EVROPSKÁ KOMISE

V Bruselu dne 30.9.2010
SEK(2010) 1123 v konečném znění

PRACOVNÍ DOKUMENT ÚTVARŮ KOMISE

SHRNUTÍ POSOUZENÍ DOPADŮ

Průvodní dokument k

návrhu

SMĚRNICE EVROPSKÉHO PARLAMENTU A RADY

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

{COM(2010) 517 final}
{SEC(2010) 1122 final}

SHRNUTÍ POSOUZENÍ DOPADŮ

1. VYMEZENÍ PROBLÉMU

Od doby přijetí rámcového rozhodnutí o útocích proti informačním systémům („RR o útocích“) se počet útoků proti informačním systémům výrazně zvýšil. Jedna z předních firem pro bezpečnost na internetu oznámila, že se v roce 2008 značně zvýšilo ohrožení důvěrných informací (oproti veřejně dostupným informacím), a to z 624 267 na 1 656 227 nově identifikovaných hrozeb v roce 2008[1]. Kromě toho byla zaznamenána řada útoků dosud nevídaného rozsahu a úrovně nebezpečí, například v Estonsku v roce 2007 a v Litvě v roce 2008. V březnu 2009 na počítačové systémy vlád a soukromých organizací 103 zemí zaútočila síť manipulovaných počítačů a extrahovala citlivé a tajné dokumenty[2]. Útok byl proveden za pomoci tzv. botnetů[3], sítě napadených počítačů, které lze ovládat na dálku. V současné době jsme svědky šíření botnetu s názvem „Conficker“ (známého rovněž jako Downup, Downadup a Kido), který se šíří a působí v bezprecedentním měřítku od listopadu 2008 a ovlivňuje miliony počítačů po celém světě[4].

Kvůli nedostatečné spolupráci členských států, zejména donucovacích a justičních orgánů v EU, je obtížné reagovat na tyto útoky koordinovaně a efektivně. Přestože zpráva o provedení rámcové směrnice o útocích ukázala, že většina členských států zřídila stálá kontaktní místa vyžadovaná článkem 11 RR o útocích, jejich schopnost odpovídat a reagovat na naléhavé žádosti o spolupráci zůstává problematická[5].

Existence kontaktních bodů není zárukou jejich řádného fungování. Při oznamování Komisi některé členské státy uvedly, že zřídily kontaktní místa, ale neprovozují je 24 hodin denně, jak vyžaduje RR o útocích. Znamená to, že tato kontaktní místa nemohou odpovědět na naléhavé žádosti mimo úřední hodiny. Nízká výkonnost kontaktních míst nebo jejich neschopnost řešit žádosti o spolupráci podané soukromým sektorem často negativně ovlivňuje spolupráci veřejného sektoru se soukromým.

Dosud není k dispozici dostatek údajů o kybernetických útocích a o policejních a justičních krocích navazujících na takové útoky. Některé členské státy údaje o kybernetických útocích neshromažďují. Státy, které je shromažďují, tak nečiní způsobem, který by umožňoval srovnání, protože používají rozdílné statistické metodiky.

---

1 http://eval.symantec.com/mktginfo/enterprise/white_papers/b-whitepaper_internet_security_threat_report_xiv_04-2009.en-us.pdf, p.10.

2 ww.theglobeandmail.com/servlet/story/RTGAM.20090328.wspy0328/BNStory/International/home?cid=al_gam_mostemail

3 Pojmem „botnet“ se rozumí síť počítačů, které byly napadeny škodlivým softwarem (počítačovým virem). Síť napadených počítačů („zombies“) lze aktivovat za účelem provedení konkrétních akcí, například útoků na počítačové systémy (počítačové útoky). Počítače „zombies“ 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.

4 http://www.lemonde.fr/technologies/article/2009/03/31/virus-conficker-catastrophe-ou-poisson-d-avril_1174916_651865.html

5 Zpráva Komise Radě založená na článku 12 rámcového rozhodnutí Rady ze dne 24. února 2005 o útocích proti informačním systémům, KOM(2008) 0448 v konečném znění.

Mezi oběti rozsáhlých útoků na informační systémy patří široká veřejnost, sestávající z uživatelů informačních systémů, i centrální a místní státní správa, mezinárodní organizace a soukromé subjekty.

Útoky mohou být vedeny ze třetích zemí na cíle v EU nebo opačným směrem.

2. SUBSIDIARITA

Kybernetická trestná činnost je skutečně mezinárodním problémem, s nímž lze jen málokdy bojovat v čistě vnitrostátním kontextu. Obecně se uznává, že k předcházení a potírání tohoto druhu trestné činnosti je třeba přijímat opatření na úrovni EU a na mezinárodní úrovni. Většina útoků překračuje hranice EU. Týká se všech členských států a existují důkazy, že významná část těchto útoků zahrnuje činnosti směřované z jednoho členského státu do druhého. Informační systémy jsou často vzájemně technicky propojené a závislé, bez ohledu na hranice. Odborníci se shodují, že je proto nutné přijímat opatření na mezinárodní úrovni i na úrovni EU a že cíle efektivního boje s takovou trestnou činností nelze uspokojivým způsobem dosáhnout na úrovni samotných členských států.

Pokud by se přijímala pouze vnitrostátní opatření, hrozilo by, že boj s kybernetickou činností bude v Evropě roztříštěný a neefektivní. Rozdílné vnitrostátní přístupy a nedostatek systematické přeshraniční spolupráce podstatně snižují účinnost vnitrostátních opatření. Částečně je to dáno vzájemným propojením informačních systémů, protože nízká úroveň bezpečnosti v jednom státě potenciálně zvyšuje zranitelné stránky v jiných státech.

3. JAKÉ JSOU CÍLE OPATŘENÍ?

3.1 Obecné, specifické a operativní cíle

Celkovým cílem opatření EU je potírat a stíhat trestnou činnost, ať už organizovanou či nikoli, v souladu s článkem 67 Smlouvy o fungování Evropské unie, bojem s rozsáhlými kybernetickými útoky proti informačním systémům.

A Specifický cíl: Stíhat a usvědčovat pachatele rozsáhlých útoků sbližováním trestního práva v oblasti útoků proti informačním systémům

B. Specifický cíl: Zlepšení přeshraniční spolupráce donucovacích agentur

C. Specifický cíl: Zavedení efektivního systému sledování a sběru údajů

4. JAKÉ MOŽNOSTI POLITIKY SE NABÍZEJÍ?

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

Z této možnosti vyplývá, že EU nepřijme žádná další opatření na boj s tímto konkrétním typem kybernetické trestné činnosti. Pokračovala by probíhající opatření, zejména programy na posílení ochrany kritické informační infrastruktury a zlepšování spolupráce veřejného a soukromého sektoru v boji proti kybernetické trestné činnosti.

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

Nelegislativní opatření by doplnila program na ochranu kritické informační infrastruktury tím, že by se zaměřila na přeshraniční prosazování práva a spolupráci mezi veřejným a soukromým sektorem a usnadnila by další koordinovaná opatření na úrovni EU. Nelegislativní opatření by zahrnovala taková opatření, jako je posílení existující sítě kontaktních míst s nepřetržitým provozem pro donucovací orgány, zřízení evropské sítě kontaktních míst pro spolupráci mezi veřejným a soukromým sektorem, do níž by byli zapojeni odborníci na kybernetickou trestnou činnost a donucovací orgány, a vypracování standardní evropské dohody o úrovni služeb pro spolupráci se subjekty soukromého sektoru při prosazování práva.

4.3 Varianta 3: Cílená aktualizace RR o útocích s cílem řešit konkrétní hrozbu, kterou představují rozsáhlé útoky proti informačním systémům

Při použití této varianty by byly zavedeny konkrétní cílené (tedy omezené) právní předpisy na předcházení zvláště nebezpečným rozsáhlým útokům proti informačním systémům. Tyto cílené právní předpisy by byly propojeny s opatřeními na posílení operativní přeshraniční spolupráce v oblasti útoků proti informačním systémům a se zvýšením již stanovených minimálních trestů. Tato varianta by měla podobu aktualizace stávajícího RR o útocích doplněného řadou nelegislativních opatření, například zvýšením připravenosti, bezpečnosti a odolnosti ochrany kritické informační infrastruktury a posílením nástrojů a postupů pro spolupráci v oblasti přeshraničního prosazování práva a výměny osvědčených postupů.

4.4 Varianta 4: Zavedení uceleného souboru právních předpisů EU proti kybernetické trestné činnosti

Zjištění, že je třeba rychle přijmout opatření bránící rozvoji sofistikovaných útoků proti informačním systémům, vyvolává otázku, zda by nebylo vhodné zavést rovněž širší právní předpisy EU o kybernetické trestné činnosti obecně. Tyto právní předpisy by se nezabývaly pouze útoky proti informačním systémům, ale i takovými tématy, jako jsou finanční kybernetická trestná činnost, nelegální internetový obsah, získávání/ukládání/předávání elektronických důkazů a podrobnější pravidla o soudní pravomoci. Tato legislativa EU by platila souběžně s úmluvou Rady Evropy o kybernetické trestné činnosti, která by byla doplněna novými ustanoveními, která se v EU pokládají za nutná.

4.5 Varianta 5: Aktualizace Úmluvy Rady Evropy o kybernetické trestné činnosti

Tato varianta by vyžadovala rozsáhlá jednání o přepracování současné úmluvy, což je zdlouhavý 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.

5. POSOUZENÍ DOPADŮ

Možné varianty	Hospodářské dopady	Sociální dopad	Dopady na základní práva	Dopad na třetí země	Význam pro cíle A, B, C	Soulad s mezinárodním právem
Varianta 1: Status quo / Žádné nové opatření ze strany EU	0	0	0	-	0	0
Varianta 2: Vypracování programu na zvýšení úsilí o odrážení útoků na informační systémy prostřednictvím nelegislativních opatření	-/+	++	-/+	++	A + B ++ C +	-/+
Varianta 3: Cílená aktualizace RR o útocích s cílem řešit konkrétní hrozbu, kterou představují rozsáhlé útoky proti informačním systémům	--/++	-/+++	-/++	+++	A +++ B +++ C +++	++
Varianta 4: Zavedení uceleného souboru právních předpisů EU proti kybernetické trestné činnosti	---/+++	+++	--/++	++	A ++ B ++ C ++	-/++
Upřednostňovaná varianta (varianty 2 a 3): kombinace nelegislativních opatření s cílenou aktualizací RR o útocích	--/+++	+++	-/++	+++	A +++ B +++ C +++	++

6. CO VYPLÝVÁ ZE SROVNÁNÍ RŮZNÝCH VARIANT?

6.1 Varianta 1: Zachování současného stavu

Tato varianta nevyhnutelně povede k oslabení pozice soukromých subjektů, členských států a Unie jako celé při řešení kybernetické trestné činnosti, s ohledem na její povahu a růst. I při zachování úrovně opatření, která existují v současné době, by bylo třeba zajistit koordinaci na evropské úrovni.

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

Tato varianta má všechny výhody a nevýhody právně nevynutitelného nástroje. Pozitivní stránkou je možnost popsat každou politickou možnost způsobem, který odpovídá osvědčeným vnitrostátním postupům, a tak usnadnit identifikaci nejefektivnějších opatření.

Tato varianta je však méně efektivní, pokud jde o dosahování cílů.

6.3 Varianta 3: Cílená aktualizace RR o útocích s cílem řešit hrozbu, kterou představují rozsáhlé útoky proti informačním systémům

Tato varianta nabízí včasnou a cílenou reakci na zjištěné problémy. Řeší trestněprávní témata, která jsou nezbytná k efektivnímu stíhání pachatelů tohoto trestného činu. Kromě toho zlepšuje mezinárodní spolupráci zavedením mechanismu okamžité mezinárodní pomoci v případě naléhavých žádostí o spolupráci a prostřednictvím doprovodných opatření podporuje spolupráci se soukromým sektorem, například formou setkání odborníků. Tato varianta rovněž zavádí řadu přitěžujících okolností, mezi něž patří například rozsáhlost útoku, útoky spáchané za utajení skutečné totožnosti pachatele a působící újmu skutečnému nositeli totožnosti.

Za účelem měření rozsahu problému se zavádí povinnost sledování.

6.4 Varianta 4: Zavedení uceleného souboru právních předpisů EU proti kybernetické trestné činnosti

Tato varianta, podobně jako varianta 3, přináší přidanou hodnotu zavedením závazných ustanovení, při jejím plném provedení se proto očekává vysoká úroveň efektivity. Rovněž se očekává, že tato varianta zvýší na maximum pozitivní dopad legislativních i nelegislativních nástrojů v širším okruhu kybernetických trestných činů, ne pouze u rozsáhlých útoků. Kromě toho by se zabývala trestněprávním rámcem a zároveň by zlepšila přeshraniční spolupráci při prosazování práva. Tento ucelený přístup však v této fázi neodráží konsensus zúčastněných stran, přestože by jeho provedení dovedlo boj s kybernetickou trestnou činností o krok dále než všechny ostatní varianty.

7. UPŘEDNOSTŇOVANÁ VARIANTA

Po analýze hospodářského a sociálního dopadu a dopadu na základní práva se jako nejvhodnější k dosažení vymezených cílů jeví varianty 2 a 3.

Upřednostňovaná varianta by byla kombinací variant politiky 2 a 3, protože tyto varianty se doplňují, a proto by nejlépe splnila vymezené cíle, pokud jde o podstatu i časový rámec.

8. SLEDOVÁNÍ A HODNOCENÍ

Do dvou let od vstupu této směrnice v platnost by měla být zveřejněna zpráva o provádění. Zpráva by se měla zaměřit na přesné provádění směrnice členskými státy.

Kromě toho by se měla provádět pravidelná hodnocení, aby se zjistilo, jak a do jaké míry směrnice přispěla k dosažení v ní vymezených cílů. První hodnocení by mělo být provedeno do pěti let po vstupu směrnice v platnost, poté bude Komise zveřejňovat hodnotící zprávy každých pět let a zahrne do nich informace o provádění. Na základě závěrů a doporučení hodnocení by Komise měla uvažovat o dalších změnách nebo dalším možném vývoji směrnice.