EURÓPSKA KOMISIA

Brusel, 30.9.2010
KOM(2010) 517 v konečnom znení

2010/0273 (COD)

Návrh

# SMERNICA EURÓPSKEHO PARLAMENTU A RADY

## o útokoch na informačné systémy a ktorou sa zrušuje rámcové rozhodnutie Rady 2005/222/SVV

{SEK(2010) 1122 final}
{SEK(2010) 1123 final}

# DÔVODOVÁ SPRÁVA

## 1. DÔVODY A CIELE NÁVRHU

Cieľom tohto návrhu je nahradiť rámcové rozhodnutie Rady 2005/222/SVV z 24. februára 2005 o útokoch na informačné systémy[1]. Rámcové rozhodnutie, ako bolo uvedené v jeho odôvodneniach, sa zameriavalo na zlepšenie spolupráce medzi súdnymi a inými príslušnými orgánmi, vrátane policajných a iných špecializovaných orgánov presadzovania práva v členských štátoch, prostredníctvom aproximácie pravidiel trestného práva v členských štátoch v oblasti útokov na informačné systémy. Zaviedlo právne predpisy EÚ na boj proti trestným činom, ako sú protiprávny prístup k informačným systémom, protiprávny zásah do systému a protiprávny zásah do údajov, ako aj osobitné pravidlá týkajúce sa zodpovednosti právnických osôb, súdnej právomoci a výmeny informácií. Členské štáty boli vyzvané prijať všetky nevyhnutné opatrenia potrebné na dosiahnutie súladu s ustanoveniami tohto rámcového rozhodnutia do 16. marca 2007.

Komisia 14. júla 2008 uverejnila správu o vykonávaní rámcového rozhodnutia[2]. Ako bolo uvedené v záveroch správy, vo väčšine členských štátov sa dosiahol výrazný pokrok a úroveň implementácie bola relatívne dobrá, avšak v niektorých členských štátoch ešte nebola ukončená. Ďalej sa v správe uvádzalo, že od „prijatia rámcového rozhodnutia došlo k nedávnym útokom v celej Európe, čo ešte viac zdôraznilo viacero nových hrozieb, predovšetkým vznik masívnych simultánnych útokov na informačné systémy a zvýšené zločinné využívanie tzv. botnetov“. Tieto útoky neboli v centre pozornosti, keď sa rámcové rozhodnutie prijímalo. Vzhľadom na tento vývoj Komisia zváži opatrenia, ktorých cieľom bude nájsť lepšie odpovede na túto hrozbu (pozri ďalší oddiel na vysvetlenie pojmu botnet).

Dôležitosť prijatia ďalších opatrení na posilnenie boja proti počítačovej kriminalite bola zdôraznená v Haagskom programe z roku 2004 o posilňovaní slobody, bezpečnosti a spravodlivosti v Európskej únii, ako aj v Štokholmskom programe z roku 2009 a príslušnom akčnom pláne[3]. Okrem toho nedávno predložená Digitálna agenda pre Európu[4], prvá hlavná iniciatíva prijatá v rámci stratégie Európa 2020, uznáva potrebu riešiť nárast nových foriem trestnej činnosti, najmä počítačovej kriminality na európskej úrovni. V akčnej oblasti zameranej na dôveru a bezpečnosť je Komisia odhodlaná presadzovať opatrenia na boj proti počítačovým útokom na informačné systémy.

Dohovor Rady Európy o počítačovej kriminalite podpísaný 23. novembra 2001 je na medzinárodnej úrovni považovaný za najúplnejšiu súčasnú medzinárodnú normu, keďže poskytuje komplexný a ucelený rámec zahŕňajúci viaceré aspekty počítačovej kriminality[5]. Dohovor doteraz podpísalo všetkých 27 členských štátov, avšak iba 15 členských štátov ho ratifikovalo[6]. Dohovor nadobudol platnosť 1. júla 2004. EÚ nie je zmluvnou stranou dohovoru. Vzhľadom na význam tohto nástroja Komisia aktívne povzbudzuje zostávajúce členské štáty EÚ, aby tento dohovor čo najskôr ratifikovali.

---

1 Ú. v. EÚ L 69, 16.3.2005, s. 68.

2 Správa Komisie Rade založená na článku 12 rámcového rozhodnutia Rady z 24. februára 2005 o útokoch na informačné systémy − KOM(2008) 448.

3 Ú. v. EÚ C 198, 12.8.2005; Ú. v. EÚ C 115, 4.5.2010; KOM(2010) 171, 20.4.2010.

4 Oznámenie Komisie − KOM(2010) 245, 19.5.2010.

5 Dohovor Rady Európy o počítačovej kriminalite, Budapešť, 23. novembra 2001, CETS č. 185.

6 Pozri prehľad ratifikácie dohovoru (CETS č. 185): http://conventions.coe.int/Treaty/Commun/ChercheSig.asp?NT=185&CM=&DF=&CL=ENG.

- **Všeobecný kontext**

Hlavnou príčinou výskytu počítačovej kriminality je zraniteľnosť systémov vyplývajúca z celého radu faktorov. Nedostatočná reakcia mechanizmov presadzovania práva prispieva k rozmachu tohto fenoménu, zvyšuje ťažkosti, pretože niektoré formy trestných činov presahujú hranice štátov. Hovoriť o tomto druhu trestného činu je často neprimerané, čiastočne z toho dôvodu, že niektoré trestné činy ostanú bez povšimnutia a čiastočne preto, že obete (hospodárske subjekty a spoločnosti) nenahlásia trestné činy zo strachu, aby nezískali zlú povesť a aby ich budúce obchodné vyhliadky neboli ovplyvnené verejným odhalením ich zraniteľnosti.

Okrem toho rozdiely v trestnom práve a trestných konaniach môžu spôsobovať rozdielnosť vo vyšetrovacích postupoch a trestnom stíhaní, ktoré vedú k odlišnému zaobchádzaniu s týmito trestnými činmi. Rozvoj informačných technológií zvýšil naliehavosť týchto problémov, pretože uľahčil výrobu a distribúciu nástrojov („malware“ a „botnetov“) a súčasne páchateľom zabezpečil anonymitu a spôsobil rozšírenie trestnoprávnej zodpovednosti na viacero jurisdikcií. Keďže stíhanie je zložité, organizovaná trestná činnosť dokáže pri malom riziku prinášať značné zisky.

Tento návrh zohľadňuje nové metódy páchania počítačových trestných činov, najmä použitie botnetov. Pojem „botnet“ označuje sieť počítačov, ktoré boli infikované škodlivým softvérom (počítačovým vírusom). Takáto sieť kompromitovaných počítačov („zombies“) môže byť aktivovaná na vykonávanie špecifických činností, ako sú útoky na informačné systémy (počítačové útoky). Tieto „zombies“ môžu byť − často bez vedomia užívateľov kompromitovaných počítačov − kontrolované iným počítačom. Tento „kontrolujúci“ počítač je tiež známy ako „riadiace a kontrolné centrum“. Osoby, ktoré kontrolujú toto centrum, patria k páchateľom, keďže používajú kompromitované počítače na útoky na informačné systémy. Je veľmi náročné vystopovať týchto páchateľov, keďže počítače, ktoré tvoria botnet a vykonávajú útok, sa môžu nachádzať na inom mieste, ako je samotný páchateľ.

Útoky vykonávané prostredníctvom botnetu sa často uskutočňujú vo veľkom rozsahu. V prípade masívnych útokov ide buď o útoky realizované použitím nástrojov, ktoré postihujú veľké množstvo informačných systémov (počítačov), alebo o také, ktoré spôsobujú značné škody, napr. narušenie systémových služieb, finančné náklady, straty osobných údajov atď. Škody spôsobené masívnymi útokmi majú významný vplyv na fungovanie samotného cieľa útoku a/alebo na jeho pracovné prostredie. V tomto zmysle sa „veľký botnet“ chápe tak, že môže spôsobiť vážnu škodu. Je ťažké definovať botnety podľa veľkosti, avšak najväčšie pozorované botnety sa odhadovali na 40 000 až 100 000 pripojení (t. j. infikovaných počítačov) za 24 hodín[7].

[7] Počet pripojení za 24 hodín je bežne používaná meracia jednotka na odhad veľkosti botnetov.

- **Existujúce ustanovenia v oblasti návrhu**

Na úrovni EÚ sa rámcovým rozhodnutím ustanovila minimálna úroveň aproximácie právnych predpisov členských štátov s cieľom kriminalizovať viacero počítačových trestných činov, vrátane protiprávneho prístupu k informačným systémom, protiprávneho zásahu do systému a protiprávneho zásahu do údajov, ako aj navádzanie, pomoc a podnecovanie pri páchaní trestných činov a pokus o ne.

Ustanovenia rámcového rozhodnutia boli síce vo všeobecnosti implementované členskými štátmi, rozhodnutie však vzhľadom na rastúci rozsah a počet trestných činov (počítačových útokov) vykazuje rad nedostatkov. K aproximácii právnych predpisov dochádza len v obmedzenom počte trestných činov, avšak na potenciálnu hrozbu, ktorú pre spoločnosť predstavujú masívne útoky, sa plne nereaguje. Dostatočne sa nezohľadňuje ani vážnosť trestných činov a sankcie proti nim.

Ďalšie platné alebo pripravované iniciatívy a programy EÚ do určitej miery riešia problémy spojené s počítačovými útokmi alebo otázkami, ako sú bezpečnosť siete a bezpečnosť internetových užívateľov. Medzi ne patria akcie podporované v rámci programov „Prevencia a boj proti trestnej činnosti“[8], „Trestná justícia“[9], „Bezpečnejší internet“[10] a „Iniciatíva kritickej informačnej infraštruktúry“[11]. Okrem už spomínaného rámcového rozhodnutia ďalším významným platným právnym nástrojom je rámcové rozhodnutie 2004/68/SVV o boji proti sexuálnemu zneužívaniu a sexuálnemu vykorisťovaniu detí a proti detskej pornografii.

Na správnej úrovni je postup, pri ktorom sa infikujú počítače a stávajú z nich „botnety“, už zakázaný podľa predpisov EÚ týkajúcich sa ochrany súkromia a pravidiel ochrany údajov[12]. Najmä národné administratívne agentúry už spolupracujú v rámci Európskej kontaktnej siete orgánov pre spam. Podľa týchto pravidiel sa vyžaduje, aby členské štáty zakázali zachytávanie komunikácií na verejných komunikačných sieťach a verejne dostupných elektronických komunikačných službách bez súhlasu dotknutého užívateľa alebo zákonného povolenia.

Tento návrh je v súlade s týmito pravidlami. Členské štáty by mali dbať o zlepšenie spolupráce medzi správnymi orgánmi a orgánmi presadzovania práva v prípadoch, ktoré podliehajú správnym aj trestným sankciám.

- **Súlad s inými politikami a cieľmi Únie**

Ciele sú v súlade s politikami EÚ týkajúcimi sa boja proti organizovanej trestnej činnosti, zvýšenia odolnosti počítačových sietí, ochrany kritickej informačnej infraštruktúry a ochrany údajov. Ciele sú takisto v súlade s programom Bezpečnejší internet, ktorý bol vytvorený na podporu bezpečného používania internetu a nových on-line technológií, a na boj proti protiprávnemu obsahu.

---

8 Pozri: http://ec.europa.eu/justice_home/funding/isec/funding_isec_en.htm.

9 Pozri: http://ec.europa.eu/justice_home/funding/jpen/funding_jpen_en.htm.

10 Pozri: http://ec.europa.eu/information_society/activities/sip/index_en.htm.

11 Pozri: http://ec.europa.eu/information_society/policy/nis/strategy/activities/ciip/index_en.htm.

12 Smernica o súkromí a elektronických komunikáciách (Ú. v. ES L 201, 31.7.2002), zmenená a doplnená smernicou 2009/136/ES (Ú. v. EÚ L 337, 18.12.2009).

Tento návrh bol podrobený dôkladnej kontrole, aby sa zabezpečil plný súlad jeho ustanovení so základnými právami, najmä s ochranou osobných údajov, slobodou prejavu a právom na informácie, právom na spravodlivý proces, prezumpciou neviny a právom na obhajobu, ako aj so zásadami zákonnosti a primeranosti trestných činov a trestov.

## 2. KONZULTÁCIE SO ZAINTERESOVANÝMI STRANAMI A POSÚDENIE VPLYVU

- **Konzultácie so zainteresovanými stranami**

Konali sa viaceré rôzne stretnutia k rozličnými aspektom boja proti počítačovej kriminalite, vrátane ďalších súdnych krokov (trestného stíhania), na ktorých sa diskutovalo so širokou škálou odborníkov v tejto oblasti. Patrili medzi nich najmä zástupcovia vlád členských štátov a súkromného sektora, špecializovaní sudcovia alebo prokurátori, zástupcovia medzinárodných organizácií, európskych agentúr a odborných orgánov. Niekoľko odborníkov a organizácií následne zaslalo svoje návrhy a poskytlo informácie.

Hlavné pripomienky nadväzujúce na konzultáciu sú:

– potreba, aby EÚ v tejto oblasti konala,

– potreba kriminalizovať tie formy trestných činov, ktoré neboli zahrnuté do súčasného rámcového rozhodnutia, najmä nové formy počítačových útokov (botnety),

– potreba odstrániť prekážky vo vyšetrovaní a trestnom stíhaní cezhraničných prípadov.

Pripomienky prijaté počas konzultácie boli zohľadnené v posúdení vplyvu.

**Získavanie a využívanie expertízy**

Externé odborné posudky boli získané počas viacerých stretnutí so zainteresovanými stranami.

**Posúdenie vplyvu**

Skúmané boli rôzne možnosti politiky ako prostriedky na dosiahnutie cieľa.

- Možnosť č. 1: status quo/žiadne nové opatrenia EÚ

Táto možnosť znamená, že EÚ neprijme žiadne ďalšie opatrenia na boj proti tejto špecifickej forme počítačovej kriminality, t. j. útokom na informačné systémy. Prebiehajúce opatrenia budú naďalej pokračovať, najmä programy na posilnenie ochrany kritickej informačnej štruktúry a zlepšenie spolupráce medzi verejným a súkromným sektorom v boji proti počítačovej kriminalite.

- Možnosť č. 2: rozvoj programu na posilnenie úsilia o odvrátenie útokov na informačné systémy prostredníctvom nelegislatívnych opatrení

Nelegislatívne opatrenia by sa spolu s programom na ochranu kritickej informačnej štruktúry zameriavali na cezhraničné trestné stíhanie a spoluprácu medzi verejným a súkromným sektorom. Cieľom týchto nástrojov tzv. mäkkého zákona („soft law“) by bolo podporovať ďalšie koordinované opatrenia na úrovni EÚ, vrátane posilnenia existujúcej siete kontaktných

miest pre orgány presadzovania práva, ktoré sú k dispozícii dvadsaťštyri hodín denne a sedem dní v týždni; zriadenia siete kontaktných miest EÚ medzi verejným a súkromným sektorom zahŕňajúce odborníkov na počítačovú kriminalitu a orgány presadzovania práva; vypracovania štandardnej dohody EÚ o úrovni služieb spolupráce orgánov presadzovania práva s prevádzkovateľmi v súkromnom sektore a podpory organizovania programov odbornej prípravy v oblasti vyšetrovania počítačovej kriminality pre orgány presadzovania práva.

- Možnosť č. 3: cielená aktualizácia pravidiel rámcového rozhodnutia (súčasné rámcové rozhodnutie nahradí nová smernica) zameraná na otázky, ako sú hrozby masívnych útokov na informačné systémy (botnety), účinnosť kontaktných miest orgánov presadzovania práva v členských štátoch v prípadoch, ak bol trestný čin vykonaný s utajením skutočnej identity páchateľa a spôsobil ujmu právoplatnému vlastníkovi identity, a nedostatok štatistických údajov o počítačových útokoch

Táto možnosť poskytuje zavedenie špecifických cielených (t. j. obmedzených) právnych predpisov na zabránenie masívnym útokom na informačné systémy. Takto posilnené právne predpisy by boli sprevádzané nelegislatívnymi opatreniami na posilnenie operačnej cezhraničnej spolupráce proti útokom, čím by sa zjednodušila implementácia legislatívnych opatrení. Cieľom týchto opatrení by bolo zvýšenie pripravenosti, bezpečnosti a odolnosti kritickej informačnej infraštruktúry a výmena osvedčených postupov.

- Možnosť č. 4: zavedenie komplexných právnych predpisov EÚ proti počítačovej kriminalite

Táto možnosť by obsahovalo nové komplexné právne predpisy EÚ. Okrem zavedenia opatrení mäkkého práva (možnosť č. 2) a aktualizácie (možnosť č. 3) by sa táto možnosť takisto dotýkala aj právnych problémov súvisiacich s používaním internetu. Takéto opatrenia by zahŕňali nielen útoky na informačné systémy, ale aj otázky, ako sú finančná počítačová kriminalita, protiprávny internetový obsah, zber/úschova/prenos elektronických dôkazov a podrobnejšie pravidlá súdnej právomoci. Právne predpisy by sa uplatňovali súbežne s Dohovorom Rady Európy o počítačovej kriminalite a zahŕňali by už uvedené sprievodné nelegislatívne opatrenia.

- Možnosť č. 5: aktualizácia Dohovoru Rady Európy o počítačovej kriminalite

Táto možnosť by vyžadovala podstatné prerokovanie súčasného dohovoru, čo predstavuje dlhý proces a je v rozpore s časovým akčným rámcom navrhnutým v posúdení vplyvu. Zdá sa, že neexistuje žiadna ochota ešte raz prerokovať dohovor na medzinárodnej úrovni. Aktualizáciu dohovoru preto nemožno považovať za realizovateľnú možnosť, keďže nespadá do časového akčného rámca.

Uprednostňovaná možnosť: kombinácia nelegislatívnych opatrení (možnosť č. 2) s cielenou aktualizáciou rámcového rozhodnutia (možnosť č. 3)

Na základe analýzy hospodárskeho a spoločenského dosahu a dosahu na základné práva, možnosti č. 2 a 3 predstavujú najlepší postup na riešenie problémov a dosiahnutie cieľov návrhu.

Pri vypracovaní tohto návrhu Komisia vykonala posúdenie vplyvu.

## 3. PRÁVNE PRVKY NÁVRHU

- **Zhrnutie navrhovaného opatrenia**

V smernici, ktorou sa zrušuje rámcové rozhodnutie 2005/222/SVV, sa zachovajú jeho súčasné ustanovenia a pribudnú tieto nové prvky:

– V oblasti trestného práva hmotného vo všeobecnosti, smernica:

A. ukladá tresty za výrobu, predaj, obstarávanie na použitie, dovoz, distribúciu alebo akékoľvek získavanie zariadení/nástrojov, ktoré sa používajú na spáchanie trestných činov;

B. zaraďuje priťažujúce okolnosti:

- rozsiahlosť útokov − botnety alebo podobné nástroje by sa riešili zavedením nových priťažujúcich okolností v tom zmysle, že čin umiestnenia botnetu alebo podobného nástroja by bol priťažujúcim faktorom pri spáchaní trestných činov uvedených v súčasnom rámcovom rozhodnutí,

- okolnosť, keď bola pri spáchaní trestného činu utajená skutočná identita páchateľa a spôsobená ujma právoplatnému vlastníkovi identity. Všetky tieto pravidlá by museli byť v súlade so zásadami zákonnosti a primeranosti trestných činov a trestov a v súlade so súčasnými právnymi predpismi o ochrane osobných údajov[13];

C. zavádza ako trestný čin „protiprávne zachytávanie údajov“;

D. zavádza opatrenia na zlepšenie európskej spolupráce v trestných veciach posilnením existujúcej štruktúry kontaktných miest, ktoré sú k dispozícii dvadsaťštyri hodín denne a sedem dní v týždni[14]:

- navrhuje povinnosť operačných kontaktných miest (uvedených v článku 14 smernice) vyhovieť žiadosti o pomoc do stanovenej lehoty. Dohovor o počítačovej kriminalite nešpecifikuje záväzné ustanovenie tohto druhu. Cieľom tohto opatrenia je zabezpečiť, aby kontaktné miesta v rámci určitej vymedzenej lehoty uviedli, či sú schopné poskytnúť riešenie na žiadosť o pomoc a dokedy požiadané kontaktné miesto počíta s nájdením riešenia. Skutočný obsah riešení nie je špecifikovaný;

E. poukazuje na potrebu poskytovať štatistické údaje o počítačovej kriminalite tým, že ukladá členským štátom povinnosť zabezpečiť primeraný systém na zaznamenávanie, výrobu a poskytovanie štatistických údajov o trestných činoch uvedených v súčasnom rámcovom rozhodnutí a o novom trestnom čine „protiprávneho zachytávania údajov“.

---

[13] Ako je 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) (v súčasnosti sa reviduje) a ako je všeobecná smernica o ochrane údajov 95/46/ES.

[14] Zavedené dohovorom a rámcovým rozhodnutím 2005/222/SVV o útokoch proti informačným systémom.

Smernica obsahuje vo vymedzení trestných činov uvedených v článkoch 3, 4, 5 (protiprávny prístup k informačným systémom, protiprávny zásah do systému a protiprávny zásah do údajov) ustanovenie, podľa ktorého môžu členské štáty v procese transpozície smernice do vnútroštátnych právnych predpisov kriminalizovať iba „prípady, ktoré nie sú menej závažné“. Tento prvok flexibility má členským štátom umožniť nevšímať si prípady, ktoré by teoreticky boli obsiahnuté v základnom vymedzení pojmov, avšak neboli by vnímané ako poškodzovanie chráneného právneho záujmu. Sem patria najmä konania mladých ľudí, ktorí sa snažia preukázať svoje odborné znalosti v oblasti informačných technológií. Táto možnosť obmedziť rozsah kriminalizácie by však nemala viesť k zavádzaniu dodatočných znakov skutkovej podstaty trestných činov presahujúcich už znaky zahrnuté v smernici, pretože by to viedlo k situácii, že len trestné činy spáchané za priťažujúcich okolností by boli obsiahnuté. V procese transpozície by sa členské štáty mali zdržať najmä pridávania dodatočných znakov skutkovej podstaty základných trestných činov, ako sú napríklad osobitný zámer čerpať nezákonné príjmy z trestného činu alebo osobitný účinok spôsobovať značnú škodu.

- **Právny základ**

Článok 83 ods. 1 Zmluvy o fungovaní Európskej únie[15].

- **Zásada subsidiarity**

Zásada subsidiarity sa uplatňuje na opatrenia Európskej Únie. Ciele návrhu nie je možné uspokojivo dosiahnuť na úrovni samotných členských štátov z týchto dôvodov:

Počítačová kriminalita a konkrétnejšie útoky na informačné systémy majú značný cezhraničný rozsah, ktorý je najviac badateľný pri masívnych útokoch, keďže pripojenia v rámci jedného útoku sa často nachádzajú na rôznych miestach a v rôznych krajinách. Na tento účel je potrebné prijať opatrenia na úrovni EÚ, najmä aby sa udržal krok so súčasným trendom smerom k masívnym útokom v Európe a vo svete. Prijatie opatrení na úrovni EÚ a aktualizácia rámcového rozhodnutia 2005/222/SVV sa takisto požadovali v záveroch Rady z novembra 2008[16], keďže samotné členské štáty nemôže dostatočne dosiahnuť cieľ účinnej ochrany občanov pred počítačovou kriminalitou.

Ciele návrhu sa lepšie dosiahnu pomocou opatrení na úrovni Európskej únie z týchto dôvodov:

Návrhom sa vo väčšej miere dosiahne aproximácia trestného práva hmotného a procesných pravidiel členských štátov, čo bude mať pozitívny vplyv na boj proti týmto trestným činom. Po prvé ide o možnosť zabrániť páchateľom presťahovať sa do členských štátov, v ktorých sú právne predpisy proti počítačovým útokom miernejšie. Po druhé spoločným vymedzením pojmov sa umožní výmena informácií, zhromažďovanie a porovnanie relevantných údajov. Po tretie sa takisto zvýši účinnosť preventívnych opatrení v celej EÚ a medzinárodná spolupráca.

Návrh je preto v súlade so zásadou subsidiarity.

---

15 Ú. v. EÚ C 83, 30.3.2010, s. 49.

16 „Koordinovaná stratégia a praktické opatrenia proti počítačovej kriminalite“, 2987. zasadnutie Rady pre SPRAVODLIVOSŤ a VNÚTORNÉ VECI, Brusel, 27. − 28. novembra 2008.

- **Zásada proporcionality**

Návrh je v súlade so zásadou proporcionality z tohto dôvodu:

Táto smernica sa obmedzuje na minimum požadované v záujme dosiahnutia týchto cieľov na európskej úrovni a neprekračuje rámec nevyhnutný na tento účel, pričom súčasne zohľadňuje potrebu precíznych právnych predpisov v oblasti trestného práva.

- **Výber nástrojov**

Navrhovaný nástroj: smernica.

Iné prostriedky by neboli primerané z tohto dôvodu:

Právny základ si vyžaduje smernicu.

Nelegislatívne opatrenia a samoregulácia by zlepšili situáciu v určitých oblastiach, v ktorých je implementácia takýchto opatrení veľmi potrebná. V iných oblastiach, v ktorých je potrebné prijať nové právne predpisy, by však prínos nelegislatívnych opatrení a samoregulácie nebol taký výrazný.

## 4. VPLYV NA ROZPOČET

Vplyv tohto návrhu na rozpočet Únie je malý. Viac než 90 % odhadovaných nákladov v sume 5 913 000 EUR by niesli členské štáty a existuje možnosť uchádzať sa o finančné prostriedky EÚ na zníženie nákladov.

## 5. DOPLŇUJÚCE INFORMÁCIE

- **Zrušenie platných právnych predpisov**

Prijatie návrhu bude viesť k zrušeniu existujúcich právnych predpisov.

- **Územná pôsobnosť**

Táto smernica je určená členským štátom v súlade so zmluvami.

2010/0273 (COD)

Návrh

# SMERNICA EURÓPSKEHO PARLAMENTU A RADY

## o útokoch na informačné systémy a ktorou sa zrušuje rámcové rozhodnutie Rady 2005/222/SVV

EURÓPSKY PARLAMENT A RADA EURÓPSKEJ ÚNIE,

so zreteľom na Zmluvu o fungovaní Európskej únie, a najmä

na jej článok 83 ods. 1,

so zreteľom na návrh Európskej komisie[17],

po predložení návrhu právneho predpisu národným parlamentom,

so zreteľom na stanovisko Európskeho hospodárskeho a sociálneho výboru,

so zreteľom na stanovisko Výboru regiónov,

konajúc v súlade s riadnym legislatívnym postupom,

keďže:

(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.

(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.

(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.

---

[17] Ú. v. EÚ C [...], [...], s. [...].

(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.

(5) Existuje potreba dosiahnuť spoločný prístup k znakom skutkovej podstaty trestných činov zavedením spoločných trestných činov protiprávneho prístupu k informačným systémom, protiprávneho zásahu do systému, protiprávneho zásahu do údajov a protiprávneho zachytávania údajov.

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

(7) Je vhodné ustanoviť prísnejšie sankcie, ak je útok na informačný systém spáchaný zločineckou organizáciou, ako je stanovené v rámcovom rozhodnutí Rady 2008/841/SVV z 24. októbra 2008 o boji proti organizovanému zločinu[18], ak je útok vykonaný vo veľkom rozsahu, alebo ak je trestný čin vykonaný s utajením skutočnej identity páchateľa a spôsobil ujmu právoplatnému vlastníkovi identity. Je tiež primerané stanoviť prísnejšie sankcie, ak útok spôsobil vážne škody alebo poškodil základné záujmy.

(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.

(9) Vzhľadom na rôzne spôsoby realizovania útokov a vzhľadom na rýchly rozvoj v oblasti hardvéru a softvéru, táto smernica odkazuje na „nástroje“, ktoré môžu byť použité na spáchanie trestných činov uvedených v tejto smernici. Tieto nástroje sa týkajú napríklad škodlivého softvéru vrátane botnetov, ktoré sa používajú na spáchanie počítačových útokov.

(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.

(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 vyšetrovaniach 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.

(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

[18] Ú. v. EÚ L 300, 11.11.2008, s. 42.

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.

(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 zvýrazňujú 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.

(14) Keďže ciele tejto smernice, t. j. zabezpečiť, aby útoky na informačné systémy boli trestané vo všetkých členských štátoch účinnými, primeranými a odradzujúcimi sankciami, a zdokonaliť a podporiť súdnu spoluprácu odstránením potenciálnych komplikácií, nemožno postačujúcim spôsobom dosiahnuť na úrovni členských štátov, pretože pravidlá musia byť spoločné a kompatibilné, a preto ich možno lepšie dosiahnuť na úrovni Únie. Únia môže prijať opatrenia v súlade so zásadou subsidiarity, ako je stanovené v článku 5 Zmluvy o Európskej únie. Táto smernica neprekračuje rámec toho, čo je nevyhnutné na dosiahnutie týchto cieľov.

(15) Všetky osobné údaje spracované v súvislosti s vykonávaním tejto smernice by mali byť chránené v súlade s pravidlami ochrany údajov stanovenými v rámcovom rozhodnutí Rady 2008/977/SVV z 27. novembra 2008 o ochrane osobných údajov spracúvaných v rámci policajnej a justičnej spolupráce v trestných veciach[19] so zreteľom na tie operácie spracovávania, ktoré spadajú do jeho účinnosti, a nariadenie Európskeho parlamentu a Rady (ES) č. 45/2001 z 18. decembra 2000 o ochrane jednotlivcov so zreteľom na spracovanie osobných údajov inštitúciami a orgánmi Spoločenstva a o voľnom pohybe takýchto údajov[20].

(16) Táto smernica rešpektuje základné práva a dodržiava zásady uznané najmä v Charte základných práv Európskej únie, vrátane ochrany osobných údajov, slobody prejavu a práva na informácie, práva na spravodlivý proces, prezumpcie neviny a práva na obhajobu, ako aj zásad zákonnosti a primeranosti trestných činov a trestov. Zámerom tejto smernice je predovšetkým zabezpečiť plné dodržiavanie týchto práv a zásad a je potrebné ju primerane uplatňovať.

(17) [V súlade s článkami 1, 2, 3 a 4 Protokolu o postavení Spojeného kráľovstva a Írska s ohľadom na priestor slobody, bezpečnosti a spravodlivosti, ktorý je pripojený k Zmluve o fungovaní Európskej únie, Spojené kráľovstvo a Írsko oznámili svoje želanie zúčastniť sa na prijatí a uplatňovaní tejto smernice] ALEBO [Bez toho, aby bol dotknutý článok 4 Protokolu o postavení Spojeného kráľovstva a Írska s ohľadom na priestor slobody, bezpečnosti a spravodlivosti, Spojené kráľovstvo a Írsko sa nebudú zúčastňovať na prijatí tejto smernice a nebudú ňou viazané ani nebudú podliehať jej uplatňovaniu].

---

[19] Ú. v. EÚ L 350, 30.12.2008, s. 60.
[20] Ú. v. ES L 8, 12.1.2001, s. 1.

(18) V súlade s článkami 1 a 2 Protokolu o postavení Dánska, ktorý je pripojený k Zmluve o fungovaní Európskej únie, sa Dánsko nezúčastňuje na prijímaní tejto smernice, nie je ňou viazané ani nepodlieha jej uplatňovaniu,

PRIJALI TÚTO SMERNICU

*Článok 1*
**Predmet úpravy**

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.

*Článok 2*
**Vymedzenie pojmov**

Na účely tejto smernice sa uplatňujú tieto vymedzenia pojmov:

a) „Informačný systém“ znamená akékoľvek zariadenie alebo skupinu navzájom prepojených a súvisiacich zariadení, z ktorých jeden alebo viaceré vykonávajú automatické spracúvanie počítačových údajov podľa programu, ako aj skladovanie, spracúvanie, opätovné získavanie alebo prenos počítačových údajov prostredníctvom týchto zariadení na účely ich fungovania, používania, ochrany a údržby.

b) „Počítačové údaje“ znamenajú akékoľvek zastúpenie skutočností, informácií alebo pojmov vo forme vhodnej na spracovanie v informačnom systéme vrátane programu uspôsobeného na to, že informačný systém vykoná funkciu.

c) „Právnická osoba“ znamená akýkoľvek subjekt, ktorý má takéto postavenie podľa uplatniteľného práva, s výnimkou štátov alebo iných verejnoprávnych orgánov pri výkone štátnej moci a s výnimkou verejnoprávnych medzinárodných organizácií.

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

*Článok 3*
**Protiprávny prístup k informačným systémom**

Členské štáty prijmú nevyhnutné opatrenia, aby zabezpečili, že úmyselný prístup bez oprávnenia k celému informačnému systému alebo akejkoľvek jeho časti je trestný aspoň v prípadoch, ktoré nie sú menej závažné.

*Článok 4*
**Protiprávny zásah do systému**

Členské štáty prijmú nevyhnutné opatrenia, aby zabezpečili, že úmyselné závažné bránenie alebo prerušenie fungovania informačného systému vložením, prenosom, poškodením,

vymazaním, zhoršením, pozmenením, zadržaním alebo zneprístupnením počítačových údajov je trestné, ak je spáchané bez oprávnenia, aspoň v prípadoch, ktoré nie sú menej závažné.

*Článok 5*
**Protiprávny zásah do údajov**

Členské štáty prijmú nevyhnutné opatrenia, aby zabezpečili, že úmyselné vymazanie, poškodenie, zhoršenie, pozmenenie, zadržanie alebo zneprístupnenie počítačových údajov v informačnom systéme je trestné, ak je spáchané bez oprávnenia, aspoň v prípadoch, ktoré nie sú menej závažné.

*Článok 6*
**Protiprávne zachytávanie údajov**

Členské štáty prijmú nevyhnutné opatrenia, aby zabezpečili, že úmyselné zachytávanie údajov prostredníctvom technických prostriedkov neverejného prenosu počítačových údajov z informačného systému alebo v rámci neho vrátane elektromagnetického vysielania z informačného systému a nesúceho tieto počítačové údaje je trestné, ak je spáchané bez oprávnenia.

*Článok 7*
**Nástroje na spáchanie trestných činov**

Členské štáty prijmú nevyhnutné opatrenia, aby zabezpečili, že výroba, predaj, obstarávanie na použitie, dovoz, vlastníctvo, distribúcia alebo akékoľvek sprístupnenie týchto nástrojov je trestné, ak je spáchané úmyselne a bez oprávnenia na účely spáchania akéhokoľvek z trestných činov uvedených v článkoch 3 až 6:

a) zariadenia vrátane počítačového programu určeného alebo primárne prispôsobeného na spáchanie akýchkoľvek trestných činov uvedených v článkoch 3 až 6;

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

*Článok 8*
**Navádzanie, pomoc, podnecovanie a pokus**

1. Členské štáty zabezpečia, že navádzanie, pomoc a podnecovanie pri páchaní trestných činov, ktoré sú uvedené v článkoch 3 až 7, sú trestné.

2. Členské štáty zabezpečia, že pokus o spáchanie trestných činov, ktoré sú uvedené v článkoch 3 až 6, je trestný.

*Článok 9*
**Sankcie**

1. Členské štáty prijmú nevyhnutné opatrenia, aby zabezpečili, že za trestné činy uvedené v článkoch 3 až 8 sú uložené účinné, primerané a odradzujúce sankcie.

2. Členské štáty prijmú nevyhnutné opatrenia, aby zabezpečili, že za trestné činy uvedené v článkoch 3 až 7 bola horná hranica sadzby trestu odňatia slobody stanovená najmenej na dva roky.

*Článok 10*
**Priťažujúce okolnosti**

1. Členské štáty prijmú nevyhnutné opatrenia, aby zabezpečili, že za trestné činy uvedené v článkoch 3 až 7 bola horná hranica sadzby trestu odňatia slobody stanovená najmenej na 5 rokov, ak boli spáchané v rámci zločineckej organizácie vymedzenej v rámcovom rozhodnutí 2008/841/SVV.

2. Členské štáty prijmú 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.

3. Členské štáty prijmú nevyhnutné opatrenia, aby zabezpečili, že za trestné činy uvedené v článkoch 3 až 6 bola horná hranica sadzby trestu odňatia slobody stanovená najmenej na 5 rokov, ak boli spáchané s utajením skutočnej identity páchateľa a spôsobili ujmu právoplatnému vlastníkovi identity.

*Článok 11*
**Zodpovednosť právnických osôb**

1. Členské štáty prijmú nevyhnutné opatrenia, aby zabezpečili, že právnické osoby môžu byť trestne zodpovedné za trestné činy uvedené v článkoch 3 až 8, spáchané v ich prospech akoukoľvek osobou konajúcou buď samostatne, alebo ako súčasť orgánu právnickej osoby, ktorá má v rámci právnickej osoby vedúce postavenie, na základe:

   a) právomoci zastupovať právnickú osobu;

   b) právomoci prijímať rozhodnutia v mene právnickej osoby;

   c) právomoci vykonávať kontrolu právnickej osoby.

2. Členské štáty prijmú nevyhnutné opatrenia, aby zabezpečili, že právnické osoby môžu byť trestne zodpovedné, ak nedostatočný dozor alebo kontrola vykonávaná osobou uvedenou v odseku 1 umožnili spáchanie niektorého z trestných činov uvedených v článkoch 3 až 8 v prospech tejto právnickej osoby osobou, ktorá podlieha jej právomoci.

3. Zodpovednosť právnickej osoby podľa odsekov 1 a 2 nevylučuje trestné konanie proti fyzickým osobám, ktoré sú páchateľmi niektorého z trestných činov uvedených v článkoch 3 až 8 alebo pomocníkmi pri ich spáchaní.

*Článok 12*
**Sankcie voči právnickým osobám**

1. Členské štáty prijmú nevyhnutné opatrenia, aby zabezpečili, že právnickej osobe trestne zodpovednej podľa článku 11 ods. 1 sú uložené účinné, primerané a odradzujúce sankcie, ktoré zahŕňajú trestné alebo iné ako trestné peňažné sankcie a ktoré môžu zahŕňať iné sankcie, ako sú:

   a) vylúčenie z nároku na štátne dávky alebo pomoc;

   b) dočasný alebo trvalý zákaz výkonu obchodnej činnosti;

   c) nariadenie súdneho dohľadu;

   d) súdne rozhodnutie o zrušení;

   e) dočasné alebo trvalé zatvorenie prevádzok, ktoré sa použili na spáchanie trestného činu.

2. Členské štáty prijmú nevyhnutné opatrenia, aby zabezpečil, že právnickej osobe trestne zodpovednej podľa článku 11 ods. 2 sú uložené účinné, primerané a odradzujúce sankcie alebo opatrenia.

*Článok 13*
**Právomoc**

1. Členské štáty stanovia svoju súdnu právomoc pre trestné činy uvedené v článkoch 3 až 8, ak boli trestné činy spáchané:

   a) na celom území dotknutého členského štátu alebo jeho časti; alebo

   b) niektorým z jeho štátnych príslušníkov alebo osobou s obvyklým pobytom na území dotknutého členského štátu; alebo

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

2. Členské štáty po tom, čo stanovia súdnu právomoc podľa odseku 1 písm. a), zabezpečia, že táto súdna právomoc zahŕňa prípady, keď:

   a) páchateľ spácha trestný čin, keď je fyzicky prítomný na území dotknutého členského štátu, bez ohľadu na to, či bol trestný čin spáchaný proti informačnému systému na jeho území; alebo

   b) bol trestný čin spáchaný proti informačnému systému na území dotknutého členského štátu bez ohľadu na to, či páchateľ spáchal trestný čin, keď bol fyzicky prítomný na jeho území.

*Článok 14*
**Výmena informácií**

1. Na účely výmeny informácií, ktoré sa týkajú trestných činov uvedených v článkoch 3 až 8, a v súlade s pravidlami ochrany osobných údajov členské 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.

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.

*Článok 15*
**Monitorovanie a štatistika**

1. Členské štáty zabezpečia primeraný systém na zaznamenávanie, výrobu a poskytovanie štatistických údajov o trestných činoch uvedených v článkoch 3 až 8.

2. Tieto štatistické údaje uvedené v odseku 1 zahŕňajú minimálne počet trestných činov uvedených v článkoch 3 až 8, ktoré boli nahlásené v členských štátoch, a ďalšie kroky po týchto hláseniach a uvádzajú počet hlásených vyšetrovaných prípadov za rok, počet stíhaných osôb a počet osôb odsúdených za trestné činy uvedené v článkoch 3 až 8.

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

*Článok 16*
**Ustanovenie o zrušení rámcového rozhodnutia 2005/222/SVV**

Týmto sa zrušuje rámcové rozhodnutie 2005/222/SVV bez toho, aby boli dotknuté povinnosti členských štátov týkajúce sa lehoty na transpozíciu do vnútroštátneho práva.

Odkazy na zrušené rámcové rozhodnutie sa považujú za odkazy na túto smernicu.

*Článok 17*
**Transpozícia**

1. Členské štáty uvedú do účinnosti zákony, iné právne predpisy a správne opatrenia potrebné na dosiahnutie súladu s touto smernicou najneskôr do [dvoch rokov od prijatia]. Komisii bezodkladne oznámia znenie týchto predpisov a poskytnú jej tabuľku zhody medzi týmito predpismi a touto smernicou. Členské štáty uvedú priamo v prijatých predpisoch alebo pri ich úradnom uverejnení odkaz na túto smernicu. Podrobnosti o odkaze upravia členské štáty.

2. Členské štáty oznámia Komisii znenie hlavných ustanovení vnútroštátnych právnych predpisov, ktoré prijmú v oblasti pôsobnosti tejto smernice.

*Článok 18*
**Predkladanie správ**

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.

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.

*Článok 19*
**Nadobudnutie účinnosti**

Táto smernica nadobúda účinnosť dvadsiatym dňom po jej uverejnení v *Úradnom vestníku Európskej únie*.

*Článok 20*
**Adresáti**

Táto smernica je určená členským štátom v súlade so zmluvami.

V Bruseli

| | |
|---|---|
| *Za Európsky parlament* | *Za Radu* |
| *predseda* | *predseda* |