EURÓPAI BIZOTTSÁG

Brüsszel, 30.9.2010
SEC(2010) 1123 végleges

BIZOTTSÁGI SZOLGÁLATI MUNKADOKUMENTUM

A HATÁSVIZSGÁLAT ÖSSZEFOGLALÁSA

kísérődokumentum a következőhöz:

Javaslat:

AZ EURÓPAI PARLAMENT ÉS A TANÁCS IRÁNYELVE

az információs rendszerek elleni támadásokról és a 2005/222/IB tanácsi kerethatározat hatályon kívül helyezéséről

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

A HATÁSVIZSGÁLAT ÖSSZEFOGLALÁSA

1. PROBLÉMAMEGHATÁROZÁS

Az információs rendszerek elleni támadások száma az információs rendszerek elleni támadásokról szóló kerethatározat (a továbbiakban: a támadásokról szóló kerethatározat) elfogadása óta jelentősen megnőtt. Az egyik vezető internetes biztonsági cég jelentése szerint (a nyilvánosan elérhető adatokkal szemben) a bizalmas információkat fenyegető veszélyek nagy mértékben fokozódtak 2008-ban, amikor is az azonosított új fenyegetések száma 624 267-ről 1 656 227-re emelkedett.[1] Emellett számos, eddig nem tapasztalt kiterjedésű, fenyegetést jelentő támadásról számoltak be, például 2007-ben Észtországban, 2008-ban pedig Litvániában. 2009 márciusában 103 ország kormányzatának és magánszervezetének számítógépes hálózatát támadta meg kompromittált számítógépek hálózata, amely ilyen módon kényes és bizalmas jellegű dokumentumokat szerzett meg.[2] Mindezt „botneteknek", vagyis a fertőzött számítógépek távolból irányítható hálózatának a felhasználásával követték el[3]. Végül pedig, a világon jelenleg egyre jobban terjeszkedik a „Conficker" (más néven Downup, Downadup vagy Kido) nevű botnet, amely 2008 novembere óta világszerte több millió számítógépet megfertőzve eddig sosem tapasztalt mértékben és körben szaporodott el és működik.[4]

Másrészt, a tagállami, de különösen az Európai Unióban működő bűnüldöző szervek és igazságügyi hatóságok közötti együttműködés hiányosságai nehezítik meg a támadások elleni összehangolt és hatékony válaszlépéseket. A támadásokról szóló kerethatározat végrehajtási jelentése szerint a tagállamok többsége létrehozta ugyan a támadásokról szóló kerethatározat 11. cikkében előírt állandó kapcsolattartó pontokat, azonban azok reakcióképességével és a sürgős együttműködési kérésekre adott válaszadási készségével kapcsolatban továbbra is problémák merülnek fel.[5]

A kapcsolattartó pont megléte nem garantálja annak megfelelő működését. A Bizottságnak címzett értesítésében számos tagállam jelezte, hogy létrehozta ugyan a kapcsolattartó pontot, de a támadásokról szóló kerethatározat előírása ellenére az nem működik a nap 24 órájában. Ebből kifolyólag munkaidőn túl nem tud sürgős kérésekre választ adni. A köz- és a magánszféra együttműködését gyakran akadályozza, hogy a kapcsolattartó pontok nem elég hatékonyak, vagy nem tudják kezelni a magánszférából érkező együttműködési kéréseket.

---

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

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

3 A botnet fogalma alatt rosszindulatú szoftver (számítógépes vírus) által megfertőzött számítógépek hálózata értendő. A fertőzött számítógépek („zombik") hálózatát meghatározott tevékenységek elvégzésére, például információs rendszerek megtámadására (számítógépes támadások) lehet használni. Ezeket a „zombikat" egy másik számítógépről irányítani lehet, gyakran a fertőzött számítógép felhasználójának a tudtán kívül. Az „irányító" számítógép az „ellenőrző és irányító központ". A központot kezelő személyek bűnelkövetők, mivel információs rendszereket támadnak meg a fertőzött számítógépekkel. Az elkövetőket rendkívül nehéz felkutatni, mivel a botnetet alkotó, támadásokat elkövető számítógépek nem feltétlenül ugyanott találhatók, ahol az elkövető.

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

5 A Bizottság jelentése a Tanácsnak az információs rendszerek elleni támadásokról szóló, 2005. február 24-i tanácsi kerethatározat 12. cikke alapján, COM (2008)0448 végleges.

Harmadrészt, még mindig kevés adat áll rendelkezésre a számítógépes támadásokról, illetve azok rendőrségi és igazságügyi következményeiről. Nem minden tagállam gyűjti a számítógépes támadásokkal kapcsolatos adatokat. Abban az esetben pedig, ha gyűjtenek adatokat, azokat nem lehet összehasonlítani a tagállamok eltérő statisztikai módszerei miatt.

Az információs rendszerek ellen intézett támadások áldozatai között az információs rendszerek lakossági felhasználói, a kormányok, az önkormányzatok, valamint a nemzetközi illetve magánszervezetek egyaránt ott vannak.

Támadásokat lehet indítani harmadik országból az Európai Unióban található célpont ellen, illetve fordítva.

2. SZUBSZIDIARITÁS

A számítógépes bűnözés valódi nemzetközi probléma, amely ellen ritkán lehet pusztán tagállami keretek között küzdeni. Általánosan elfogadott, hogy megelőzése és leküzdése érdekében uniós és nemzetközi intézkedésekre van szükség. A támadások a legtöbb esetben átlépik az Európai Unió határait. Minden tagállamra kihatnak, emellett bizonyítható, hogy számos esetben az egyik tagállamból a másikba irányuló cselekményekről van szó. Az információs rendszerek gyakran egymáshoz kapcsolódnak és egymástól függenek, az államhatárokra való tekintet nélkül. A szakértők ezért azon a közös álláspontón vannak, hogy nemzetközi, illetve uniós intézkedésekre van szükség, és hogy a tagállamok önállóan nem tudják megvalósítani a számítógépes bűncselekmények elleni hatásos küzdelem célkitűzését.

A számítógépes bűnözésnek a kizárólag tagállami szintű megközelítése az összeurópai erőfeszítések elaprózódásának és hatástalanságának kockázatát hordozza magában. A nemzeti módszerek különbözőségei és a határokon átnyúló, szervezett együttműködés hiánya jelentősen csökkentik a tagállami ellenintézkedések hatékonyságát. Ez részben annak köszönhető, hogy az egyik országnak az információs rendszerei közötti szoros kapcsolatokból eredő alacsony biztonsági szintje adott esetben a többi országot is sebezhetővé teszi.

3. MIK A CÉLKITŰZÉSEK?

3.1. Általános, konkrét és működési célkitűzések

Az uniós fellépés átfogó célja a szervezett vagy egyéb bűnözés leküzdése és szankcionálása az információs rendszerek elleni nagyszabású számítógépes támadások visszaszorításával, az Európai Unió működéséről szóló szerződés 67. cikkének megfelelően.

A) Konkrét célkitűzés: a nagyszabású támadásokért felelős bűnelkövetők bíróság elé állítása és elítélése az információs rendszerek elleni támadásokra vonatkozó büntetőjogi jogszabályok közelítése által.

B) Konkrét célkitűzés: a bűnüldöző szervek közötti, határokon átnyúló együttműködés javítása.

C) Konkrét célkitűzés: hatékony megfigyelési rendszerek és adatgyűjtés megvalósítása.

4. MIK A SZAKPOLITIKAI VÁLASZTÁSI LEHETŐSÉGEK?

4.1. 1. választási lehetőség: a jelenlegi helyzet / új európai uniós fellépés mellőzése

E választási lehetőség értelmében az Európai Unió nem hoz további intézkedéseket a számítógépes bűnözés e típusának a leküzdése érdekében. A folyamatban lévő intézkedések, különösen a kritikus informatikai infrastruktúrák védelmének erősítésére, valamint a köz- és a magánszféra számítógépes bűnözés elleni együttműködésének javítására irányuló programok folytatódnának.

4.2. 2. választási lehetőség: az információs rendszerek elleni támadások visszaverésére irányuló erőfeszítéseknek a nem jogalkotási intézkedések segítségével történő erősítését célzó program kidolgozása

A nem jogalkotási intézkedések a kritikus informatikai infrastruktúrák védelmével foglalkozó program mellett a határokon átnyúló bűnüldözésre, valamint a magán- és a közszféra közötti együttműködésre összpontosítanának, és megkönnyítenék az uniós szinten összehangolt további intézkedéseket. Egy nem jogalkotási javaslat olyan intézkedéseket tartalmazhat, mint amilyen például bűnüldöző szervek kapcsolattartó pontjainak meglévő, a hét minden napjának 24 órájában működő hálózatának erősítése, a magán- és a közszféra kapcsolattartó pontjaiból álló uniós hálózatnak a számítógépes bűnözési szakértők és a bűnüldöző szervek bevonásával történő létrehozása, valamint a magánszféra szereplőivel való bűnüldözési együttműködésre irányuló, szolgáltatási szintű, alapvető uniós megállapodásnak a kidolgozása.

4.3. 3. választási lehetőség: a támadásokról szóló kerethatározat célzott frissítése az információs rendszerek elleni nagyszabású támadások által jelentett fenyegetés kezelése érdekében

Ez a választási lehetőség célzott (vagyis korlátozott) jogszabályokat vezetne be az információs rendszerek elleni, különösen veszélyes, nagyszabású támadások megakadályozása érdekében. Ilyen célzott jogszabály kapcsolódna az információs rendszerek elleni támadások leküzdésére irányuló operatív, határokon átnyúló együttműködés erősítéséhez, illetve a már meghatározott minimális szankciók növeléséhez. Ez a választási lehetőség a támadásokról szóló meglévő kerethatározat frissítése lenne, és olyan, nem jogalkotási intézkedések egészítenék ki, mint amilyen például a kritikus informatikai infrastruktúrák felkészültségének, biztonságának és rugalmasságának a javítása, valamint a bűnüldöző szerveknek a határokon átnyúló együttműködését és a bevált gyakorlatok cseréjét szolgáló eszközök és eljárások erősítése.

4.4. 4. választási lehetőség: a számítógépes bűnözés elleni, átfogó, uniós jogi szabályozás bevezetése

Az információs rendszerek elleni kifinomult támadások fejlődésével szembeni gyors fellépés szükségességének az azonosítása felveti azt a kérdést, hogy nem volna-e helyénvaló a számítógépes bűnözésre vonatkozó, szélesebb körű, általános uniós jogszabály bevezetése. Az említett jogszabály nemcsak az információs rendszerek elleni támadásokkal foglalkozna, hanem olyan kérdésekkel is, mint amilyen a pénzügyi számítógépes bűnözés, a jogsértő internetes tartalmak, az elektronikus bizonyítékok gyűjtése, tárolása és átvitele, valamint az alaposabb jogi szabályozás. Egy ilyen uniós jogszabály az Európa Tanács számítógépes bűnözésről szóló egyezménye mellett lenne alkalmazható, és különösen az Európai Unióban szükségesnek ítélt új rendelkezések egészítenék ki.

4.5. 5. választási lehetőség: az Európa Tanács számítógépes bűnözésről szóló egyezményének a frissítése

E választási lehetőség keretében részletesen újra kellene tárgyalni a jelenlegi egyezményt, ami hosszadalmas folyamat lenne, és nem felelne meg a hatásvizsgálat által javasolt cselekvési időkeretnek. Az egyezmény újratárgyalására nem mutatkozik nemzetközi szintű hajlandóság. Az egyezmény frissítése mint választási lehetőség ezért nem valósítható meg, mivel túllépi a megszabott cselekvési időkeretet.

5. A HATÁSOK ELEMZÉSE

Választási lehetőségek	Gazdasági hatás	Társadalmi hatás	Alapvető jogokra gyakorolt hatás	Harmadik országokra gyakorolt hatás	Jelentőség az A), B), C) célkitűzés szempontjából	A nemzetközi joggal való összhang
1. választási lehetőség: a jelenlegi helyzet / új európai uniós fellépés mellőzése	0	0	0	-	0	0
2. választási lehetőség: az információs rendszerek elleni támadások visszaverésére irányuló erőfeszítéseknek a nem jogalkotási intézkedések segítségével történő erősítését célzó program kidolgozása	-/+	++	-/+	++	A + B ++ C +	-/+
3. választási lehetőség: a támadásokról szóló kerethatározat célzott frissítése az információs rendszerek elleni nagyszabású támadások jelentette fenyegetés kezelése érdekében	--/++	-/+++	-/++	+++	A +++ B +++ C +++	++
4. választási lehetőség: a számítógépes bűnözés elleni, átfogó, uniós jogi szabályozás bevezetése	---/+++	+++	--/++	++	A ++ B ++ C ++	-/++
Előnyben részesített választási lehetőség (2. és 3. választási lehetőség): a nem jogalkotási intézkedéseknek és a támadásokról szóló kerethatározat célzott frissítésének a kombinációja.	--/+++	+++	-/++	+++	A +++ B +++ C +++	++

6. A SZAKPOLITIKAI VÁLASZTÁSI LEHETŐSÉGEK ÖSSZEHASONLÍTÁSA

6.1 1. választási lehetőség: a jelenlegi helyzet

E választási lehetőség hatására a számítógépes bűnözés természetéből és növekedési üteméből kifolyólag az ellene folytatott harcban sebezhetőbbé válnak a magánszereplők, a tagállamok, valamint az Európai Unió egésze. A jelenlegi intézkedések fenntartásához is szükség van európai szintű koordinációra.

6.2. 2. választási lehetőség: az információs rendszerek elleni támadások visszaverésére irányuló erőfeszítéseknek a nem jogalkotási intézkedések segítségével történő erősítését célzó program kidolgozása

Ez a választási lehetőség magában hordozza a nem kötelező jogi eszközök minden előnyét és hátrányát. Pozitív vetülete, hogy lehetővé teszi a szakpolitikai választási lehetőségeknek a bevált tagállami gyakorlatokkal való összevetését, ezáltal megkönnyítve a leghatékonyabb intézkedések azonosítását.

Ez a választási lehetőség azonban kevésbé hatékony a célkitűzések elérésének tekintetében.

6.3. 3. választási lehetőség: a támadásokról szóló kerethatározat célzott frissítése az információs rendszerek elleni nagyszabású támadások által jelentett fenyegetés kezelése érdekében

Ez a választási lehetőség időszerű és célirányos választ kínál az azonosított problémákra. Foglalkozik az említett bűncselekményeket elkövetők bíróság elé állításának hatékonyságával kapcsolatos büntetőjogi kérdésekkel is. Továbbá a sürgős együttműködési kérések esetén történő azonnali nemzetközi segítségnyújtásra szolgáló mechanizmus bevezetésével javítja a nemzetközi együttműködést, valamint kísérő intézkedésekkel, például szakértői találkozókkal támogatja a magánszektorral való együttműködést. Ez a választási lehetőség emellett számos súlyosító körülményt is bevezet, mint amilyen például a támadások nagyszabású jellege, valamint az elkövető valódi személyazonosságának eltitkolása és a személyazonosság jogos tulajdonosának okozott kár a támadások végrehajtása során.

Az irányelv végül nyomon követési kötelezettséget vezet be a probléma nagyságának a felmérése érdekében.

6.4. 4. választási lehetőség: a számítógépes bűnözés elleni, átfogó, uniós jogi szabályozás bevezetése

Ennek a választási lehetőségnek a 3. választási lehetőséghez hasonlóan az a hozzáadott értéke, hogy kötelező erejű rendelkezéseket vezet be, ezért teljes körű végrehajtásával nagyobb hatékonyságot lehet elérni. Várhatóan maximalizálja mind a jogalkotási, mind a nem jogalkotási eszközök pozitív hatását nemcsak a nagyszabású támadások, hanem a számítógépes bűncselekmények szélesebb köre esetében is. Ezenkívül foglalkozna a büntetőjogi kerettel is, emellett pedig javítaná a bűnüldöző szervek határokon átnyúló együttműködését. Ez a holisztikus megközelítés a jelenlegi szakaszban nem tükrözi az érintettek közötti egyetértést, bár végrehajtása a többi választási lehetőséghez képest egy lépéssel előbbre vinné a számítógépes bűnözés elleni küzdelmet.

7. ELŐNYBEN RÉSZESÍTETT SZAKPOLITIKAI LEHETŐSÉG

A gazdaságra, a társadalomra és az alapvető jogokra gyakorolt hatás elemzését követően a 2. és a 3. választási lehetőség kínálja a legjobb megoldásokat a probléma kezelésére, szem előtt tartva az azonosított célkitűzések elérését is.

Mindent összevetve, az előnyben részesített választási lehetőség a 2. és a 3. szakpolitikai választási lehetőség kombinációja lenne, mivel az említett lehetőségek kiegészítik egymást, és ezért a célkitűzések megvalósításának a legjobb módját kínálják mind tartalmilag, mind időben.

8. NYOMON KÖVETÉS ÉS ÉRTÉKELÉS

Az irányelv hatálybalépését követő 2 éven belül végrehajtási jelentést kell közzétenni. A jelentésnek figyelembe kell vennie az irányelv pontos tagállami végrehajtását.

Továbbá rendszeres értékeléseket kell készíteni annak felmérése céljából, hogy az irányelv hogyan és milyen mértékben járult hozzá a célkitűzés eléréséhez. Az első értékelést az irányelv hatálybalépését követő 5 éven belül kell elkészíteni, azután pedig a Bizottság ötévente a végrehajtással kapcsolatos információkat tartalmazó értékelő jelentéseket tesz közzé. A Bizottság az értékelések következtetései és ajánlásai alapján mérlegeli az irányelv további módosításának vagy más módon történő továbbfejlesztésének a lehetőségét.