(Akty prijaté v súlade s hlavou VI Zmluvy o založení Európskej únie)

RÁMCOVÉ ROZHODNUTIE RADY 2005/222/SVV

z 24. februára 2005

o útokoch na informačné systémy

RADA EURÓPSKEJ ÚNIE,

so zreteľom na Zmluvu o Európskej únii, a najmä na jej článok 29, článok 30 ods. 1 písm. a), článok 31 ods. 1 písm. e) a článok 34 ods. 2 písm. b),

so zreteľom na návrh Komisie,

so zreteľom na stanovisko Európskeho parlamentu [1],

keďže:

(1) Cieľom tohto rámcového rozhodnutia je zlepšiť spoluprácu medzi súdnymi a inými príslušnými orgánmi, vrátane policajných a iných špecializovaných orgánov členských štátov činných v trestnom konaní, prostredníctvom aproximácie pravidiel trestného práva v členských štátoch v oblasti útokov na informačné systémy.

(2) Existuje dôkaz o útokoch na informačné systémy najmä ako výsledok hrozby zo strany organizovaného zločinu a rastúca obava z potenciálnych teroristických útokov na informačné systémy, ktoré tvoria časť kritickej infraštruktúry členských štátov. Toto predstavuje hrozbu dosiahnutia bezpečnejšej informačnej spoločnosti a priestoru slobody, bezpečnosti a spravodlivosti, a preto si vyžaduje reakciu na úrovni Európskej únie.

(3) Účinná reakcia na tieto hrozby si vyžaduje komplexný prístup k bezpečnosti sietí a informácií, ako je zdôraznené v Akčnom pláne *e*Europe a v oznámení Komisie Bezpečnosť sietí a informácií: Návrh prístupu tvorby európskej politiky a v uznesení Rady z 28. januára 2002 o spoločnom prístupe a špecifických činnostiach v oblasti bezpečnosti sietí a informácií [2].

(4) Potreba ďalšieho zvyšovania povedomia o problémoch týkajúcich sa informačnej bezpečnosti a poskytovania praktickej pomoci bola taktiež zdôraznená v uznesení Európskeho parlamentu z 5. septembra 2001.

(5) Významné medzery a rozdiely v právnych predpisoch členských štátov v tejto oblasti môžu brániť boju proti organizovanému zločinu a terorizmu a môžu skomplikovať účinnú policajnú a súdnu spoluprácu v oblasti útokov na informačné systémy. Nadnárodný a bezhraničný charakter moderných informačných systémov znamená, že útoky proti týmto systémom sú často cezhraničného charakteru, a tak zvýrazňujú naliehavú potrebu ďalšej aproximácie trestných právnych predpisov v tejto oblasti.

(6) Akčný plán Rady a Komisie o tom, ako najlepšie vykonať ustanovenia Amsterdamskej zmluvy o priestore slobody, bezpečnosti a spravodlivosti [3], Európska rada v Tampere z 15. a 16. októbra 1999, Európska rada v Santa Maria da Feira z 19. a 20. júna 2000, Komisia vo svojej „výsledkovej tabuľke“ a Európsky parlament vo svojom uznesení z 19. mája 2000 poukazujú alebo vyzývajú na legislatívnu činnosť na potlačenie trestnej činnosti páchanej modernými technológiami vrátane spoločných definícií, obvinení a sankcií.

(7) Je dôležité doplniť činnosť medzinárodných organizácií, najmä činnosť Rady Európy o aproximácii trestných právnych predpisov a činnosť G8 o nadnárodnej spolupráci v oblasti trestnej činnosti páchanej modernými technológiami, poskytnutím spoločného prístupu v Európskej únii v tejto oblasti. Táto výzva bola ďalej rozpracovaná v oznámení Komisie Rade, Európskemu parlamentu, Hospodárskemu a sociálnemu výboru a Výboru regiónov o „vytváraní bezpečnejšej informačnej spoločnosti zdokonaľovaním bezpečnosti informačných infraštruktúr a boja proti počítačovej trestnej činnosti“.

(8) Trestné právo v oblasti útokov na informačné systémy by malo byť aproximované, aby sa zabezpečila v čo najväčšej možnej miere policajná a súdna spolupráca v oblasti trestných činov spojených s útokmi na informačné systémy a aby sa prispelo k boju proti organizovanému zločinu a terorizmu.

[1] Ú. v. EÚ C 300 E, 11.12.2003, s. 26.
[2] Ú. v. ES C 43, 16.2.2002, s. 2.
[3] Ú. v. ES C 19, 23.1.1999, s. 1.

(9) Všetky členské štáty ratifikovali Dohovor Rady Európy z 28. januára 1981 o ochrane jednotlivcov pri automatizovanom spracovaní osobných údajov. Osobné údaje spracované v súvislosti s vykonávaním tohto rámcového rozhodnutia by mali byť chránené v súlade so zásadami uvedeného dohovoru.

(10) Spoločné definície v tejto oblasti, najmä informačných systémov a počítačových údajov, sú dôležité na zabezpečenie konzistentného prístupu v členských štátoch pri uplatňovaní tohto rámcového rozhodnutia.

(11) Existuje potreba dosiahnuť spoločný prístup k znakom skutkovej podstaty trestných činov spoločným ustanovením trestných činov protiprávneho prístupu k informačnému systému, protiprávneho zásahu do systému a protiprávneho zásahu do údajov.

(12) V záujme boja proti počítačovým trestným činom by mal každý členský štát zabezpečiť účinnú súdnu spoluprácu, pokiaľ ide o trestné činy založené na typoch správania uvedených v článkoch 2, 3, 4 a 5.

(13) Existuje potreba vyhnúť sa prílišnej kriminalizácii, najmä v prípadoch menšej závažnosti, ako aj potreba vyhnúť sa kriminalizácii držiteľov práv a oprávnených osôb.

(14) Existuje potreba členských štátov ustanoviť sankcie za útoky na informačné systémy. Takto upravené sankcie musia byť účinné, primerané a odradzujúce.

(15) Je primerané stanoviť prísnejšie tresty, ak bol útok na informačné systémy spáchaný v rámci zločineckej organizácie, ako je definované v jednotnej akcii 98/733/SVV z 21. decembra 1998, ktorou sa stanovuje, že účasť v zločineckej organizácii je v členských štátoch Európskej únie trestným činom [1]. Je tiež primerané stanoviť prísnejšie tresty, ak útok spôsobil vážne škody alebo poškodil základné záujmy.

(16) Mali by sa tiež pripravovať opatrenia zamerané na účely spolupráce medzi členskými štátmi s cieľom zabezpečiť účinnú akciu proti útokom na informačné systémy. Členské štáty by mali preto využiť existujúcu sieť operačných kontaktných miest, uvedených v odporúčaní Rady z 25. júna 2001 o kontaktných miestach, ktoré udržujú dvadsaťštyrihodinovú službu pre boj s trestnou činnosťou páchanou modernými technológiami [2], na výmenu informácií.

(17) Keďže ciele tohto rámcového rozhodnutia, ktorým sa zabezpečuje, že útoky na informačné systémy budú sankcionované vo všetkých členských štátoch účinnými, primeranými a odradzujúcimi trestami, a zdokonaľuje sa a podporuje súdna spolupráca odstránením potenciálnych komplikácií, nemožno postačujúcim spôsobom dosiahnuť členskými štátmi, 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 založení ES. V súlade so zásadou proporcionality, ako je uvedené v citovanom článku, toto rámcové rozhodnutie nepresahuje rámec toho, čo je potrebné na dosiahnutie týchto cieľov.

(18) Toto rámcové rozhodnutie rešpektuje základné práva a dodržiava zásady uznané v článku 6 Zmluvy o Európskej únii a vyjadrené v Charte základných práv Európskej únie, najmä v jej kapitolách II a VI,

PRIJALA TOTO RÁMCOVÉ ROZHODNUTIE:

Článok 1

Vymedzenie pojmov

Na účely tohto rámcového rozhodnutia sa uplatňujú tieto vymedzené pojmy:

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.

[1] Ú. v. ES L 351, 29.12.1998, s. 1.

[2] Ú. v. ES C 187, 3.7.2001, s. 5.

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

Článok 2

Protiprávny prístup k informačnému systému

1. Každý členský štát prijme nevyhnutné opatrenia, aby zabezpečil, že úmyselný prístup bez oprávnenia na celý informačný systém alebo akúkoľvek jeho časť je trestný aspoň v prípadoch, ktoré nie sú menej závažné.

2. Každý členský štát sa môže rozhodnúť, že konanie uvedené v odseku 1 je trestné, len ak je trestný čin spáchaný porušením bezpečnostného opatrenia.

Článok 3

Protiprávny zásah do systému

Každý členský štát prijme nevyhnutné opatrenia, aby zabezpečil, 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 pre prípady, ktoré nie sú menej závažné.

Článok 4

Protiprávny zásah do údajov

Každý členský štát prijme nevyhnutné opatrenia, aby zabezpečil, 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 5

Navádzanie, pomoc, podnecovanie a pokus

1. Každý členský štát zabezpečí, že navádzanie, pomoc a podnecovanie pri páchaní trestných činov, ktoré sú uvedené v článkoch 2, 3 a 4, sú trestné.

2. Každý členský štát zabezpečí, že pokus o spáchanie trestných činov, ktoré sú uvedené v článkoch 2, 3 a 4, je trestný.

3. Každý členský štát sa môže rozhodnúť neuplatňovať odsek 2 pre trestné činy uvedené v článku 2.

Článok 6

Sankcie

1. Každý členský štát prijme nevyhnutné opatrenia, ktorými zabezpečí, aby sa za trestné činy uvedené v článkoch 2, 3, 4 a 5 ukladali účinné, primerané a odradzujúce tresty.

2. Každý členský štát prijme nevyhnutné opatrenia, ktorými zabezpečí, aby sa za trestné činy uvedené v článkoch 3 a 4 ukladali tresty odňatia slobody s hornou hranicou najmenej 1 až 3 roky.

Článok 7

Priťažujúce okolnosti

1. Každý členský štát prijme nevyhnutné opatrenia, ktorými zabezpečí, aby sa za trestné činy uvedené v článku 2 ods. 2 a trestné činy uvedené v článkoch 3 a 4 ukladali tresty odňatia slobody s hornou hranicou najmenej 2 až 5 rokov, ak boli spáchané v rámci zločineckej organizácie, ako je definované v jednotnej akcii 98/733/SVV mimo úrovne tam uvedených trestov.

2. Členský štát môže tiež prijať opatrenia uvedené v odseku 1, ak sa trestným činom spôsobili vážne škody alebo boli poškodené základné záujmy.

Článok 8

Zodpovednosť právnických osôb

1. Každý členský štát prijme nevyhnutné opatrenia, aby zabezpečil, že právnické osoby môžu byť trestne zodpovedné za trestné činy uvedené v článkoch 2, 3, 4 a 5, 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; alebo

b) právomoci prijímať rozhodnutia v mene právnickej osoby; alebo

c) právomoci vykonávať kontrolu právnickej osoby.

2. Okrem prípadov upravených v odseku 1 členské štáty zabezpečia, aby právnické osoby mohli byť trestne zodpovedné, ak nedostatočný dozor alebo kontrola vykonávaná osobou uvedenou v odseku 1 umožnili spáchanie trestného činu uvedeného v článkoch 2, 3, 4 a 5 v prospech tejto právnickej osoby osobou, ktorá podlieha jej právomoci.

3. Zodpovednosť právnických osôb podľa odsekov 1 a 2 nevylučuje trestné stíhanie fyzických osôb, ktoré sú páchateľmi, navádzačmi alebo pomocníkmi niektorého z trestných činov uvedených v článkoch 2, 3, 4 a 5.

Článok 9

Sankcie pre právnické osoby

1. Každý členský štát prijme nevyhnutné opatrenia, aby zabezpečil, že právnickej osobe trestne zodpovednej podľa článku 8 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) umiestnenie pod súdny dohľad; alebo

d) súdne rozhodnutie o likvidácii.

2. Každý členský štát prijme nevyhnutné opatrenia, aby zabezpečil, že právnickej osobe trestne zodpovednej podľa článku 8 ods. 2 sú uložené účinné, primerané a odradzujúce sankcie alebo opatrenia.

Článok 10

Súdna právomoc

1. Každý členský štát založí svoju súdnu právomoc, pokiaľ ide o trestné činy uvedené v článkoch 2, 3, 4 a 5, ak boli trestné činy spáchané:

a) na celom jeho území alebo jeho časti; alebo

b) niektorým z jeho štátnych príslušníkov; alebo

c) v prospech právnickej osoby, ktorá má svoje ústredie na území tohto členského štátu.

2. Každý členský štát po tom, čo stanoví svoju súdnu právomoc podľa odseku 1 písm. a), zabezpečí, že táto súdna právomoc zahŕňa prípady, keď:

a) páchateľ spácha trestný čin, keď je fyzicky prítomný na jeho území, 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 jeho území bez ohľadu na to, či páchateľ spáchal trestný čin, keď bol fyzicky prítomný na jeho území.

3. Členský štát, ktorý podľa svojich právnych predpisov ešte nevydáva alebo neodovzdáva svojich štátnych príslušníkov na trestné stíhanie, prijme nevyhnutné opatrenia na stanovenie svojej súdnej právomoci, a ak je to vhodné, na stíhanie trestných činov uvedených v článkoch 2, 3, 4 a 5, ak sú spáchané jeho vlastnými štátnymi príslušníkmi mimo jeho územia.

4. Ak trestný čin patrí do súdnej právomoci viac ako jedného členského štátu a ak akýkoľvek z dotknutých členských štátov môže účinne stíhať na základe rovnakých faktov, dotknuté členské štáty spolupracujú s cieľom určenia, ktorý z nich bude stíhať páchateľov s cieľom, ak je to možné, sústrediť trestné konania v jedinom členskom štáte. Na tento účel sa členské štáty môžu obrátiť na akýkoľvek orgán alebo mechanizmus ustanovený v rámci Európskej únie s cieľom uľahčiť spoluprácu medzi svojimi súdnymi orgánmi a koordináciu svojich činností. Nasledujúce faktory môžu byť zohľadnené postupným spôsobom:

— príslušný členský štát bude ten, na ktorom území boli spáchané trestné činy podľa odseku 1 písm. a) a odseku 2,

— príslušný členský štát bude ten, ktorého štátnym príslušníkom je páchateľ,

— príslušný členský štát bude ten, na ktorého území bol páchateľ zadržaný.

5. Členský štát môže rozhodnúť neuplatňovať alebo uplatňovať len v osobitných prípadoch alebo okolnostiach pravidlá súdnej právomoci ustanovené v odseku 1 písm. b) a c).

6. Členské štáty oznámia generálnemu sekretariátu Rady a Komisii, keď sa rozhodnú uplatniť odsek 5, ak je to potrebné, s uvedením osobitných prípadov alebo okolností, za ktorých sa rozhodnutie uplatňuje.

Článok 11

Výmena informácií

1. Na účely výmeny informácií, ktoré sa týkajú trestných činov uvedených v článkoch 2, 3, 4 a 5, a v súlade s pravidlami na ochranu osobných údajov členské štáty zabezpečia využívanie existujúcej siete operačných kontaktných miest, ktoré sú k dispozícii dvadsaťštyri hodín denne a sedem dní v týždni.

2. Každý členský štát oznámi generálnemu sekretariátu Rady a Komisii svoje určené kontaktné miesto na účely výmeny informácií o trestných činoch, ktoré sa týkajú útokov na informačné systémy. Generálny sekretariát bezodkladne odovzdá túto informáciu ostatným členským štátom.

Článok 12

Vykonanie

1. Členské štáty prijmú všetky nevyhnutné opatrenia potrebné na dosiahnutie súladu s ustanoveniami tohto rámcového rozhodnutia do 16 marca 2007.

2. Do 16 marca 2007 členské štáty doručia generálnemu sekretariátu Rady a Komisii text akýchkoľvek ustanovení, ktoré transponujú do ich vnútroštátneho práva povinnosti, ktoré im ukladá toto rámcové rozhodnutie. Do 16 septembra 2007, na základe správy vypracovanej podľa týchto údajov a správy Komisie, Rada zhodnotí, do akej miery členské štáty dosiahli súlad s ustanoveniami tohto rámcového rozhodnutia.

Článok 13

Nadobudnutie účinnosti

Toto rámcové rozhodnutie nadobúda účinnosť dňom jeho uverejnenia v *Úradnom vestníku Európskej únie*.

V Bruseli 24. februára 2005

Za Radu

predseda

N. SCHMIT