ЕВРОПЕЙСКА КОМИСИЯ

Брюксел, 30.9.2010
SEC(2010) 1123 окончателен

РАБОТЕН ДОКУМЕНТ НА СЛУЖБИТЕ НА КОМИСИЯТА

РЕЗЮМЕ НА ОЦЕНКАТА НА ВЪЗДЕЙСТВИЕТО

придружителен документ към

предложение за

ДИРЕКТИВА НА ЕВРОПЕЙСКИЯ ПАРЛАМЕНТ И НА СЪВЕТА

относно атаките срещу информационните системи и за отмяна на Рамково решение 2005/222/ПВР на Съвета

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

РЕЗЮМЕ НА ОЦЕНКАТА НА ВЪЗДЕЙСТВИЕТО

1. ФОРМУЛИРАНЕ НА ПРОБЛЕМА

Броят на атаките срещу информационните системи се е увеличил значително след приемането на Рамковото решение относно атаките срещу информационни системи ("РР относно атаките"). Една от водещите фирми за сигурност в интернет съобщи, че заплахите, надвиснали над поверителната информация (за разлика от публично достъпната информация), са се увеличили значително през 2008 г., от 624 267 до 1 656 227 идентифицирани нови заплахи през 2008 г.[1] Освен това се наблюдават многобройни атаки от невиждан до този момент по своята големина и опасност мащаб като, например, в Естония и Литва съответно през 2007 г. и 2008 г. През март 2009 г. компютърните системи на държавни и частни организации от 103 страни са били атакувани от мрежа, състояща се от заразени компютри, която е извличала чувствителни и класифицирани документи[2]. Това е извършено чрез използване на "ботнети"[3]— мрежи от заразени компютри, които могат да бъдат контролирани от разстояние. На последно място в момента сме свидетели на разпространението по целия свят на ботнет, наречен "Conficker" (известен също като Downup, Downadup и Kido), който от ноември 2008 г. се е размножил в безпрецедентен мащаб и обхват и е поразил милиони компютри в света[4].

Второ, недостатъчното сътрудничество между държавите-членки, и по-специално между правоприлагащите и съдебните органи в рамките на ЕС, затруднява координираното и ефективното противодействие на тези атаки. Макар и от доклада за прилагането на РР относно атаките да личи, че мнозинството от държавите-членки са създали постоянни звена за контакт, както се изисква в член 11 от РР относно атаките, все още съществуват проблеми по отношение на тяхната готовност да откликнат и способността им да реагират на спешни искания за сътрудничество[5].

Наличието на звено за контакт не е гаранция за правилното му функциониране. В уведомленията си до Комисията редица държави-членки посочиха, че макар и съответните им звена за контакт да са създадени, те не работят 24 часа в денонощието,

---

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

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

3 С термина "ботнет“ се назовава мрежа от компютри, които са били заразени от зловреден софтуер (компютърен вирус). Такава мрежа от заразени компютри ("зомбита") може да бъде активирана за извършване на определени действия, като атаки срещу информационни системи (кибератаки). Тези "зомбита" могат да бъдат контролирани от друг компютър - често без знанието на потребителите на заразените компютри. Този "контролиращ" компютър е познат още като "командно-контролен център". Лицата, които контролират този център, са сред нарушителите, тъй като те използват заразените компютри, за да започнат атаки срещу информационните системи. Много е трудно извършителите да бъдат проследени, тъй като компютрите, които образуват ботнет и извършат атаката, могат да се намират на различно място от самия престъпник.

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

5 Доклад от Комисията до Съвета въз основа на член 12 от Рамково решение на Съвета от 24 февруари 2005 година относно атаките срещу информационните системи COM (2008) 0448 окончателен.

както се изисква в РР относно атаките. Това показва, че те не могат да отговорят на неотложни искания извън работно време. Публично-частното сътрудничество често е възпрепятствано от ниската ефективност на звената за контакт или неспособността им да откликнат на искания за сътрудничество от страна частния сектор.

Трето, все още има малко данни за атаки в кибернетичното пространство, както и за последващите действия на полицията и съдебните органи срещу тези атаки. Не всички държави-членки събират данни за атаки в кибернетичното пространство. Тези, които ги събират, правят това по начин, който не дава възможност те да бъдат сравнявани поради разликите в статистическите методологии, използвани от държавите-членки.

Сред жертвите на широкомащабни атаки срещу информационни системи е широката публика, състояща се от потребители на информационни системи, както и централните и местните власти, международни организации и частни структури.

Атаките могат да бъдат започнати в трети страни срещу цели в рамките на ЕС, както и обратното.

2. СУБСИДИАРНОСТ

Престъпленията в кибернетичното пространство представляват истински международен проблем, който едва ли може да бъде решен в тесен национален контекст. По принцип се приема, че са необходими действия на ЕС и международни действия с цел той да бъде предотвратен и решен. Повечето атаки пресичат границите на ЕС. Те засягат всички държави-членки и има доказателства, че значителна част от тях включват дейности от една държава-членка към друга. Информационните системи често са технически взаимосвързани и взаимозависими зад граница. Сред експертите има консенсус, че поради това са необходими международни действия и действия на ЕС и че целта за ефективната борба с такива престъпления не може да бъде постигната в достатъчна степен от държавите-членки.

Прилагането на национален подход към престъпността в кибернетичното пространство носи риск от пораждане на разпокъсаност и неефективност в цяла Европа. Различията в националните подходи и липсата на систематично трансгранично сътрудничество съществено намаляват ефективността на националните мерки за противодействие. Това отчасти се дължи на взаимосвързаността на информационните системи, като ниското ниво на сигурност в една страна може да увеличи на уязвимостта в други страни.

3. КАКВИ СА ЦЕЛИТЕ?

3.1 Общи, конкретни и оперативни цели

Общата цел на действията на ЕС е борбата и преследването на организираната или други форми на престъпност в съответствие с член 67 от Договора за функционирането на Европейския съюз, посредством борбата широкомащабни атаки в кибернетичното пространство срещу информационните системи.

А Конкретна цел: преследване и осъждане на престъпниците, отговорни за широкомащабни атаки, чрез сближаване на наказателното право в сферата на атаките срещу информационните системи.

Б Конкретна цел: подобряване на трансграничното сътрудничество между правоприлагащите агенции (ППА).

В Конкретна цел: създаване на ефективни системи за наблюдение и събиране на данни

4. КАКВИ СА ВАРИАНТИТЕ НА ПОЛИТИКАТА?

4.1 Вариант (1) : запазване на статуквото/без нови действия от страна на ЕС

Този вариант предполага, че ЕС няма да предприеме по-нататъшни действия за борба с този конкретен вид престъпления в кибернетичното пространство. Очаква се сегашните действия да продължат, по-специално програмите за укрепване на защитата на особено важната информационна инфраструктура и подобряване на публично-частното сътрудничество срещу престъпността в кибернетичното пространство.

4.2 Вариант (2): разработка на програма за по-енергични усилия за противодействие на атаките срещу информационните системи посредством незаконодателни мерки

В допълнение към програмата за защита на особено важната информационна инфраструктура, незаконодателните мерки биха се съсредоточили върху трансграничното правоприлагане и публично-частното партньорство и следва да улеснят по-нататъшните координирани действия на равнище ЕС. Едно незаконодателно предложение може да включва действия като засилване на съществуващата за правоприлагащите органи мрежа от звена за контакт, които са на тяхно разположение 24 часа в денонощието и седем дни в седмицата, създаване на мрежа на ЕС от публично-частни звена за контакт, в които да участват експерти по престъпления в кибернетичното пространство и експерти по правоприлагане и разработка на типово споразумение на ЕС за нивото на обслужване при сътрудничество с операторите в частния сектор в областта на правоприлагането.

4.3 Вариант (3): целенасочена актуализация на правилата на РР относно атаките, която да отговори на конкретната заплаха от широкомащабни атаки срещу информационни системи

Този вариант предполага въвеждане на специфично целево (*m.e.* ограничено) законодателство срещу особено опасни широкомащабни атаки срещу информационни системи. Такова целево законодателство ще бъде свързано с мерки за укрепване на оперативното трансгранично сътрудничество срещу атаки по информационните системи и увеличаване на вече предвидените минимални наказания. Този вариант ще има формата на актуализация на съществуващото РР относно атаките, допълнена с редица незаконодателни мерки като подобряване на готовността, сигурността и устойчивостта на особено важната информационна инфраструктура, защитата и укрепването на инструментите и процедурите за сътрудничество в областта на трансгранично правоприлагане, както и обмена на добри практики.

4.4 Вариант (4): въвеждане ново всеобхватно законодателство на ЕС срещу престъпленията в кибернетичното пространство

Признаването на необходимостта от предприемане на бързи действия срещу разработването на усъвършенствани атаки срещу информационните системи поставя въпроса дали би било целесъобразно да се въведе по-широко законодателство на ЕС срещу престъпленията в кибернетичното пространство като цяло. Такова законодателство би обхванало не само атаките срещу информационните системи, но и проблеми като финансовите престъпления в кибернетичното пространство, незаконно съдържание в интернет, събиране/съхранение/прехвърляне на електронни доказателства и по-подробни правила за компетентност. Такова законодателство на ЕС ще бъде приложимо заедно с Конвенцията на Съвета на Европа за престъпленията в кибернетичното пространство, която по-специално ще бъде допълнена с разпоредби, които се считат за необходими в рамките на ЕС.

4.5 Вариант (5): актуализация на Конвенцията на Съвета на Европа за престъпленията в кибернетичното пространство

За този вариант ще се изисква съществено предоговаряне на сегашната конвенция, а това е продължителен процес и е в противоречие със сроковете за действие, предложени в оценката на въздействието. На международно равнище не личи да има готовност за предоговаряне на конвенцията. Следователно актуализацията на конвенцията не може да се приеме за осъществим вариант, тъй като не спазва задължителните срокове за действие.

5. ОЦЕНКА НА ВЪЗДЕЙСТВИЯТА

Варианти	Икономи-ческо въздействие	Социално въздействие	Въздей-ствие върху основните права	Въздействие върху трети държави	Значение за цели А, Б, В	Съгла-суваност с междуна родното право
Вариант 1: запазване на съществуващото положение/без нови действия от страна на ЕС	0	0	0	-	0	0
Вариант 2: разработка на програма за по-енергични усилия за противодействие на атаките срещу информационните системи посредством незаконодателни мерки	-/+	++	-/+	++	А + Б ++ В +	-/+
Вариант 3: целенасочена актуализация на правилата на РР, която да отговори на заплахата от широкомащабни атаки срещу информационни системи	--/++	-/+++	-/++	+++	А +++ Б +++ В +++	++
Вариант 4: въвеждане на всеобхватно законодателство на ЕС срещу престъпленията в кибернетичното пространство	---/+++	+++	--/++	++	А ++ Б ++ В ++	-/++
Предпочитан вариант (варианти 2 и 3) комбинация от незаконодателни мерки с целенасочена актуализация на РР относно атаките	--/+++	+++	-/++	+++	А +++ Б +++ В +++	++

6. КАКВО ПОКАЗВА СРАВНЕНИЕТО НА ВАРИАНТИТЕ ЗА ПОЛИТИКА?

6.1 Вариант 1 – Запазване на съществуващото положение

Този вариант неизбежно ще постави в по-уязвимо положение представителите на частния сектор, държавите-членки и ЕС като цяло в борбата им с престъпленията в кибернетичното пространство, особено като се има предвид тяхното естество и растеж. Дори при стабилно равнище на сега съществуващите действия, в Европа ще е необходима координация.

6.2 Вариант (2): разработка на програма за по-енергични усилия за противодействие на атаките срещу информационните системи посредством незаконодателни мерки

Този вариант притежава всички предимства и недостатъци на един незадължителен правен инструмент. Положителният аспект е възможността да се опише всеки вариант на политика по начин, който е съобразен с най-добрите национални практики, като така се улеснява намирането най-добрите мерки от гледна точка на тяхната ефективност.

Този вариант обаче е по-малко ефективен за постигане на целите.

6.3 Вариант (3): целенасочена актуализация на правилата на РР относно атаките, която да отговори на заплахата от широкомащабни атаки срещу информационни системи

С този вариант се предлага навременен и целенасочен отговор на набелязаните проблеми. С него се решават наказателноправни въпроси за ефективното преследване на извършителите на такива престъпления. С него се подобрява също международното сътрудничество чрез въвеждане на механизъм за незабавно международно съдействие при спешни искания за сътрудничество и се насърчава сътрудничеството с частния сектор чрез съпътстващи мерки като например срещи на експерти. С този вариант се въвеждат също редица утежняващи вината обстоятелства като например широкомащабния характер на атаките, както и нападения, извършени с прикриване на истинската самоличност на извършителя и нанасящи щети на законния собственик на идентичността.

Накрая, за да е възможно да се измери мащаба на проблема, се въвеждат задължения за мониторинг.

6.4 Вариант (4): въвеждане ново всеобхватно законодателство на ЕС срещу престъпленията в кибернетичното пространство

Тази вариант, като и вариант 3, притежават добавена стойност, изразяваща се в създаването на обвързващи разпоредби, и следователно се очаква по-високо равнище на ефективност, ако бъдат напълно приложени. Очаква се също да се извлече максимална полза от положителното въздействие както от законодателните, така и от незаконодателните инструменти върху по-широк кръг от въпроси, свързани с престъпленията в кибернетичното пространство, а не само върху широкомащабни атаки. В допълнение с него ще се очертае правната рамка за наказателно право и същевременно ще се подобри трансграничното сътрудничество в областта на правоприлагането. За този цялостен подход обаче, на този етап заинтересованите страни не са постигнали консенсус, въпреки че ако бъде приведен в изпълнение,

борбата с престъпленията в кибернетичното пространство ще напредне много повече отколкото с всички други варианти.

7. ПРЕДПОЧЕТЕНИЯТ ВАРИАНТ НА ПОЛИТИКА

След анализа на икономическото въздействие, социалното въздействие и въздействието върху основните права, варианти 2 и 3 представляват най-добрият подход към проблемите с оглед постигане на поставените цели.

Като цяло предпочитаният вариант би бил комбинация от варианти на политиката 2 и 3, тъй като те взаимно се допълват и поради това отговарят най-добре на определените цели както по същество, така и спрямо сроковете.

8. НАБЛЮДЕНИЕ И ОЦЕНКА

В срок от 2 години след датата на влизане в сила на директивата следва да се публикува доклад за прилагането ѝ. В този доклад трябва да се обърне внимание на точното прилагане на директивата от държавите-членки.

Освен това следва да се извършват редовни оценки, за да се прецени как и до каква степен директивата ще е допринесла за постигането на своите цели. Първата оценка следва да бъде извършена в срок от 5 години след влизане в сила на директивата. След това на всеки 5 години Комисията ще публикува доклади за оценка, които ще включват информация за прилагането. Въз основа на заключенията и препоръките от извършените оценки Комисията следва да вземе предвид всички по-нататъшни изменения или други вероятни развития на директивата.