



EURÓPSKY PARLAMENT

2009 - 2014

Výbor pre priemysel, výskum a energetiku

2010/0273(COD)

11.11.2011

STANOVISKO

Výboru pre priemysel, výskum a energetiku

pre Výbor pre občianske slobody, spravodlivosť a vnútorné veci

k návrhu smernice Európskeho parlamentu a Rady o útokoch na informačné systémy a ktorou sa zrušuje rámcové rozhodnutie Rady 2005/222/SVV (KOM(2010)0517 – C7-0293/2010 – 2010/0273(COD))

Spravodajca výboru požiadaneho o stanovisko: Christian Ehler

PA_Legam

POZMEŇUJÚCE A DOPLŇUJÚCE NÁVRHY

Výbor pre priemysel, výskum a energetiku vyzýva Výbor občianske slobody, spravodlivosť a vnútorné veci, aby ako gestorský výbor zaradil do svojej správy tieto pozmeňujúce a doplňujúce návrhy:

Pozmeňujúci a doplňujúci návrh 1

Návrh smernice Odôvodnenie 1

Text predložený Komisiou

(1) Cieľom tejto smernice je aproximácia pravidiel trestného práva v členských štátoch v oblasti útokov na informačné systémy a zlepšenie spolupráce medzi súdnymi a inými príslušnými orgánmi vrátane policajných a iných špecializovaných orgánov presadzovania práva v členských štátoch.

Pozmeňujúci a doplňujúci návrh

(1) ***Ako súčasť všeobecnej stratégie Únie s cieľom bojovať proti organizovanej trestnej činnosti, zvyšovať odolnosť počítačových sietí, chrániť kľúčovú informačnú infraštruktúru a ochraňovať údaje je cieľom tejto smernice aproximácia pravidiel trestného práva v členských štátoch v oblasti útokov na informačné systémy a zlepšenie spolupráce medzi súdnymi a inými príslušnými orgánmi vrátane policajných a iných špecializovaných orgánov presadzovania práva v členských štátoch, Komisie, Eurojustu, Europolu a Európskej agentúry pre bezpečnosť sietí a informácií, aby Únia mohla uplatňovať spoločný a komplexný prístup.***

Pozmeňujúci a doplňujúci návrh 2

Návrh smernice Odôvodnenie 1a (nové)

Text predložený Komisiou

Pozmeňujúci a doplňujúci návrh

(1a) Informačné systémy sú kľúčovým prvkom politickej, sociálnej a hospodárskej interakcie v Európe. Spoločnosť je veľmi závislá od takýchto systémov a táto závislosť je čoraz väčšia. Bezproblémová prevádzka a bezpečnosť týchto systémov v Európe je rozhodujúca pre rozvoj vnútorného trhu a

konkurencieschopného a inovatívneho hospodárstva. Informačné systémy nielenže poskytujú veľké výhody, ale pre našu bezpečnosť prinášajú aj množstvo rizík v dôsledku ich komplexnosti a zraniteľnosti rôznymi druhmi počítačovej kriminality. Bezpečnosť informačných systémov je teda stálym problémom, ktorý si vyžaduje účinnú reakciu zo strany členských štátov a Únie.

Pozmeňujúci a doplňujúci návrh 3

Návrh smernice Odôvodnenie 2

Text predložený Komisiou

(2) Útoky na informačné systémy – **najmä v rámci** organizovanej trestnej činnosti – predstavujú rastúce ohrozenie a zvyšuje sa obava z potenciálnych teroristických alebo politicky motivovaných útokov na informačné systémy, ktoré tvoria časť kritickej infraštruktúry členských štátov a Únie. Tým je ohrozené dosiahnutie bezpečnejšej informačnej spoločnosti a priestoru slobody, bezpečnosti a spravodlivosti, a preto je potrebné prijať opatrenia na úrovni Európskej únie.

Pozmeňujúci a doplňujúci návrh

(2) Útoky na informačné systémy **môžu byť spôsobené rozličnými subjektmi, napríklad teroristami, skupinami z prostredia** organizovanej trestnej činnosti, **štátmi či izolovanými jednotlivcami**. Predstavujú rastúce ohrozenie **fungovania informačných systémov v Únii i vo svete** a zvyšuje sa obava z potenciálnych teroristických alebo politicky motivovaných útokov na informačné systémy, ktoré tvoria časť kritickej infraštruktúry členských štátov a Únie. **Cezhraničný charakter niektorých trestných činov a relatívne nízke riziko a náklady pre páchatel'ov spolu s obrovskými ziskami, ktoré možno dosiahnuť, a škodou, ktorú možno útokmi spôsobiť, významným spôsobom zvyšujú nebezpečenstvo tejto hrozby.** Tým je ohrozené dosiahnutie bezpečnejšej informačnej spoločnosti a priestoru slobody, **demokracie**, bezpečnosti a spravodlivosti, **bráni sa vytvoreniu európskeho digitálneho vnútorného trhu**, a preto je potrebné prijať opatrenia na úrovni Európskej únie, **ako aj na medzinárodnej úrovni, napríklad prostredníctvom dohovoru Rady Európy o**

Pozmeňujúci a doplňujúci návrh 4

Návrh smernice

Odôvodnenie 2a (nové)

Text predložený Komisiou

Pozmeňujúci a doplňujúci návrh

(2a) Nedávne počítačové útoky na európske siete alebo informačné systémy spôsobili Únii značné hospodárske a bezpečnostné škody.

Odôvodnenie

So zreteľom na počítačové útoky na európske inštitúcie z marca 2011, ako aj na početné prípady vniknutia do európskeho systému obchodovania s emisiami, ktorých výsledkom bolo odcudzenie miliónov EUR v emisiách;

Pozmeňujúci a doplňujúci návrh 5

Návrh smernice

Odôvodnenie 3

Text predložený Komisiou

Pozmeňujúci a doplňujúci návrh

(3) Existuje tendencia smerom k čoraz nebezpečnejším a opakujúcim sa masívnym útokom na informačné systémy, ktoré sú pre **štáty** alebo určité funkcie verejného alebo súkromného sektora rozhodujúce. Táto tendencia je sprevádzaná vývojom čoraz dokonalejších nástrojov, ktoré páchatelia používajú na počítačové útoky rôznych druhov.

(3) Existuje tendencia smerom k čoraz nebezpečnejším a opakujúcim sa masívnym útokom **vrátane útokov typu distribuovaného odopretia služieb** na informačné systémy, ktoré sú pre **medzinárodné organizácie, krajiny**, Úniu alebo určité funkcie verejného alebo súkromného sektora rozhodujúce. **Takéto útoky môžu spôsobiť značné hospodárske škody v dôsledku prerušenia prevádzky informačných systémov a samotných komunikácií a v dôsledku straty alebo pozmenenia dôverných informácií alebo iných údajov, ktoré sú dôležité z obchodného hľadiska. Inovatívnym malým a stredným podnikom, ktoré sú závislé od riadneho fungovania a dostupnosti informačných systémov, pričom môžu potenciálne vyčleniť len**

menší objem zdrojov na bezpečnosť informácií, hrozí, že budú obzvlášť zasiahnuté. Táto tendencia je sprevádzaná rýchlym vývojom informačných technológií, a teda i čoraz dokonalejších nástrojov, ktoré páchatelia používajú na počítačové útoky rôznych druhov, pričom niektoré z nich majú významný potenciál spôsobiť hospodárske a sociálne škody.

Pozmeňujúci a doplňujúci návrh 6

Návrh smernice Odôvodnenie 4

Text predložený Komisiou

(4) Spoločné vymedzenie pojmov v tejto oblasti, najmä informačných systémov **a** počítačových údajov, je **dôležité** na zabezpečenie konzistentného prístupu v členských štátoch pri uplatňovaní tejto smernice.

Pozmeňujúci a doplňujúci návrh

(4) Spoločné vymedzenie pojmov v tejto oblasti, najmä pojmov z oblasti informačných systémov, počítačových údajov **a trestných činov týkajúcich sa informačných systémov a počítačových údajov**, je **zásadné** na zabezpečenie konzistentného **a jednotného prístupu** v členských štátoch pri uplatňovaní tejto smernice.

Pozmeňujúci a doplňujúci návrh 7

Návrh smernice Odôvodnenie 6

Text predložený Komisiou

(6) Členské štáty **by** mali ustanoviť sankcie za útoky na informačné systémy. Uložené sankcie **by** mali byť účinné, primerané a odrádzajúce.

Pozmeňujúci a doplňujúci návrh

(6) **Okrem opatrení členských štátov, Únie a súkromného sektora zameraných na zvyšovanie bezpečnosti a integrity informačných systémov a na predchádzanie útokom a minimalizovanie ich dosahu by** členské štáty mali ustanoviť sankcie za útoky na informačné systémy. Uložené sankcie **by** mali byť účinné, primerané a odrádzajúce. **Z dôvodu často cezhraničnej povahy hrozieb je potrebná konvergencia sankcií a postihov, ktoré ukladajú členské štáty, zameraná na**

zníženie rozdielov medzi členskými štátmi v prístupe k trestným činom spáchaným v Únii .

Pozmeňujúci a doplňujúci návrh 8

Návrh smernice
Odôvodnenie 6a (nové)

Text predložený Komisiou

Pozmeňujúci a doplňujúci návrh

(6a) Členské štáty, Únia a súkromný sektor by mali v spolupráci s Európskou agentúrou pre bezpečnosť sietí a informácií prijať kroky na zvýšenie bezpečnosti a integrity informačných systémov, na prevenciu proti útokom a na zníženie dosahu útokov.

Pozmeňujúci a doplňujúci návrh 9

Návrh smernice
Odôvodnenie 8

Text predložený Komisiou

Pozmeňujúci a doplňujúci návrh

(8) V záveroch Rady z 27. – 28. novembra 2008 sa uvádza, že by sa mala spolu s členskými štátmi a Komisiou vytvoriť nová stratégia, ktorá by zohľadňovala obsah Dohovoru Rady Európy o počítačovej kriminalite z roku 2001. Tento dohovor je právnym referenčným rámcom pre boj proti počítačovej kriminalite vrátane útokov na informačné systémy. Táto smernica sa zakladá na tomto dohovore.

(8) V záveroch Rady z 27. – 28. novembra 2008 sa uvádza, že by sa mala spolu s členskými štátmi a Komisiou vytvoriť nová stratégia, ktorá by zohľadňovala obsah Dohovoru Rady Európy o počítačovej kriminalite z roku 2001. **Rada a Komisia by mali povzbudzovať členské štáty, ktoré ešte dohovor neratifikovali, aby tak čo najskôr urobili.** Tento dohovor je právnym referenčným rámcom pre boj proti počítačovej kriminalite vrátane útokov na informačné systémy. Táto smernica zohľadňuje príslušné ustanovenia uvedeného dohovoru.

Pozmeňujúci a doplňujúci návrh 10

Návrh smernice Odôvodnenie 10

Text predložený Komisiou

(10) Touto smernicou sa neudeľuje trestná zodpovednosť v prípadoch, ak sú trestné činy spáchané bez trestného úmyslu, ako je oprávnené testovanie alebo ochrana počítačových systémov.

Pozmeňujúci a doplňujúci návrh

(10) ***Táto smernica sa nevzťahuje na opatrenia prijaté s cieľom zaistiť bezpečnosť informačných systémov, napr. schopnosť informačného systému brániť sa pred trestnými činmi definovanými v tejto smernici, či odstrániť nástroje, ktoré sa na tieto účely používajú alebo sú na takéto používanie určené.*** Touto smernicou sa neudeľuje ani trestná zodpovednosť v prípadoch, ak sú splnené objektívne kritériá trestných činov uvedených v tejto smernici, ale tieto činy sú spáchané bez trestného úmyslu, ako je oprávnené testovanie alebo ochrana počítačových systémov.

Odôvodnenie

Vzhlľadom na to, že hranica medzi prístupom so zlým úmyslom a bez neho (automatické aktualizácie atď.) je niekedy nejasná, cieľom tohto pozmeňujúceho a doplňujúceho návrhu je objasniť, že napríklad pôsobenie antivírusového softvéru alebo nástrojov na odstránenie vírusov či izolovanie zavírených nástrojov je úplne mimo rozsahu pôsobnosti tejto smernice.

Pozmeňujúci a doplňujúci návrh 11

Návrh smernice Odôvodnenie 11

Text predložený Komisiou

(11) Touto smernicou sa posilňuje význam sietí, ako je G8 alebo *Radou iniciovaná európska sieť* kontaktných miest na výmenu informácií, ktoré sú k dispozícii dvadsaťštyri hodín denne a sedem dní v týždni, aby mohli poskytovať okamžitú pomoc pri vyšetrovaníach alebo konaniach týkajúcich sa trestných činov v oblasti informačných systémov a údajov alebo pri zhromažďovaní dôkazov trestného činu

Pozmeňujúci a doplňujúci návrh

(11) Touto smernicou sa posilňuje význam sietí, ako je G8 alebo sieť kontaktných miest na výmenu informácií *Rady Európy*, ktoré sú k dispozícii dvadsaťštyri hodín denne a sedem dní v týždni, aby mohli poskytovať okamžitú pomoc pri vyšetrovaníach alebo konaniach týkajúcich sa trestných činov v oblasti informačných systémov a údajov alebo pri zhromažďovaní dôkazov trestného činu

v elektronickej forme. Vzhľadom na rýchlosť, akou môžu byť masívne útoky realizované, *by členské štáty mali byť schopné rýchlo reagovať* na žiadosti o pomoc zo siete kontaktných miest. Takáto pomoc by mala zahŕňať uľahčenie alebo priame vykonanie týchto opatrení: poskytnutie technického poradenstva, zachovanie údajov, zhromažďovanie dôkazov, poskytnutie právnych informácií a vypátranie podozrivých.

alebo úmyslu spáchať trestný čin. Vzhľadom na rýchlosť, akou môžu byť masívne útoky realizované, *by mali byť členské štáty, Únia a Európska agentúra pre bezpečnosť sietí a informácií schopné rýchlo reagovať* na žiadosti o pomoc zo siete kontaktných miest. Takáto pomoc by mala zahŕňať uľahčenie alebo priame vykonanie týchto opatrení: poskytnutie technického poradenstva *vrátane poradenstva súvisiaceho s obnovou funkčnosti informačného systému*, ochrana údajov *v súlade so zásadami ochrany osobných údajov*, zhromažďovanie dôkazov, poskytnutie právnych informácií, *identifikácia ohrozených a/alebo získaných informácií* a vypátranie a identifikácia podozrivých.

Pozmeňujúci a doplňujúci návrh 12

Návrh smernice

Odôvodnenie 11a (nové)

Text predložený Komisiou

Pozmeňujúci a doplňujúci návrh

(11a) Spolupráca verejných orgánov so súkromným sektorom a občianskou spoločnosťou má vysoký význam pre prevenciu a boj proti útokom na informačné systémy. S týmito partnermi by sa mal nadviazať trvalý dialóg so zreteľom na to, do akej miery využívajú informačné systémy a ako je potrebné rozdeliť zodpovednosť za stabilnú a riadnu prevádzku týchto systémov. Zvyšovanie povedomia o využívaní informačných systémov medzi všetkými účastníkmi je dôležité pre vytvorenie kultúry bezpečnosti informačných technológií.

Pozmeňujúci a doplňujúci návrh 13

Návrh smernice

Odôvodnenie 12

Text predložený Komisiou

(12) V rámci tejto smernice existuje potreba zhromažďovať údaje o trestných činoch, aby sa získal komplexnejší obraz o probléme na úrovni Únie a tým sa prispelo k vypracovaniu účinnejších riešení. Tieto údaje okrem toho pomôžu špecializovaným agentúram, ako sú Europol a Európska agentúra pre bezpečnosť sietí a informácií, lepšie posúdiť rozsah počítačovej kriminality a stav siete a informačnej bezpečnosti v Európe.

Pozmeňujúci a doplňujúci návrh

(12) V rámci tejto smernice existuje potreba zhromažďovať údaje o trestných činoch, aby sa získal komplexnejší obraz o probléme na úrovni Únie a tým sa prispelo k vypracovaniu účinnejších riešení.
Členské štáty s podporou Komisie a Európskej agentúry pre bezpečnosť sietí a informácií musia zlepšiť výmenu informácií o útokoch na informačné systémy. Tieto údaje okrem toho pomôžu špecializovaným **orgánom a** agentúram, ako sú **CERT v členských štátoch**, Europol a Európska agentúra pre bezpečnosť sietí a informácií, lepšie posúdiť rozsah počítačovej kriminality a stav siete a informačnej bezpečnosti v **Únii a podporiť členské štáty v prijímaní opatrení v dôsledku incidentov narušenia bezpečnosti informácií. Lepšia znalosť súčasných a budúcich rizík pomôže dosiahnuť vhodnejšie rozhodnutia týkajúce sa zabraňovania útokom na informačné systémy, boja proti nim alebo obmedzovania škôd, ktoré spôsobujú.**

Pozmeňujúci a doplňujúci návrh 14

Návrh smernice

Odôvodnenie 12a (nové)

Text predložený Komisiou

Pozmeňujúci a doplňujúci návrh

(12a) Hoci táto smernica musí spĺňať prísne požiadavky právnej istoty a predvídateľnosti v trestnom práve, existuje zároveň potreba – ktorú naplňajú ustanovenia tejto smernice o zhromažďovaní údajov, výmene informácií a povinnosti Komisie pravidelne informovať o jej uplatňovaní a predkladať potrebné návrhy – zabezpečiť flexibilný mechanizmus, ktorý by umožnil prispôsobiť sa budúcemu vývoju, čo by mohlo viesť k rozšíreniu rozsahu

pôsobnosti tejto smernice. Budúci vývoj zahŕňa akýkoľvek technologický vývoj, ktorý umožní napríklad účinné presadzovanie práva v oblasti útokov na informačné systémy alebo uľahčí prevenciu či zmierňovanie účinkov týchto útokov.

Odôvodnenie

Hoci zavedenie sankcií je vítané, komplexný prístup Únie k boju proti počítačovej kriminalite by sa nemal zameriavať len na účinné presadzovanie práva, ale aj na vytváranie stratégií a nástrojov na prevenciu tejto trestnej činnosti.

Pozmeňujúci a doplňujúci návrh 15

Návrh smernice

Odôvodnenie 12b (nové)

Text predložený Komisiou

Pozmeňujúci a doplňujúci návrh

(12b) Európska agentúra pre bezpečnosť sietí a informácií by mala plniť strategickú úlohu v koordinácii úsilia medzi členskými štátmi a inštitúciami Únie. Agentúra môže byť napríklad poverená dohľadom nad výmenou informácií medzi nimi, pričom bude fungovať ako spoločné kontaktné miesto a ako register EÚ pre incidenty narušenia počítačovej bezpečnosti. Môže byť poverená aj centralizovaním štatistických údajov o trestných činoch uvedených v tejto smernici na úrovni Únie a môže ich používať ako základ pri príprave hlásení o stave bezpečnosti informačných systémov a počítačových údajov v celej únii

Pozmeňujúci a doplňujúci návrh 16

Návrh smernice

Odôvodnenie 13

Text predložený Komisiou

Pozmeňujúci a doplňujúci návrh

(13) Významné medzery a rozdiely v

(13) Významné medzery a rozdiely v

právnych predpisoch členských štátov v oblasti útokov na informačné systémy môžu brániť boju proti organizovanej trestnej činnosti a terorizmu a môžu skomplikovať účinnú policajnú a súdnu spoluprácu v tejto oblasti. Nadnárodný a bezhraničný charakter moderných informačných systémov znamená, že útoky na tieto systémy majú často cezhraničný charakter, a tak zvyrazňujú naliehavú potrebu ďalšej aproximácie trestných právnych predpisov v tejto oblasti. Koordinácia stíhania prípadov útokov na informačné systémy by mala byť okrem toho uľahčená prijatím rámcového rozhodnutia Rady 2009/948/SVV o predchádzaní kolíziám pri výkone právomoci v trestných veciach a ich urovnávaní.

právnych predpisoch členských štátov v oblasti útokov na informačné systémy môžu brániť boju proti organizovanej trestnej činnosti a terorizmu a môžu skomplikovať účinnú policajnú a súdnu spoluprácu v tejto oblasti. Nadnárodný a bezhraničný charakter moderných informačných systémov znamená, že útoky na tieto systémy majú často cezhraničný charakter, a tak zvyrazňujú naliehavú potrebu ďalšej aproximácie **vnútroštátnych** trestných právnych predpisov v tejto oblasti **na úrovni Únie. Únia by sa podobne mala snažiť o väčšiu medzinárodnú spoluprácu v oblasti bezpečnosti siet'ových a informačných systémov a zapojiť do nej všetkých relevantných medzinárodných účastníkov.** Koordinácia stíhania prípadov útokov na informačné systémy by mala byť okrem toho uľahčená prijatím rámcového rozhodnutia Rady 2009/948/SVV o predchádzaní kolíziám pri výkone právomoci v trestných veciach a ich urovnávaní.

Pozmeňujúci a doplňujúci návrh 17

Návrh smernice Článok 1 – odsek 1

Text predložený Komisiou

Touto smernicou sa vymedzujú trestné činy v oblasti útokov na informačné systémy a stanovujú minimálne pravidlá týkajúce sa sankcií za tieto trestné činy. Jej cieľom je takisto zaviesť spoločné ustanovenia na zabránenie týmto útokom a zlepšenie európskej spolupráce **v trestných veciach** v tejto oblasti.

Pozmeňujúci a doplňujúci návrh

Touto smernicou sa vymedzujú trestné činy v oblasti útokov na informačné systémy a stanovujú **harmonizované** minimálne pravidlá týkajúce sa sankcií za tieto trestné činy. Jej cieľom je takisto zaviesť spoločné ustanovenia na zabránenie týmto útokom **i na boj proti nim** a na zlepšenie európskej spolupráce v tejto oblasti, **najmä pokiaľ ide o trestné veci.**

Pozmeňujúci a doplňujúci návrh 18

Návrh smernice

Článok 2 – písmeno d

Text predložený Komisiou

(d) „Bez oprávnenia“ znamená prístup alebo zásah nepovolený vlastníkom, iným držiteľom práv systému alebo jeho časti, alebo nepovolený **vnútroštátnymi právnymi predpismi**.

Pozmeňujúci a doplňujúci návrh

(d) „Bez oprávnenia“ znamená prístup alebo zásah nepovolený vlastníkom, iným držiteľom práv systému alebo jeho časti, alebo nepovolený **vnútroštátnym právom alebo právom Únie**.

Pozmeňujúci a doplňujúci návrh 19

Návrh smernice

Článok 7 – písmeno b

Text predložený Komisiou

(b) počítačového hesla, prístupového kódu alebo podobných údajov, ktorými je možné získať prístup k celému informačnému systému alebo akejkoľvek jeho časti.

Pozmeňujúci a doplňujúci návrh

(b) počítačového hesla, prístupového kódu, **digitálneho alebo fyzického bezpečnostného kľúča** alebo podobných údajov, ktorými je možné získať prístup k celému informačnému systému alebo akejkoľvek jeho časti.

Pozmeňujúci a doplňujúci návrh 20

Návrh smernice

Článok 8 – odsek 1a (nový)

Text predložený Komisiou

Pozmeňujúci a doplňujúci návrh

1a. Členské štáty zabezpečia, aby nepovolené postupovanie identifikačných údajov iným osobám so zámerom uskutočniť niektorú z činností uvedených v článkoch 3 až 7 bolo trestným činom.

Pozmeňujúci a doplňujúci návrh 21

Návrh smernice

Článok 8 – odsek 1b (nový)

Text predložený Komisiou

Pozmeňujúci a doplňujúci návrh

1b. Členské štáty zabezpečia, aby sa spáchanie trestného činu v zmysle článkov 3 až 7 osobou, ktorá má v rámci právomocí vyplývajúcich z jej zamestnania prístup k bezpečnostným systémom informačných systémov, považovalo za priť ažujúcu okolnosť a bolo trestným činom.

Pozmeňujúci a doplňujúci návrh 22

Návrh smernice Článok 10 – odsek 2

Text predložený Komisiou

2. Členské štáty prijímú opatrenia potrebné na zabezpečenie, aby za trestné činy uvedené v článkoch 3 až 6 bola horná hranica sadzby trestu odňatia slobody stanovená najmenej na 5 rokov, ak boli spáchané použitím nástroja určeného na vykonanie útokov postihujúcich veľké množstvo informačných systémov alebo útokov, ktoré spôsobujú značné škody, ako sú narušené systémové služby, finančné náklady alebo straty osobných údajov.

Pozmeňujúci a doplňujúci návrh

2. Členské štáty prijímú opatrenia potrebné na zabezpečenie, aby za trestné činy uvedené v článkoch 3 až 6 bola horná hranica sadzby trestu odňatia slobody stanovená najmenej na 5 rokov, ak boli spáchané použitím nástroja určeného na vykonanie útokov postihujúcich veľké množstvo informačných systémov alebo útokov, ktoré spôsobujú značné škody, ako sú narušené systémové služby, finančné náklady alebo straty osobných údajov ***alebo citlivých informácií.***

Pozmeňujúci a doplňujúci návrh 23

Návrh smernice Článok 13 – odsek 1 – písmeno c

Text predložený Komisiou

(c) v prospech právnickej osoby, ktorá ***má svoje sídlo*** na území dotknutého členského štátu.

Pozmeňujúci a doplňujúci návrh

(c) v prospech právnickej osoby, ktorá ***je zapísaná do obchodného registra*** na území dotknutého členského štátu.

Pozmeňujúci a doplňujúci návrh 24

Návrh smernice

Článok 14 – odsek 1

Text predložený Komisiou

1. Na účely výmeny informácií, ktoré sa týkajú trestných činov uvedených v článkoch 3 až 8, a v súlade s pravidlami ochrany osobných údajov členskej štáty **využívajú existujúcu** sieť operačných kontaktných miest, ktoré sú k dispozícii dvadsaťštyri hodín denne a sedem dní v týždni. Členské štáty takisto zabezpečia, že majú postupy, ktoré im umožňujú reagovať maximálne do ôsmich hodín na súrne žiadosti. Takáto odpoveď **prinajmenšom obsahuje, či a v akej forme bude žiadosť o pomoc zodpovedaná a kedy**.

Pozmeňujúci a doplňujúci návrh

1. Na účely výmeny informácií, ktoré sa týkajú trestných činov uvedených v článkoch 3 až 8, a v súlade s pravidlami ochrany osobných údajov členskej štáty **zabezpečia, aby mali funkčné vnútroštátne kontaktné miesto a využívali** sieť operačných kontaktných miest, ktoré sú k dispozícii dvadsaťštyri hodín denne a sedem dní v týždni. Členské štáty takisto zabezpečia, že majú postupy, ktoré im umožňujú reagovať maximálne do ôsmich hodín na súrne žiadosti. Takáto odpoveď **je účinná a v prípade potreby je jej súčasťou umožnenie alebo priame vykonávanie týchto opatrení: poskytnutie technického poradenstva vrátane poradenstva súvisiaceho s obnovou funkčnosti informačného systému, ochrana údajov v súlade so zásadami ochrany osobných údajov, zhromažďovanie dôkazov, poskytnutie právnych informácií a vypátranie a identifikácia podozrivých. Kontaktné miesta určujú, v akej forme a lehote sa bude reagovať na žiadosti o pomoc**.

Pozmeňujúci a doplňujúci návrh 25

Návrh smernice

Článok 14 – odsek 2

Text predložený Komisiou

2. Členské štáty oznámia Komisii svoje určené kontaktné miesto na účely výmeny informácií o trestných činoch uvedených v článkoch 3 až 8. Komisia bezodkladne odovzdá túto informáciu ostatným členským štátom.

Pozmeňujúci a doplňujúci návrh

2. Členské štáty oznámia Komisii, **Eurojustu a Európskej agentúre pre bezpečnosť sietí a informácií** svoje určené kontaktné miesto na účely výmeny informácií o trestných činoch uvedených v článkoch 3 až 8. Komisia bezodkladne

odovzdá túto informáciu ostatným členským štátom.

Pozmeňujúci a doplňujúci návrh 26

Návrh smernice

Článok 15 – odsek 3

Text predložený Komisiou

3. Členské štáty postúpia Komisii údaje zozbierané v súlade s týmto článkom. Zabezpečia, aby sa uverejnil konsolidovaný prehľad ich štatistických hlásení.

Pozmeňujúci a doplňujúci návrh

3. Členské štáty postúpia Komisii, ***Europolu a Európskej agentúre pre bezpečnosť sietí a informácií*** údaje zozbierané v súlade s týmto článkom a zabezpečia, aby sa uverejnil ***pravidelný*** konsolidovaný prehľad ich štatistických hlásení.

Pozmeňujúci a doplňujúci návrh 27

Návrh smernice

Článok 18 – odsek 1

Text predložený Komisiou

1. Komisia predloží do [ŠTYROCH ROKOV OD PRIJATIA SMERNICE] a potom každé tri roky správu Európskemu parlamentu a Rade o vykonávaní tejto smernice v členských štátoch vrátane prípadných návrhov.

Pozmeňujúci a doplňujúci návrh

1. Komisia ***po konzultácii so všetkými príslušnými zainteresovanými stranami*** predloží do [ŠTYROCH ROKOV OD PRIJATIA SMERNICE] a potom každé tri roky správu Európskemu parlamentu a Rade o vykonávaní tejto smernice v členských štátoch vrátane prípadných návrhov. ***V každej správe uvedie a s ohľadom na akýkoľvek potrebný návrh vezme do úvahy technické riešenia umožňujúce účinnejšie presadzovanie práva v Únii v oblasti útokov na informačné systémy vrátane technických riešení, ktoré by mohli slúžiť na prevenciu alebo zmierňovanie účinkov týchto útokov.***

Pozmeňujúci a doplňujúci návrh 28

Návrh smernice

Článok 18 – odsek 2

PE472.192v02-00

16/18

AD\883144SK.doc

Text predložený Komisiou

2. Členské štáty zašlú Komisii všetky informácie potrebné na prípravu správy uvedenej v odseku 1. Tieto informácie obsahujú podrobný opis legislatívnych a nelegislatívnych opatrení prijatých pri vykonávaní tejto smernice.

Pozmeňujúci a doplňujúci návrh

2. Členské štáty **a Európska agentúra pre bezpečnosť sietí a informácií** zašlú Komisii všetky informácie potrebné na prípravu správy uvedenej v odseku 1. Tieto informácie obsahujú podrobný opis legislatívnych a nelegislatívnych opatrení prijatých pri vykonávaní tejto smernice.

POSTUP

Názov	Útoky na informačné systémy a zrušenie rámcového rozhodnutia Rady 2005/222/SVV
Referenčné čísla	KOM(2010)0517 – C7-0293/2010 – 2010/0273(COD)
Gestorský výbor dátum oznámenia na schôdzi	LIBE 7.10.2010
Výbor požiadaný o stanovisko dátum oznámenia na schôdzi	ITRE 7.10.2010
Spravodajca výboru požiadaného o stanovisko dátum vymenovania	Christian Ehler 24.11.2010
Prerokovanie vo výbore	13.4.2011 6.10.2011
Dátum prijatia	10.11.2011
Výsledok záverečného hlasovania	+: 49 -: 0 0: 1
Poslanci prítomní na záverečnom hlasovaní	Ivo Belet, Bendt Bendtsen, Maria Da Graça Carvalho, Giles Chichester, Pilar del Castillo Vera, Christian Ehler, Ioan Enciu, Adam Gierek, Norbert Glante, Robert Goebbels, Fiona Hall, Jacky Hélin, Kent Johansson, Romana Jordan Cizelj, Lena Kolarska-Bobińska, Béla Kovács, Philippe Lamberts, Bogdan Kazimierz Marcinkiewicz, Marisa Matias, Judith A. Merkies, Angelika Niebler, Jaroslav Paška, Aldo Patriciello, Anni Podimata, Miloslav Ransdorf, Herbert Reul, Michèle Rivasi, Jens Rohde, Paul Rübig, Amalia Sartori, Francisco Sosa Wagner, Konrad Szymański, Michael Theurer, Ioannis A. Tsoukalas, Claude Turmes, Niki Tzavela, Marita Ulvskog, Vladimir Urutchev, Adina-Ioana Vălean
Náhradníci prítomní na záverečnom hlasovaní	Antonio Cancian, Jolanta Emilia Hibner, Yannick Jadot, Ivailo Kalfin, Bernd Lange, Werner Langen, Markus Pieper, Mario Pirillo, Hannes Swoboda, Silvia-Adriana Țicău
Náhradníci (čl. 187 ods. 2) prítomní na záverečnom hlasovaní	Eider Gardiazábal Rubial