

(Akty přijaté podle hlavy VI Smlouvy o Evropské unii)

RÁMCOVÉ ROZHODNUTÍ RADY 2005/222/SVV

ze dne 24. února 2005

o útocích proti informačním systémům

RADA EVROPSKÉ UNIE,

s ohledem na Smlouvu o Evropské unii, a zejména na článek 29, čl. 30 odst. 1 písm. a), čl. 31 odst. 1 písm. e) a čl. 34 odst. 2 písm. b) této smlouvy,

s ohledem na návrh Komise,

s ohledem na stanovisko Evropského parlamentu⁽¹⁾,

vzhledem k těmto důvodům:

- (1) Cílem tohoto rámcového rozhodnutí je zlepšit spolupráci mezi justičními a jinými příslušnými orgány, včetně policie a dalších donucovacích orgánů členských států, prostřednictvím sbližování trestněprávních předpisů v členských státech v oblasti útoků proti informačním systémům.
- (2) Existují důkazy o útocích proti informačním systémům, zejména v důsledku hrozby organizované trestné činnosti, a rostoucí obavy z možných teroristických útoků proti informačním systémům, které tvoří součást kritické infrastruktury členských států. To představuje hrozbu z hlediska dosažení bezpečnější informační společnosti a prostoru svobody, bezpečnosti a práva, a proto vyžaduje reakci na úrovni Evropské unie.
- (3) Účinná reakce na tyto hrozby vyžaduje komplexní přístup k síťové a informační bezpečnosti, jak je zdůrazněno v akčním plánu eEvropa ve sdělení Komise „Síťová a informační bezpečnost: návrh přístupu evropské politiky“ a v usnesení Rady ze dne 28. ledna 2002 o společném přístupu a konkrétních krocích v oblasti síťové a informační bezpečnosti⁽²⁾.
- (4) Potřeba dále zvyšovat povědomí o otázkách souvisejících s informační bezpečností a poskytovat praktickou pomoc byla rovněž zdůrazněna v usnesení Evropského parlamentu ze dne 5. září 2001.

(5) Významné mezery a rozdíly v právních předpisech členských států v této oblasti mohou ztěžovat boj proti organizované trestné činnosti a terorismu a mohou komplikovat účinnou policejní a soudní spolupráci v oblasti útoků proti informačním systémům. Nadnárodní a bezhraniční povaha moderních informačních systémů znamená, že útoky proti takovým systémům jsou často přeshraničního rázu, což zdůrazňuje naléhavou potřebu dalších kroků pro sbližování trestněprávních předpisů v této oblasti.

(6) Akční plán Rady a Komise o tom, jak nejlépe provést ustanovení Amsterodamské smlouvy o prostoru svobody, bezpečnosti a práva⁽³⁾, závěry Evropské rady z Tampere konané ve dnech 15.–16. října 1999, závěry Evropské rady ze Santa Maria da Feira konané ve dnech 19.–20. června 2000, stejně jako Komise ve svém „vysvědčení“ a Evropský parlament ve svém usnesení ze dne 19. května 2000 uvádějí nebo vyzývají k legislativním krokům proti trestné činnosti v oblasti špičkové techniky, včetně společných definic, obvinění a sankcí.

(7) Je nutné doplnit práci vykonanou mezinárodními organizacemi, zejména práci Rady Evropy na sbližování trestního práva a práci skupiny G8 na nadnárodní spolupráci v oblasti trestné činnosti v oblasti špičkové techniky, zajištěním společného přístupu v této oblasti v rámci Evropské unie. Tato výzva byla dále rozvinuta sdělením Komise Radě, Evropskému parlamentu, Hospodářskému a sociálnímu výboru a Výboru regionů o „Vytvoření bezpečnější informační společnosti zlepšením bezpečnosti informačních infrastruktur a bojem proti počítačové trestné činnosti“.

(8) Mělo by dojít ke sblížení trestního práva v oblasti útoků proti informačním systémům, aby se zajistila co možná nejširší policejní a soudní spolupráce v oblasti trestních činů souvisejících s útoky proti informačním systémům a aby se přispělo k boji proti organizované trestné činnosti a terorismu.

⁽¹⁾ Úř. věst. C 300 E, 11.12.2003, s. 26.

⁽²⁾ Úř. věst. C 43, 16.2.2002, s. 2.

⁽³⁾ Úř. věst. C 19, 23.1.1999, s. 1.

- (9) Všechny členské státy ratifikovaly úmluvu Rady Evropy ze dne 28. ledna 1981 o ochraně osob se zřetelem na automatizované zpracování osobních dat. Osobní údaje zpracované v rámci provádění tohoto rámcového rozhodnutí by měly být chráněny v souladu se zásadami uvedené úmluvy.
- (10) Společné definice v této oblasti, zejména definice informačních systémů a počítačových dat, jsou důležité v zájmu zajištění jednotného přístupu v členských státech při používání tohoto rámcového rozhodnutí.
- (11) Je třeba dosáhnout společného přístupu ke znakům skutkových podstat trestných činů a stanovit tak společné trestné činy protiprávního přístupu do informačního systému, protiprávního zásahu do systému a protiprávního zásahu do dat.
- (12) V zájmu boje proti počítačové trestné činnosti by měl každý členský stát zajistit účinnou soudní spolupráci ve vztahu k trestným činům založeným na družích jednání uvedených v člancích 2, 3, 4 a 5.
- (13) Je třeba zamezit přílišné kriminalizaci, zejména v případech menšího významu, jakož i zamezit kriminalizaci držitelů práv a oprávněných osob.
- (14) Je třeba, aby členské státy stanovily sankce za útoky proti informačním systémům. Tyto sankce musí být účinné, přiměřené a odrazující.
- (15) Je vhodné stanovit přísnější sankce v případech spáchání útoku proti informačnímu systému v rámci zločinného spolčení, jak je vymezeno ve společné akci 98/733/SVV ze dne 21. prosince 1998, kterou se stanoví, že účast na zločinném spolčení je v členských státech Evropské unie trestným činem⁽¹⁾. Je rovněž vhodné stanovit přísnější sankce pro případy útoku, který způsobil vážné škody nebo poškodil základní zájmy.
- (16) Měla by také být učiněna opatření za účelem spolupráce mezi členskými státy v zájmu zajištění účinných kroků proti útokům proti informačním systémům. Členské státy

by proto měly za účelem výměny informací využít dosa-
vadní síť operativních kontaktních míst uvedených
v doporučení Rady ze dne 25. června 2001
o nepřetržité službě kontaktních míst pro boj proti
trestné činnosti páchané prostřednictvím pokročilých
technologií⁽²⁾.

- (17) Jelikož cílů tohoto rámcového rozhodnutí, tedy zajištění
trestání útoků proti informačním systémům ve všech
členských státech účinnými, přiměřenými a odrazujícími
tresty a zdokonalení a podpory soudní spolupráce odstra-
něním případných komplikací, nemůže být uspokojivě
dosaženo na úrovni členských států, protože pravidla
musejí být společná a slčitelná, a může jich být lépe
dosaženo na úrovni Unie, může Unie přijmout opatření
v souladu se zásadou subsidiarity podle článku 5
Smlouvy o ES. V souladu se zásadou proporcionality,
jak je stanovena v uvedeném článku, toto rozhodnutí
nepřekračuje rámec toho, co je pro dosažení uvedených
cílů nezbytné.
- (18) Toto rámcové rozhodnutí respektuje základní práva
a dodržuje zásady uznané článkem 6 Smlouvy
o Evropské unii a vyjádřené v Listině základních práv
Evropské unie, a zejména v kapitolách II a VI této listiny,

PŘIJALA TOTO RÁMCOVÉ ROZHODNUTÍ:

Článek 1

Definice

Pro účely tohoto rámcového rozhodnutí se rozumí:

- a) „informačním systémem“ jakýkoli přístroj nebo skupina
vzájemně propojených nebo přidružených přístrojů,
z nichž jeden nebo více provádí na základě programu auto-
matické zpracování počítačových dat, jakož i data těmito
přístroji uložená, zpracovaná, opětovně vyhledaná nebo
přenesená za účelem jejich provozu, použití, ochrany
a údržby;
- b) „počítačovými daty“ jakékoli zachycení skutečností, údajů
nebo pojmů ve formě vhodné ke zpracování informačním
systémem, včetně programu vhodného k zajištění provedení
nějaké funkce informačním systémem;
- c) „právní osobou“ každý právní subjekt, který má toto
postavení podle platného vnitrostátního práva, s výjimkou
států nebo jiných veřejnoprávních subjektů jednajících při
výkonu státní moci a s výjimkou organizací mezinárodního
práva veřejného;

⁽¹⁾ Úř. věst. L 351, 29.12.1998, s. 1.

⁽²⁾ Úř. věst. C 187, 3.7.2001, s. 5.

d) „neoprávněným“ přístup nebo zásah, který není povolen majitelem systému či jiným držitelem práv k systému nebo k jeho části nebo který není povolen vnitrostátními právními předpisy.

Článek 2

Protiprávní přístup k informačním systémům

1. Každý členský stát přijme nezbytná opatření k zajištění toho, aby neoprávněný úmyslný přístup k celému informačnímu systému nebo k některé jeho části byl trestným činem, a to alespoň pokud se nejedná o případ menšího významu.

2. Každý členský stát může rozhodnout, že jednání uvedené v odstavci 1 je trestné, pouze pokud bylo spácháno překonáním bezpečnostního opatření.

Článek 3

Protiprávní zásah do systému

Každý členský stát přijme nezbytná opatření k zajištění toho, aby úmyslné závažné narušení nebo přerušení fungování informačního systému vložením, přenosem, poškozením, vymazáním, znehodnocením, pozměněním, potlačením nebo znepřístupněním počítačových dat, je-li spácháno neoprávněně, bylo trestným činem, a to alespoň pokud se nejedná o případy menšího významu.

Článek 4

Protiprávní zásah do dat

Každý členský stát přijme nezbytná opatření k zajištění toho, aby úmyslné vymazání, poškození, znehodnocení, pozměnění, potlačení nebo znepřístupnění počítačových dat v informačním systému bylo trestným činem, je-li spácháno neoprávněně, a to alespoň pokud se nejedná o případy menšího významu.

Článek 5

Návod, pomoc, účastenství a pokus

1. Každý členský stát přijme opatření nezbytná k zajištění trestnosti návodu, pomoci a účastenství na spáchání trestných činů uvedených v článcích 2, 3 a 4.

2. Každý členský stát přijme opatření nezbytná k zajištění trestnosti pokusu o spáchání trestných činů uvedených v článcích 2, 3 a 4.

3. Každý členský stát se může rozhodnout nepoužít odstavec 2 pro trestné činy uvedené v článku 2.

Článek 6

Sankce

1. Každý členský stát přijme nezbytná opatření k zajištění toho, aby za trestné činy uvedené v článcích 2, 3, 4 a 5 bylo možné uložit účinné, přiměřené a odrazující tresty.

2. Každý členský stát přijme nezbytná opatření k zajištění toho, aby se na trestné činy uvedené v článcích 3 a 4 vztahovaly tresty odnětí svobody s horní hranicí trestní sazby nejméně 1 až 3 roky.

Článek 7

Přítěžující okolnosti

1. Každý členský stát přijme nezbytná opatření k zajištění toho, aby se na trestný čin uvedený v čl. 2 odst. 2 a na trestné činy uvedené v článcích 3 a 4 vztahovaly tresty odnětí svobody s horní hranicí trestní sazby nejméně 2 až 5 let, pokud byly spáchány v rámci zločinného spolčení, jak je vymezeno ve společné akci 98/733/SVV, a to nezávisle na výši trestů v ní uvedených.

2. Členský stát může rovněž přijmout opatření uvedená v odstavci 1, pokud trestný čin způsobil vážné škody nebo poškodil základní zájmy.

Článek 8

Odpovědnost právnických osob

1. Každý členský stát přijme nezbytná opatření, aby zajistil, že právnické osoby lze činit odpovědnými za trestné činy uvedené v článcích 2, 3, 4 a 5, které v jejich prospěch spáchá jakákoli osoba jednající samostatně nebo jako člen orgánu dotyčné právnické osoby, která v této právnické osobě působí ve vedoucím postavení na základě:

a) oprávnění zastupovat tuto právnickou osobu, nebo

b) pravomoci přijímat rozhodnutí jménem této právnické osoby, nebo

c) pravomoci vykonávat kontrolu v rámci této právnické osoby.

2. Kromě případů uvedených v odstavci 1 přijme každý členský stát opatření nezbytná k zajištění odpovědnosti právnických osob v případech, kdy nedostatek dohledu nebo kontroly ze strany osoby uvedené v odstavci 1 umožnil spáchání některého z trestných činů uvedených v článcích 2, 3, 4 a 5 ve prospěch uvedené právnické osoby osobou jí podřízenou.

3. Odpovědnost právnických osob podle odstavců 1 a 2 nevylučuje trestní stíhání fyzických osob, které jsou pachateli, návodci nebo účastníky při spáchání některého z trestných činů uvedených v člancích 2, 3, 4 a 5.

Článek 9

Sankce ukládané právnickým osobám

1. Členské státy přijmou nezbytná opatření k zajištění toho, aby právnickou osobu odpovědnou podle čl. 8 odst. 1 bylo možné postihnout účinnými, přiměřenými a odrazujícími sankcemi, které zahrnují pokuty trestní nebo jiné povahy a mohou zahrnovat jiné sankce, například:

- a) zbavení oprávnění pobírat veřejné výhody nebo podpory;
- b) dočasný nebo trvalý zákaz provozování obchodních činností;
- c) uložení soudního dohledu, nebo
- d) zrušení rozhodnutím soudu.

2. Každý členský stát přijme nezbytná opatření k zajištění toho, aby právnickou osobu odpovědnou podle čl. 8 odst. 2 bylo možné postihnout účinnými, přiměřenými a odrazujícími sankcemi nebo opatřeními.

Článek 10

Soudní pravomoc

1. Členský stát stanoví svou soudní pravomoc pro trestné činy uvedené v člancích 2, 3, 4 a 5, je-li

- a) trestný čin zcela nebo zčásti spáchán na jeho území, nebo
- b) pachatel jeho státním příslušníkem, nebo
- c) trestný čin spáchán ve prospěch právnické osoby, která má své sídlo na území daného členského státu.

2. Při stanovení své soudní pravomoci podle odst. 1 písm. a) každý členský stát zajistí, aby zahrnovala případy, kdy

- a) pachatel trestný čin spáchal v době své fyzické přítomnosti na jeho území, a to bez ohledu na to, zda byl trestný čin namířen proti informačnímu systému na jeho území či nikoli, nebo
- b) trestný čin byl namířen proti informačnímu systému na jeho území, a to bez ohledu na to, zda pachatel spáchal trestný čin v době své fyzické přítomnosti na jeho území či nikoli.

3. Členský stát, který v souladu se svými právními předpisy dosud nevydává nebo nepředává své státní příslušníky, přijme

opatření nezbytná pro stanovení své soudní pravomoci a stíhání za trestný čin uvedený v člancích 2, 3, 4 a 5, je-li trestný čin spáchán jeho státním příslušníkem mimo jeho území.

4. Spadá-li trestný čin do soudní pravomoci více členských států a může-li každý z těchto členských států vést účinné trestní stíhání na základě stejných skutečností, spolupracují dotyčné členské státy při rozhodování, který z nich bude pachatele stíhat, aby se soudní řízení pokud možno soustředilo v jednom členském státě. Za tímto účelem se členské státy mohou obracet ke kterékoli instituci nebo využít kteréhokoli mechanismu, který byl k tomuto účelu v Evropské unii zřízen, aby tak usnadnily spolupráci svých soudních orgánů a koordinaci jejich postupu. Postupně je brán zřetel na tyto faktory:

— příslušným členským státem je ten, na jehož území byly trestné činy spáchány podle odst. 1 písm. a) a odstavce 2,

— příslušným členským státem je ten, jehož je pachatel státním příslušníkem,

— příslušným členským státem je ten, na jehož území byl pachatel zadržen.

5. Členský stát se může rozhodnout nepoužít úpravu soudní pravomoci uvedenou v odst. 1 písm. b) a odst. 1 písm. c) nebo ji použít pouze pro konkrétní případy nebo okolnosti.

6. Členské státy uvědomí Generální sekretariát Rady a Komisi, pokud se rozhodnou použít odstavce 5, přičemž v případě potřeby uvedou, pro které konkrétní případy a okolnosti toto rozhodnutí platí.

Článek 11

Výměna informací

1. Za účelem výměny informací týkajících se trestných činů uvedených v člancích 2, 3, 4 a 5 a v souladu s pravidly ochrany údajů členské státy využívají stávající síť operativních kontaktních míst s nepřetržitým provozem.

2. Každý členský stát uvědomí Generální sekretariát Rady a Komisi o jím stanoveném kontaktním místě pro výměny informací o trestných činech souvisejících s útoky proti informačním systémům. Generální sekretariát informací předá ostatním členským státům.

Článek 12**Provedení**

1. Členské státy přijmou opatření nezbytná pro dosažení souladu s tímto rámcovým rozhodnutím do 16. března 2007.

2. Členské státy sdělí do 16. března 2007 Generálnímu sekretariátu Rady a Komisi znění předpisů, kterými ve svém vnitrostátním právu provádějí povinnosti, jež pro ně vyplývají z tohoto rámcového rozhodnutí. Na základě zprávy vypracované na základě informací a písemné zprávy Komise vyhodnotí Rada do 16. září 2007, do jaké míry členské státy vyhověly ustanovením tohoto rámcového rozhodnutí.

Článek 13**Vstup v platnost**

Toto rámcové rozhodnutí vstupuje v platnost dnem zveřejnění v *Úředním věstníku Evropské unie*.

V Bruselu dne 24. února 2005.

Za Radu
N. SCHMIT
předseda