

CS

CS

CS



EVROPSKÁ KOMISE

V Bruselu dne 30.9.2010
KOM(2010) 517 v konečném znění

2010/0273 (COD)

Návrh

SMĚRNICE EVROPSKÉHO PARLAMENTU A RADY

**o útocích proti informačním systémům a zrušení rámcového rozhodnutí Rady
2005/222/SVV**

{SEK(2010) 1122 final}

{SEK(2010) 1123 final}

DŮVODOVÁ ZPRÁVA

1. ODŮVODNĚNÍ A CÍLE NÁVRHU

Cílem tohoto návrhu je nahradit rámcové rozhodnutí Rady 2005/222/SVV ze dne 24. února 2005 o útocích proti informačním systémům¹. Rámcové rozhodnutí bylo, jak je uvedeno v jeho odůvodnění, zaměřeno na zlepšení spolupráce 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. Zavedlo právní předpisy EU pro boj s takovými trestnými činy, jako jsou protiprávní přístup k informačním systémům, protiprávní zásah do systému a protiprávní zásad do dat, i konkrétní pravidla odpovědnosti právnických osob, soudní pravomoci a výměny informací. Členské státy měly přijmout opatření nezbytná pro dosažení souladu s rámcovým rozhodnutím do dne 16. března 2007.

Dne 14. července 2008 Komise zveřejnila zprávu o provádění rámcového rozhodnutí². V závěrech této zprávy bylo uvedeno, že většina členských států dosáhla výrazného pokroku a že úroveň provádění je poměrně dobrá, ale že v některých členských státech provádění stále probíhá. Dále ve zprávě bylo uvedeno, že nedávne „útoky, k nimž došlo po přijetí RR na různých místech Evropy, zdůraznily několik nově se objevujících hrozeb. Jedná se zejména o nový druh masivních souběžných útoků proti informačním systémům a zvýšené trestné používání tzv. botnetů“. V době přijetí rámcového rozhodnutí tyto útoky ještě nebyly v centru pozornosti. Vzhledem k popsanému vývoji bude Komise uvažovat o přijetí opatření, která by umožnila lépe na tuto hrozbu reagovat (vysvětlení pojmu botnet je uvedeno v dalším oddíle).

Význam přijímání dalších opatření na zvýšení boje proti kybernetické trestné činnosti byl zdůrazněn v Haagském programu o posílení svobody, bezpečnosti a práva v Evropské unii z roku 2004 i ve Stockholmském programu a souvisejícím akčním plánu³. Kromě toho byla v nedávno předložené Digitální agendě pro Evropu⁴, první vzorové iniciativě přijaté v rámci strategie Evropa 2020, zdůrazněna potřeba řešit nárůst nových forem trestné činnosti, zejména kybernetické trestné činnosti, na evropské úrovni. Komise je odhodlána provádět v akční oblasti zaměřené na důvěru a bezpečnost opatření na boj s kybernetickými útoky proti informačním systémům.

Na mezinárodní úrovni se za dosud nejúplnější mezinárodní normu považuje Úmluva Rady Evropy o kybernetické trestné činnosti („úmluva o kybernetické trestné činnosti“) ze dne 23. listopadu 2001, protože poskytuje rozsáhlý a ucelený rámec pro různé aspekty kybernetické trestné činnosti⁵. Úmluvu podepsalo všech 27 členských států, ale pouze 15 členských států ji zatím ratifikovalo⁶. Úmluva vstoupila v platnost dne 1. července 2004. EU není jejím signatářem. S ohledem na význam tohoto nástroje Komise aktivně povzbuzuje zbývající členské státy EU k jeho co nejrychlejší ratifikaci.

¹ Úř. věst. L 69, 16.3.2005, s. 68.

² Zpráva Komise Radě založená na článku 12 rámcového rozhodnutí Rady ze dne 24. února 2005 o útocích proti informačním systémům, KOM(2008) 448.

³ Úř. věst. C 198, 12.8.2005, Úř. věst. C 115, 4.5.2010, KOM(2010) 171, 20.4.2010.

⁴ Sdělení Komise KOM(2010) 245, 19.5.2010.

⁵ Úmluva Rady Evropy o kybernetické trestné činnosti, Budapešť, 23.11.2001, CETS č. 185.

⁶ Viz přehled ratifikace úmluvy (CETS 185):

<http://conventions.coe.int/Treaty/Commun/ChercheSig.asp?NT=185&CM=&DF=&CL=ENG>

- **Obecné souvislosti**

Hlavní příčinou kybernetické trestné činnosti je zranitelnost vyplývající z řady faktorů. Nedostatečná reakce mechanismů prosazování práva přispívá k šíření tohoto jevu a prohlubuje problémy, protože některé druhy trestných činů překračují hranice států. Oznamování tohoto typu trestné činnosti je často neuspokojivé, částečně proto, že některé trestné činy nejsou zjištěny, částečně proto, že oběti (ekonomické subjekty a podniky) trestné činy nenahlásí ze strachu před získáním špatné pověsti nebo z toho, že si zveřejněním svých slabých stránek zhorší své podnikatelské vyhlídky.

Kromě toho mohou rozdíly v trestním právu a postupech členských států vést k odlišnému způsobu vyšetřování a stíhání, v jehož důsledku nejsou uvedené trestné činy posuzovány jednotně. Problémy ještě vyostřil vývoj v oblasti informačních technologií, který usnadnil výrobu a šíření nástrojů („škodlivého softwaru“ a „botnetů“) a zároveň zajistil pachatelům anonymitu a rozšířil odpovědnost na více států. Kvůli obtížím při zahajování trestního stíhání může organizovaná trestná činnost přinášet značné zisky bez velkého rizika.

Předložený návrh bere ohled na nové metody páchaní kybernetické trestné činnosti, zvláště na používání botnetů. Pojmem „botnet“ se rozumí síť počítačů, které byly napadeny škodlivým softwarem (počítačovým virem). Síť napadených počítačů („zombie“) lze aktivovat za účelem provedení konkrétních akcí, například útoků na počítačové systémy (kybernetické útoky). Počítače „zombie“ může ovládat jiný počítač, často bez vědomí uživatelů napadeného počítače. „Řídící“ počítač je rovněž znám jako „řídící a kontrolní středisko“. Osoby, které toto středisko ovládají, patří mezi pachatele trestných činů, protože používají napadené počítače k útokům na počítačové systémy. Vypátrání těchto pachatelů je velice obtížné, protože počítače, které vytvářejí botnet a provádějí útoky, se mohou nacházet jinde než pachatel sám.

Útoky prováděné pomocí botnetů jsou často velice rozsáhlé. Za rozsáhlé útoky se považují buď útoky provedené pomocí nástrojů, které ovlivňují vysoký počet počítačových systémů (počítačů), nebo útoky, které způsobí značnou škodu, např. z hlediska narušení systémových služeb, finančních nákladů, ztráty osobních informací atd. Škody způsobené rozsáhlými útoky mají velký dopad na fungování samotného cíle a/nebo ovlivňují jeho pracovní prostředí. Za „velký botnet“ se proto považuje botnet schopný způsobit závažnou škodu. Je obtížné vymezit botnety podle velikosti, ale největší doložené botnety měly podle odhadů 40 000 až 100 000 připojení (tedy napadených počítačů) během 24 hodin⁷.

⁷

Počet připojení za 24 hodin je běžně používanou měřicí jednotkou k odhadnutí velikosti botnetů.

- **Platné předpisy vztahující se na oblast návrhu**

Na úrovni EU rámcové rozhodnutí zavádí minimální úroveň sblížení právních předpisů členských států s cílem učinit trestnými řadu kybernetických trestných činů, včetně protiprávního přístupu k informačním systémům, protiprávního zásahu do systému, protiprávního zásahu do dat a navádění, napomáhání, účastenství a pokusu souvisejícími s výše uvedenými trestnými činy.

Přestože ustanovení rámcové směrnice byla v členských státech většinou provedena, má směrnice kvůli rostoucímu rozsahu a počtu trestných činů (kybernetických útoků) řadu nedostatků. Sblíží právní předpisy pouze u omezeného počtu trestných činů, ale nepřináší komplexní řešení potenciální hrozby, kterou pro společnost představují útoky velkého rozsahu. Kromě toho dostatečně nezohledňuje závažnost trestných činů a související sankce.

Problémy spojenými s kybernetickými útoky nebo aspekty kybernetické trestné činnosti, například bezpečností sítí nebo bezpečností uživatelů internetu, se v různé míře zabývají i některé další stávající nebo plánované iniciativy a programy EU. Patří mezi ně opatření podporovaná z programů „Předcházení trestné činnosti a boj proti ní“⁸, „Trestní soudnictví“⁹, „Bezpečnější internet“¹⁰ a „Iniciativa pro kritickou informační infrastrukturu“¹¹. Kromě rámcového rozhodnutí je dalším relevantním platným právním nástrojem rámcové rozhodnutí 2004/68/SVV o boji proti pohlavnímu vykořisťování dětí a dětské pornografii.

Na správní úrovni je napadání počítačů a jejich přeměna na „botnety“ již zakázáno na základě pravidel EU pro ochranu soukromí a údajů¹². Státní správní agentury již spolupracují v rámci evropské kontaktní sítě agentur pro ochranu před spamem. Tato pravidla vyžadují, aby členské státy zakázaly sledování komunikací na veřejných komunikačních sítích a veřejně dostupných elektronických komunikačních službách bez souhlasu dotčených uživatelů nebo soudního povolení.

Předkládaný návrh je s těmito pravidly v souladu. Členské státy by měly věnovat pozornost zlepšení spolupráce mezi správními agenturami a orgány pro prosazování práva v případech, které podléhají správním i trestním sankcím.

- **Soulad s ostatními politikami a cíli Unie**

Cíle jsou v souladu s politikami EU v oblasti boje proti organizované trestné činnosti, zvyšování odolnosti počítačových sítí, ochrany kritické informační infrastruktury a ochrany údajů. Cíle jsou rovněž v souladu s Programem pro bezpečnější internet, který má podpořit bezpečnější využívání internetu a nových online technologií a bojovat proti nedovolenému obsahu.

Návrh byl pečlivě posouzen, aby se zajistilo, že jeho ustanovení jsou plně v souladu se základními právy, zejména s ochranou osobních údajů, svobodou projevu a informací, právem

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

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

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

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

¹² Směrnice o ochraně soukromí v odvětví elektronických komunikací, Úř. věst. L 2010, 31.7.2002, ve znění směrnice 2009/136/ES (Úř. věst. L 337, 18.12.2009).

na spravedlivý soud, presumpcí nevinu a právem na obhajobu, i se zásadami zákonnosti a přiměřenosti trestných činů a trestů.

2. KONZULTACE ZÚČASTNĚNÝCH STRAN A POSOUZENÍ DOPADŮ

• Konzultace zúčastněných stran

Byla uspořádána řada schůzí, na nichž se s širokým spektrem odborníků jednalo o různých stránkách boje proti kybernetické trestné činnosti, včetně soudních kroků (stíhání) navazujících na tyto trestné činy. Mezi konzultované odborníky patřili především zástupci vlád členských států i soukromého sektoru, specializovaní soudci a státní zástupci, zástupci mezinárodních organizací, evropských agentur a odborných subjektů. Řada odborníků a organizací následně zaslala připomínky a poskytla informace.

Z konzultací vyplynuly tyto klíčové poznatky:

- potřeba činnosti EU v této oblasti,
- potřeba učinit trestnými formy jednání, které nebyly začleněny do stávajícího rámcového rozhodnutí, zejména nové formy kybernetických útoků (botnety),
- potřeba odstranit překážky bránící vyšetřování a stíhání v přeshraničních případech.

Výsledky získané v průběhu konzultací byly zohledněny v posouzení dopadů.

Sběr a využití výsledků odborných konzultací

Externí poznatky byly získány na jednání s různými zúčastněnými stranami.

Posouzení dopadů

Byly posouzeny různé varianty politiky, které by umožnily dosažení cíle.

• Varianta politiky 1: Status quo / Žádné nové opatření ze strany EU

Tato varianta znamená, že EU nepřijme žádná další opatření na potírání tohoto konkrétního typu kybernetické trestné činnosti, tedy útoků na informační systémy. Probíhající opatření budou pokračovat, zejména opatření na posílení ochrany kritické informační infrastruktury a zlepšování spolupráce veřejného a soukromého sektoru v boji proti kybernetické trestné činnosti.

• Varianta politiky 2: Vypracování programu na zvýšení úsilí o odrážení útoků na informační systémy prostřednictvím nelegislativních opatření

Nelegislativní opatření by se spolu s programem na ochranu kritické informační infrastruktury zaměřila na přeshraniční prosazování práva a spolupráci mezi veřejným a soukromým sektorem. Cílem těchto právně nevynutitelných předpisů by bylo podporovat další koordinovaná opatření na úrovni EU, včetně posílení existující sítě kontaktních bodů pro donucovací orgány, která funguje 24 hodin denně 7 dnů v týdnu, zřízení evropské sítě kontaktních bodů pro spolupráci mezi veřejným a soukromým sektorem, do níž by byli zapojeni odborníci na kybernetickou trestnou činnost a donucovací orgány, vypracování standardní evropské dohody o úrovni služeb pro spolupráci se subjekty soukromého sektoru

při prosazování práva a podpory při organizaci vzdělávacích programů pro donucovací orgány na téma vyšetřování kybernetických trestných činů.

- Varianta politiky (3): Cílená aktualizace pravidel rámcového rozhodnutí (stávající rámcové rozhodnutí by nahradila nová směrnice), která by se zabývala hrozbou rozsáhlých útoků proti informačním systémům (botnety), efektivností kontaktních míst členských států pro donucovací orgány v případech, kdy byla při spáchání trestného činu utajena skutečná totožnost pachatele a byl poškozen skutečný nositel totožnosti, a nedostatkem statistických údajů o kybernetických útocích.

Při použití této varianty by byly zavedeny konkrétní cílené (tedy omezené) právní předpisy na předcházení rozsáhlým útokům proti informačním systémům. Tyto posílené právní předpisy by byly doplněny o nelegislativní opatření na zvýšení operační přeshraniční spolupráce proti těmto útokům, která by usnadnila provádění legislativních opatření. Cílem těchto opatření by bylo zvýšit připravenost, bezpečnost a odolnost kritické informační infrastruktury a zajistit výměnu osvědčených postupů.

- Varianta politiky (4): Zavedení uceleného souboru právních předpisů EU proti kybernetické trestné činnosti

Tato varianta by sestávala z nového, uceleného souboru právních předpisů EU. Byly by zavedeny právně nevynutitelné předpisy uvedené ve variantě politiky 2, byla by provedena aktualizace uvedená ve variantě 3 a kromě toho by se řešily i další právní problémy související s užíváním internetu. Přijatá opatření by se nezabývala pouze útoky proti informačním systémům, ale i takovými tématy, jako jsou finanční kybernetická trestná činnost, nelegální internetový obsah, sběr/skladování/převod elektronických důkazů a podrobnější pravidla o soudní pravomoci. Právní předpisy by fungovaly souběžně s Úmluvou Rady Evropy o kybernetické trestné činnosti a byla by k nim připojena další, výše uvedená nelegislativní opatření.

- Varianta politiky (5): Aktualizace Úmluvy Rady Evropy o kybernetické trestné činnosti

Tato varianta by vyžadovala rozsáhlá jednání o přepracování současné úmluvy, což je zdoluhavý proces, který neodpovídá časovému rámci akce navrhovanému v posouzení dopadů. Zdá se, že o nové projednávání úmluvy není na mezinárodní úrovni zájem. Aktualizaci úmluvy tedy nelze považovat za použitelnou variantu, protože neodpovídá požadovanému časovému rámci akce.

Upřednostňovaná možnost politiky: kombinace nelegislativních opatření (varianta 2) s cílenou aktualizací rámcového rozhodnutí (varianta 3)

Z analýzy hospodářského dopadu, sociálních dopadů a dopadů na základní práva vyplývá, že nejlepší přístup k řešení problémů a dosažení cílů návrhu představují varianty 2 a 3.

Komise při přípravě tohoto návrhu provedla posouzení dopadů.

3. PRÁVNÍ PRVKY NÁVRHU

• Shrnutí navrhovaného opatření

Směrnice, kterou se ruší rámcové rozhodnutí 2005/22/SVV, zachová jeho stávající ustanovení a doplní následující nové prvky:

– v oblasti trestního práva hmotného obecně směrnice:

- A. Zařadí mezi trestné činy výrobu, prodej, opatření si k užívání, dovoz, distribuci nebo jinou formu zpřístupnění zařízení/nástrojů používaných k páčání trestných činů.
- B. Zahrne přitěžující okolnosti:
- velký rozsah útoku – problematika botnetů nebo podobných nástrojů by se řešila zavedením nových přitěžujících okolností v tom smyslu, že by vytvoření botnetu nebo podobného nástroje bylo považováno za přitěžující okolnost při spáchání trestných činů vyjmenovaných ve stávajícím rámcovém rozhodnutí;
 - v případě, že byla při útoku utajena skutečná totožnost pachatele a byl poškozen skutečný nositel totožnosti. Tato pravidla by musela být v souladu se zásadou zákonnosti a přiměřenosti trestných činů a trestů a být v souladu se stávajícími právními předpisy o ochraně osobních údajů¹³.
- C. Zavádí trestný čin „protiprávní sledování“.
- D. Zavádí opatření na zlepšení evropské spolupráce v oblasti trestního soudnictví posílením existující struktury kontaktních míst s nepřetržitým provozem¹⁴:
- navrhuje se zavést povinnost vyhovět žádosti o pomoc podané operativním kontaktním místem (stanoveným v článku 14 směrnice) do určité časové lhůty. Úmluva o kybernetické trestné činnosti neobsahuje závazné ustanovení tohoto druhu. Cílem tohoto opatření je zajistit, aby kontaktní místa ve stanoveném čase uvedla, zda jsou schopna žádost o pomoc řešit, a aby žádající kontaktní místo informovala, jak dlouho bude nalezení takového řešení trvat. Konkrétní náplň řešení není uvedena.
- E. Řeší potřebu získat statistické údaje o kybernetických trestných činech tím, že zavádí pro členské státy povinnost zajistit vhodný systém pro záznam, produkci a poskytování statistických údajů o trestných činech uvedených ve stávajícím rámcovém rozhodnutí a o novém trestném činu „protiprávní sledování“.

V definicích trestných činů vyjmenovaných v člancích 3, 4, 5 (protiprávní přístup k informačním systémům, protiprávní zásah do systému a protiprávní zásah do dat) směrnice obsahuje ustanovení, které při jejím provádění do vnitrostátního práva umožní stanovit trestní sankce pouze, „pokud se nejedná o případy menšího významu“. Cílem tohoto prvku

¹³ Například se směrnicí Evropského parlamentu a Rady 2002/58/ES ze dne 12.7.2002 o zpracování osobních údajů a ochraně soukromí v odvětví elektronických komunikací (směrnice o soukromí a elektronických komunikacích) Úř. věst. L 201, 31.7.2002, s. 37 (v současné době probíhá přezkum) a s obecnou směrnicí o ochraně údajů 95/46/ES.

¹⁴ Zavedena úmluvou a RR 2005/222/SVV o útocích proti informačním systémům.

flexibility je umožnit členským státům, aby nezahrnuly případy, na které by se *in abstracto* vztahovala základní definice, ale v nichž se nemá za to, že poškozují chráněný právní zájem, jedná se především např. o činy spáchané mladými lidmi, kteří si chtějí dokázat své schopnosti v informatice. Možnost omezit rozsah trestnosti by však neměla vést k doplňování dalších konstitutivních prvků trestných činů mimo ty, které již směrnice obsahuje, protože v takové situaci by se pak vztahovala pouze na trestné činy spáchané za přitěžujících okolností. Při provádění do vnitrostátního práva by se členské státy měly především zdržet doplňování konstitutivních prvků k základním trestným činům, neměly by například zahrnout zvláštní záměr získat nelegální zisk z trestného činu nebo z přítomnosti jeho zvláštních účinků, např. ze způsobení značné škody.

- **Právní základ**

Ustanovení čl. 83 odst. 1 Smlouvy o fungování Evropské unie¹⁵.

- **Zásada subsidiarity**

Na činnosti Evropské unie se vztahuje zásada subsidiarity. Cílů návrhu nemůže být uspokojivě dosaženo na úrovni členských států z následujících důvodů:

Kybernetická trestná činnost, konkrétně útoky proti informačním systémům, má výrazný přeshraniční rozměr, který je nejvíce patrný u rozsáhlých útoků, při němž jsou prvky útoku často umístěny na různých místech a v různých státech. Na úrovni EU je proto třeba jednat, zejména udržovat krok se současnými trendy rozsáhlých útoků v Evropě a ve světě. Opatření na úrovni EU a aktualizaci rámcového rozhodnutí 2005/222/SVV požadovaly i závěry Rady z listopadu 2008¹⁶, neboť cíle účinné ochrany občanů před kybernetickými trestnými činy nelze uspokojivě dosáhnout pouze na úrovni členských států.

Opatření Evropské unie lépe dosáhnou cílů návrhu z těchto důvodů:

Návrh ve větší míře sblíží trestní právo hmotné a procesní členských států, což bude mít kladný dopad na boj proti těmto zločinům. Zaprvé se jedná o způsob, kterým lze pachatele trestných činů odradit od přesunů do členských států s mírnějšími právními předpisy v oblasti kybernetických útoků. Zadruhé společné definice umožňují výměnu informací a sběr a srovnávání relevantních údajů. Zatřetí je posílena účinnost preventivních opatření v EU a mezinárodní spolupráce.

Návrh je tedy v souladu se zásadou subsidiarity.

- **Zásada proporcionality**

Návrh je v souladu se zásadou proporcionality z tohoto důvodu:

Tato směrnice se omezuje na minimum nutné k dosažení uvedených cílů na evropské úrovni a nepřekračuje rámec toho, co je pro tento účel nezbytné, bere přitom v úvahu nutnost přesnosti trestněprávních předpisů.

¹⁵ Úř. věst. C 83, 30.3.2010, s. 49.

¹⁶ „Závěry Rady o společné pracovní strategii a konkrétních opatřeních v oblasti boje proti počítačové trestné činnosti“, 2987. zasedání Rady ve složení pro SPRAVEDLNOST a VNITRO, Brusel, 27.-28. listopadu 2008.

- **Volba nástrojů**

Navrhovaný nástroj: směrnice.

Jiné prostředky by nebyly přiměřené z tohoto důvodu:

Právní základ vyžaduje směrnici.

Nelegislativní opatření a samoregulace by zlepšily situaci v určitých oblastech, ve kterých má provádění těchto opatření zásadní význam. V dalších oblastech, ve kterých je nutné přijmout nové právní předpisy, by přínosy byly jen mírné.

4. ROZPOČTOVÉ DŮSLEDKY

Důsledky návrhu na rozpočet Unie jsou nízké. Více než 90 % odhadovaných nákladů, tedy 5 913 000 EUR, by nesly členské státy, přičemž je možné využít ke snížení jejich nákladů prostředky EU.

5. DODATEČNÉ INFORMACE

- **Zrušení platných právních předpisů**

Přijetí tohoto návrhu povede ke zrušení platného právního předpisu.

- **Místní působnost**

Tato směrnice je v souladu se Smlouvami určena členským státům.

Návrh

SMĚRNICE EVROPSKÉHO PARLAMENTU A RADY

o útocích proti informačním systémům a zrušení rámcového rozhodnutí Rady 2005/222/SVV

EVROPSKÝ PARLAMENT A RADA EVROPSKÉ UNIE,

s ohledem na Smlouvu o fungování Evropské unie, a zejména na

čl. 83 odst. 1 této smlouvy,

s ohledem na návrh Evropské komise¹⁷,

poté, co postoupila návrh legislativního aktu vnitrostátním parlamentům,

s ohledem na stanovisko Evropského hospodářského a sociálního výboru,

s ohledem na stanovisko Výboru regionů,

v souladu s řádným legislativním postupem,

vzhledem k těmto důvodům:

- (1) Cílem této směrnice je sblížit trestněprávní předpisy členských států v oblasti útoků proti informačním systémům a zlepšit spolupráci mezi justičními a jinými příslušnými orgány, včetně policie a dalších specializovaných donucovacích orgánů členských států.
- (2) Útoky proti informačním systémům, zejména v důsledku organizované trestné činnosti, představují rostoucí hrozbu a zvyšuje se obava z potenciálních teroristických anebo politicky motivovaných útoků na informační systémy, které jsou součástí kritické infrastruktury členských států a Unie. Tato skutečnost ohrožuje vytváření bezpečnější informační společnosti a oblasti svobody, bezpečnosti a práva, a proto je třeba na ni reagovat na úrovni Evropské unie.
- (3) Existují důkazy o směřování k čím dál tím nebezpečnějším a opakovaným rozsáhlým útokům namířeným na informační systémy, které mají kritický význam pro státy nebo pro konkrétní funkce ve veřejném nebo soukromém sektoru. Tuto tendenci doprovází vývoj čím dál tím vyspělejších nástrojů, které mohou pachatelé trestných činů využívat k provádění kybernetických útoků různého druhu.

¹⁷ Úř. věst. C [...], [...], s. [...].

- (4) Pro zajištění konsistentního přístupu členských států k provádění této směrnice. je třeba v této oblasti přijmout společné definice, zejména definice informačních systémů a počítačových dat.
- (5) Je třeba dosáhnout společného přístupu k základním prvkům trestných činů zavedením společných trestných činů protiprávního přístupu k informačním systémům, protiprávního zásahu do systému, protiprávního zásahu do dat a protiprávního sledování.
- (6) Členské státy by měly stanovit sankce za útoky proti informačním systémům. Stanovené sankce by měly být účinné, přiměřené a odrazující.
- (7) Je vhodné zavést přísnější sankce v případech, že útok proti informačnímu systému byl spáchán v rámci zločinného spolčení vymezeného v rámcovém rozhodnutí Rady 2008/841/SVV ze dne 24. října 2008 o boji proti organizované trestné činnosti¹⁸, pokud se jednalo o rozsáhlý útok nebo pokud byla při spáchání trestného činu utajena skutečná totožnost pachatele a vznikla újma skutečnému nositeli totožnosti. Je rovněž vhodné stanovit přísnější sankce, pokud takový útok způsobil vážné škody nebo měl dopad na klíčové zájmy.
- (8) V závěrech zasedání Rady ve dnech 27. a 28. listopadu 2008 bylo uvedeno, že by se ve spolupráci s členskými státy a Komisí měla připravit nová strategie, která by přihlížela k obsahu Úmluvy Rady Evropy o kybernetické trestné činnosti z roku 2001. Tato úmluva představuje právní referenční rámec pro boj s kybernetickou trestnou činností, včetně útoků proti informačním systémům. Tato směrnice z úmluvy vychází.
- (9) S ohledem na různé způsoby, jimiž lze útoky provést, a na rychlý vývoj hardwaru a softwaru tato směrnice odkazuje na „nástroje“, které lze používat k páčání trestných činů uvedených v této směrnici. Nástroje odkazují například na škodlivý software, včetně botnetů, používaných k páčání kybernetických trestných činů.
- (10) Cílem směrnice není zavést trestní odpovědnost v případě, kdy jsou činy spáchány bez protiprávního záměru, například v případě povoleného testování nebo ochrany informačních systémů.
- (11) Tato směrnice posiluje význam sítí, např. sítě G8 nebo sítě kontaktních bodů s nepřetržitým provozem zřízené na základě úmluvy Rady Evropy, pro výměnu informací, aby se zajistila okamžitá pomoc pro účely šetření nebo řízení týkajících se trestných činů souvisejících s informačními systémy nebo daty nebo pro sběr elektronických údajů o trestném činu. Vzhledem k rychlosti, kterou lze provést rozsáhlé útoky, by členské státy měly být schopny rychle reagovat na naléhavé žádosti z této sítě kontaktních bodů. Poskytnutá pomoc by měla zahrnovat usnadnění nebo přímé provedení následujících opatření: poskytnutí technického poradenství, ochrana údajů, získávání důkazů, poskytování právních informací a lokalizace podezřelých osob.
- (12) Je třeba shromažďovat údaje o trestných činech, na které se vztahuje tato směrnice, aby bylo možné vytvořit si ucelenější představu o tomto problému na úrovni Unie a tak přispět k přípravě efektivnějších odpovědí. Údaje kromě toho pomohou

¹⁸ Úř. věst. L 300, 11.11.2008, s. 42.

specializovaným agenturám, například Europolu a Evropské agentuře pro bezpečnost sítí a informací, lépe vyhodnotit rozsah kybernetické trestné činnosti a stav bezpečnosti sítí a informací v Evropě.

- (13) Výrazné odchylky a rozdíly v právu členských států v oblasti útoků proti informačním systémům mohou bránit boji s organizovanou trestnou činností a terorismem a mohou komplikovat efektivní policejní a justiční spolupráci v této oblasti. Z nadnárodní a bezhraniční povahy moderních informačních systémů vyplývá, že útoky proti těmto systémům mají přeshraniční rozměr, což podtrhuje naléhavou potřebu dalších opatření na sbližování trestněprávních předpisů v této oblasti. Kromě toho by koordinace stíhání případů útoků proti informačním systémům měla být usnadněna přijetím rámcového rozhodnutí Rady 2009/948/SVV o předcházení kompetenčním sporům při výkonu pravomoci v trestním řízení a jejich řešení.
- (14) Vzhledem k tomu, že cíle této směrnice, tedy zajistit, že útoky proti informačním systémům jsou trestány ve všech členských státech účinnými, přiměřenými a odrazujícími tresty, a zlepšit a podpořit soudní spolupráci odstraněním potenciálních komplikací, nelze uspokojivě dosáhnout na úrovni členských států, protože pravidla musejí být společná a slučitelná, a lze ho tedy lépe dosáhnout na úrovni Unie, může Unie přijmout opatření v souladu se zásadou subsidiarity stanovenou v článku 5 Smlouvy o Evropské unii. Tato směrnice nepřekračuje rámec toho, co je pro dosažení těchto cílů nezbytné.
- (15) Veškeré osobní údaje zpracovávané při provádění této směrnice by měly být chráněny podle pravidel stanovených v rámcovém rozhodnutí Rady 2008/977/SVV ze dne 27. listopadu 2008 o ochraně osobních údajů zpracovávaných v rámci policejní a justiční spolupráce v trestních věcech¹⁹, pokud jde o zpracování, které spadá do jeho oblasti působnosti, a podle nařízení Evropského parlamentu a Rady (ES) č. 45/2001 ze dne 18. prosince 2000 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů orgány a institucemi Společenství a o volném pohybu těchto údajů²⁰.
- (16) Tato směrnice respektuje základní práva a dodržuje zásady uznané zejména Listinou základních práv Evropské unie, včetně ochrany osobních údajů, svobody projevu a informací, práva na spravedlivý soud, presumpce nevinoty a práva na obhajobu i zásady zákonnosti a přiměřenosti trestných činů a trestů. Cílem této směrnice je zejména zajistit plné dodržování těchto práv a zásad a v souladu s nimi musí být provedena.
- (17) [V souladu s články 1, 2, 3 a 4 Protokolu o postavení Spojeného království a Irsko s ohledem na prostor svobody, bezpečnosti a práva, připojeného ke Smlouvě o fungování Evropské unie, Spojené království a Irsko oznámily své přání účastnit se přijímání a používání této směrnice.] NEBO [Aniž je dotčen článek 4 Protokolu o postavení Spojeného království a Irsko s ohledem na prostor svobody, bezpečnosti a práva, Spojené království a Irsko se neúčastní přijímání této směrnice, a proto pro ně není závazná ani použitelná.].
- (18) V souladu s články 1 a 2 Protokolu o postavení Dánska, připojeného ke Smlouvě o fungování Evropské unie, se Dánsko neúčastní přijímání této směrnice, a proto pro ně není závazná ani použitelná,

¹⁹ Úř. věst. L 350, 30.12.2008, s.60.

²⁰ Úř. věst. L 8, 12.1.2001, s.1.

PŘIJALY TUTO SMĚRNICI:

Článek 1 **Předmět**

Tato směrnice definuje trestné činy v oblasti útoků proti informačním systémům a stanoví minimální pravidla týkající se sankcí za tyto trestné činy. Jejím cílem je rovněž zavést společná ustanovení zaměřená na předcházení takovým útokům a na zlepšení evropské spolupráce v této oblasti trestního soudnictví.

Článek 2 **Definice**

Pro účely této směrnice se rozumí:

- a) „informačním systémem“ jakýkoli přístroj nebo skupina vzájemně propojených nebo přidružených přístrojů, z nichž jeden nebo více provádí na základě programu automatické zpracování počítačových dat, jakož i počítačová 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 právní postavení podle platného vnitrostátního práva, s výjimkou států nebo jiných veřejnoprávních subjektů jednajících při výkonu státní moci a s výjimkou organizací mezinárodního práva veřejného;
- 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 3 **Protiprávní přístup k informačním systémům**

Členské státy přijmou nezbytná opatření k zajištění toho, aby úmyslný neoprávněný přístup k celému informačnímu systému nebo k některé jeho části byl trestným činem, a to alespoň pokud se nejedná o případy menšího významu.

Článek 4 **Protiprávní zásah do systému**

Členské státy přijmou 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 bylo trestným činem, je-li spácháno neoprávněně, a to alespoň pokud se nejedná o případy menšího významu.

Článek 5

Protiprávní zásah do dat

Členské státy přijmou 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 6

Protiprávní sledování

Členské státy přijmou nezbytná opatření k zajištění toho, aby úmyslné sledování, prováděné technickými prostředky, neveřejných přenosů počítačových dat do, z nebo uvnitř informačního systému, včetně elektromagnetického záření z informačního systému nesoucího taková počítačová data, bylo trestným činem, je-li spácháno neoprávněně.

Článek 7

Prostředky použité k páčání trestných činů

Členské státy přijmou nezbytná opatření k zajištění toho, aby výroba, prodej, opatření si k užití, dovoz, držení, distribuce nebo jiné formy zpřístupnění následujících položek bylo trestným činem, je-li spácháno úmyslně a neoprávněně pro účely spáchání některého z trestných činů uvedených v článcích 3 až 6:

- a) nástrojů, včetně počítačového programu, který byl navržen nebo přizpůsoben prvotně pro účely spáchání některého z trestných činů uvedených v článcích 3 až 6;
- b) počítačového hesla, přístupového kódu nebo obdobných dat, která umožňují přístup k celému informačnímu systému nebo k jeho části.

Článek 8

Návod, pomoc, účastenství a pokus

- 1. Členské státy přijmou opatření nezbytná k zajištění trestnosti návodu, pomoci a účastenství na spáchání trestných činů uvedených v článcích 3 až 7.
- 2. Členské státy přijmou opatření nezbytná k zajištění trestnosti pokusu o spáchání trestných činů uvedených v článcích 3 až 6.

Článek 9

Sankce

- 1. Členské státy přijmou nezbytná opatření k zajištění toho, aby za trestné činy uvedené v článcích 3 až 8 bylo možné uložit účinné, přiměřené a odrazující tresty.
- 2. Členské státy přijmou nezbytná opatření k zajištění toho, aby se na trestné činy uvedené v článcích 3 až 7 vztahovaly tresty odnětí svobody s horní hranicí trestní sazby nejméně dva roky.

Článek 10

Přitěžující okolnosti

1. Členské státy přijmou nezbytná opatření k zajištění toho, aby se na trestné činy uvedené v člancích 3 až 7 vztahovaly tresty odnětí svobody s horní hranicí trestní sazby nejméně pět let, pokud byly spáchány v rámci zločinného spolčení, jak je vymezeno v rámcovém rozhodnutí 2008/841/SVV.
2. Členské státy přijmou nezbytná opatření k zajištění toho, aby se na trestné činy uvedené v člancích 3 až 6 vztahovaly tresty odnětí svobody s horní hranicí trestní sazby nejméně pět let, pokud byly spáchány pomocí nástroje určeného k provedení útoků s dopadem na velké množství informačních systémů nebo útoků působících značnou škodu, například v podobě narušených systémových služeb, finančních nákladů nebo ztráty osobních údajů.
3. Členské státy přijmou nezbytná opatření k zajištění toho, aby se na trestné činy uvedené v člancích 3 až 6 vztahovaly tresty odnětí svobody s horní hranicí trestní sazby nejméně pět let, pokud byly spáchány za utajení skutečné totožnosti pachatele a způsobily újmu skutečnému nositeli totožnosti.

Článek 11

Odpovědnost právnických osob

1. Členské státy přijmou nezbytná opatření, aby zajistily, že právnické osoby lze činit odpovědnými za trestné činy uvedené v člancích 3 až 8, které v jejich prospěch spáchá jakákoliv 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;
 - b) pravomoci přijímat rozhodnutí jménem této právnické osoby;
 - c) pravomoci vykonávat kontrolu v rámci této právnické osoby.
2. Členské státy přijmou opatření nezbytná k zajištění odpovědnosti právnických osob v případech, kdy nedostatek dohledu nebo kontroly ze strany osoby uvedené v odstavci 1 umožnil spáchání některého trestných činů uvedených v člancích 3 až 8 ve prospěch právnické osoby osobou jí podřízenou.
3. Odpovědnost právnických osob podle odstavců 1 a 2 nevylučuje trestní stíhání fyzických osob, které jsou pachateli nebo účastníky při spáchání některého z trestných činů uvedených v člancích 3 až 8.

Článek 12

Sankce ukládané právnickým osobám

1. Členské státy přijmou opatření nezbytná k zajištění možnosti postihnout právnickou osobu odpovědnou podle čl. 11 odst. 1 účinnými, přiměřenými a odrazujícími sankcemi, které zahrnují pokuty trestní nebo jiné povahy a mohou zahrnovat i jiné sankce, například:

- a) zbavení oprávnění pobírat veřejné výhody nebo podpory;
 - b) dočasný nebo trvalý zákaz provozování obchodní činnosti;
 - c) uložení soudního dohledu;
 - d) zrušení rozhodnutím soudu;
 - e) dočasné nebo trvalé uzavření provozoven použitých ke spáchání trestného činu.
2. Členské státy přijmou opatření nezbytná k zajištění možnosti postihnout právnickou osobu odpovědnou podle čl. 11 odst. 2 účinnými, přiměřenými a odrazujícími sankcemi nebo opatřeními.

Článek 13 **Soudní pravomoc**

1. Členské státy stanoví svou soudní pravomoc pro trestné činy uvedené v člancích 3 až 8 a spáchané:
- a) zcela nebo zčásti na území dotčeného členského státu, nebo
 - b) jejich státním příslušníkem nebo osobou, která má místo obvyklého pobytu na území dotčeného členského státu nebo
 - c) ve prospěch právnické osoby se sídlem na území dotčeného členského státu.
2. Při stanovení soudní pravomoci podle odst. 1 písm. a) členské státy zajistí, aby tato pravomoc zahrnovala případy, kdy:
- a) pachatel spáchal trestný čin v době své fyzické přítomnosti na území dotčeného členského státu, 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 území dotčeného členského státu, a to bez ohledu na to, zda pachatel spáchal trestný čin v době své fyzické přítomnosti na jeho území či nikoli.

Článek 14 **Výměna informací**

1. Za účelem výměny informací týkajících se trestných činů uvedených v člancích 3 až 8 a v souladu s pravidly ochrany údajů členské státy využívají stávající síť operativních kontaktních míst s nepřetržitým provozem. Členské státy rovněž zavedou postupy, které jim umožní odpovídat na naléhavé dotazy nejpozději do osmi hodin. V takové odpovědi se uvede alespoň zda a v jaké formě se odpoví na žádost o pomoc a kdy.
2. Členské státy uvědomí Komisi o kontaktních místech, která jmenovaly pro účely výměny informací o trestných činech uvedených v člancích 3 až 8. Komise tyto informace předá ostatním členským státům.

Článek 15

Sledování a statistika

1. Členské státy zajistí, aby existoval systém pro záznam, produkci a poskytování statistických údajů o trestných činech uvedených v člancích 3 až 8.
2. Statistické údaje uvedené v odstavci 1 zahrnují alespoň počet trestných činů uvedených v člancích 3 až 8 oznámených členským státům a opatření přijatá v návaznosti na tato oznámení a uvádějí na ročním základě počet vyšetřovaných oznámených případů, počet stíhaných osob a počet osob usvědčených z trestných činů uvedených v člancích 3 až 8.
3. Údaje sebrané podle tohoto článku předávají členské státy Komisi. Rovněž zajistí zveřejňování komplexních přehledů těchto statistických zpráv.

Článek 16

Zrušení rámcového rozhodnutí 2005/222/SVV

Tímto se zrušuje rámcové rozhodnutí 2005/222/SVV, aniž by byly dotčeny další povinnosti členských států týkající se lhůt pro provedení směrnice ve vnitrostátním právu. Odkazy na zrušené rámcové rozhodnutí se považují za odkazy na tuto směrnici.

Článek 17

Provedení

1. Členské státy uvedou v účinnost právní a správní předpisy nezbytné pro dosažení souladu s touto směrnicí nejpozději do [dvou let od jejího přijetí]. Neprodleně sdělí Komisi jejich znění a srovnávací tabulku mezi těmito předpisy a touto směrnicí. Tyto předpisy přijaté členskými státy musí obsahovat odkaz na tuto směrnici nebo musí být takový odkaz učiněn při jejich úředním vyhlášení. Způsob odkazu si stanoví členské státy.
3. Členské státy sdělí Komisi znění hlavních ustanovení vnitrostátních právních předpisů, které přijmou v oblasti působnosti této směrnice.

Článek 18

Podávání zpráv

1. Do [ČTYŘ LET OD PŘIJETÍ SMĚRNICE] a následně jednou za tři roky Komise předloží Evropskému parlamentu a Radě zprávu o provádění směrnice v členských státech, včetně případných potřebných návrhů.
2. Členské státy předají Komisi veškeré informace potřebné pro vypracování zprávy uvedené v odstavci 1. Součástí těchto informací je podrobný popis legislativních a nelegislativních opatření přijatých při provádění této směrnice.

Článek 19
Vstup v platnost

Tato směrnice vstupuje v platnost dvacátým dnem po vyhlášení v *Úředním věstníku Evropské unie*.

Článek 20
Určení

Tato směrnice je určena členským státům v souladu se Smlouvami.

V Bruselu dne

Za Evropský parlament
předseda

Za Radu
předseda