok 15 – odsek 2

Text predložený Komisiou	*Pozmeňujúci návrh*
2. Správa obsahuje konkrétne politické odporúčania na zvýšenie úrovne kybernetickej bezpečnosti v celej Únii a zhrnutie zistení za konkrétne obdobie z technických situačných správ EÚ o kybernetickej bezpečnosti, ktoré vydala agentúra ENISA v súlade s článkom 7 ods. 6 nariadenia (EÚ) 2019/881.	2. Správa obsahuje ***identifikáciu prekážok a*** konkrétne politické odporúčania na zvýšenie úrovne kybernetickej bezpečnosti v celej Únii a zhrnutie zistení za konkrétne obdobie z technických situačných správ EÚ o kybernetickej bezpečnosti, ktoré vydala agentúra ENISA v súlade s článkom 7 ods. 6 nariadenia (EÚ) 2019/881.

Pozmeňujúci návrh 172

Návrh smernice
Článok 15 – odsek 2 a (nový)

Text predložený Komisiou	*Pozmeňujúci návrh*
	2a. Agentúra ENISA v spolupráci s Komisiou a s usmernením skupiny pre spoluprácu a siete jednotiek CSIRT pripraví metodiku vrátane príslušných premenných indexu kybernetickej bezpečnosti uvedeného v odseku 1 písm. c).

Pozmeňujúci návrh 173

Návrh smernice
Článok 16 – odsek 1 – úvodná časť

Text predložený Komisiou	*Pozmeňujúci návrh*
1. Komisia po konzultácii so skupinou pre spoluprácu a agentúrou ENISA a najneskôr 18 mesiacov od nadobudnutia účinnosti tejto smernice stanoví metodiku a obsah systému partnerského preskúmania na posúdenie účinnosti politík členských štátov v oblasti kybernetickej bezpečnosti. Preskúmania vykonávajú technickí experti v oblasti kybernetickej bezpečnosti vybraní z iných členských štátov, než je skúmaný členský štát, a zameriavajú sa aspoň na:	1. Komisia po konzultácii so skupinou pre spoluprácu a agentúrou ENISA a najneskôr ***… /***18 mesiacov od nadobudnutia účinnosti tejto smernice***/*** stanoví metodiku a obsah systému partnerského preskúmania na posúdenie účinnosti politík členských štátov v oblasti kybernetickej bezpečnosti. ***Partnerské*** preskúmania vykonávajú ***v konzultácii s agentúrou ENISA*** technickí experti v oblasti kybernetickej bezpečnosti vybraní z ***aspoň dvoch*** iných členských štátov, než je skúmaný členský štát, a zameriavajú sa aspoň na:

Pozmeňujúci návrh 174

Návrh smernice
Článok 16 – odsek 1 – bod iii

Text predložený Komisiou	*Pozmeňujúci návrh*
iii) operačné schopnosti a účinnosť jednotiek CSIRT;	iii) operačné schopnosti a účinnosť jednotiek CSIRT ***pri vykonávaní ich úloh***;

Pozmeňujúci návrh 175

Návrh smernice
Článok 16 – odsek 3

Text predložený Komisiou	*Pozmeňujúci návrh*
3. O organizačných aspektoch partnerských preskúmaní rozhoduje Komisia s podporou agentúry ENISA a po konzultácii so skupinou pre spoluprácu tieto aspekty vychádzajú z kritérií vymedzených v metodike uvedenej v odseku 1. V partnerských preskúmaniach sa posudzujú aspekty uvedené v odseku 1 pre všetky členské štáty a odvetvia vrátane vybraných problémov špecifických pre jeden alebo viacero členských štátov alebo pre jedno alebo viacero odvetví.	3. O organizačných aspektoch partnerských preskúmaní rozhoduje Komisia s podporou agentúry ENISA a po konzultácii so skupinou pre spoluprácu tieto aspekty vychádzajú z kritérií vymedzených v metodike uvedenej v odseku 1. V partnerských preskúmaniach sa posudzujú aspekty uvedené v odseku 1 pre všetky členské štáty a odvetvia vrátane vybraných problémov špecifických pre jeden alebo viacero členských štátov alebo pre jedno alebo viacero odvetví. ***Určení experti, ktorí vykonávajú preskúmanie, oznámia tieto vybrané problémy***

	členskému štátu, ktorý je predmetom partnerského preskúmania, pred jeho začatím.

Pozmeňujúci návrh 176

Návrh smernice
Článok 16 – odsek 3 a (nový)

Text predložený Komisiou	*Pozmeňujúci návrh*
	3a. Pred začatím postupu partnerského preskúmania vykoná členský štát, ktorý je predmetom partnerského preskúmania, sebahodnotenie skúmaných aspektov a poskytne toto sebahodnotenie určeným expertom.

Pozmeňujúci návrh 177

Návrh smernice
Článok 16 – odsek 4

Text predložený Komisiou	*Pozmeňujúci návrh*
4. Partnerské preskúmania zahŕňajú skutočné alebo virtuálne návštevy na mieste a výmenu informácií na diaľku. Vzhľadom na zásadu dobrej spolupráce členské štáty, ktoré sú predmetom preskúmania, poskytnú určeným expertom požadované informácie potrebné na posúdenie skúmaných aspektov. Všetky informácie získané v procese partnerského preskúmania sa použijú výlučne na uvedený účel. Experti, ktorí sa zúčastňujú na partnerskom preskúmaní, nesmú sprístupniť tretím stranám žiadne citlivé alebo dôverné informácie získané v priebehu tohto preskúmania.	4. Partnerské preskúmania zahŕňajú skutočné alebo virtuálne návštevy na mieste a výmenu informácií na diaľku. Vzhľadom na zásadu dobrej spolupráce členské štáty, ktoré sú predmetom preskúmania, poskytnú určeným expertom požadované informácie potrebné na posúdenie skúmaných aspektov. ***Komisia v spolupráci s agentúrou ENISA vypracuje vhodné kódexy správania na podporu pracovných metód určených expertov.*** Všetky informácie získané v procese partnerského preskúmania sa použijú výlučne na uvedený účel. Experti, ktorí sa zúčastňujú na partnerskom preskúmaní, nesmú sprístupniť tretím stranám žiadne citlivé alebo dôverné informácie získané v priebehu tohto preskúmania.

Pozmeňujúci návrh 178

Návrh smernice
Článok 16 – odsek 6

Text predložený Komisiou	*Pozmeňujúci návrh*
6. Členský štát zabezpečí, aby sa akékoľvek riziko konfliktu záujmov týkajúce sa určených expertov ***bez zbytočného odkladu*** oznámilo ostatným členským štátom, Komisii a agentúre ENISA.	6. Členský štát zabezpečí, aby sa akékoľvek riziko konfliktu záujmov týkajúce sa určených expertov oznámilo ostatným členským štátom, Komisii a agentúre ENISA ***pred začatím postupu partnerského preskúmania***.

Pozmeňujúci návrh 179

Návrh smernice
Článok 16 – odsek 7

Text predložený Komisiou	*Pozmeňujúci návrh*
7. Experti zúčastňujúci sa na partnerských preskúmaniach vypracujú správy o zisteniach a záveroch preskúmaní. Správy sa predkladajú Komisii, skupine pre spoluprácu, sieti jednotiek CSIRT a agentúre ENISA. Prediskutujú sa v skupine pre spoluprácu a v sieti jednotiek CSIRT. Správy možno uverejniť na vyhradenom webovom sídle skupiny pre spoluprácu.	7. Experti zúčastňujúci sa na partnerských preskúmaniach vypracujú správy o zisteniach a záveroch preskúmaní. ***Správy obsahujú odporúčania s cieľom umožniť zlepšenie, pokiaľ ide o aspekty, ktoré sú predmetom postupu partnerského preskúmania.*** Správy sa predkladajú Komisii, skupine pre spoluprácu, sieti jednotiek CSIRT a agentúre ENISA. Prediskutujú sa v skupine pre spoluprácu a v sieti jednotiek CSIRT. Správy možno uverejniť na vyhradenom webovom sídle skupiny pre spoluprácu ***s výnimkou citlivých a dôverných informácií***.

Pozmeňujúci návrh 180

Návrh smernice
Článok 17 – odsek 2

Text predložený Komisiou	*Pozmeňujúci návrh*
2. Členské štáty zabezpečia, aby členovia riadiaceho orgánu ***pravidelne*** absolvovali osobitnú odbornú prípravu s cieľom získať dostatočné znalosti a zručnosti s cieľom zachytiť a posúdiť riziká a postupy riadenia v oblasti kybernetickej bezpečnosti a ich vplyv na ***činnosť subjektu***.	2. Členské štáty zabezpečia, aby členovia riadiaceho orgánu ***kľúčových a dôležitých subjektov*** absolvovali osobitnú odbornú prípravu, ***a podnietia kľúčové a dôležité subjekty, aby pravidelne ponúkali podobnú odbornú prípravu všetkým zamestnancom*** s cieľom získať dostatočné znalosti a zručnosti s cieľom zachytiť a posúdiť riziká a postupy riadenia v oblasti kybernetickej bezpečnosti a ich vplyv na

služby poskytované subjektom.

Pozmeňujúci návrh 181

Návrh smernice
Článok 18 – odsek 1

Text predložený Komisiou	*Pozmeňujúci návrh*
1. Členské štáty zabezpečia, aby kľúčové a dôležité subjekty prijali vhodné a primerané technické a organizačné opatrenia na riadenie rizík súvisiacich s bezpečnosťou sietí a informačných systémov, ktoré tieto subjekty využívajú ***pri poskytovaní*** svojich služieb. S ohľadom na najnovší technický vývoj tieto opatrenia zabezpečujú takú úroveň bezpečnosti sietí a informačných systémov, ktorá zodpovedá miere daného rizika.	1. Členské štáty zabezpečia, aby kľúčové a dôležité subjekty prijali vhodné a primerané technické***, operačné*** a organizačné opatrenia na riadenie rizík súvisiacich s bezpečnosťou sietí a informačných systémov, ktoré tieto subjekty využívajú ***na svoju činnosť alebo na poskytovanie*** svojich služieb ***a na prevenciu alebo minimalizáciu vplyvu incidentov na príjemcov ich služieb a na ďalšie služby***. S ohľadom na najnovší technický vývoj ***a na európske alebo medzinárodné normy*** tieto opatrenia zabezpečujú takú úroveň bezpečnosti sietí a informačných systémov, ktorá zodpovedá miere daného rizika.

Pozmeňujúci návrh 182

Návrh smernice
Článok 18 – odsek 2 – písmeno b

Text predložený Komisiou	*Pozmeňujúci návrh*
b) riešenie incidentov ***(predchádzanie incidentom, ich odhaľovanie a reakcia na ne)***;	b) riešenie incidentov;

Pozmeňujúci návrh 183

Návrh smernice
Článok 18 – odsek 2 – písmeno c

Text predložený Komisiou	*Pozmeňujúci návrh*
c) kontinuita činností a krízové riadenie;	c) kontinuita činností***, ako je riadenie zálohovania a obnova systému po havárii,*** a krízové riadenie;

Pozmeňujúci návrh 184

Návrh smernice
Článok 18 – odsek 2 – písmeno d

Text predložený Komisiou	*Pozmeňujúci návrh*
d) bezpečnosť dodávateľského reťazca vrátane bezpečnostných aspektov týkajúcich sa vzťahov medzi každým subjektom a jeho dodávateľmi alebo poskytovateľmi služieb***, ako sú napríklad poskytovatelia služieb ukladania a spracúvania dát alebo riadených bezpečnostných služieb***;	d) bezpečnosť dodávateľského reťazca vrátane bezpečnostných aspektov týkajúcich sa vzťahov medzi každým subjektom a jeho dodávateľmi alebo poskytovateľmi služieb;

Pozmeňujúci návrh 185

Návrh smernice
Článok 18– odsek 2 – písmeno f

Text predložený Komisiou	*Pozmeňujúci návrh*
f) politiky a postupy (testovanie a audit) na posúdenie účinnosti opatrení na riadenie kybernetickobezpečnostných rizík;	f) politiky a postupy (***odborná príprava,*** testovanie a audit) na posúdenie účinnosti opatrení na riadenie kybernetickobezpečnostných rizík;

Pozmeňujúci návrh 186

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

Text predložený Komisiou	*Pozmeňujúci návrh*
	fa) základné postupy kybernetickej hygieny a odborná príprava v oblasti kybernetickej bezpečnosti;

Pozmeňujúci návrh 187

Návrh smernice
Článok 18 – odsek 2 – písmeno g

Text predložený Komisiou	*Pozmeňujúci návrh*
g) používanie kryptografie ***a šifrovania.***	g) ***v prípade potreby*** používanie kryptografie***, ako je šifrovanie;***

Pozmeňujúci návrh 188

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

Text predložený Komisiou	*Pozmeňujúci návrh*
	ga) v prípade potreby používanie riešení viacstupňovej alebo kontinuálnej autentifikácie, zabezpečenej hlasovej, obrazovej a textovej komunikácie a zabezpečených systémov komunikácie v núdzových situáciách v rámci subjektu.

Pozmeňujúci návrh 189
Návrh smernice
Článok 18 – odsek 4

Text predložený Komisiou	*Pozmeňujúci návrh*
4. Členské štáty zabezpečia, aby subjekt po zistení, že jeho služby alebo úlohy nie sú v súlade s požiadavkami stanovenými v odseku 2, prijal bez zbytočného odkladu všetky potrebné nápravné opatrenia a danú službu s týmito požiadavkami zosúladil.	4. Členské štáty zabezpečia, aby subjekt po zistení, že jeho služby alebo úlohy nie sú v súlade s požiadavkami stanovenými v odseku 2, prijal bez zbytočného odkladu všetky potrebné***, vhodné a primerané*** nápravné opatrenia a danú službu s týmito požiadavkami zosúladil.

Pozmeňujúci návrh 190

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.	***vypúšťa sa***

Pozmeňujúci návrh 191

Návrh smernice
Článok 18 – odsek 6

Text predložený Komisiou	*Pozmeňujúci návrh*
6. Komisia je splnomocnená prijímať delegované akty v súlade s článkom 36 s cieľom doplniť prvky stanovené v odseku 2 na zohľadnenie nových kybernetických hrozieb, technologického vývoja alebo odvetvových špecifík.	6. Komisia je splnomocnená prijímať delegované akty v súlade s článkom 36 s cieľom doplniť prvky stanovené v odseku 2 ***tohto článku*** na zohľadnenie nových kybernetických hrozieb, technologického vývoja alebo odvetvových špecifík ***a zároveň doplniť túto smernicu stanovením technických a metodických špecifikácií opatrení uvedených v odseku 2 tohto článku.***

Pozmeňujúci návrh 192

Návrh smernice
Článok 19 – odsek 1

Text predložený Komisiou	*Pozmeňujúci návrh*
1. Skupina pre spoluprácu môže v spolupráci s Komisiou a agentúrou ENISA vykonávať koordinované posúdenia bezpečnostného rizika dodávateľských reťazcov konkrétnych kritických služieb, systémov alebo produktov IKT, pričom zohľadní technické a prípadne aj netechnické faktory rizík.	1. Skupina pre spoluprácu môže v spolupráci s Komisiou a agentúrou ENISA vykonávať koordinované posúdenia bezpečnostného rizika dodávateľských reťazcov konkrétnych kritických služieb, systémov alebo produktov IKT ***a informačného a komunikačného systému (IKS)***, pričom zohľadní technické a prípadne aj netechnické faktory rizík.

Pozmeňujúci návrh 193

Návrh smernice
Článok 19 – odsek 2

Text predložený Komisiou	*Pozmeňujúci návrh*
2. Komisia po konzultácii so skupinou pre spoluprácu a agentúrou ENISA určí konkrétne kritické služby, systémy alebo produkty IKT, ktoré môžu podliehať koordinovanému posúdeniu rizika uvedenému v odseku 1.	2. Komisia po konzultácii so skupinou pre spoluprácu a agentúrou ENISA ***a v prípade potreby príslušnými zainteresovanými stranami*** určí konkrétne kritické služby, systémy alebo produkty IKT ***a IKS***, ktoré môžu podliehať koordinovanému posúdeniu rizika uvedenému v odseku 1.

Pozmeňujúci návrh 194

Návrh smernice
Článok 20 – odsek 1

Text predložený Komisiou	*Pozmeňujúci návrh*
1. Členské štáty zabezpečia, aby kľúčové a dôležité subjekty bez zbytočného odkladu oznámili ***príslušným orgánom alebo*** jednotke CSIRT v súlade s odsekmi 3 a 4 každý incident ***so závažným vplyvom na poskytovanie ich služieb***. ***V prípade potreby tieto subjekty bez zbytočného odkladu oznámia príjemcom svojich služieb incidenty, ktoré by mohli nepriaznivo ovplyvniť ich poskytovanie.*** Členské štáty zabezpečia, aby tieto subjekty oznamovali okrem iného informácie umožňujúce ***príslušným orgánom alebo*** jednotke CSIRT určiť prípadný cezhraničný vplyv incidentu.	1. Členské štáty zabezpečia, aby kľúčové a dôležité subjekty bez zbytočného odkladu oznámili jednotke CSIRT v súlade s odsekmi 3 a 4 každý ***závažný*** incident. Členské štáty zabezpečia, aby tieto subjekty oznamovali okrem iného informácie umožňujúce jednotke CSIRT určiť prípadný cezhraničný vplyv incidentu.

Pozmeňujúci návrh 195

Návrh smernice
Článok 20 – odsek 2

Text predložený Komisiou	*Pozmeňujúci návrh*
2. ***Členské štáty zabezpečia, aby kľúčové a dôležité subjekty bez zbytočného odkladu oznámili príslušným orgánom alebo jednotke CSIRT každú závažnú kybernetickú hrozbu, ktorú tieto subjekty zistia a ktorá by mohla potenciálne viesť k závažnému incidentu.***	
Uvedené subjekty v príslušných prípadoch bez zbytočného odkladu ***oznámia príjemcom*** svojich služieb***, ktorých potenciálne zasiahla závažná kybernetická hrozba, všetky opatrenia alebo nápravné kroky***, ktoré ***títo*** príjemcovia ***môžu v reakcii na danú hrozbu*** prijať**.** Subjekty v ***prípade potreby týmto príjemcom oznámia aj informáciu*** o ***samotnej hrozbe. Oznámenie nesmie mať'*** pre oznamujúci subjekt za následok vyššiu zodpovednosť.	2. ***Členské štáty*** v príslušných prípadoch ***zabezpečia, aby kľúčové a dôležité subjekty*** bez zbytočného odkladu ***informovali príjemcov*** svojich služieb ***o ochranných opatreniach alebo nápravných krokoch proti konkrétnym incidentom a známym rizikám***, ktoré ***môžu*** príjemcovia prijať. Subjekty v ***príslušných prípadoch informujú príjemcov svojich služieb*** o ***samotnom incidente alebo známom riziku***. ***Informovanie príjemcov sa uskutočňuje s vynaložením***

maximálneho úsilia a nemá pre oznamujúci subjekt za následok vyššiu zodpovednosť.

Pozmeňujúci návrh 196

Návrh smernice
Článok 20 – odsek 3 – úvodná časť

Text predložený Komisiou	*Pozmeňujúci návrh*
3. ***Incident sa považuje za závažný, ak***:	3. ***S cieľom určiť závažnosť incidentu sa zohľadnia tieto parametre, ak sú k dispozícii***:

Pozmeňujúci návrh 197

Návrh smernice
Článok 20 – odsek 3 – písmeno a

Text predložený Komisiou	*Pozmeňujúci návrh*
a) ***dotknutému subjektu spôsobil alebo môže spôsobiť podstatné narušenie prevádzky alebo finančné straty;***	a) ***počet príjemcov služieb zasiahnutých incidentom;***

Pozmeňujúci návrh 198

Návrh smernice
Článok 20 – odsek 3 – písmeno b

Text predložený Komisiou	*Pozmeňujúci návrh*
b) ***zasiahol alebo môže zasiahnuť iné fyzické alebo právnické osoby spôsobením značných hmotných alebo nehmotných strát.***	b) ***dĺžka trvania incidentu;***

Pozmeňujúci návrh 199

Návrh smernice
Článok 20 – odsek 3 – písmeno b a (nové)

Text predložený Komisiou	*Pozmeňujúci návrh*
	ba) geografické rozloženie oblasti zasiahnutej incidentom;

Pozmeňujúci návrh 200

Návrh smernice
Článok 20 – odsek 3 – písmeno b b (nové)

Text predložený Komisiou	*Pozmeňujúci návrh*
	bb) rozsah, v akom incident zasiahol fungovanie a kontinuitu služby;

Pozmeňujúci návrh 201

Návrh smernice
Článok 20 – odsek 3 – písmeno b c (nové)

Text predložený Komisiou	*Pozmeňujúci návrh*
	bc) rozsah vplyvu incidentu na hospodárske a spoločenské činnosti.

Pozmeňujúci návrh 202

Návrh smernice
Článok 20 – odsek 4 – pododsek 1 – úvodná časť

Text predložený Komisiou	*Pozmeňujúci návrh*
Členské štáty zabezpečia, aby dotknuté subjekty na účely oznámenia podľa odseku 1 predložili ***príslušným orgánom alebo*** jednotke CSIRT:	Členské štáty zabezpečia, aby dotknuté subjekty na účely oznámenia podľa odseku 1 predložili jednotke CSIRT:

Pozmeňujúci návrh 203

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) prvotné oznámenie ***závažného incidentu, ktoré obsahuje informácie, ktoré má oznamujúci subjekt k dispozícii pri vynaložení maximálneho úsilia, takto:***

Pozmeňujúci návrh 204

Návrh smernice
Článok 20 – odsek 4 – pododsek 1 – písmeno a – bod i (nový)

Text predložený Komisiou	*Pozmeňujúci návrh*
	i) pokiaľ ide o incidenty, ktoré významne narúšajú dostupnosť služieb poskytovaných subjektom, jednotka CSIRT je informovaná bez zbytočného odkladu a v každom prípade do 24 hodín od zistenia incidentu;

Pozmeňujúci návrh 205

Návrh smernice
Článok 20 – odsek 4 – pododsek 1 – písmeno a – bod ii (nový)

Text predložený Komisiou	*Pozmeňujúci návrh*
	ii) pokiaľ ide o incidenty, ktoré majú iný významný vplyv na subjekt okrem vplyvu na dostupnosť služieb poskytovaných týmto subjektom, jednotka CSIRT je informovaná bez zbytočného odkladu a v každom prípade do 72 hodín od zistenia incidentu;

Pozmeňujúci návrh 206

Návrh smernice
Článok 20 – odsek 4 – pododsek 1 – písmeno a – bod iii (nový)

Text predložený Komisiou	*Pozmeňujúci návrh*
	iii) pokiaľ ide o incidenty, ktoré majú významný vplyv na služby poskytovateľa dôveryhodných služieb v zmysle článku 3 bodu 19 nariadenia (EÚ) č. 910/2014 alebo na osobné údaje uchovávané týmto poskytovateľom dôveryhodných služieb, jednotka CSIRT je informovaná bez zbytočného odkladu a v každom prípade do 24 hodín od zistenia incidentu;

Pozmeňujúci návrh 207

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

Text predložený Komisiou	*Pozmeňujúci návrh*
b) na žiadosť ***príslušného orgánu alebo*** jednotky CSIRT priebežnú správu o relevantných aktualizáciách daného stavu;	b) na žiadosť jednotky CSIRT priebežnú správu o relevantných aktualizáciách daného stavu;

Pozmeňujúci návrh 208

Návrh smernice
Článok 20 – odsek 4 – pododsek 1 – písmeno c – úvodná časť

Text predložený Komisiou	*Pozmeňujúci návrh*
c) najneskôr jeden mesiac po predložení oznámenia ***podľa písmena a) konečnú*** správu, ktorá obsahuje aspoň tieto informácie:	c) najneskôr jeden mesiac po predložení ***prvotného*** oznámenia ***komplexnú*** správu, ktorá obsahuje aspoň tieto informácie:

Pozmeňujúci návrh 209

Návrh smernice
Článok 20 – odsek 4 – pododsek 1 – písmeno c a (nové)

Text predložený Komisiou	*Pozmeňujúci návrh*
	ca) v prípade, že v čase predloženia komplexnej správy uvedenej v písmene c) incident stále prebieha, predloží sa záverečná správa jeden mesiac po vyriešení incidentu.

Pozmeňujúci návrh 210

Návrh smernice
Článok 20 – odsek 4 – pododsek 2

Text predložený Komisiou	*Pozmeňujúci návrh*
Členské štáty zabezpečia, aby sa v riadne odôvodnených prípadoch a po dohode s ***príslušnými orgánmi alebo*** jednotkou CSIRT mohol príslušný subjekt odchýliť od lehôt stanovených v ***písmenách*** a) a c).	Členské štáty zabezpečia, aby sa v riadne odôvodnených prípadoch a po dohode s jednotkou CSIRT mohol príslušný subjekt odchýliť od lehôt stanovených v ***písmene*** a) ***bode i) a ii)*** a ***v písmene*** c). ***Členské štáty zabezpečia dôvernosť a primeranú ochranu citlivých informácií o incidentoch, ktoré sa vymieňajú s jednotkami CSIRT, a prijmú opatrenia a postupy na výmenu a opakované použitie***

informácií o incidentoch.

Pozmeňujúci návrh 211

Návrh smernice
Článok 20 – odsek 4 a (nový)

Text predložený Komisiou	*Pozmeňujúci návrh*
	4a. Členské štáty zriadia jednotné kontaktné miesto pre všetky oznámenia požadované podľa tejto smernice a ďalších relevantných právnych predpisov Únie. Agentúra ENISA v spolupráci so skupinou pre spoluprácu vypracúva a neustále zlepšuje spoločné vzorové formuláre oznámení prostredníctvom usmernení na zjednodušenie a zefektívnenie oznamovania informácií požadovaných v právnych predpisoch Únie a na zníženie záťaže pre oznamujúce subjekty.

Pozmeňujúci návrh 212

Návrh smernice
Článok 20 – odsek 4 b (nový)

Text predložený Komisiou	*Pozmeňujúci návrh*
	4b. Kľúčové a dôležité subjekty uvedené v článku 24 ods. 1 môžu spĺňať požiadavky odseku 1 tohto článku tým, že informujú jednotku CSIRT členského štátu, v ktorom majú subjekty hlavné miesto podnikateľskej činnosti v Únii, a tým, že informujú kľúčové a dôležité subjekty, ktorým poskytujú služby, o každom závažnom incidente, o ktorom je známe, že má vplyv na príjemcu služieb.

Pozmeňujúci návrh 213

Návrh smernice
Článok 20 – odsek 5

Text predložený Komisiou	*Pozmeňujúci návrh*
5. ***Príslušné vnútroštátne orgány alebo***	5. Jednotka CSIRT ***poskytne***

jednotka CSIRT ***poskytnú*** oznamujúcemu subjektu do 24 hodín od prijatia prvotného oznámenia uvedeného v odseku 4 písm. a) odpoveď vrátane počiatočnej spätnej väzby k incidentu a na žiadosť subjektu usmernenia k vykonávaniu možných zmierňujúcich opatrení. ***Ak jednotka CSIRT nedostala oznámenie uvedené v odseku 1, usmernenie poskytne príslušný orgán v spolupráci s jednotkou CSIRT.*** Jednotka CSIRT poskytne doplňujúcu technickú podporu, ak o to príslušný subjekt požiada. Ak existuje podozrenie, že incident má trestnoprávnu povahu, ***príslušné vnútroštátne orgány alebo*** jednotka CSIRT ***poskytnú*** aj usmernenia týkajúce sa oznamovania incidentu orgánom presadzovania práva.

oznamujúcemu subjektu do 24 hodín od prijatia prvotného oznámenia uvedeného v odseku 4 písm. a) odpoveď vrátane počiatočnej spätnej väzby k incidentu a na žiadosť subjektu usmernenia ***a využiteľné poradenstvo*** k vykonávaniu možných zmierňujúcich opatrení. Jednotka CSIRT poskytne doplňujúcu technickú podporu, ak o to príslušný subjekt požiada. Ak existuje podozrenie, že incident má trestnoprávnu povahu, jednotka CSIRT ***poskytne*** aj usmernenia týkajúce sa oznamovania incidentu orgánom presadzovania práva. ***Jednotka CSIRT si môže informácie o incidente vymieňať s inými kľúčovými a dôležitými subjektmi, pričom zabezpečí dôvernosť informácií poskytnutých oznamujúcim subjektom.***

Pozmeňujúci návrh 214

Návrh smernice
Článok 20 – odsek 6

Text predložený Komisiou	*Pozmeňujúci návrh*
6. V prípade potreby, a najmä ak sa incident uvedený v odseku 1 týka dvoch alebo viacerých členských štátov, ***príslušný orgán alebo*** jednotka CSIRT informuje o incidente ostatné zasiahnuté členské štáty a agentúru ENISA. ***Príslušné orgány,*** jednotky CSIRT a jednotné kontaktné miesta pri tom v súlade s právom Únie alebo vnútroštátnymi právnymi predpismi, ktoré sú v súlade s právom Únie, chránia bezpečnosť a obchodné záujmy subjektu, ako aj dôvernosť poskytnutých informácií.	6. V prípade potreby, a najmä ak sa incident uvedený v odseku 1 týka dvoch alebo viacerých členských štátov, jednotka CSIRT informuje o incidente ostatné zasiahnuté členské štáty a agentúru ENISA ***a poskytne relevantné informácie***. Jednotky CSIRT a jednotné kontaktné miesta pri tom v súlade s právom Únie alebo vnútroštátnymi právnymi predpismi, ktoré sú v súlade s právom Únie, chránia bezpečnosť a obchodné záujmy subjektu, ako aj dôvernosť poskytnutých informácií.

Pozmeňujúci návrh 215

Návrh smernice
Článok 20 – odsek 7

Text predložený Komisiou	*Pozmeňujúci návrh*
7. Po porade s dotknutým subjektom môže ***príslušný orgán alebo*** jednotka CSIRT a prípadne ***orgány alebo*** jednotky	7. Po porade s dotknutým subjektom môže jednotka CSIRT a prípadne jednotky CSIRT ďalších dotknutých členských

CSIRT ďalších dotknutých členských štátov informovať o incidente verejnosť alebo požiadať o to daný subjekt, ak je informovanosť verejnosti potrebná na zabránenie incidentu alebo riešenie prebiehajúceho incidentu alebo ak je zverejnenie incidentu vo verejnom záujme z iného dôvodu.

štátov informovať o incidente verejnosť alebo požiadať o to daný subjekt, ak je informovanosť verejnosti potrebná na zabránenie incidentu alebo riešenie prebiehajúceho incidentu alebo ak je zverejnenie incidentu vo verejnom záujme z iného dôvodu.

Pozmeňujúci návrh 216

Návrh smernice
Článok 20 – odsek 7 a (nový)

Text predložený Komisiou	*Pozmeňujúci návrh*
	7a. Jednotky CSIRT bez zbytočného odkladu poskytnú jednotnému kontaktnému miestu a v relevantných prípadoch príslušným orgánom informácie o závažných incidentoch oznámených v súlade s odsekom 1.

Pozmeňujúci návrh 217

Návrh smernice
Článok 20 – odsek 8

Text predložený Komisiou	*Pozmeňujúci návrh*
8. Na žiadosť ***príslušného orgánu alebo*** jednotky CSIRT jednotné kontaktné miesto postúpi doručené oznámenia podľa ***odsekov 1 a 2*** jednotným kontaktným miestam ostatných zasiahnutých členských štátov.	8. Na žiadosť jednotky CSIRT jednotné kontaktné miesto postúpi doručené oznámenia podľa ***odseku 1*** jednotným kontaktným miestam ostatných zasiahnutých členských štátov***, pričom zabezpečí dôvernosť a primeranú ochranu informácií poskytnutých oznamujúcim subjektom***.

Pozmeňujúci návrh 218

Návrh smernice
Článok 20 – odsek 9

Text predložený Komisiou	*Pozmeňujúci návrh*
9. Jednotné kontaktné miesto predkladá agentúre ENISA každý mesiac súhrnnú správu s anonymizovanými a	9. Jednotné kontaktné miesto predkladá agentúre ENISA každý mesiac súhrnnú správu s anonymizovanými

agregovanými údajmi o incidentoch, závažných kybernetických hrozbách a udalostiach odvrátených v poslednej chvíli oznámených v súlade s ***odsekmi 1 a 2 a v súlade s*** článkom 27. S cieľom prispieť k poskytovaniu porovnateľných informácií môže agentúra ENISA vydať technické usmernenia týkajúce sa parametrov informácií uvedených v súhrnnej správe.

a agregovanými údajmi o incidentoch, závažných kybernetických hrozbách a udalostiach odvrátených v poslednej chvíli oznámených v súlade s ***odsekom 1 tohto článku a*** článkom 27. S cieľom prispieť k poskytovaniu porovnateľných informácií môže agentúra ENISA vydať technické usmernenia týkajúce sa parametrov informácií uvedených v súhrnnej správe.

Pozmeňujúci návrh 219

Návrh smernice
Článok 20 – odsek 10

Text predložený Komisiou	*Pozmeňujúci návrh*
10. Príslušné orgány poskytnú príslušným orgánom určeným podľa smernice (EÚ) XXXX/XXXX [smernica o odolnosti kritických subjektov] informácie o incidentoch a kybernetických hrozbách, ktoré v súlade s ***odsekmi 1 a 2*** oznámili kľúčové subjekty identifikované ako kritické subjekty alebo ako subjekty rovnocenné s kritickými subjektmi podľa smernice (EÚ) XXXX/XXXX [smernica o odolnosti kritických subjektov].	10. Príslušné orgány poskytnú príslušným orgánom určeným podľa smernice (EÚ) XXXX/XXXX [smernica o odolnosti kritických subjektov] informácie o incidentoch a kybernetických hrozbách, ktoré v súlade s ***odsekom 1 tohto článku a článkom 27*** oznámili kľúčové subjekty identifikované ako kritické subjekty alebo ako subjekty rovnocenné s kritickými subjektmi podľa smernice (EÚ) XXXX/XXXX [smernica o odolnosti kritických subjektov].

Pozmeňujúci návrh 220

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	11. Komisia môže prijať vykonávacie akty, v ktorých bližšie určí postup oznámenia predkladaného podľa ***odseku 1 tohto článku a článku 27***. Uvedené vykonávacie akty sa prijmú v súlade s postupom preskúmania, na ktorý sa odkazuje v článku 37 ods. 2.

odkazuje v článku 37 ods. 2.

Pozmeňujúci návrh 221

Návrh smernice
Článok 20 – odsek 11 a (nový)

Text predložený Komisiou	*Pozmeňujúci návrh*
	11a. Komisia je splnomocnená prijímať delegované akty v súlade s článkom 36 s cieľom doplniť túto smernicu určením druhu informácií, ktoré sa majú predkladať podľa odseku 1 tohto článku, a podrobnejším vymedzením parametrov, ktoré sa majú zohľadniť pri určovaní závažnosti incidentu, ako sa uvádza v odseku 3 tohto článku.

Pozmeňujúci návrh 222

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. Členské štáty ***na základe usmernení agentúry ENISA, Komisie a skupiny pre spoluprácu nabádajú*** kľúčové a dôležité subjekty***, aby*** certifikovali určité produkty IKT, služby IKT a procesy IKT ***vytvorené kľúčovým alebo dôležitým subjektom alebo obstarané od tretích strán*** v rámci európskych systémov kybernetickej bezpečnosti prijatých podľa článku 49 nariadenia (EÚ) 2019/881 ***alebo, ak ešte nie sú k dispozícii, v rámci podobných medzinárodne uznávaných systémov certifikácie***. ***Členské štáty navyše nabádajú kľúčové a dôležité subjekty, aby využívali kvalifikované dôveryhodné služby podľa nariadenia (EÚ) č. 910/2014.***

Pozmeňujúci návrh 223

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 podľa ***odseku 1***. Delegované akty ***sa prijímajú v súlade s článkom 36***.	2. Komisia je splnomocnená prijímať delegované akty ***v súlade s článkom 36 s cieľom doplniť túto smernicu tým, že*** bližšie určí, od ktorých kategórií kľúčových ***a dôležitých*** subjektov sa vyžaduje získanie certifikátu v rámci konkrétnych európskych systémov kybernetickej bezpečnosti podľa ***článku 49 nariadenia (EÚ) 2019/881***. ***Takéto*** delegované akty ***sa zvážia v prípade, že sa zistí nedostatočná úroveň kybernetickej bezpečnosti, pričom im bude predchádzať posúdenie vplyvu a stanoví sa v nich obdobie vykonávania.***

Pozmeňujúci návrh 224

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. Komisia môže ***po konzultácii so skupinou pre spoluprácu a európskou skupinou pre certifikáciu kybernetickej bezpečnosti*** 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.

Pozmeňujúci návrh 225

Návrh smernice
Článok 22 – odsek 2

Text predložený Komisiou	*Pozmeňujúci návrh*
2. Agentúra ENISA v spolupráci s členskými štátmi vypracúva odporúčania a usmernenia týkajúce sa technických oblastí, ktoré sa majú zvážiť v súvislosti s odsekom 1, ako aj odporúčania a usmernenia týkajúce sa už existujúcich noriem vrátane vnútroštátnych noriem	2. Agentúra ENISA v spolupráci s členskými štátmi ***a v prípade potreby po konzultácii s príslušnými zainteresovanými stranami*** vypracúva odporúčania a usmernenia týkajúce sa technických oblastí, ktoré sa majú zvážiť v súvislosti s odsekom 1, ako aj

členských štátov, ktoré by sa mohli vzťahovať na uvedené oblasti.

odporúčania a usmernenia týkajúce sa už existujúcich noriem vrátane vnútroštátnych noriem členských štátov, ktoré by sa mohli vzťahovať na uvedené oblasti.

Pozmeňujúci návrh 226

Návrh smernice
Článok 22 – odsek 2 a (nový)

Text predložený Komisiou	*Pozmeňujúci návrh*
	2a. Komisia v spolupráci s agentúrou ENISA podporuje a presadzuje vypracovanie a vykonávanie noriem, ktoré stanovia príslušné orgány Únie a medzinárodné normalizačné organizácie na harmonizované vykonávanie článku 18 ods. 1 a 2. Komisia podporuje aktualizáciu noriem s ohľadom na technologický vývoj.

Pozmeňujúci návrh 227

Návrh smernice
Článok 23 – nadpis

Text predložený Komisiou	*Pozmeňujúci návrh*
Databázy doménových mien a registračných údajov	***Databázová štruktúra*** doménových mien a registračných údajov

Pozmeňujúci návrh 228

Návrh smernice
Článok 23 – odsek 1

Text predložený Komisiou	*Pozmeňujúci návrh*
1. S cieľom prispieť k bezpečnosti, stabilite a odolnosti DNS členské štáty ***zabezpečia***, aby správcovia TLD a subjekty poskytujúce služby registrácie doménových mien ***pre TLD*** zbierali a uchovávali presné a úplné registračné údaje o doménových menách ***vo vyhradenom databázovom zariadení s náležitou starostlivosťou, na ktoré sa vzťahujú právne predpisy Únie o ochrane údajov,***	1. S cieľom prispieť k bezpečnosti, stabilite a odolnosti DNS členské štáty ***vyžadujú***, aby správcovia TLD a subjekty poskytujúce služby registrácie doménových mien zbierali a uchovávali presné***, overené*** a úplné registračné údaje o doménových menách ***v databázovej štruktúre prevádzkovanej na tento účel***.

pokiaľ ide o údaje, ktoré sú osobnými údajmi.

Pozmeňujúci návrh 229

Návrh smernice
Článok 23 – odsek 2

Text predložený Komisiou	*Pozmeňujúci návrh*
2. Členské štáty zabezpečia, aby ***databázy*** s registračnými údajmi o doménových menách ***uvedené*** v odseku 1 ***obsahovali*** relevantné informácie na identifikáciu a kontaktovanie držiteľov doménových mien a kontaktných miest spravujúcich doménové mená v rámci TLD.	2. Členské štáty zabezpečia, aby ***databázová štruktúra*** s registračnými údajmi o doménových menách ***uvedená*** v odseku 1 ***obsahovala*** relevantné informácie***, ktoré zahŕňajú aspoň mená držiteľov domén, ich fyzické a e-mailové adresy, ako aj telefónne čísla,*** na identifikáciu a kontaktovanie držiteľov doménových mien a kontaktných miest spravujúcich doménové mená v rámci TLD.

Pozmeňujúci návrh 230

Návrh smernice
Článok 23 – odsek 3

Text predložený Komisiou	*Pozmeňujúci návrh*
3. Členské štáty zabezpečia, aby správcovia TLD a subjekty poskytujúce služby registrácie doménových mien ***pre TLD*** mali zavedené politiky a postupy s cieľom zabezpečiť, aby ***databázy obsahovali*** presné a úplné informácie. Členské štáty zabezpečia, aby takéto politiky a postupy boli verejne dostupné.	3. Členské štáty zabezpečia, aby správcovia TLD a subjekty poskytujúce služby registrácie doménových mien mali zavedené politiky a postupy s cieľom zabezpečiť, aby ***databázová štruktúra obsahovala*** presné***, overené*** a úplné informácie. Členské štáty zabezpečia, aby takéto politiky a postupy boli verejne dostupné.

Pozmeňujúci návrh 231

Návrh smernice
Článok 23 – odsek 4

Text predložený Komisiou	*Pozmeňujúci návrh*
4. Členské štáty zabezpečia, aby správcovia TLD a subjekty poskytujúce služby registrácie doménových mien ***pre***	4. Členské štáty zabezpečia, aby správcovia TLD a subjekty poskytujúce služby registrácie doménových mien bez

TLD bez zbytočného odkladu po registrácii mena domény ***uverejnili*** registračné údaje domény, ktoré nie sú osobnými údajmi.	zbytočného odkladu po registrácii mena domény ***zverejnili*** registračné údaje domény, ktoré nie sú osobnými údajmi. ***V prípade právnických osôb ako držiteľov domén zahŕňajú verejne dostupné registračné údaje domény aspoň meno držiteľa domény, jeho fyzickú a e-mailovú adresu, ako aj telefónne číslo.***

Pozmeňujúci návrh 232

Návrh smernice
Článok 23 – odsek 5

Text predložený Komisiou	*Pozmeňujúci návrh*
5. Členské štáty ***zabezpečia***, aby registre TLD a subjekty poskytujúce služby registrácie doménových mien ***pre TLD*** poskytovali prístup k špecifickým registračným údajom o doménových menách na základe ***zákonných a*** riadne odôvodnených žiadostí oprávnených záujemcov o prístup v súlade s právnymi predpismi Únie o ochrane údajov. Členské štáty ***zabezpečia***, aby správcovia TLD a subjekty poskytujúce služby registrácie doménových mien ***pre TLD*** odpovedali bez zbytočného odkladu ***na všetky žiadosti*** o prístup. Členské štáty zabezpečia, aby politiky a postupy zverejňovania takýchto údajov boli verejne dostupné. Oddiel II Jurisdikcia a registrácia Článok 24 Jurisdikcia a teritorialita	5. Členské štáty ***vyžadujú***, aby registre TLD a subjekty poskytujúce služby registrácie doménových mien poskytovali prístup k špecifickým registračným údajom o doménových menách ***vrátane osobných údajov*** na základe riadne odôvodnených žiadostí oprávnených záujemcov o prístup v súlade s právnymi predpismi Únie o ochrane údajov. Členské štáty ***vyžadujú***, aby správcovia TLD a subjekty poskytujúce služby registrácie doménových mien odpovedali bez zbytočného odkladu ***a v každom prípade do 72 hodín od prijatia žiadostí*** o prístup. Členské štáty zabezpečia, aby politiky a postupy zverejňovania takýchto údajov boli verejne dostupné. Oddiel II Jurisdikcia a registrácia Článok 24 Jurisdikcia a teritorialita

Pozmeňujúci návrh 233

Návrh smernice
Článok 24 – odsek 2

Text predložený Komisiou	*Pozmeňujúci návrh*
2. Na účely tejto smernice sa predpokladá, že subjekty uvedené v odseku 1 majú hlavné miesto podnikateľskej činnosti v Únii v členskom štáte, v ktorom sa prijímajú rozhodnutia týkajúce sa opatrení na riadenie	2. Na účely tejto smernice sa predpokladá, že subjekty uvedené v odseku 1 majú hlavné miesto podnikateľskej činnosti v Únii v členskom štáte, v ktorom sa prijímajú rozhodnutia týkajúce sa opatrení na riadenie

kybernetickobezpečnostných rizík. Ak sa takéto rozhodnutia neprijímajú v žiadnom mieste podnikateľskej činnosti v Únii, predpokladá sa, že hlavné miesto podnikateľskej činnosti je v členskom štáte, v ktorom majú subjekty miesto podnikateľskej činnosti s najvyšším počtom zamestnancov v Únii.	kybernetickobezpečnostných rizík. Ak sa takéto rozhodnutia neprijímajú v žiadnom mieste podnikateľskej činnosti v Únii, predpokladá sa, že hlavné miesto podnikateľskej činnosti je v členskom štáte, v ktorom majú subjekty ***buď*** miesto podnikateľskej činnosti s najvyšším počtom zamestnancov v Únii***, alebo miesto podnikateľskej činnosti, kde sa vykonávajú kybernetickobezpečnostné operácie***.

Pozmeňujúci návrh 234

Návrh smernice
Článok 25 – nadpis

Text predložený Komisiou	*Pozmeňujúci návrh*
Register ***kľúčových a dôležitých subjektov***	Register ***agentúry ENISA***

Pozmeňujúci návrh 235

Návrh smernice
Článok 25 – odsek 1 – úvodná časť

Text predložený Komisiou	*Pozmeňujúci návrh*
1. Agentúra ENISA vytvorí a vedie register kľúčových a dôležitých subjektov uvedených v článku 24 ods. 1. ***Subjekty predložia agentúre ENISA najneskôr [12 mesiacov od nadobudnutia účinnosti tejto smernice]*** tieto informácie:	1. Agentúra ENISA vytvorí a vedie ***zabezpečený*** register kľúčových a dôležitých subjektov uvedených v článku 24 ods. 1***, ktorý obsahuje*** tieto informácie:

Pozmeňujúci návrh 236

Návrh smernice
Článok 25 – odsek 1 – písmeno c

Text predložený Komisiou	*Pozmeňujúci návrh*
c) aktuálne kontaktné údaje vrátane e-mailových adries ***a*** telefónnych čísel subjektov.	c) aktuálne kontaktné údaje vrátane e-mailových adries***, rozsahov IP adries,*** telefónnych čísel ***a príslušných odvetví a pododvetví*** subjektov ***uvedených v prílohách I a II***.

Pozmeňujúci návrh 237

Návrh smernice
Článok 25 – odsek 1 – pododsek 1 a (nový)

Text predložený Komisiou	*Pozmeňujúci návrh*
	Do ... [12 mesiacov od dátumu nadobudnutia účinnosti tejto smernice] predložia kľúčové a dôležité subjekty agentúre ENISA informácie uvedené v prvom pododseku.

Pozmeňujúci návrh 238

Návrh smernice
Článok 26 – odsek 1 – úvodná časť

Text predložený Komisiou	*Pozmeňujúci návrh*
1. ***Bez toho, aby bolo dotknuté nariadenie (EÚ) 2016/679,*** členské štáty zabezpečia, aby si kľúčové a dôležité subjekty mohli medzi sebou vymieňať relevantné informácie o kybernetickej bezpečnosti vrátane informácií o kybernetických hrozbách, zraniteľnostiach, ***ukazovateľoch kompromitácie, taktikách***, technikách a postupoch, kybernetickobezpečnostných varovaniach ***a konfiguračných nástrojoch***, ak takáto výmena informácií:	1. Členské štáty zabezpečia, aby si kľúčové a dôležité subjekty ***a ďalšie príslušné subjekty, ktoré nepatria do rozsahu pôsobnosti tejto smernice,*** mohli medzi sebou vymieňať relevantné informácie o kybernetickej bezpečnosti vrátane informácií o kybernetických hrozbách, ***udalostiach odvrátených v poslednej chvíli,*** zraniteľnostiach, technikách a postupoch, ***metaúdajoch a obsahových údajoch, ukazovateľoch kompromitácie, protichodných taktikách, modoch operandi, informáciách špecifických pre jednotlivých aktérov,*** kybernetickobezpečnostných varovaniach***, taktikách priemyselnej špionáže a odporúčaných konfiguráciách bezpečnostných nástrojov***, ak takáto výmena informácií:

Pozmeňujúci návrh 239

Návrh smernice
Článok 26 – odsek 1 – písmeno b

Text predložený Komisiou	*Pozmeňujúci návrh*
b) zvyšuje úroveň kybernetickej bezpečnosti, najmä zvyšovaním povedomia	b) zvyšuje úroveň kybernetickej bezpečnosti, najmä zvyšovaním povedomia

o kybernetických hrozbách, obmedzovaním alebo zabraňovaním možnosti šírenia takýchto hrozieb, podporou celej škály obranných kapacít, zverejňovaním informácií o zraniteľnosti a jej nápravou, technikami odhaľovania hrozieb, stratégiami zmierňovania, alebo fázami reakcie a obnovy.	o kybernetických hrozbách, obmedzovaním alebo zabraňovaním možnosti šírenia takýchto hrozieb, podporou celej škály obranných kapacít, zverejňovaním informácií o zraniteľnosti a jej nápravou, technikami odhaľovania***, zamedzovania šírenia a prevencie*** hrozieb, stratégiami zmierňovania, alebo fázami reakcie a obnovy***, resp. podporou spoločného výskumu kybernetických hrozieb medzi verejnými a súkromnými subjektmi***.

Pozmeňujúci návrh 240

Návrh smernice
Článok 26 – odsek 2

Text predložený Komisiou	*Pozmeňujúci návrh*
2. Členské štáty ***zabezpečia, aby sa výmena*** informácií ***uskutočňovala v rámci*** dôveryhodných komunít kľúčových a dôležitých subjektov. Takáto výmena sa uskutočňuje prostredníctvom mechanizmov spoločného využívania informácií vzhľadom na potenciálne citlivú povahu vymieňaných informácií ***a v súlade s pravidlami práva Únie uvedenými v odseku 1***.	2. Členské štáty ***uľahčia výmenu*** informácií ***tým, že umožnia vytvorenie*** dôveryhodných komunít kľúčových a dôležitých subjektov ***a ich poskytovateľov služieb alebo v relevantných prípadoch iných dodávateľov***. Takáto výmena sa uskutočňuje prostredníctvom mechanizmov spoločného využívania informácií vzhľadom na potenciálne citlivú povahu vymieňaných informácií.

Pozmeňujúci návrh 241

Návrh smernice
Článok 26 – odsek 3

Text predložený Komisiou	*Pozmeňujúci návrh*
3. Členské štáty ***stanovia pravidlá, v ktorých sa konkretizuje postup,*** operačné prvky (vrátane využívania špecializovaných platforiem IKT), obsah ***a podmienky dohôd o výmene informácií uvedených v odseku 2***. ***V týchto pravidlách sa*** stanovia ***aj*** podrobnosti o zapojení orgánov verejnej moci do takýchto dohôd***, ako aj operačné prvky vrátane využívania špecializovaných IT platforiem***. Členské štáty poskytnú pri	3. Členské štáty ***uľahčia vytvorenie mechanizmov spoločného využívania informácií o kybernetickej bezpečnosti uvedených v odseku 2 tým, že sprístupnia*** operačné prvky (vrátane využívania špecializovaných platforiem IKT ***a nástrojov na automatizáciu***) ***a*** obsah. ***Členské štáty*** stanovia podrobnosti o zapojení orgánov verejnej moci do takýchto dohôd ***a môžu stanoviť určité podmienky, pokiaľ ide o informácie, ktoré***

uplatňovaní takýchto opatrení podporu v súlade so svojimi politikami uvedenými v článku 5 ods. 2 písm. g).	***sprístupnili príslušné orgány alebo jednotky CSIRT***. Členské štáty poskytnú pri uplatňovaní takýchto opatrení podporu v súlade so svojimi politikami uvedenými v článku 5 ods. 2 písm. g).

Pozmeňujúci návrh 242

Návrh smernice
Článok 27 – odsek 1

Text predložený Komisiou	*Pozmeňujúci návrh*
Členské štáty zabezpečia, aby ***subjekty, ktoré nepatria do rozsahu pôsobnosti tejto smernice,*** mohli dobrovoľne podávať ***oznámenia o závažných incidentoch, kybernetických hrozbách alebo udalostiach odvrátených v poslednej chvíli, a to bez toho, aby bol dotknutý článok 3***. ***Členské štáty pri spracúvaní oznámení konajú v súlade s postupom stanoveným v článku 20. Členské štáty môžu uprednostniť spracúvanie povinných oznámení pred dobrovoľnými oznámeniami. V dôsledku dobrovoľného oznámenia nevznikajú oznamujúcemu subjektu žiadne ďalšie povinnosti, ktoré by sa naň neboli vzťahovali, ak by oznámenie nepodal.***	Členské štáty zabezpečia, aby ***jednotke CSIRT*** mohli ***oznámenia*** dobrovoľne podávať:

Pozmeňujúci návrh 243

Návrh smernice
Článok 27 – odsek 1 – písmeno a (nové)

Text predložený Komisiou	*Pozmeňujúci návrh*
	a) kľúčové a dôležité subjekty v súvislosti s kybernetickými hrozbami a udalosťami odvrátenými v poslednej chvíli;

Pozmeňujúci návrh 244

Návrh smernice
Článok 27 – odsek 1 – písmeno b (nové)

Text predložený Komisiou	*Pozmeňujúci návrh*
	b) subjekty, ktoré nepatria do rozsahu pôsobnosti tejto smernice, v súvislosti so závažnými incidentmi, kybernetickými hrozbami alebo udalosťami odvrátenými v poslednej chvíli;

Pozmeňujúci návrh 245

Návrh smernice
Článok 27 – odsek 1 – pododsek 1 a (nový)

Text predložený Komisiou	*Pozmeňujúci návrh*
	Členské štáty pri spracúvaní takýchto oznámení konajú v súlade s postupom stanoveným v článku 20. Členské štáty môžu uprednostniť spracúvanie povinných oznámení pred dobrovoľnými oznámeniami. Jednotky CSIRT v prípade potreby poskytnú jednotnému kontaktnému miestu a v relevantných prípadoch príslušným orgánom informácie o oznámeniach doručených podľa tohto článku, pričom zabezpečia dôvernosť a primeranú ochranu informácií poskytnutých oznamujúcim subjektom. V dôsledku dobrovoľného oznámenia nevznikajú oznamujúcemu subjektu žiadne ďalšie povinnosti, ktoré by sa naň neboli vzťahovali, ak by oznámenie nepodal.

Pozmeňujúci návrh 246

Návrh smernice
Článok 28 – odsek 2

Text predložený Komisiou	*Pozmeňujúci návrh*
2. Príslušné orgány pri riešení incidentov, ktoré majú za následok porušenie ochrany osobných údajov, úzko spolupracujú s orgánmi na ochranu údajov.	2. Príslušné orgány pri riešení incidentov, ktoré majú za následok porušenie ochrany osobných údajov, úzko spolupracujú s orgánmi na ochranu údajov. ***Uskutočňuje sa to v súlade s ich právomocami a úlohami podľa nariadenia (EÚ) 2016/679.***

Pozmeňujúci návrh 247

Návrh smernice
Článok 29 – odsek 2 – písmeno a

Text predložený Komisiou	*Pozmeňujúci návrh*
a) kontrolám na mieste a dohľadu na diaľku vrátane náhodných kontrol;	a) kontrolám na mieste a dohľadu na diaľku vrátane náhodných kontrol***, ktoré vykonávajú vyškolení odborníci***;

Pozmeňujúci návrh 248

Návrh smernice
Článok 29 – odsek 2 – písmeno a a (nové)

Text predložený Komisiou	*Pozmeňujúci návrh*
	aa) vyšetreniu prípadov nedodržania povinností a súvisiacich účinkov na bezpečnosť služieb;

Pozmeňujúci návrh 249

Návrh smernice
Článok 29 – odsek 2 – písmeno b

Text predložený Komisiou	*Pozmeňujúci návrh*
b) ***pravidelným*** auditom;	b) ***ročným a cieleným bezpečnostným*** auditom ***vykonávaným kvalifikovaným nezávislým orgánom alebo príslušným orgánom***;

Pozmeňujúci návrh 250

Návrh smernice
Článok 29 – odsek 2 – písmeno c

Text predložený Komisiou	*Pozmeňujúci návrh*
c) ***cieleným bezpečnostným*** auditom ***založeným na posúdeniach rizika alebo dostupných informáciách súvisiacich s rizikom***;	c) auditom ***ad hoc v prípadoch odôvodnených závažným incidentom alebo nedodržaním povinností zo strany kľúčového subjektu***;

Pozmeňujúci návrh 251

Návrh smernice
Článok 29 – odsek 2 – pododseky 1 a a 1 b (nové)

Text predložený Komisiou	*Pozmeňujúci návrh*
	Cielené bezpečnostné audity uvedené v prvom pododseku písm. b) sú založené na posúdeniach rizika, ktoré vykonal príslušný orgán alebo auditovaný subjekt, alebo na iných dostupných informáciách týkajúcich sa rizík.
	Výsledky každého cieleného bezpečnostného auditu sa sprístupnia príslušnému orgánu. Náklady na takýto cielený bezpečnostný audit, ktorý vykonáva kvalifikovaný nezávislý orgán, hradí dotknutý subjekt.

Pozmeňujúci návrh 252

Návrh smernice
Článok 29 – odsek 2 a (nový)

Text predložený Komisiou	*Pozmeňujúci návrh*
	2a. Pri výkone svojich právomocí podľa odseku 2 písm. a) až d) príslušné orgány minimalizujú vplyv na obchodné procesy subjektu.

Pozmeňujúci návrh 253

Návrh smernice
Článok 29 – odsek 4 – písmeno b

Text predložený Komisiou	*Pozmeňujúci návrh*
b) vydávať záväzné pokyny alebo príkazy, ktorými sa od týchto subjektov vyžaduje napraviť zistené nedostatky alebo porušenia povinností stanovených v tejto smernici;	b) vydávať záväzné pokyny, ***a to aj v súvislosti s opatreniami potrebnými na prevenciu alebo nápravu incidentu, ako aj lehotami na vykonávanie takýchto opatrení a podávanie správ o ich vykonávaní,*** alebo príkazy, ktorými sa od týchto subjektov vyžaduje napraviť zistené nedostatky alebo porušenia povinností stanovených v tejto smernici;

Pozmeňujúci návrh 254

Návrh smernice
Článok 29 – odsek 4 – bod i

Text predložený Komisiou	*Pozmeňujúci návrh*
i) vydať verejné vyhlásenie, v ktorom sa uvedie právnická a fyzická osoba alebo osoby zodpovedné za porušenie povinnosti stanovenej v tejto smernici a povaha tohto porušenia;	***vypúšťa sa***

Pozmeňujúci návrh 255

Návrh smernice
Článok 29 – odsek 4 – písmeno j

Text predložený Komisiou	*Pozmeňujúci návrh*
j) uložiť správnu sankciu alebo požiadať o jej uloženie podľa článku 31 príslušné orgány alebo súdy ***podľa vnútroštátnych zákonov***, a to popri opatreniach uvedených v písmenách a) až i) tohto odseku ***alebo namiesto týchto opatrení,*** v závislosti od okolností každého jednotlivého prípadu.	j) uložiť správnu sankciu alebo požiadať o jej uloženie podľa článku 31 príslušné orgány alebo súdy ***v súlade s vnútroštátnym právom***, a to popri opatreniach uvedených v písmenách a) až i) tohto odseku v závislosti od okolností každého jednotlivého prípadu.

Pozmeňujúci návrh 256

Návrh smernice
Článok 29 – odsek 5 – pododsek 1 – písmeno a

Text predložený Komisiou	*Pozmeňujúci návrh*
a) pozastaviť certifikáciu alebo povoľovanie alebo požiadať certifikačný alebo povoľujúci subjekt, aby pozastavil certifikáciu alebo povoľovanie týkajúce sa časti alebo všetkých služieb alebo činností, ktoré poskytuje kľúčový subjekt;	a) ***dočasne*** pozastaviť certifikáciu alebo povoľovanie alebo požiadať certifikačný alebo povoľujúci subjekt, aby ***dočasne*** pozastavil certifikáciu alebo povoľovanie týkajúce sa časti alebo všetkých ***relevantných*** služieb alebo činností, ktoré poskytuje kľúčový subjekt;

Pozmeňujúci návrh 257

Návrh smernice
Článok 29 – odsek 5 – pododsek 1 – písmeno b

Text predložený Komisiou	*Pozmeňujúci návrh*
b) ***uložiť dočasný zákaz alebo*** od príslušných orgánov alebo súdov ***podľa vnútroštátnych zákonov*** požadovať uloženie dočasného zákazu vykonávať riadiace funkcie v tomto kľúčovom subjekte, a to každej osobe vykonávajúcej riadiace úlohy na úrovni výkonného riaditeľa alebo právneho zástupcu v tomto kľúčovom subjekte ***a akejkoľvek inej fyzickej osobe zodpovednej za porušenie***.	b) ***ako ultima ratio*** od príslušných orgánov alebo súdov ***v súlade s vnútroštátnym právom*** požadovať uloženie dočasného zákazu vykonávať riadiace funkcie v tomto kľúčovom subjekte, a to každej osobe vykonávajúcej riadiace úlohy na úrovni výkonného riaditeľa alebo právneho zástupcu v tomto kľúčovom subjekte.

Pozmeňujúci návrh 258

Návrh smernice
Článok 29 – odsek 5 – pododsek 2

Text predložený Komisiou	*Pozmeňujúci návrh*
Tieto sankcie sa uplatňujú len dovtedy, kým subjekt neprijme potrebné opatrenia na nápravu nedostatkov alebo nesplní požiadavky príslušného orgánu, ktorý takéto sankcie uplatnil.	***Dočasné pozastavenia alebo zákazy podľa tohto odseku*** sa uplatňujú len dovtedy, kým ***dotknutý*** subjekt neprijme potrebné opatrenia na nápravu nedostatkov alebo nesplní požiadavky príslušného orgánu, ktorý takéto sankcie uplatnil. ***Ukladanie takýchto dočasných pozastavení alebo zákazov musí podliehať primeraným procesným zárukám v súlade so všeobecnými zásadami práva Únie a charty vrátane účinnej súdnej ochrany, riadneho procesu, prezumpcie neviny a práva na obhajobu.***

Pozmeňujúci návrh 259

Návrh smernice
Článok 29 – odsek 7 – písmeno c

Text predložený Komisiou	*Pozmeňujúci návrh*
c) ***skutočné*** spôsobené škody alebo vzniknuté straty ***alebo potenciálne škody alebo straty, ktoré mohli vzniknúť, pokiaľ ich možno určiť. Pri hodnotení tohto aspektu sa okrem iného zohľadnia skutočné alebo potenciálne finančné*** alebo ***hospodárske straty***, ***účinky*** na iné	c) spôsobené škody alebo vzniknuté straty ***vrátane finančných*** alebo ***hospodárskych strát***, ***účinkov*** na iné služby ***a*** počtu dotknutých používateľov;

služby***, počet*** dotknutých ***alebo potenciálne dotknutých*** používateľov;

Pozmeňujúci návrh 260

Návrh smernice
Článok 29 – odsek 7 – písmeno c a (nové)

Text predložený Komisiou	*Pozmeňujúci návrh*
	ca) akékoľvek relevantné predchádzajúce prípady porušenia zo strany dotknutého subjektu;

Pozmeňujúci návrh 261

Návrh smernice
Článok 29 – odsek 9

Text predložený Komisiou	*Pozmeňujúci návrh*
9. Členské štáty zabezpečia, aby ich príslušné orgány informovali relevantné príslušné orgány ***dotknutého členského štátu*** určené podľa smernice (EÚ) XXXX/XXXX [smernica o odolnosti kritických subjektov], keď vykonávajú svoje právomocí v oblasti dohľadu a presadzovania práva zamerané na zabezpečenie dodržiavania povinností podľa tejto smernice zo strany kľúčového subjektu identifikovaného ako kritický alebo ako rovnocenný s kritickým subjektom podľa smernice (EÚ) XXXX/XXXX [smernica o odolnosti kritických subjektov]. Príslušné orgány môžu na žiadosť príslušných orgánov podľa smernice (EÚ) XXXX/XXXX [smernica o odolnosti kritických subjektov] vykonávať svoje právomoci v oblasti dohľadu a presadzovania práva vo vzťahu ku kľúčovému subjektu identifikovanému ako kritický alebo ako rovnocenný subjekt.	9. Členské štáty zabezpečia, aby ich príslušné orgány informovali relevantné príslušné orgány ***všetkých príslušných členských štátov*** určené podľa smernice (EÚ) XXXX/XXXX [smernica o odolnosti kritických subjektov], keď vykonávajú svoje právomocí v oblasti dohľadu a presadzovania práva zamerané na zabezpečenie dodržiavania povinností podľa tejto smernice zo strany kľúčového subjektu identifikovaného ako kritický alebo ako rovnocenný s kritickým subjektom podľa smernice (EÚ) XXXX/XXXX [smernica o odolnosti kritických subjektov]. Príslušné orgány môžu na žiadosť príslušných orgánov podľa smernice (EÚ) XXXX/XXXX [smernica o odolnosti kritických subjektov] vykonávať svoje právomoci v oblasti dohľadu a presadzovania práva vo vzťahu ku kľúčovému subjektu identifikovanému ako kritický alebo ako rovnocenný subjekt.

Pozmeňujúci návrh 262

Návrh smernice
Článok 29 – odsek 9 a (nový)

Text predložený Komisiou	*Pozmeňujúci návrh*
	9a. Členské štáty zabezpečia, aby ich príslušné orgány spolupracovali s relevantnými príslušnými orgánmi dotknutého členského štátu určenými podľa nariadenia (EÚ) XXXX/XXXX [nariadenie DORA].

Pozmeňujúci návrh 263

Návrh smernice
Článok 30 – odsek 1

Text predložený Komisiou	*Pozmeňujúci návrh*
1. Ak členské štáty dostanú dôkaz alebo indíciu, že dôležitý subjekt nedodržiava povinnosti stanovené v tejto smernici, a najmä v článkoch 18 a 20, zabezpečia, aby príslušné orgány konali v prípade potreby prostredníctvom opatrení dohľadu ex post.	1. Ak členské štáty dostanú dôkaz alebo indíciu, že dôležitý subjekt nedodržiava povinnosti stanovené v tejto smernici, a najmä v článkoch 18 a 20, zabezpečia, aby príslušné orgány konali v prípade potreby prostredníctvom opatrení dohľadu ex post. ***Členské štáty zabezpečia, aby boli tieto opatrenia účinné, primerané a odrádzajúce, pričom zohľadnia okolnosti každého konkrétneho prípadu.***

Pozmeňujúci návrh 264

Návrh smernice
Článok 30 – odsek 2 – písmeno a

Text predložený Komisiou	*Pozmeňujúci návrh*
a) kontrolám na mieste a dohľadu ex post na diaľku;	a) kontrolám na mieste a dohľadu ex post na diaľku***, ktoré vykonávajú vyškolení odborníci***;

Pozmeňujúci návrh 265

Návrh smernice
Článok 30 – odsek 2 – písmeno a a (nové)

Text predložený Komisiou	*Pozmeňujúci návrh*
	aa) vyšetreniu prípadov nedodržania povinností a súvisiacich účinkov na

bezpečnosť služieb;

Pozmeňujúci návrh 266

Návrh smernice
Článok 30 – odsek 2 – písmeno b

Text predložený Komisiou	*Pozmeňujúci návrh*
b) cieleným bezpečnostným auditom ***založeným na posúdeniach rizika alebo dostupných informáciách súvisiacich s rizikom***;	b) cieleným bezpečnostným auditom ***vykonávaným kvalifikovaným nezávislým orgánom alebo príslušným orgánom***;

Pozmeňujúci návrh 267

Návrh smernice
Článok 30 – odsek 2 – písmeno c

Text predložený Komisiou	*Pozmeňujúci návrh*
c) bezpečnostným kontrolám založeným na objektívnych, spravodlivých a transparentných kritériách posúdenia rizika;	c) bezpečnostným kontrolám založeným na objektívnych, ***nediskriminačných,*** spravodlivých a transparentných kritériách posúdenia rizika;

Pozmeňujúci návrh 268

Návrh smernice
Článok 30 – odsek 2 – pododseky 1 a a 1 b (nové)

Text predložený Komisiou	*Pozmeňujúci návrh*
	Cielené bezpečnostné audity uvedené v prvom pododseku písm. b) sú založené na posúdeniach rizika, ktoré vykonal príslušný orgán alebo auditovaný subjekt, alebo na iných dostupných informáciách týkajúcich sa rizík.
	Výsledky každého cieleného bezpečnostného auditu sa sprístupnia príslušnému orgánu. Náklady na takýto cielený bezpečnostný audit, ktorý vykonáva kvalifikovaný nezávislý orgán, hradí dotknutý subjekt.

Pozmeňujúci návrh 269

Návrh smernice
Článok 30 – odsek 4 – písmeno h

Text predložený Komisiou	*Pozmeňujúci návrh*
h) vydať verejné vyhlásenie, v ktorom sa uvedie právnická a fyzická osoba alebo osoby zodpovedné za porušenie povinnosti stanovenej v tejto smernici a povaha tohto porušenia;	***vypúšťa sa***

Pozmeňujúci návrh 270

Návrh smernice
Článok 30 – odsek 4 – bod i

Text predložený Komisiou	*Pozmeňujúci návrh*
i) uložiť správnu sankciu alebo požiadať o jej uloženie podľa článku 31 príslušné orgány alebo súdy ***podľa vnútroštátnych zákonov***, a to popri opatreniach uvedených v písmenách a) až h) tohto odseku ***alebo namiesto týchto opatrení,*** v závislosti od okolností každého jednotlivého prípadu.	i) uložiť správnu sankciu alebo požiadať o jej uloženie podľa článku 31 príslušné orgány alebo súdy ***v súlade s vnútroštátnym právom***, a to popri opatreniach uvedených v písmenách a) až h) tohto odseku v závislosti od okolností každého jednotlivého prípadu.

Pozmeňujúci návrh 271

Návrh smernice
Článok 31 – odsek 2

Text predložený Komisiou	*Pozmeňujúci návrh*
2. Správne sankcie sa v závislosti od okolností každého jednotlivého prípadu ukladajú popri opatreniach uvedených v článku 29 ods. 4 písm. a) až i), článku 29 ods. 5 a článku 30 ods. 4 písm. a) až h) a j) ***alebo namiesto týchto opatrení***.	2. Správne sankcie sa v závislosti od okolností každého jednotlivého prípadu ukladajú popri opatreniach uvedených v článku 29 ods. 4 písm. a) až i), článku 29 ods. 5 a článku 30 ods. 4 písm. a) až h) a j).

Pozmeňujúci návrh 272

Návrh smernice
Článok 32 – odsek 1

Text predložený Komisiou	*Pozmeňujúci návrh*
1. Ak majú príslušné orgány indície, že kľúčový alebo dôležitý subjekt pri porušení povinností stanovených v článkoch 18 a 20 porušil aj ochranu osobných údajov, ako sa vymedzuje v článku 4 bode 12 nariadenia (EÚ) 2016/679, pričom takéto porušenie sa oznamuje podľa článku 33 uvedeného nariadenia, ***v primeranej lehote*** o tom informujú príslušné dozorné orgány podľa článkov 55 a 56 uvedeného nariadenia.	1. Ak majú príslušné orgány indície, že kľúčový alebo dôležitý subjekt pri porušení povinností stanovených v článkoch 18 a 20 porušil aj ochranu osobných údajov, ako sa vymedzuje v článku 4 bode 12 nariadenia (EÚ) 2016/679, pričom takéto porušenie sa oznamuje podľa článku 33 uvedeného nariadenia, ***bezodkladne a v každom prípade do 72 hodín od zistenia porušenia ochrany údajov*** o tom informujú príslušné dozorné orgány podľa článkov 55 a 56 uvedeného nariadenia.

Pozmeňujúci návrh 273

Návrh smernice
Článok 32 – odsek 3

Text predložený Komisiou	*Pozmeňujúci návrh*
3. Ak je dozorný orgán, príslušný podľa nariadenia (EÚ) 2016/679, usadený v inom členskom štáte než príslušný orgán, príslušný orgán ***môže informovať*** dozorný orgán usadený v tom istom členskom štáte.	3. Ak je dozorný orgán, príslušný podľa nariadenia (EÚ) 2016/679, usadený v inom členskom štáte než príslušný orgán, príslušný orgán ***informuje*** dozorný orgán usadený v tom istom členskom štáte.

Pozmeňujúci návrh 274

Návrh smernice
Článok 35 – odsek 1

Text predložený Komisiou	*Pozmeňujúci návrh*
Komisia ***pravidelne preskúmava*** fungovanie tejto smernice a ***podáva*** o tom správu Európskemu parlamentu a Rade. V správe sa posúdi najmä relevantnosť odvetví, pododvetví, veľkosti a typu subjektov uvedených v prílohách I a II pre fungovanie hospodárstva a spoločnosti v súvislosti s kybernetickou bezpečnosťou. Na tento účel a s cieľom ďalej napredovať v strategickej a operačnej spolupráci Komisia zohľadní správy skupiny pre spoluprácu a siete jednotiek CSIRT o skúsenostiach získaných na strategickej	Komisia ***do ... [42 mesiacov po dátume nadobudnutia účinnosti tejto smernice] a následne každých 36 mesiacov preskúma*** fungovanie tejto smernice a ***podá*** o tom správu Európskemu parlamentu a Rade. V správe sa posúdi najmä relevantnosť odvetví, pododvetví, veľkosti a typu subjektov uvedených v prílohách I a II pre fungovanie hospodárstva a spoločnosti v súvislosti s kybernetickou bezpečnosťou. Na tento účel a s cieľom ďalej napredovať v strategickej a operačnej spolupráci Komisia zohľadní správy skupiny pre

a operačnej úrovni. ***Prvá správa*** sa ***predloží do … [54 mesiacov po dátume nadobudnutia účinnosti tejto smernice].***	spoluprácu a siete jednotiek CSIRT o skúsenostiach získaných na strategickej a operačnej úrovni. ***K správe*** sa ***podľa potreby pripojí legislatívny návrh***.

Pozmeňujúci návrh 275

Návrh smernice
Článok 36 – odsek 2

Text predložený Komisiou	*Pozmeňujúci návrh*
2. Právomoc prijímať delegované akty uvedené v článku 18 ods. 6 a článku 21 ods. 2 sa Komisii udeľuje na obdobie piatich rokov od [...].	2. Právomoc prijímať delegované akty uvedené v článku 18 ods. 6***, článku 20 ods. 11a*** a článku 21 ods. 2 sa Komisii udeľuje na obdobie piatich rokov od [...].

Pozmeňujúci návrh 276

Návrh smernice
Článok 36 – odsek 3

Text predložený Komisiou	*Pozmeňujúci návrh*
3. Delegovanie právomoci uvedené v článku 18 ods. 6 a článku 21 ods. 2 môže Európsky parlament alebo Rada kedykoľvek odvolať. Rozhodnutím o odvolaní sa ukončuje delegovanie právomoci, ktoré sa v ňom uvádza. Rozhodnutie nadobúda účinnosť dňom nasledujúcim po jeho uverejnení v Úradnom vestníku Európskej únie alebo k neskoršiemu dátumu, ktorý je v ňom určený. Nie je ním dotknutá platnosť delegovaných aktov, ktoré už nadobudli účinnosť.	3. Delegovanie právomoci uvedené v článku 18 ods. 6***, článku 20 ods. 11a*** a článku 21 ods. 2 môže Európsky parlament alebo Rada kedykoľvek odvolať. Rozhodnutím o odvolaní sa ukončuje delegovanie právomoci, ktoré sa v ňom uvádza. Rozhodnutie nadobúda účinnosť dňom nasledujúcim po jeho uverejnení v Úradnom vestníku Európskej únie alebo k neskoršiemu dátumu, ktorý je v ňom určený. Nie je ním dotknutá platnosť delegovaných aktov, ktoré už nadobudli účinnosť.

Pozmeňujúci návrh 277

Návrh smernice
Článok 36 – odsek 6

Text predložený Komisiou	*Pozmeňujúci návrh*
6. Delegovaný akt prijatý podľa článku 18 ods. 6 a článku 21 ods. 2 nadobudne	6. Delegovaný akt prijatý podľa článku 18 ods. 6***, článku 20 ods. 11a*** a článku 21

účinnosť, len ak Európsky parlament alebo Rada voči nemu nevzniesli námietku v lehote dvoch mesiacov odo dňa oznámenia uvedeného aktu Európskemu parlamentu a Rade alebo ak pred uplynutím uvedenej lehoty Európsky parlament a Rada informovali Komisiu o svojom rozhodnutí nevzniesť námietku. Na podnet Európskeho parlamentu alebo Rady sa táto lehota predĺži o dva mesiace.	ods. 2 nadobudne účinnosť, len ak Európsky parlament alebo Rada voči nemu nevzniesli námietku v lehote dvoch mesiacov odo dňa oznámenia uvedeného aktu Európskemu parlamentu a Rade alebo ak pred uplynutím uvedenej lehoty Európsky parlament a Rada informovali Komisiu o svojom rozhodnutí nevzniesť námietku. Na podnet Európskeho parlamentu alebo Rady sa táto lehota predĺži o dva mesiace.

Pozmeňujúci návrh 278

Návrh smernice
Článok 42 – odsek 1 a (nový)

Text predložený Komisiou	*Pozmeňujúci návrh*
	Články 39 a 40 sa však uplatňujú od... [18 mesiacov po dátume nadobudnutia účinnosti tejto smernice].

Pozmeňujúci návrh 279

Návrh smernice
Príloha I – bod 2 – písmeno d – zarážka 2 (nová)

Text predložený Komisiou	*Pozmeňujúci návrh*
2. Doprava	d) Cestná doprava	— ***Prevádzkovatelia služieb inteligentného nabíjania pre elektrické vozidlá***

Pozmeňujúci návrh 280

Návrh smernice
Príloha II – tabuľka – riadok 6 a (nový)

Text predložený Komisiou

Pozmeňujúci návrh

6a. Vzdelávanie a výskum		***— Inštitúcie vysokoškolského vzdelávania a výskumné inštitúcie***