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

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,

po postúpení návrhu legislatívneho aktu národným parlamentom,

so zreteľom na stanovisko Európskeho hospodárskeho a sociálneho výboru ([1]),

konajúc v súlade s riadnym legislatívnym postupom ([2]),

keďže:

(1) Ciele tejto smernice sú aproximácia trestného práva členských štátov v oblasti útokov na informačné systémy ustanovením minimálnych pravidiel týkajúcich sa vymedzenia trestných činov a príslušných sankcií, ako aj zlepšenie spolupráce medzi príslušnými orgánmi vrátane policajných a iných špecializovaných orgánov presadzovania práva v členských štátoch a príslušných špecializovaných agentúr a orgánov Únie, akými sú Eurojust, Europol a jeho Európske centrum pre počítačovú kriminalitu, či Európska agentúra pre bezpečnosť sietí a informácií (ENISA).

(2) Informačné systémy sú kľúčovým prvkom politickej, sociálnej a hospodárskej interakcie v Únii. Spoločnosť je od takýchto systémov veľmi závislá a táto závislosť je čoraz väčšia. Bezproblémová prevádzka a bezpečnosť týchto systémov v Únii je rozhodujúca pre rozvoj vnútorného trhu a konkurencieschopného a inovačného hospodárstva. Zabezpečenie primeranej úrovne ochrany informačných systémov by malo byť súčasťou účinného komplexného rámca preventívnych opatrení, ktoré sprevádzajú trestnoprávnu reakciu na počítačovú kriminalitu.

(3) Útoky na informačné systémy, a najmä útoky prepojené na organizovanú trestnú činnosť, predstavujú rastúce ohrozenie na úrovni Únie a na celosvetovej úrovni, pričom sa zvyšujú obavy z potenciálnych teroristických alebo politicky motivovaných útokov na informačné systémy, ktoré sú súčasťou kritickej infraštruktúry členských štátov a Únie. Tým je ohrozené dosiahnutie bezpečnejšej informačnej spoločnosti a priestoru slobody, bezpečnosti a spravodlivosti, a preto je potrebné na úrovni Únie prijať opatrenia a na medzinárodnej úrovni zabezpečiť lepšiu spoluprácu a koordináciu.

(4) V Únii existuje množstvo kritických infraštruktúr, ktorých narušenie alebo zničenie by malo závažné cezhraničné dôsledky. Z potreby zlepšiť schopnosť ochrany kritickej infraštruktúry v Únii vyplýva, že opatrenia proti počítačovým útokom by mali dopĺňať prísne trestné sankcie odrážajúce závažnosť týchto útokov. Kritická infraštruktúra by sa mohla chápať ako zložka, systém alebo ich časť nachádzajúca sa v členských štátoch, ktorá je nevyhnutná pre zachovanie základných funkcií spoločnosti, zdravia, bezpečnosti, ochrany, kvality života obyvateľov z ekonomického a sociálneho hľadiska, ako napríklad elektrárne, dopravné siete alebo vládne siete, a ktorých narušenie alebo zničenie by malo závažné dôsledky v členskom štáte z dôvodu nemožnosti zachovať tieto funkcie.

(5) Existujú dôkazy o tendencii smerom k čoraz nebezpečnejším a opakujúcim sa rozsiahlym útokom na informačné systémy, ktoré môžu byť často pre členské štáty alebo určité funkcie verejného alebo súkromného sektora kritické. Spolu s touto tendenciou prichádza rozvoj čoraz sofistikovanejších metód, akými sú napríklad vytváranie a používanie tzv. botnetov, ktoré zahŕňa niekoľko štádií trestného činu, pričom každé takéto štádium by mohlo samo o sebe predstavovať závažné riziko pre verejné záujmy. Cieľom tejto smernice je okrem iného zaviesť trestné sankcie pre vytvorenie botnetov, konkrétne akt vytvorenia diaľkovej kontroly nad významným počtom počítačov prostredníctvom ich napadnutia škodlivým softvérom formou cielených počítačových útokov. Po svojom vytvorení sa napadnutá sieť počítačov, ktoré vytvárajú botnet, môže aktivovať bez vedomia používateľov počítača na účely spustenia rozsiahleho počítačového útoku, ktorý je zvyčajne schopný spôsobiť závažné škody, ako sa uvádza v tejto smernici. Členské štáty môžu určiť, čo podľa ich vnútroštátneho práva a praxe predstavuje závažnú škodu, ako napríklad narušenie systémových služieb zásadného spoločenského významu alebo spôsobenie veľkých finančných nákladov či strata osobných údajov alebo citlivých informácií.

(6) Rozsiahle počítačové útoky môžu spôsobiť značné hospodárske škody v dôsledku prerušenia prevádzky informačných systémov a komunikácie a v dôsledku straty alebo pozmenenia dôverných informácií alebo iných údajov, ktoré sú dôležité z obchodného hľadiska. Osobitná pozornosť by sa mala venovať zvyšovaniu povedomia inovačných malých a stredných podnikov o hrozbách súvisiacich s takýmito útokmi a ich napadnuteľnosti takýmito útokmi, a to z hľadiska ich rastúcej závislosti od riadneho fungovania a dostupnosti informačných systémov, a aj často obmedzených zdrojov pre bezpečnosť informácií.

([1]) Ú. v. EÚ C 218, 23.7.2011, s. 130.

([2]) Pozícia Európskeho parlamentu zo 4. júla 2013 (zatiaľ neuverejnená v úradnom vestníku) a rozhodnutie Rady z 22. júla 2013.

(7) Na zabezpečenie konzistentného prístupu v členských štátoch pri uplatňovaní tejto smernice je dôležité spoločné vymedzenie pojmov v tejto oblasti.

(8) Je potrebné dosiahnuť spoločný prístup k znakom skutkových podstát trestných činov zavedením spoločných trestných činov protiprávneho prístupu k informačným systémom, protiprávneho zásahu do systému, protiprávneho zásahu do údajov a protiprávneho zachytávania údajov.

(9) Zachytávanie zahŕňa, ale nemusí sa nevyhnutne obmedzovať len na odpočúvanie a monitorovanie obsahu komunikácie či jej sledovanie, získavanie obsahu údajov buď priamo, prostredníctvom prístupu a využívania informačného systému, alebo nepriamo, prostredníctvom využívania elektronického odpočúvania alebo odpočúvacieho zariadenia technickými prostriedkami.

(10) Členské štáty by mali stanoviť sankcie za útoky na informačné systémy. Tieto sankcie by mali byť účinné, primerané a odrádzajúce a mali by zahŕňať trest odňatia slobody a/alebo pokuty.

(11) Touto smernicou sa ustanovujú trestné sankcie prinajmenšom pre tie prípady, ktoré nie sú menej závažné. Členské štáty môžu určiť, čo predstavuje menej závažný prípad podľa ich vnútroštátneho práva a praxe. Za menej závažný sa môže považovať napríklad prípad, keď škoda spôsobená protiprávnym činom a/alebo riziko pre verejné alebo súkromné záujmy, akými sú napríklad integrita počítačového systému alebo počítačových údajov, alebo bezúhonnosť, práva či iné záujmy osoby, sú nepatrné alebo takej povahy, že uloženie trestnej sankcie v rámci zákonom ustanovenej sadzby alebo určenie trestnoprávnej zodpovednosti nie je potrebné.

(12) Identifikácia a oznamovanie hrozby počítačových útokov a súvisiacej napadnuteľnosti informačných systémov sú dôležité pre účinnú ochranu pred počítačovými útokmi, reakcie na ne a zvyšovanie bezpečnosti informačných systémov. Posilniť by ju mohlo aj poskytovanie stimulov na oznamovanie nedostatkov v bezpečnosti. Členské štáty by sa mali snažiť o umožnenie zákonného odhaľovania a oznamovania bezpečnostných nedostatkov.

(13) Je vhodné zaviesť prísnejšie sankcie, ak útok na informačný systém spácha zločinecká organizácia, ako sa vymedzuje v rámcovom rozhodnutí Rady 2008/841/SVV z 24. októbra 2008 o boji proti organizovanému zločinu [1], ak je útok rozsiahlej povahy a postihuje veľký počet informačných systémov vrátane prípadu, ak je jeho zámerom vytvoriť botnet, alebo ak počítačový útok spôsobuje závažnú škodu, a to aj vtedy, ak sa realizuje prostredníctvom botnetu. Je tiež vhodné ustanoviť prísnejšie sankcie, ak sa útok spácha na kritickej infraštruktúre členského štátu alebo Únie.

(14) Ďalší dôležitý prvok integrovaného prístupu proti počítačovej kriminalite predstavuje stanovenie účinných opatrení proti krádeži identity a iným trestným činom súvisiacim s identitou. Akákoľvek potreba konania zo strany Únie proti takémuto typu trestnej činnosti by sa mohla zvážiť aj v kontexte hodnotenia potreby komplexného horizontálneho nástroja Únie.

(15) V záveroch Rady z 27. až 28. novembra 2008 sa uvádza, že by sa mala v spolupráci s členskými štátmi a Komisiou vytvoriť nová stratégia, v ktorej by sa zohľadňoval 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. Zakladá sa na ňom aj táto smernica. Čo najrýchlejšie dokončenie procesu ratifikácie tohto dohovoru všetkými členskými štátmi by sa malo považovať za prioritu.

(16) 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 smernice. Tieto nástroje by mohli zahŕňať škodlivý softvér, ktorý sa používa na spáchanie počítačových útokov, vrátane nástrojov schopných vytvárať botnety. Dokonca aj v prípade, ak je takýto nástroj vhodný, či obzvlášť vhodný na páchanie niektorého z trestných činov uvedených v tejto smernici, je možné, že sa vytvoril na legitímny účel. So zámerom trestnoprávne nepostihovať tie prípady, v ktorých sú takéto nástroje vytvorené a uvedené na trh na legitímne účely, ako napríklad na testovanie spoľahlivosti produktov informačných technológií alebo bezpečnosti informačných systémov, okrem požiadavky všeobecného úmyslu musí byť splnená aj požiadavka priameho úmyslu, že tieto nástroje sa použijú na spáchanie jedného alebo viacerých trestných činov stanovených v tejto smernici.

(17) Táto smernica neukladá trestnoprávnu zodpovednosť v prípadoch, keď sú síce splnené objektívne znaky pre trestné činy uvedené v tejto smernici, ale dané činy sa spáchali bez úmyslu spáchať trestný čin, napríklad ak osoba nevie o neoprávnenosti prístupu alebo v prípade povereného testovania alebo ochrany informačných systémov, ako napríklad ak danú osobu poverí spoločnosť alebo predajca, aby otestovala silu jej bezpečnostného systému. V kontexte tejto smernice by zmluvné povinnosti alebo dohody, v ktorých sa prostredníctvom pravidiel pre používateľov alebo podmienok poskytovania služby obmedzuje prístup k informačným systémom, ako aj pracovnoprávne spory v súvislosti s prístupom do informačných systémov zamestnávateľa a ich používaním na súkromné účely, nemali viesť k trestnoprávnej zodpovednosti, ak by sa daný prístup za takýchto podmienok považoval za neoprávnený, a tak by predstavoval výlučný základ pre začatie trestného konania. Touto smernicou nie je dotknuté právo na prístup k informáciám, ktoré sa ustanovuje vo vnútroštátnom práve a práve Únie, pričom však zároveň nesmie slúžiť ako odôvodnenie nezákonného či svojvoľného prístupu k informáciám.

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

(18) Počítačové útoky by mohli uľahčovať rôzne okolnosti, napríklad ak má páchateľ v rámci svojho zamestnania prístup k bezpečnostným systémom v rámci napadnutých informačných systémov. V kontexte vnútroštátneho práva by sa takéto okolnosti mali primerane zohľadniť v rámci trestného konania.

(19) Členské štáty by mali vo svojom vnútroštátnom práve stanoviť priťažujúce okolnosti v súlade s platnými pravidlami svojich právnych systémov, ktoré sa týkajú priťažujúcich okolností. Mali by zabezpečiť, aby boli takéto priťažujúce okolnosti k dispozícii sudcom pri súdení páchateľov, aby ich mohli zohľadniť. Posúdenie týchto okolností spolu s inými skutočnosťami konkrétneho prípadu ostáva na sudcovi.

(20) Touto smernicou sa neupravujú podmienky vykonávania súdnej právomoci nad ktorýmkoľvek z trestných činov v nej uvedených, ako napríklad oznámenie obete v mieste, kde bol trestný čin spáchaný, alebo oznámenie zo štátu, na území ktorého sa nachádza miesto, kde bol trestný čin spáchaný, alebo nestíhanie páchateľa v mieste, kde bol trestný čin spáchaný.

(21) V kontexte tejto smernice sú štáty a verejnoprávne subjekty naďalej v plnom rozsahu a v súlade s platnými medzinárodnými záväzkami povinné zaručiť dodržiavanie ľudských práv a základných slobôd.

(22) 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. Tieto kontaktné miesta by mali byť schopné poskytovať účinnú pomoc, čím by sa napríklad uľahčovala výmena dostupných príslušných informácií a poskytovanie technického poradenstva alebo právnych informácií na účely vyšetrovaní alebo konaní týkajúcich sa trestných činov v oblasti informačných systémov a súvisiacich údajov, ktoré sa týkajú žiadajúceho členského štátu. Na zabezpečenie bezproblémového fungovania sietí by malo mať každé kontaktné miesto kapacitu na urýchlenú komunikáciu s kontaktným miestom iného členského štátu, ktorú by okrem iného podporoval vyškolený a dobre vybavený personál. Vzhľadom na rýchlosť, akou môžu byť rozsiahle počítačové útoky páchané, by členské štáty mali byť schopné rýchlo reagovať na naliehavé žiadosti o pomoc zo siete kontaktných miest. V takých prípadoch môže byť vhodné, aby žiadosť o informácie dopĺňal telefonický kontakt s cieľom zaistiť, aby danú žiadosť dožiadaný členský štát spracoval rýchlo a aby sa spätná väzba poskytla do ôsmich hodín.

(23) Pre predchádzanie útokom na informačné systémy a boj proti nim má veľký význam na jednej strane spolupráca medzi verejnými orgánmi a na druhej strane medzi súkromným sektorom a občianskou spoločnosťou. Je potrebné podporiť a zlepšiť spoluprácu medzi poskytovateľmi služieb, výrobcami, orgánmi presadzovania práva a justičnými orgánmi, a to pri plnom rešpektovaní zásad právneho štátu. Táto spolupráca by mohla zahŕňať podporu zo strany poskytovateľov služieb pri snahe o zachovanie potenciálnych dôkazov, pri poskytovaní prvkov pomáhajúcich odhaľovať páchateľov a ako posledná možnosť pri úplnom alebo čiastočnom vypínaní informačných systémov alebo funkcií, ktoré boli narušené alebo používané na protiprávne účely, a to v súlade s vnútroštátnym právom a praxou. Členské štáty by mali tiež zvážiť nadviazanie spolupráce a zriadenie partnerských sietí s poskytovateľmi služieb a výrobcami na výmenu informácií v súvislosti s trestnými činmi patriacimi do rozsahu pôsobnosti tejto smernice.

(24) Existuje potreba zhromažďovať porovnateľné údaje o trestných činoch uvedených v tejto smernici. Príslušné údaje by sa mali sprístupniť príslušným špecializovaným agentúram a orgánom Únie, ako napríklad Europolu a ENISA, v súlade s ich úlohami a informačnými potrebami, aby sa získal úplnejší obraz o probléme počítačovej kriminality a bezpečnosti sietí a informácií na úrovni Únie, a tým sa prispelo k vypracovaniu účinnejšieho riešenia. Členské štáty by mali predložiť Europolu a jeho Európskemu centru pre počítačovú kriminalitu informácie o spôsobe páchania trestnej činnosti na vykonanie posúdení hrozieb a strategických analýz počítačovej kriminality v súlade s rozhodnutím Rady 2009/371/SVV zo 6. apríla 2009 o zriadení Európskeho policajného úradu (Europol) ([1]). Poskytovaním informácií možno umožniť lepšie chápanie súčasných a budúcich hrozieb a tak prispieť k primeranejšiemu a adresnejšiemu rozhodovaniu o boji proti útokom na informačné systémy a predchádzaniu takýmto útokom.

(25) Komisia by mala predložiť správu o uplatňovaní tejto smernice a potrebné legislatívne návrhy, ktoré by mohli viesť k rozšíreniu rozsahu jej rozsahu pôsobnosti vzhľadom na vývoj v oblasti počítačovej kriminality. Tento vývoj by mohol zahŕňať technologický vývoj, ktorý napríklad umožní účinnejšie presadzovanie práva v oblasti útokov na informačné systémy alebo uľahčí predchádzanie takýmto útokom, či minimalizuje účinky týchto útokov. Na tento účel by mala Komisia zohľadniť dostupné analýzy a správy pripravené príslušnými aktérmi a predovšetkým Europolom a ENISA.

(26) Na účinný boj proti počítačovej kriminalite je potrebné zvýšiť odolnosť informačných systémov prijatím primeraných opatrení na ich účinnejšiu ochranu proti počítačovým útokom. Členské štáty by mali prijať potrebné opatrenia na ochranu svojej kritickej infraštruktúry pred počítačovými útokmi, v rámci čoho by mali zvážiť ochranu svojich informačných systémov a súvisiacich údajov. Zásadnou súčasťou komplexného prístupu k účinnému boju proti počítačovej kriminalite je zabezpečenie adekvátnej úrovne ochrany a bezpečnosti informačných

([1]) Ú. v. EÚ L 121, 15.5.2009, s. 37.

systémov zo strany právnických osôb, napríklad v súvislosti s poskytovaním verejne prístupných služieb elektronických komunikácií v súlade s platnými právnymi predpismi Únie v oblasti ochrany súkromia, elektronickej komunikácie a údajov. Mala by sa poskytovať primeraná úroveň ochrany v súvislosti s logicky rozpoznateľnými hrozbami a napadnuteľnými miestami v súlade s aktuálnym stavom v jednotlivých odvetviach a s konkrétnymi situáciami v oblasti spracúvania údajov. Náklady a záťaž takejto ochrany by mali byť primerané pravdepodobnej škode, ktorú by počítačový útok spôsobil dotknutým osobám. Členské štáty sa nabádajú, aby ustanovili príslušné opatrenia, na základe ktorých by v kontexte ich vnútroštátneho práva vznikala zodpovednosť v prípade, ak právnická osoba zjavne neposkytla primeranú úroveň ochrany proti počítačovým útokom.

(27) Významné medzery a rozdiely v zákonoch a trestnom konaní členských štátov v oblasti útokov na informačné systémy môžu brániť boju proti organizovanej trestnej činnosti a terorizmu a môžu skomplikovať účinnú policajnú a justičnú spoluprácu v tejto oblasti. Nadnárodný a bezhraničný charakter moderných informačných systémov znamená, že útoky na tieto systémy majú cezhraničný charakter, a tak zvýrazňujú naliehavú potrebu ďalšej aproximácie trestného práva v tejto oblasti. Koordinácia stíhania prípadov útokov na informačné systémy by mala byť okrem toho uľahčená náležitým vykonávaním a uplatňovaním rámcového rozhodnutia Rady 2009/948/SVV z 30. novembra 2009 o predchádzaní kolíziám pri výkone právomoci v trestných veciach a ich urovnávaní ([1]). Členské štáty by sa v spolupráci s Úniou mali usilovať o zlepšenie medzinárodnej spolupráce v oblasti bezpečnosti informačných systémov, počítačových sietí a počítačových údajov. V akejkoľvek medzinárodnej dohode, ktorá sa týka výmeny údajov, by sa mala riadne zohľadňovať bezpečnosť prenosu údajov a ich ukladania.

(28) V účinnom boji proti počítačovej kriminalite je nevyhnutná lepšia spolupráca medzi príslušnými orgánmi presadzovania práva a justičnými orgánmi v celej Únii. V tomto kontexte by sa malo podporovať zvýšenie úsilia pri poskytovaní primeranej odbornej prípravy príslušných orgánov s cieľom zvýšiť povedomie o počítačovej kriminalite a jej vplyve a podnietiť spoluprácu a výmenu najlepších postupov, napríklad prostredníctvom príslušných špecializovaných agentúr a orgánov Únie. Zámerom takejto odbornej prípravy by malo byť okrem iného zvyšovanie povedomia o rôznych vnútroštátnych právnych systémoch, možných právnych a technických výzvach v rámci vyšetrovania trestnej činnosti a o rozdelení právomocí medzi príslušné vnútroštátne orgány.

(29) V tejto smernici sa rešpektujú ľudské práva a základné slobody a dodržiavajú zásady uznané najmä v Charte základných práv Európskej únie a Európskom dohovore o ochrane ľudských práv a základných slobôd vrátane ochrany osobných údajov, práva na súkromie, 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 úplné dodržiavanie týchto práv a zásad a je potrebné ju primerane vykonať.

(30) Ochrana osobných údajov je základným právom v súlade s článkom 16 ods. 1 Zmluvy o fungovaní Európskej únie a článkom 8 Charty základných práv Európskej únie. Preto by malo byť každé spracovanie osobných údajov v kontexte vykonávania tejto smernice v plnom súlade s príslušným právom Únie v oblasti ochrany údajov.

(31) V súlade s článkom 3 Protokolu o postavení Spojeného kráľovstva a Írska s ohľadom na priestor slobody, bezpečnosti a spravodlivosti, ktorý je pripojený k Zmluve o Európskej únii a k Zmluve o fungovaní Európskej únie, tieto členské štáty oznámili svoje želanie zúčastniť sa na prijatí a uplatňovaní tejto smernice.

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

(33) Keďže ciele tejto smernice, a to, aby útoky na informačné systémy podliehali vo všetkých členských štátoch účinným, primeraným a odrádzajúcim trestným sankciám, a zdokonaliť a podporiť spoluprácu medzi justičnými a inými príslušnými orgánmi, nie je možné uspokojivo dosiahnuť na úrovni jednotlivých členských štátov, ale z dôvodov ich rozsahu a účinkov ich možno lepšie dosiahnuť na úrovni Únie, môže Únia prijať opatrenia v súlade so zásadou subsidiarity podľa článku 5 Zmluvy o Európskej únii. V súlade so zásadou proporcionality podľa uvedeného článku táto smernica neprekračuje rámec nevyhnutný na dosiahnutie týchto cieľov.

(34) Cieľom tejto smernice je zmeniť a rozšíriť ustanovenia rámcového rozhodnutia Rady 2005/222/SVV z 24. februára 2005 o útokoch na informačné systémy ([2]). Keďže zmeny, ktoré sa majú vykonať, sú početné a ich povaha je závažná, rámcové rozhodnutie 2005/222/SVV by sa v záujme jasnosti malo nahradiť vo svojej celistvosti vo vzťahu k členským štátom, ktoré sa zúčastňujú na prijatí tejto smernice,

([1]) Ú. v. EÚ L 328, 15.12.2009, s. 42.

([2]) Ú. v. EÚ L 69, 16.3.2005, s. 67.

PRIJALI TÚTO SMERNICU:

Článok 1

Predmet úpravy

Touto smernicou sa ustanovujú minimálne pravidlá týkajúce sa vymedzenia trestných činov a sankcií v oblasti útokov na informačné systémy. Jej cieľom je tiež uľahčiť predchádzanie takýmto trestným činom a zlepšiť spoluprácu medzi justičnými a inými príslušnými orgánmi.

Článok 2

Vymedzenie pojmov

Na účely tejto smernice sa uplatňujú tieto vymedzenia pojmov:

a) „informačný systém“ je zariadenie alebo skupina navzájom prepojených alebo súvisiacich zariadení, z ktorých jedno alebo viaceré automaticky spracúvajú počítačové údaje podľa programu, ako aj počítačové údaje, ktoré toto zariadenie alebo skupina zariadení ukladá, spracúva, opätovne získava alebo prenáša na účely svojho fungovania, používania, ochrany a údržby;

b) „počítačové údaje“ sú zastúpenia skutočností, informácií alebo pojmov vo forme vhodnej na spracovanie v informačnom systéme vrátane programu, ktorý zabezpečí, aby informačný systém vykonal funkciu;

c) „právnická osoba“ je subjekt, ktorý má postavenie právnickej osoby podľa uplatniteľného práva, ale nejde o štáty alebo verejnoprávne subjekty pri výkone štátnej moci ani o verejnoprávne medzinárodné organizácie;

d) „bez oprávnenia“ je konanie uvedené v tejto smernici vrátane prístupu, zásahu alebo zachytávania údajov, ktoré nie je povolené zo strany vlastníka či iného držiteľa práv systému alebo jeho časti, alebo ktoré nie je povolené vnútroštátnym právom.

Článok 3

Protiprávny prístup do informačných systémov

Členské štáty prijmú potrebné opatrenia na zabezpečenie toho, aby ako trestný čin bolo sankcionované úmyselné získanie prístupu do celého informačného systému alebo akejkoľvek jeho časti bez oprávnenia, ak bolo spáchané porušením bezpečnostného opatrenia, a to aspoň v prípadoch, ktoré nie sú menej závažné.

Článok 4

Protiprávny zásah do systému

Členské štáty prijmú potrebné opatrenia na zabezpečenie toho, aby ako trestný čin bolo sankcionované úmyselné závažné bránenie fungovaniu informačného systému alebo prerušenie jeho fungovania vložením počítačových údajov, prenosom, poškodením, vymazaním, zhoršením, pozmenením alebo potlačením takýchto údajov alebo ich zneprístupnením bez oprávnenia, a to aspoň v prípadoch, ktoré nie sú menej závažné.

Článok 5

Protiprávny zásah do údajov

Členské štáty prijmú potrebné opatrenia na zabezpečenie toho, aby ako trestný čin bolo sankcionované úmyselné vymazanie, poškodenie, zhoršenie, pozmenenie, potlačenie počítačových údajov v informačnom systéme alebo zneprístupnenie takýchto údajov bez oprávnenia, a to aspoň v prípadoch, ktoré nie sú menej závažné.

Článok 6

Protiprávne zachytávanie údajov

Členské štáty prijmú potrebné opatrenia na zabezpečenie toho, aby bolo ako trestný čin sankcionované úmyselné zachytávanie údajov prostredníctvom technických prostriedkov, neverejného prenosu počítačových údajov do informačného systému, z informačného systému alebo v rámci neho vrátane elektromagnetického vysielania z informačného systému nesúceho takéto počítačové údaje, ak je spáchané bez oprávnenia, a to aspoň v prípadoch, ktoré nie sú menej závažné.

Článok 7

Nástroje na spáchanie trestných činov

Členské štáty prijmú potrebné opatrenia na zabezpečenie toho, aby bola ako trestný čin sankcionovaná úmyselná výroba, predaj, obstarávanie na použitie, dovoz, distribúcia alebo akékoľvek sprístupnenie nasledujúcich nástrojov, ak je spáchaná bez oprávnenia a so zámerom, že sa uvedené nástroje použijú na spáchanie akéhokoľvek z trestných činov uvedených v článkoch 3 až 6, a to aspoň v prípadoch, ktoré nie sú menej závažné:

a) počítačový program určený alebo primárne prispôsobený na spáchanie akýchkoľvek trestných činov uvedených v článkoch 3 až 6;

b) počítačové heslo, prístupový kód alebo podobné údaje, ktorými je možné získať prístup k celému informačnému systému alebo akejkoľvek jeho časti.

Článok 8

Navádzanie, pomoc a podnecovanie a pokus

1. Členské štáty zabezpečia, aby bolo ako trestný čin sankcionované navádzanie alebo pomoc a podnecovanie na spáchanie trestného činu uvedeného v článkoch 3 až 7.

2. Členské štáty zabezpečia, aby bol ako trestný čin sankcionovaný pokus o spáchanie trestného činu uvedeného v článkoch 4 a 5.

Článok 9

Sankcie

1. Členské štáty prijmú potrebné opatrenia, aby zabezpečili, že za trestné činy uvedené v článkoch 3 až 8 sa uložia účinné, primerané a odrádzajúce trestné sankcie.

2. Členské štáty prijmú potrebné opatrenia na zabezpečenie toho, aby za trestné činy uvedené v článkoch 3 až 7 bola horná hranica sadzby trestu odňatia slobody stanovená najmenej na dva roky, a to aspoň v prípadoch, ktoré nie sú menej závažné.

3. Členské štáty prijmú potrebné opatrenia na zabezpečenie toho, aby za trestné činy uvedené v článkoch 4 a 5, pokiaľ boli spáchané úmyselne, bola horná hranica sadzby trestu odňatia slobody stanovená najmenej na tri roky v prípade, ak bolo

postihnuté veľké množstvo informačných systémov použitím nástroja uvedeného v článku 7, ktorý bol primárne určený alebo prispôsobený na tento účel.

4. Členské štáty prijmú nevyhnutné opatrenia na zabezpečenie toho, aby za trestné činy uvedené v článkoch 4 a 5 bola horná hranica sadzby trestu odňatia slobody stanovená najmenej na päť rokov, ak:

a) boli spáchané v rámci zločineckej organizácie, ako je vymedzená v rámcovom rozhodnutí 2008/841/SVV, bez ohľadu na trest v ňom uvedený;

b) spôsobili závažnú škodu alebo

c) boli spáchané na informačnom systému kritickej infraštruktúry.

5. Členské štáty prijmú potrebné opatrenia na zabezpečenie toho, aby sa prípad, keď sú trestné činy uvedené v článkoch 4 a 5 spáchané prostredníctvom zneužitia osobných údajov inej osoby s cieľom získať dôveru tretej strany a tým spôsobiť škodu právoplatnému nositeľovi identity, mohol v súlade s príslušným vnútroštátnym právom považovať za priťažujúce okolnosti, pokiaľ tieto okolnosti už nepatria pod iný trestný čin sankcionovaný podľa vnútroštátneho práva.

Článok 10

Zodpovednosť právnických osôb

1. Členské štáty prijmú potrebné opatrenia na zabezpečenie toho, aby mohli byť právnické osoby zodpovedné za trestné činy uvedené v článkoch 3 až 8, spáchané v ich prospech akoukoľvek osobou, ktorá koná buď samostatne, alebo ako súčasť orgánu právnickej osoby, a ktorá má v rámci tejto právnickej osoby vedúce postavenie, a to na základe:

a) právomoci zastupovať právnickú osobu;

b) oprávnenia prijímať rozhodnutia v mene právnickej osoby;

c) oprávnenia vykonávať kontrolu v rámci právnickej osoby.

2. Členské štáty prijmú potrebné opatrenia na zabezpečenie toho, aby mohli byť právnické osoby 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, navádzajú naň alebo sú pomocníkmi pri jeho spáchaní.

Článok 11

Sankcie voči právnickým osobám

1. Členské štáty prijmú potrebné opatrenia na zabezpečenie toho, aby sa právnickej osobe zodpovednej podľa článku 10 ods. 1 uložili účinné, primerané a odrádzajúce sankcie, ktoré zahŕňajú trestnoprávne alebo iné ako trestnoprávne pokuty a ktoré môžu zahŕňať iné sankcie, ako napríklad:

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 potrebné opatrenia na zabezpečenie toho, aby sa právnickej osobe zodpovednej podľa článku 10 ods. 2 uložili účinné, primerané a odrádzajúce sankcie alebo iné opatrenia.

Článok 12

Súdna právomoc

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

a) úplne alebo čiastočne na ich území, alebo

b) ich štátnym príslušníkom prinajmenšom v prípadoch, keď sa skutok považuje za trestný čin v mieste, kde bol spáchaný.

2. Pri stanovení súdnej právomoci podľa odseku 1 písm. a) členský štát zabezpečí, aby mal súdnu právomoc, keď:

a) páchateľ spácha trestný čin, keď je fyzicky prítomný na jeho území, bez ohľadu na to, či bol trestný čin spáchaný na informačnom systéme na jeho území, alebo

b) bol trestný čin spáchaný na informačnom systéme na jeho území bez ohľadu na to, či páchateľ spáchal trestný čin, keď bol fyzicky prítomný na jeho území.

3. Členský štát informuje Komisiu, ak sa rozhodne rozšíriť súdnu právomoc aj na trestný čin uvedený v článkoch 3 až 8 spáchaný mimo jeho územia vrátane prípadu, ak:

a) má páchateľ obvyklý pobyt na jeho území alebo

b) bol trestný čin spáchaný v prospech právnickej osoby so sídlom na jeho území.

Článok 13

Výmena informácií

1. Na účely výmeny informácií, ktoré sa týkajú trestných činov uvedených v článkoch 3 až 8, členské štáty zabezpečia, aby mali k dispozícii funkčné vnútroštátne kontaktné miesto a využívali existujúcu sieť funkčných kontaktných miest, ktoré sú k dispozícii 24 hodín denne a sedem dní v týždni. Členské štáty takisto zabezpečia, aby mali k dispozícii postupy, ktorými v prípade naliehavých žiadostí o pomoc príslušné orgány môžu uviesť do 8 hodín od ich prijatia aspoň to, či na žiadosť odpovedia, a formu odpovede a približne za aký čas.

2. Členské štáty oznámia Komisii svoje určené kontaktné miesto uvedené v odseku 1. Komisia postúpi túto informáciu ostatným členským štátom a príslušným špecializovaným agentúram a orgánom Únie.

3. Členské štáty prijmú potrebné opatrenia na zabezpečenie toho, aby sa sprístupnili primerané oznamovacie kanály s cieľom uľahčiť bezodkladné ohlasovanie trestných činov uvedených v článkoch 3 až 6 príslušným vnútroštátnym orgánom.

Článok 14

Monitorovanie a štatistika

1. Členské štáty zabezpečia, aby bol zavedený systém na zaznamenávanie, vytváranie a poskytovanie štatistických údajov o trestných činoch uvedených v článkoch 3 až 7.

2. Štatistické údaje uvedené v odseku 1 zahŕňajú minimálne existujúce údaje o počte trestných činov uvedených v článkoch 3 až 7, ktoré boli zaevidované členskými štátmi, a počte osôb, ktoré sú stíhané a odsúdené za trestné činy uvedené v článkoch 3 až 7.

3. Členské štáty zašlú Komisii údaje zozbierané podľa tohto článku. Komisia zabezpečí, aby sa uverejnil konsolidovaný prehľad štatistických hlásení a aby sa predložil príslušným špecializovaným agentúram a orgánom Únie.

Článok 15

Nahradenie rámcového rozhodnutia 2005/222/SVV

Rámcové rozhodnutie 2005/222/SVV sa týmto nahrádza vo vzťahu k členským štátom, ktoré sa zúčastňujú na prijatí tejto smernice, a to bez toho, aby boli dotknuté povinnosti členských štátov týkajúce sa lehoty na transpozíciu rámcového rozhodnutia do vnútroštátneho práva.

Vo vzťahu k členským štátom, ktoré sa zúčastňujú na prijatí tejto smernice, sa odkazy na rámcové rozhodnutie 2005/222/SVV považujú za odkazy na túto smernicu.

Článok 16

Transpozícia

1. Členské štáty uvedú do účinnosti zákony, iné právne predpisy a správne opatrenia potrebné na dosiahnutie súladu s touto smernicou do 4. septembra 2015.

2. Členské štáty zašlú Komisii znenie opatrení, ktorými sa do ich vnútroštátneho práva transponujú povinnosti, ktoré sa im ukladajú touto smernicou.

3. Členské štáty uvedú priamo v prijatých opatreniach alebo pri ich úradnom uverejnení odkaz na túto smernicu. Podrobnosti o odkaze upravia členské štáty.

Článok 17

Predkladanie správ

Komisia predloží do 4. septembra 2017 Európskemu parlamentu a Rade správu, v ktorej posúdi rozsah, v akom členské štáty prijali opatrenia nevyhnutné na dosiahnutie súladu s touto smernicou, a podľa potreby k nej pripojí legislatívne návrhy. Komisia zohľadní aj technický a právny vývoj v oblasti počítačovej kriminality, a to najmä s ohľadom na rozsah pôsobnosti tejto smernice.

Článok 18

Nadobudnutie účinnosti

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

Článok 19

Adresáti

Táto smernica je určená členským štátom v súlade so zmluvami.

V Bruseli 12. augusta 2013

Za Európsky parlament	*Za Radu*
predseda	*predseda*
M. SCHULZ	L. LINKEVIČIUS