КОМИСИЯ НА ЕВРОПЕЙСКИТЕ ОБЩНОСТИ

Брюксел, 30.3.2009
SEC(2009) 400

РАБОТЕН ДОКУМЕНТ НА СЛУЖБИТЕ НА КОМИСИЯТА

Придружителен документ към

СЪОБЩЕНИЕ НА КОМИСИЯТА ДО СЪВЕТА, ЕВРОПЕЙСКИЯ ПАРЛАМЕНТ, ЕВРОПЕЙСКИЯ ИКОНОМИЧЕСКИ И СОЦИАЛЕН КОМИТЕТ И КОМИТЕТА НА РЕГИОНИТЕ

относно защитата на критичната информационна инфраструктура
„Защита на Европа от широкомащабни кибернетични атаки и смущения: повишаване на готовността, сигурността и устойчивостта“

ОБОБЩЕНИЕ НА ОЦЕНКАТА НА ВЪЗДЕЙСТВИЕТО

{COM(2009) 149}
{SEC(2009) 399}

ОБОБЩЕНИЕ НА ОЦЕНКАТА НА ВЪЗДЕЙСТВИЕТО

1. КАКЪВ Е ПРОБЛЕМЪТ?

Секторът на ИКТ е от жизнено важно значение за икономиката и обществото на ЕС

Информационните и комуникационните технологии (ИКТ) се превърнаха в гръбнака на икономиката и обществото на ЕС като цяло. **Секторът на ИКТ е от жизнено важно значение за всички области на обществото. Предприятията разчитат на сектора на ИКТ** по отношение както на преките продажби, така и на ефикасността и ефективността на вътрешните процеси. ИКТ са **все по-необходими и за функционирането на правителствата и публичните администрации**: навлизането на услугите на електронното управление на всички нива, макар че гарантира по-ефикасни процедури, прави публичния сектор силно зависим от ИКТ за много операции. Не на последно място **гражданите в нарастваща степен разчитат на информационното общество и използват ИКТ в своите ежедневни дейности**: наред с отрицателните последици, които би оказало върху тези дейности смущение във функционирането на компютърните мрежи, все повече лични данни на граждани се съобщават и предават по електронен път. Неадекватните мерки за сигурност биха могли да доведат до загуба на поверителна лична информация и да породят риск за кражба на самоличност или за друга измама[1]. **Следователно повишаването на сигурността и устойчивостта на тези инфраструктури е изключително важно за защита на личните данни на гражданите и за обезпечаване на правото на неприкосновеност на личния живот.**

Базираните на ИКТ системи и услуги са жизнено важни инфраструктури сами по себе си, както и като основна платформа за други критични технологични и обществени инфраструктури. Това бе признато в Зелената книга на Европейската комисия относно Европейската програма за защита на критичната инфраструктура, която обедини чрез концепцията за **критични информационни инфраструктури (КИИ)** всички „*ИКТ-системи, които са критични инфраструктури сами по себе си, или които са от съществено значение за функционирането на критични инфраструктури (далекосъобщения, компютри/софтуер, интернет, спътници и т.н.)*“[2] подобно на подхода на ОИСР[3].

Въпреки съществуващите терминологични различия, **важното е, че концепцията за КИИ води до перспективи за систематична политика за сигурно и непрекъснато функциониране на основаващи се на ИКТ системи, услуги, мрежи и инфраструктури** (накратко „ИКТ-инфраструктури“), **много важна съставна част от които е интернет** поради своето широко разпространение и процеса на технологична конвергенция.

---

1 http://www.timesonline.co.uk/tol/news/uk/crime/article4211711.ece

2 COM(2005) 576 окончателен.

3 http://www.oecd.org/dataoecd/1/13/40825404.pdf.

Какъв е залогът?

Повсеместното прилагане на ИКТ означава, че смущенията във функционирането на компютрите и компютърните мрежи **могат да се почувстват в широк мащаб от цялото общество**.

Рисковете, дължащи се на извършени от хора атаки, природни бедствия или технически неизправности, често не се разбират напълно и/или не са анализирани. Вследствие на това информираността на участниците е недостатъчна за разработване на адекватни механизми за защита и противомерки.

Кибератаките достигнаха безпрецедентно ниво на сложност и често са извършвани от отделни лица или престъпни групи за печалба или по политически съображения. **Широкомащабните кибератаки срещу Естония, Литва и Грузия са примери за една обща тенденция.** Огромният брой на компютърните вируси, червеи и други форми на зловреден софтуер, разрастването на т.нар. ботмрежи и непрекъснатото нарастване на спама потвърждават сериозността на проблема[4]. **ИКТ-инфраструктурите са подложени на непрекъснати атаки**, последиците от които биха били много по-тежки, ако Европа не се подготви за тях.

Голямата зависимост от КИИ, тяхната трансгранична взаимосвързаност и взаимозависимостите с други инфраструктури повишават необходимостта от **разглеждане на тяхната сигурност и устойчивост от системна гледна точка като предна линия на защита** срещу неизправности и атаки в допълнение към мерки за предотвратяване, борба и преследване на престъпни и терористични дейности, насочени срещу КИИ.

Характер на проблема

Понастоящем **проблемите по сигурността и устойчивостта на КИИ се решават главно на национално равнище при незначителна паневропейска координация**. **Липсата на систематично трансгранично сътрудничество съществено намалява ефективността на вътрешните противомерки.** Освен това **ниското ниво на сигурност и устойчивост на КИИ в една държава може да увеличи уязвимостта и рисковете в други държави**.

Тъй като КИИ са глобални, тясно свързани помежду си и взаимно зависими с други инфраструктури, осигуряването на тяхната сигурност и устойчивост **не може да бъде постигнато чрез чисто национални и некоординирани подходи**. Освен това **всеобщо е схващането, че пазарните сили предоставят достатъчно стимули на частния сектор за инвестиране в защитата на КИИ в размера, който би се изисквал обикновено от правителствата**.

Основните причини за общия проблем, описан по-горе, са:

- **нееднакъв подход на държавите-членки към публичната политика относно сигурността и устойчивостта на КИИ**. Съществуват различия в политиките на държавите-членки относно сигурността и устойчивостта на КИИ. Освен това изглежда, че нивото на експертни знания и готовност не е равномерно разпределено, както се изтъква в анализа на националните подходи, извършен от Комисията, което се потвърждава и от доклад на **Европейската агенция за мрежова и информационна сигурност (ENISA)**[5];

---

4 COM(2006) 688 окончателен.

5 http://www.enisa.europa.eu/doc/pdf/resilience/stock_taking_final_report_2008.pdf

- **трудно навлизане на нови, общоевропейски модели за управление.** Повишаването на сигурността и надеждността на КИИ е свързано със специфични **проблеми по управлението**. **Правителствата** са **отговорни** за определянето на политиката по отношение на КИИ, но **включването на частния сектор е от съществено значение** за нейното **прилагане**. За справяне с това съчетание от отговорности възникнаха **публично-частни партньорства** (ПЧП) на национално ниво като основен модел. Но въпреки общото единодушие, че ПЧП са желани и на европейско ниво, до сега такива не са осъществени;

- **ограничена европейска способност за ранно предупреждаване и реагиране на инциденти**. Консултациите показаха различия в националните системи за ранно предупреждаване и реагиране на инциденти. Някои държави-членки не получават редовно доклади за инциденти по мрежовата сигурност (макар че това може да се извършва неофициално между някои оператори) и/или не са определили организация, в която да постъпват тези доклади. Сътрудничеството и информационният обмен между **правителствените органи** изглеждат **недостатъчно развити** и спъвани от липсата на надеждни механизми за обмен и координация, което от своя страна **налага всички национални/правителствени екипи за незабавно реагиране при компютърни инциденти (Computer Emergency Response Teams — CERT) да функционират добре, т.е. да се разполага с общи основни способности**. Освен това **на равнището на ЕС все още са в зародишно състояние ученията и практическите симулации**, които са от ключово значение за повишаване на сигурността и устойчивостта на КИИ;

- **слаба информираност относно рисковете за сигурността и устойчивостта на интернет**. Интернет се доказа като **доста стабилна устойчива инфраструктура** благодарение на своята децентрализирана организация с дублиращи елементи. Въпреки това е основателно да се съмняваме в способността ѝ да издържи на **растящия брой** на смущенията и кибератаките, като се има предвид нейният **феноменален растеж**, **растяща сложност** и **появата на нови услуги**.

Никоя държава не е изолирана от останалите. Глобалният характер на КИИ и особено на интернет изисква **общ глобален подход** към сигурността и устойчивостта. **Чрез интензивна координация в рамките на ЕС може да се постигне пряко въздействие на международно равнище.**

2. КОЯ Е ОСНОВНАТА ПРИЧИНА ЗА ДЕЙСТВИЯТА НА ЕС?

Чисто национален подход за справяне с гореописаните проблеми може да не е достатъчен. Поради значителни трансгранични ефекти, много заплахи за мрежовата и информационната сигурност (МИС) притежават потенциала да причинят отрицателни трансгранични външни въздействия, ефективното справяне с които не е възможно на национално равнище, като те могат да причинят смущения в други държави.

Един обединен общоевропейски подход за повишаване на сигурността и устойчивостта на КИИ ползотворно би допълнил и придал европейска добавена стойност на националните програми за защита на критичната информационна инфраструктура и на съществуващите схеми за сътрудничество между държавите-членки. Тъй като много предизвикателства и проблеми са общи, един общ подход би бил от полза за всички.

Дискусиите след атаката срещу Естония навеждат на мисълта, че последиците от подобни събития могат да бъдат ограничени чрез **превантивни мерки** — като по-

структуриран обмен на информация на европейско равнище — и **координирани действия** по време на кризата. Комисията, зачитаща изцяло **принципа на субсидиарност**, е в най-добра позиция, за да може да координира тези усилия в тясно сътрудничество с държавите-членки и други международни организации.

Освен това макар националните интереси по отношение на сигурността да играят важна роля за определяне на политиката и задълженията за МИС, те могат да доведат до регулаторна разпокъсаност и да засегнат конкурентоспособността на Европейския съюз като цяло и способността на единния европейски пазар за създаване на благосъстояние.

През 2006 г. Комисията обяви[6] своето намерение по Европейската програма за защита на критичната инфраструктура[7] (EPCIP) да разработи специфична политика за сектора на ИКТ „*с оглед да се повиши сигурността и устойчивостта на мрежите и информационните системи*“. Това изявление бе приветствано от Европейския съвет през 2007 година[8].

Тази инициатива би отразила надлежно международното измерение, основавайки се на признати принципи като принципите на Г-8 относно защитата на КИИ, Резолюция 58/199 на Общото събрание на ООН „Създаване на глобална култура за кибернетична сигурност и защитата на критични информационни инфраструктури“ и последната препоръка на ОИСР относно защитата на КИИ.

Не на последно място предложената инициатива взема предвид и не дублира дейностите на НАТО в областта на кибернетичната сигурност, които са съсредоточени върху военната отбрана — например общата политика по киберотбраната и дейностите на Управителния орган по киберотбрана (CDMA), както и на Центъра за високи научни постижения по киберотбрана (CCD-COE).

3. КАКВИ СА ЦЕЛИТЕ?

Целта на настоящата инициатива е **да се повиши нивото на готовност и способност за реагиране в цяла Европа** спрямо описаните рискове и заплахи, като се избегнат различия в подхода на държавите-членки. Ударението ще се постави върху определянето на общи процеси за гъвкаво справяне с познати и непознати заплахи. Съответните заинтересовани страни от публичния и частния сектор ще се задължат да въведат в действие на **адекватни и съгласувани нива мерки за предотвратяване, откриване, незабавно реагиране и възстановяване за постигане на надлежното равнище на сигурност и устойчивост на КИИ и за гарантиране на непрекъснатост на услугите**. Подобрената сигурност и устойчивост също така биха оказали **положително въздействие върху защитата на личните данни и за неприкосновеността на личния живот на гражданите на ЕС**.

Общата цел на настоящото предложение, т.е. **гарантирането на сигурността и устойчивостта на КИИ като предна линия на защита**, може да се постигне чрез четири специфични цели:

(1) Премахване на различията в националните политики за сигурността и устойчивостта на КИИ;

---

6 COM(2006) 251
7 COM(2006) 786
8 Резолюция на Съвета 2007/C 68/01

(2) Усъвършенстване на европейското управление за сигурността и устойчивостта на КИИ;

(3) Укрепване на способността на Европа за оперативно реагиране на инциденти;

(4) Повишаване на сигурността и устойчивостта на интернет.

4. КАКВИ СА ПОЛИТИЧЕСКИТЕ ВАРИАНТИ?

Политически вариант 1: запазване на обичайната практика

Непредлагането на допълнителни мерки не би представлявало приемлив вариант. Без хоризонтални мерки на равнището на ЕС държавите-членки биха продължили да действат индивидуално или в рамките на двустранни или ограничени многостранни договорености. Това би породило **риск, свързан с еволюцията на различни национални подходи**, които могат да са несъвместими помежду си. Освен това трансграничното сътрудничество би било *ad hoc* и може да е неефективно поради сложността и мащаба на кибератаките.

Тъй като държавите-членки биха продължили да решават с различни темпове тези проблеми, **заинтересованите страни могат да се въздържат от инвестиране в сигурността и устойчивостта**, понеже многобройните стандарти и задължения биха намалили тяхната конкурентоспособност. Различията в сигурността, устойчивостта и готовността в рамките на Европа биха изпъкнали още повече поради трансграничния характер на проблема. Уязвимостта на КИИ в Европа би останала висока и вероятно ще нараства въпреки индивидуалните усилия.

Политически вариант 2: необвързваща рамка

Комисията би предоставила **рамката за координация и сътрудничество** под формата на съобщение и план за действие за ангажиране на държавите-членки, частния сектор и гражданското общество. Съобщението може да бъде одобрено от Съвета на ЕС, а Европейският парламент също може да реши да допринесе за обсъждането.

Инициативата би се съсредоточила върху горепосочените цели, като по-конкретно се предлага:

(1) **Насърчаване на съгласуваността в националните политики за сигурност и устойчивост на КИИ** чрез:

- установяване на примери, които могат да се заимстват, за практики за публична политика и общи черти;
- учредяване на Европейски форум, в чиято рамка държавите-членки да обменят информация и практики на добра политика относно сигурността и устойчивостта на КИИ.

(2) **Усъвършенстване на европейското управление за сигурност и устойчивост на КИИ** чрез:

- поставяне на началото на **Европейско публично-частно партньорство за устойчивост (EP3R)** за подпомагане на сътрудничеството между публичния и частния сектор относно целите за сигурност и устойчивост, основните изисквания, практики и мерки на добра политика.

(3) **Укрепване на способността на Европа за оперативно реагиране на инциденти** чрез:

- създаване на добре функциониращи национални/правителствени екипи за незабавно реагиране при компютърни инциденти (CERT)[9] като основен компонент на националната структура за готовност, информационен обмен, координация и реагиране;
- договаряне относно минималното равнище на способности и услуги на националните/правителствените екипи за незабавно реагиране при компютърни инциденти;
- насърчаване на сътрудничеството в Европа между националните/правителствените екипи за незабавно реагиране при компютърни инциденти; улесняване на контакта и сътрудничеството между националните структури за реагиране; организиране на паневропейски и/или регионални учения относно симулирани широкомащабни инциденти;
- насърчаване на разработването на планове за незабавно реагиране на мрежови инциденти и за възстановяване след бедствия;
- финансиране на разработването на европейски учения относно симулирани широкомащабни инциденти по мрежовата сигурност;
- подпомагане на разработването и внедряването на Европейска система за информационен обмен и предупреждаване (ЕСИОП), която по еднакъв и ефективен начин да обслужва граждани и малки и средни предприятия.

(4) **Повишаване на сигурността и устойчивостта на интернет** чрез:

- определяне на европейските приоритети относно дългосрочната стабилност и устойчивост на интернет;
- договаряне на система от европейски и впоследствие международни принципи за сигурност и устойчивост на интернет.

Политически вариант 3: обвързваща рамка

Повечето от гореспоменатите проблеми биха се решили чрез известен брой задължителни мерки, които по целесъобразност могат да бъдат под формата на директива, регламент или решение.

Комисията може да предложи задължителни мерки за:

(1) **определяне на основа за хармонизиране на националните политики**. Тези мерки могат да се съсредоточат върху сигурността и устойчивостта на КИИ извън рамката на вече предложеното пазарно законодателство;

(2) **определяне на ролята и отговорността на обществените и частните заинтересовани страни** за сигурността и устойчивостта на КИИ;

(3) **подобряване на оперативната готовност** — например чрез:

а) минимален набор от стандарти за хармонизирано равнище на функциите и услугите на националните/правителствените екипи за незабавно реагиране при компютърни инциденти;

б) рамка за изготвяне на национални планове за действие при непредвидени ситуации с оглед разработване на такива планове за целия ЕС.

[9] Екипи за незабавно реагиране при компютърни инциденти (Computer Emergency Response Teams)

5. КАКВО ПОКАЗВА СРАВНЕНИЕТО МЕЖДУ ПОЛИТИЧЕСКИТЕ ВАРИАНТИ?

Вариантът „запазване на обичайната практика“ **не показва явен потенциал** за подобряване на сигурността и устойчивостта на КИИ в Европа. Следователно трябва да се решава между необвързваща и обвързваща рамка. Понастоящем вариантът „обвързваща рамка“ изглежда неосъществим поради *inter alia*:

- суверенитета на държавите като **политическа реалност**, която надлежно трябва да отчетена в политиката относно мрежовата и информационната сигурност на равнището на Общността;
- необходимостта да се вземе предвид широко разпределената оперативна отговорност в частния сектор;
- липсата на натрупан опит по информационен обмен и сътрудничество относно политиките за КИИ между публичния и частния сектор.

Освен това **ниското качество на** наличните понастоящем **данни** относно инциденти по сигурността — дължащо се на информационни асиметрии и интереси на националната сигурност — затруднява определянето на регулаторни мерки, които да са съгласувани от икономическа и обществено-политическа гледна точка, и поражда **проблем за спазването на принципа на пропорционалността**, тъй като предлагането на пропорционални мерки е невъзможно, когато не е разбран добре точният размер на проблема.

Накрая, подходът за обвързваща рамка не би отговорил на потребностите на всички заинтересовани страни да се действа бързо, понеже неговото осъществяване би отнело дълго време поради продължителния процес на приемане.

В заключение от настоящата оценка на въздействието може да се направи изводът, че в кратко- и средносрочна перспектива е за предпочитане политически вариант 2, като незабавно се предприемат предложените мерки и своевременно се направи преглед на резултатите, включително тези от публичния дебат за консолидирана и осъвременена политика за мрежова и информационна сигурност в ЕС. След това те биха послужили като основа за оценяване на потребностите и възможностите относно възможни бъдещи задължителни мерки.

Тогава може да стане възможно да се препоръча прилагането на мерки, сходни с тези за политически вариант 3.