ЕВРОПЕЙСКА КОМИСИЯ

Брюксел, 31.3.2011
COM(2011) 163 окончателен

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

относно защитата на критичната информационна инфраструктура

„Постижения и предстоящи стъпки за постигане на сигурност в световното кибернетично пространство“

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

относно защитата на критичната информационна инфраструктура

„Постижения и предстоящи стъпки за постигане на сигурност в световното кибернетично пространство“

1. ВЪВЕДЕНИЕ

На 30 март 2009 г. Комисията прие Съобщение относно защитата на критичната информационна инфраструктура (ЗКИИ) — „Защита на Европа от широкомащабни кибернетични атаки и смущения: повишаване на готовността, сигурността и устойчивостта“[1], в което е представен план („план за действие за ЗКИИ“) за укрепване на сигурността и устойчивостта на инфраструктури от жизненоважно значение в областта на информационните и комуникационните технологии (ИКТ). Целта беше да се стимулира и подкрепи разработването на мерки за постигане на висока степен на готовност, сигурност и устойчивост както на национално, така и на европейско равнище. Този подход получи широко одобрение от Съвета през 2009 г.[2]

Планът за действие за ЗКИИ има пет основни елемента: готовност и предотвратяване, откриване и реагиране, смекчаване на последиците и възстановяване, международно сътрудничество и критерии за критичните европейски инфраструктури в областта на ИКТ. В плана се предвиждат задачите по всеки от основните елементи, които ще бъдат изпълнявани от Комисията, държавите-членки и/или съответния сектор с подкрепата на Европейската агенция за мрежова и информационна сигурност (ENISA).

Програмата в областта на цифровите технологии за Европа[3] (DAE), приета през май 2010 г., и свързаните с нея Заключения на Съвета[4] подчертаха общото схващане, че доверието и сигурността са основни предпоставки за широкото приемане на ИКТ и поради това играят важна роля за постигане на целите от направлението „интелигентен растеж“ на стратегията Европа 2020.[5] В програмата DAE се подчертава необходимостта от обединяване на силите на всички заинтересовани страни във всеобхватно усилие за гарантиране на сигурността и устойчивостта на инфраструктурите в областта на ИКТ, при което ударението пада върху предотвратяването, готовността и осведомеността, както и върху разработването на ефективни и координирани механизми за реакция на новите и все по-сложни форми на кибернетичните атаки и компютърната престъпност. Чрез този подход се осигурява надлежното вземане под внимание както на превантивните, така и на ответните аспекти на това предизвикателство.

---

1 COM(2009) 149.

2 Резолюция на Съвета от 18 декември 2009 г. относно европейски подход на сътрудничество по отношение на мрежовата и информационната сигурност (2009/C 321/01).

3 COM(2010) 245.

4 Заключения на Съвета от 31 май 2010 г. относно Програмата в областта на цифровите технологии за Европа (10130/10).

5 COM(2010) 2020 и Заключения на Европейския съвет от 25—26 март 2010 г. (EUCO 7/10).

Следните мерки, обявени в Програмата в областта на цифровите технологии, бяха приети през последните месеци: през септември 2010 г. Комисията прие предложение за директива относно атаките срещу информационни системи.[6] Тя е насочена към засилване на борбата срещу компютърната престъпност чрез сближаване на наказателно-правните системи на държавите-членки и подобряване на сътрудничеството между правните и други компетентни органи. В нея са съдържат и разпоредби за реагиране на нови форми на кибернетични атаки, по-конкретно на тези, извършвани с помощта на мрежи от ботове (botnets). Същевременно Комисията представи допълващо предложение[7] за нов мандат за укрепване и модернизиране на Европейската агенция за мрежова и информационна сигурност (ENISA) с цел засилване на доверието и мрежовата сигурност. Укрепването и модернизирането на ENISA ще помогне на ЕС, държавите-членки и заинтересованите частни лица да развият способността и готовността си за предотвратяване, откриване и реагиране на предизвикателствата, свързани със сигурността на кибернетичното пространство.

Не на последно място програмата DAE, Програмата и планът за действие от Стокхолм[8] и Стратегията за вътрешна сигурност на ЕС в действие (ISS)[9] подчертават ангажимента на Комисията за изграждане на цифрова среда, в която всеки европеец/ всяка европейка може напълно да разгърне своя икономически и социален потенциал.

В настоящото съобщение се прави преглед на резултатите, постигнати след приемането на плана за действие за ЗКИИ през 2009 г. В него се описват предстоящите стъпки, залегнали в плана на всяко действие както на европейско, така и на международно равнище. То се занимава също с глобалното измерение на предизвикателствата и значението на укрепването на сътрудничеството между държавите-членки и частния сектор на национално, европейско и международно равнище с цел да се овладеят взаимозависимостите в глобален контекст.

2. СЦЕНАРИЙ В РАЗВИТИЕ

Оценката на въздействието, придружаваща плана за действие за ЗКИИ[10], както и широк набор анализи и доклади от страна на частни и публични заинтересовани страни, подчертават не само социалната, политическа и икономическа зависимост на Европа от ИКТ, но също бързото нарастване на броя, обхвата, сложността и потенциалното въздействие на опасностите, било от естествен характер или предизвикани от човека.

Възникнаха нови и технологично по-сложни заплахи. Постепенно става ясно тяхното глобално геополитическо измерение. Ние сме свидетели на тенденция към използване на ИКТ за постигането на политическо, икономическо и военно надмощие, включително използване на възможностите им за нанасяне на вреда. В този контекст понякога се използват термини като „кибернетична война“ и „кибернетичен тероризъм“.

---

6 COM(2010) 517 окончателен.
7 COM(2010) 521.
8 COM(2010) 171.
9 COM(2010) 673.
10 SEC(2009) 399.

Освен това, както показаха последните събития в Южното Средиземноморие, някои режими са готови и са в състояние в името на политическите си цели да лишат своите граждани от достъп до ИТ средства за комуникации, по специално интернет и мобилни комуникации, или да пречат на този достъп. Такива едностранни национални интервенции могат да имат на свой ред съществен ефект върху други части на света[11].

За по-пълното разбиране на различните заплахи, може да бъде полезно те да се групират в следните категории:

– **използване**: например „комплексни устойчиви заплахи“[12] за целите на икономически и политически шпионаж (напр. GhostNet[13]), за кражба на идентичност, най-новите атаки срещу системата за търговия с емисии[14] или срещу правителствени ИТ системи[15];

– **смущаване**: например атаки за координирано блокиране на услуги или спам, генериран от мрежи от ботове (напр. мрежата Conficker със 7 милиона машини и базираната в Испания мрежа Mariposa със 12,7 милиона машини[16]), Stuxnet[17], както и блокирането на средствата за комуникация;

– **разрушаване**: този сценарий все още не е реализиран, но предвид нарастващото използване на ИКТ в критични инфраструктури (напр. интелигентни мрежи и водни системи), той не може да бъде изключен в бъдеще.[18]

3. ЕВРОПЕЙСКИЯТ СЪЮЗ И ГЛОБАЛНИЯТ КОНТЕКСТ

Предизвикателствата, които ни очакват, засягат не само Европейския съюз и не могат да бъдат преодолени самостоятелно от него. Разпространението на ИКТ и интернет позволява по-ефикасни, ефективни и икономични комуникации, координиране и сътрудничество между заинтересованите страни, в резултат на което възниква една пулсираща екосистема от иновации във всички области на живота. Но заплахите в тази среда също могат да идват отвсякъде и вследствие на глобалните връзки да засегнат всяка част от света.

---

11 Съвместно съобщение относно партньорство за демокрация и споделен просперитет с Южното Средиземноморие; COM(2011) 200 от 8.3.2011 г.

12 Т.е. продължителни и координирани атаки срещу правителствени агенции и публичния сектор. В момента това се превръща в проблем и за частния сектор (вж. „Доклад на RSA за тенденциите в компютърната престъпност през 2011 г.“).

13 Вж. докладите на Проекта за наблюдение на информационната война (Information Warfare Monitor project): „Проследяване на GhostNet: разследване на една мрежа за кибернетичен шпионаж“ (2009 г.) и „Сенки в облака: Разследване на кибернетичния шпионаж 2.0“ (2010 г.).

14 Вж. въпросите и отговорите на адрес: http://europa.eu/rapid/pressReleasesAction.do?reference=MEMO/11/34&format=HTML&aged=0&language=EN&guiLanguage=fr.

15 Напр. най-новите атаки срещи френското правителство.

16 Вж. проекта на ОИСР/IFP за „Глобалните шокове на бъдещето“, „Намаляване на системните рискове за кибернетичната сигурност“, 14 януари 2011 г: http://www.oecd.org/dataoecd/3/42/46894657.pdf.

17 Вж. http://www.enisa.europa.eu/media/press-releases/stuxnet-analysis.

18 Вж. Световен икономически форум, Глобални рискове през 2011 г. (World Economic Forum, Global Risks 2011).

Един чисто европейски подход не е достатъчен за овладяване на предстоящите предизвикателства. Въпреки че изграждането на съгласуван подход на сътрудничество в рамките на ЕС продължава да е от важно значение, това сътрудничество трябва да бъде поместено в рамките на глобална стратегия за координиране на усилията с ключови партньори, били те отделни държави или съответни международни организации.

Необходимо е да изградим глобално виждане за рисковете, произтичащи от широкото и масивно използване на ИКТ във всички сегменти на обществото. Нещо повече, трябва да изработим стратегии за подходящо и ефективно управление — предотвратяване, противопоставяне, смекчаване на последствията и противодействие — на тези рискове. В програмата DAE се призовава „*сътрудничеството между съответните участници […] да бъде организирано на глобално ниво за постигане на ефективна способност за борба със заплахите за сигурността и тяхното ограничаване*“ и се поставя целта да се „*работи със заинтересовани страни в световен мащаб по-специално за подобряване на* ***глобалното управление на риска*** *в цифровата и физическата сфера и да се предприемат международно координирани целенасочени действия срещу компютърната престъпност и атаките спрямо сигурността*“.

4. ПРИЛАГАНЕ НА ПЛАНА ЗА ДЕЙСТВИЕ ЗА ЗКИИ: НЯКОИ ВАЖНИ МОМЕНТИ

Пълният доклад за постиженията и предстоящите стъпки по плана за действие за ЗКИИ е предоставен като приложение. По-долу са представени някои важни моменти на състоянието понастоящем.

4.1. Готовност и предотвратяване

- **Европейският форум на държавите-членки** (ЕФДЧ) постигна съществен напредък в насърчаването на дискусията и обмена на информация между съответните органи въз основа на добрите практики в политиката относно сигурността и устойчивостта на инфраструктурите в областта на ИКТ. ЕФДЧ е призната платформа за дискусии и обмен на добри практики в областта на политиката сред държавите-членки.[19] Дейността на форума в бъдеще ще продължи да се ползва с подкрепата на ENISA и ще се концентрира върху сътрудничеството между националните/правителствените екипи за незабавно реагиране при компютърни инциденти (CERT), определянето на икономически и регулаторни стимули за сигурност и устойчивост (като същевременно се спазват приложимите правила за конкуренцията и държавните помощи), оценяването на „състоянието на кибернетичната сигурност“ в Европа, провеждането на паневропейски учения и дискусията по приоритетите на международните контакти в областта на сигурността и устойчивостта.

- Беше поставено началото на **Европейско публично-частно партньорство за устойчивост** (ЕПЧПУ), играещо ролята на паневропейска рамка за управление по въпросите на устойчивостта на инфраструктурите на ИКТ. Неговата цел е да насърчи сътрудничеството между публичния и частния сектор по стратегическите за

[19] В отговора на правителството на Обединеното кралство на петия доклад на Комитета за Европейския съюз към Камарата на лордовете относно плана за действие за ЗКИИ се посочва, че ЕФДЧ „*е успех и отговор на действителната нужда на лицата, определящи политическите насоки, от възможности за обмяна на опит*“.

ЕС въпроси на сигурността и устойчивостта. ENISA имаше подпомагаща роля за работата на ЕПЧПУ и съгласно предложението на Комисията от 2010 г. за модернизиране на ENISA би предоставила дългосрочна устойчива рамка за ЕПЧПУ. ЕПЧПУ ще служи също като платформа за международни контакти по въпросите на публичната политика, икономическите и пазарните въпроси, свързани със сигурността и устойчивостта, и особено за укрепване на управлението на риска относно инфраструктурите на ИКТ в световен мащаб.

- Беше разработен **минимален набор от базови способности и услуги**[20] и свързани с тях **политически препоръки**[21], необходими за правилното функциониране на националните/правителствените CERT в ролята им на основен компонент на националните системи за готовност, обмен на информация, координиране и реагиране. Резултатите от тези действия ще бъдат в основата на създаването, с помощта на ENISA, на мрежа от добре функциониращи национални/правителствени CERT във всички държави-членки до 2012 г. Една такава мрежа ще бъде гръбначният стълб на Европейската система за информационен обмен и предупреждаване (ЕСИОП) за граждани и МСП, която трябва да се изгради с национални ресурси до 2013 г.

4.2. Откриване и реагиране

- ENISA изготви план на високо равнище за създаване на Европейска система за информационен обмен и предупреждаване (**ЕСИОП**) до 2013 г.[22], която се основава на внедряването на *базовите услуги* на равнището на националните/правителствените CERT и на включването на *услуги за оперативна съвместимост* на националните системи за обмен на информация и предупреждаване в ЕСИОП. Подходящата защита на личните данни ще бъде един от основните елементи на тази дейност.

4.3. Смекчаване на последиците и възстановяване

- До момента само 12 държави-членки са организирали учения за широкомащабно реагиране на инциденти по мрежовата сигурност и за възстановяване след бедствия[23]. ENISA разработи **ръководство с добри практики за национални учения**[24] и **политически препоръки** за разработване на национални стратегии[25] с цел да бъдат подкрепени дейностите на държавите-членки, които следва да бъдат засилени.

- На 4 ноември 2010 г. се проведе първото **паневропейско учение за широкомащабни инциденти по мрежовата сигурност** (Cyber Europe 2010), в което участваха всички държави-членки (19 от тях активно), а също така Швейцария,

---

20 Вж. http://www.enisa.europa.eu/act/cert/support/files/baseline-capabilities-for-national-governmental-certs.

21 Вж. http://www.enisa.europa.eu/act/cert/support/files/baseline-capabilities-of-national-governmental-certs-policy-recommendations.

22 http://www.enisa.europa.eu/act/cert/other-work/eisas_folder/eisas_roadmap.

23 Източник : ENISA.

24 Вж. http://www.enisa.europa.eu/act/res/policies/good-practices-1/exercises/national-exercise-good-practice-guide/at_download/fullReport.

25 Вж. http://www.enisa.europa.eu/act/cert/support/files/baseline-capabilities-of-national-governmental-certs-policy-recommendations.

Норвегия и Исландия. Бъдещите паневропейски кибернетични учения ще се възползват несъмнено от общата рамка, която се основава на националните планове за действие в непредвидени ситуации и осъществява връзката между тях, като по този начин предоставя основни механизми и процедури за комуникация и сътрудничество между държавите-членки.

4.4. Международно сътрудничество

- В контекста на ЕФДЧ бяха обсъдени и разработени **Европейски принципи и насоки за постигане на устойчив и стабилен интернет**[26]. Комисията ще обсъди със съответните заинтересовани страни и ще им препоръча тези принципи, като се обърне по-конкретно към частния сектор (посредством ЕПЧПУ), към ключови международни партньори, по-специално към САЩ, посредством двустранен диалог както и в рамките на многостранни форуми. Това тя ще стори в рамките на своите компетенции на форуми като Г-8, ОИСР, НАТО (особено въз основа на новата стратегическа концепция на организацията, приета през ноември 2010 г., и на дейността на Центъра за сътрудничество и върхови постижения за защита на кибернетичното пространство), ITU (в контекста на създаване на капацитети в областта на сигурността на кибернетичното пространство), ОССЕ (чрез нейния Форум за сигурност и сътрудничество), ASEAN, Meridian[27], и др. Целта е тези принципи и насоки да се превърнат в споделена рамка за общ международен ангажимент за постигане на устойчив и стабилен интернет в дългосрочен контекст.

4.5. Критерии за европейски критични инфраструктури в сектора на ИКТ

- Техническата дискусия в ЕФДЧ доведе до **първи проект за специфични критерии в сектора на ИКТ** за установяване на критичните инфраструктури в Европа, в който се набляга на **стационарните и мобилните комуникации и на интернет**. Техническата дискусия ще продължи и ще бъде подкрепена от консултации с частния сектор по критериите на проекта на национално и европейско (посредством ЕПЧПУ) равнище. Също така, Комисията ще обсъди с държави-членки специфичните елементи на сектора на ИКТ, които да бъдат взети предвид при преразглеждането на Директивата относно установяването и означаването на европейски критични инфраструктури и оценката на необходимостта от подобряване на тяхната защита[28] през 2012 г.

5. БЪДЕЩО РАЗВИТИЕ

Прилагането на плана за действие за ЗКИИ е белязано от положителни постижения, по-конкретно във връзка с признаването на необходимостта от подход на сътрудничество по отношение на мрежовата и информационната сигурност, който да включва всички заинтересовани страни. При това, като цяло са спазени етапните цели и графикът, определени през 2009 г. Не бива обаче да изпадаме в самодоволство, тъй като все още

---

[26] Вж. http://ec.europa.eu/information_society/policy/nis/index_en.htm.

[27] Процесът Meridian има за цел да предостави на правителствата средство за дискусия в световен мащаб на възможностите за сътрудничество на политическо равнище относно защитата на критичната информационна инфраструктура (ЗКИИ). Вж. http://meridianprocess.org/.

[28] Директива 2008/114/ЕО на Съвета.

трябва да бъде направено много както на национално, така и на европейско равнище, за да се увенчаят тези усилия с успех.

Особено важно е също тези усилия да бъдат включени в глобална стратегия за координиране и по този начин да бъдат разширени така, че да обхванат и международната сцена, включвайки всички съответни заинтересовани страни, както и други региони, държави или организации, които се занимават с подобни въпроси, и да бъдат развити партньорства с цел приемане на съвместни подходи и свързани с тях дейности и избягване на дублирането на усилия.

Необходимо е да се насърчи на световно равнище развитието на култура на управление на риска. Ударението следва да падне върху насърчаването на съгласувани действия за предотвратяване, откриване, смекчаване на последствията и противодействие на всички видове смущения — от естествен характер или предизвикани от хора — и за преследване на свързаните компютърни престъпления. Това включва провеждането на целенасочени действия срещу заплахите за сигурността и срещу компютърната престъпност.

За тази цел **Комисията възнамерява да**:

- **налага принципи за устойчивост и стабилност на интернет** — съвместно с други страни, с международни организации и, когато е уместно, със световни организации от частния сектор следва да бъдат разработени международни принципи за устойчивост и стабилност на интернет, като се използват съществуващите *форуми* и процеси, като тези, свързани с управлението на интернет. Тези принципи следва да служат на всички заинтересовани страни като инструмент, даващ рамката за техните дейности за постигане на устойчив и стабилен интернет. Европейските принципи и насоки биха могли да служат като основа за това.

- **изгражда стратегически международни партньорства** — стратегическите партньорства следва да се основават на настоящите усилия в критични области като управлението на кибернетични инциденти, включително ученията и сътрудничеството сред CERT. От особено значение е ангажирането на частния сектор, опериращ в световен мащаб. Важна стъпка в тази посока се явява Съвместната работна група ЕС—САЩ за кибернетичната сигурност и компютърните престъпления, създадена на срещата на високо равнище ЕС—САЩ през ноември 2010 г. Работната група ще се занимава основно с управлението на кибернетични инциденти, публично-частни партньорства, повишаване на осведомеността и компютърни престъпления. Тя може също да разгледа възможности за контакти с други региони или държави, особено с такива, които имат сходни проблеми, с цел да бъдат определени съвместни подходи и сродни действия и да се предотврати дублирането на усилия, когато това е уместно. В рамките на международните форуми, по-специално на Г-8, следва да се търси задълбочаване на контактите и координирането. В европейски контекст ключови фактори за успеха ще бъдат добрата координация между всички институции на ЕС, съответните агенции (по-специално ENISA и Европол) и държавите-членки.

- **насърчава доверието в „изчислителните облаци“** — от важно значение е да се засилят дискусиите относно най-добрите стратегии за управление на нововъзникващи технологии с глобален обхват, като например „изчислителните облаци“. Сред темите на тези дискусии следва определено да присъства, без да е

единствената тема, подходящата рамка за управление относно защитата на личните данни. Доверието е съществен фактор за пълното оползотворяване на предимствата на тази технология.[29]

Тъй като отговорността за сигурността е обща, споделена отговорност, всички държави-членки трябва да гарантират, че техните национални мерки и усилия ще представляват принос за създаването на съгласуван европейски подход за предотвратяване, откриване, смекчаване на последствията и противодействие на всички видове кибернетични смущения и атаки. В този смисъл **държавите-членки следва да се ангажират**:

- **да подобрят готовността на ЕС посредством създаването на мрежа от добре функциониращи национални/правителствени CERT до 2012 г.** Съответно, на равнището на институциите на ЕС също ще бъде създаден CERT до 2012 г. Всички тези усилия следва да бъдат подпомогнати от минималния набор базови способности и услуги и свързаните с тях политически препоръки, разработени от ENISA, която ще продължи да оказва подкрепа на тези инициативи. Тези дейности ще дадат тласък на развитието на Европейската система за информационен обмен и предупреждаване (ЕСИОП) за широката общественост до 2013 г.

- **да изготвят Европейски план за действие при кибернетични инциденти до 2012 г. и редовно да организират паневропейски кибернетични учения.** Тези учения са важен елемент на една съгласувана аварийна стратегия за планиране и възстановяване при кибернетични инциденти както на национално, така и на европейско равнище. В бъдеще паневропейските кибернетични учения следва да се провеждат въз основа на Европейския план за действие при кибернетични инциденти, който е създаден въз основа на националните планове за действие в непредвидени ситуации и осъществява връзката между тях. Този план следва да предоставя базови механизми и процедура за връзка между държавите-членки и не на последно място да подпомага определянето на обхвата и организацията на бъдещи паневропейски учения. ENISA ще си сътрудничи с държавите-членки при разработването на Европейския план за действие при кибернетични инциденти до 2012 г. Всички държави-членки следва да разработят в същия срок редовни планове за действие в непредвидени ситуации и учения за предотвратяване и реагиране.

- **да координират европейското участие на международни форуми и в дискусии за укрепване на сигурността и устойчивостта на интернет.** Държавите-членки следва да сътрудничат помежду си и с Комисията за насърчаване на разработването на подход, основаващ се на принципи и норми, по проблема за глобалната стабилност и устойчивост на интернет. Целта следва да е насърчаване на готовността и предотвратяването на всички равнища и с участието на всички заинтересовани страни, в противовес на настоящата тенденция дискусиите да се съсредоточават върху аспекти на военната и/или националната сигурност.

---

[29] Вж. например докладите на ENISA „Cloud Computing Information Assurance Framework“ („Рамка за подсигуряване на информацията в изчислителните облаци“) от 2009 г., на адрес: http://www.enisa.europa.eu/act/rm/files/deliverables/cloud-computing-information-assurance-framework/at_download/fullReport) и „Security and resilience in governmental clouds“ („Сигурност и устойчивост на правителствените изчислителни облаци“) от 2011 г., на адрес: http://www.enisa.europa.eu/act/rm/emerging-and-future-risk/deliverables/security-and-resilience-in-governmental-clouds/).

6. ЗАКЛЮЧЕНИЕ

Опитът показва, че чисто национални или регионални подходи не са достатъчни за овладяване на предизвикателствата по отношение на сигурността и устойчивостта. Европейското сътрудничество претърпя значително развитие от 2009 г. насам и има окуражаващи постижения, например учението Cyber Europe 2010. Но Европа следва да продължи своите усилия за изграждането на съгласуван подход на сътрудничество в рамките на ЕС. След модернизацията си ENISA следва да засили подкрепата си за държавите-членки, институциите на ЕС и частния сектор в рамките на това дългосрочно начинание.

За да се увенчаят с успех, европейските усилия трябва да бъдат обхванати от координиран подход на световно равнище. За тази цел Комисията ще насърчава на всички подходящи международни форуми дискусиите по сигурността на кибернетичното пространство.

Конференция на министрите по въпроси на ЗКИИ, организирана от унгарското председателство на ЕС, ще се състои на 14—15 април 2011 г. Това ще бъде ключова възможност да се потвърди ангажиментът за засилване на сътрудничеството и координацията сред държавите-членки както на европейско, така и на международно равнище.

ПРИЛОЖЕНИЕ

План за действие за ЗКИИ: Подробен обзор на постиженията и предстоящи стъпки

Резултатите от проведените в рамките на плана за действие за ЗКИИ дейности като цяло отговарят на етапните цели и на графика, определени от Комисията през 2009 г. В следващия текст са описани „постиженията“ и „предстоящите стъпки“ за всеки един от основните елементи. Тази моментна снимка отчита, че някои дейности са били доразвити в рамките на Програмата в областта на цифровите технологии за Европа (DAE) и на Стратегията за вътрешна сигурност в действие (ISS).

1. Готовност и предотвратяване

Базови способности и услуги за паневропейско сътрудничество

Постижения

– През 2009 г. ENISA и общността на екипите за незабавно реагиране при компютърни инциденти (CERT) в Европа разработиха и се споразумяха за минималния набор от базови способности и услуги, с които националните/правителствените CERT трябва да разполагат, за да могат ефективно да подкрепят паневропейското сътрудничество. Беше постигнат консенсус по списъка, съдържащ задължителните изисквания относно операции, технически способности, мандат и сътрудничество.[30]

– През 2010 г. ENISA, в сътрудничество с общността на CERT в Европа, работи по превръщането на горепосочените изисквания с оперативна насоченост в набор от политически препоръки за националните/правителствените CERT[31] в ролята им на основен компонент на националните системи за готовност, обмен на информация, координиране и реагиране.

– Понастоящем 20 държави-членки[32] са изградили национални/правителствени CERT и почти всички останали имат планове за изграждането на такива екипи. Както беше посочено в Програмата в областта на цифровите технологии за Европа (DAE) и уточнено в Стратегията за вътрешна сигурност в действие (ISS), Комисията предложи мерки за създаване на CERT за институциите на ЕС до 2012 г.

Предстоящи стъпки

– ENISA ще продължи да подкрепя държавите-членки, които все още не са създали национални/правителствени CERT, отговарящи на горепосочените базови изисквания, за да гарантира, че до края на 2011 г. във всички държави-членки ще има добре функциониращи национални/правителствени CERT. Постигането на тази етапна цел ще направи възможно създаването на добре функционираща мрежа от CERT на национално равнище **до 2012 г.**, както е предвидено в програмата DAE.

---

30 Вж. http://www.enisa.europa.eu/act/cert/support/files/baseline-capabilities-for-national-governmental-certs.

31 Вж. http://www.enisa.europa.eu/act/cert/support/files/baseline-capabilities-of-national-governmental-certs-policy-recommendations.

32 Източник: ENISA.

– В сътрудничество с националните/правителствените CERT ENISA ще обсъди дали и как да разшири „базовите способности“, за да актуализира способността на CERT да подкрепят държавите-членки при осигуряването на стабилност и устойчивост на жизненоважните инфраструктури на ИКТ, и за да се превърне тя в гръбнак на Европейската система за информационен обмен и предупреждаване (ЕСИОП) за граждани и МСП, която трябва да се изгради с национални ресурси **до 2013 г.**, както е обявено в ISS.

Европейско публично-частно партньорство за устойчивост (ЕПЧПУ)

Постижения

– През 2009 г. беше поставено началото на ЕПЧПУ като общоевропейска рамка за управление на устойчивостта на инфраструктурите на ИКТ, насърчаваща сътрудничеството между публичния и частния сектор относно целите на сигурността и устойчивостта, базовите изисквания, добрите политически практики и мерки. Както е посочено в ISS, ЕПЧПУ освен това ще „*работи с международни партньори за подобряване глобалното управление на риска в ИТ мрежите*“. ENISA подпомагаше дейността на ЕПЧПУ.

– Бяха проведени консултации с частните и публичните заинтересовани страни за да се изработят целите, принципите и структурата на ЕПЧПУ и да се определят стимулите, чрез които да се насърчат съответните заинтересовани страни да участват активно.[33] Приоритетните области на ЕПЧПУ бяха определени в предложението за модернизиране на ENISA.[34]

– Паралелно с изработването на структурата на ЕПЧПУ в края на 2010 г. бяха създадени три работни групи за а) ключовите активи, ресурси и функции, необходими за непрекъснатото и сигурно предоставяне на електронните съобщения в страните; б) базовите изисквания за сигурност и устойчивост на електронните съобщения; в) нуждите на координацията и сътрудничеството и механизмите за подготовка и реакция на смущения в голям мащаб, засягащи електронните съобщения.

– През 2010 г. предложението на Комисията за модернизиране на ENISA предостави дългосрочна и устойчива рамка за ЕПЧПУ: в него се предлага ENISA да „*подкрепя сътрудничеството между заинтересовани страни от публичния и частния сектор на нивото на Европейския съюз inter alia чрез насърчаване на споделянето на информация и повишаването на осведомеността и чрез подпомагане на техните усилия за разработване и използване на стандарти за управление на риска и за сигурността на електронните продукти, мрежи и услуги*“

Предстоящи стъпки

– През 2011 г. ЕПЧПУ ще продължи да укрепва сътрудничеството между заинтересованите страни от публичния и частния сектор с цел да бъдат подобрени сигурността и устойчивостта чрез новаторски мерки и инструменти и да бъдат

[33] Вж. http://ec.europa.eu/information_society/policy/nis/strategy/activities/ciip/impl_activities/index_en.htm.

[34] COM(2010) 521.

определени отговорностите на заинтересованите страни. Работните групи на ЕПЧПУ ще постигнат своите първи резултати, възползвайки се от улесняващата и подпомагаща роля на ENISA. Бъдещите дейности ще бъдат насочени и към предизвикателствата в областта на кибернетичната сигурност на интелигентните мрежи, основавайки се на подготвителната работа, извършена от Комисията и ENISA.

– ЕПЧПУ ще служи като платформа за международни контакти по въпросите на публичната политика, икономическите и пазарните въпроси, свързани със сигурността и устойчивостта. Комисията възнамерява да използва ЕПЧПУ в подкрепа на дейността на Работната група ЕС—САЩ за кибернетична сигурност и компютърни престъпления, с цел да предостави съгласувана среда за сътрудничество между публичния и частния сектор, като същевременно спазва приложимите правила относно конкуренцията и държавните помощи.

– В дългосрочен план и в съответствие с предложението за нов регламент за ENISA се предвижда ЕПЧПУ да се превърне в ключова дейност на модернизираната ENISA.

Европейски форум за държавите-членки (ЕФДЧ)

Постижения

– С цел да се насърчат дискусиите и обменът на добри политически практики между съответните публични органи през 2009 г. беше създаден Европейският форум за държавите-членки (ЕФДЧ), с идеята да се обменя информация за политически цели и приоритети във връзка със сигурността и устойчивостта на инфраструктурите на ИКТ. Този форум се ползва пряко от работата и подкрепата на ENISA. ЕФДЧ, който се събира всяко тримесечие, се подкрепя от средата на 2010 г. от специален интернет-портал, поддържан от ENISA.

– ЕФДЧ постигна съществен напредък относно: а) определянето на критерии за установяване на европейските инфраструктури на ИКТ в контекста на Директивата относно установяването и означаването на европейски критични инфраструктури;[35] б) установяването на европейските приоритети, принципи и насоки за устойчивост и стабилност на интернет; в) обмен на добри политически практики, особено на такива относно кибернетични учения.

– ЕФДЧ е призната платформа за дискусии и обмен на добри практики в областта на политиката сред държавите-членки.[36]

Предстоящи стъпки

– През 2011 г. ЕФДЧ ще приключи техническата дискусия по критериите за европейски критични инфраструктури в областта на ИКТ и ще предостави

[35] Директива на Съвета 2008/114/ЕО.

[36] В отговора на правителството на Обединеното кралство на петия доклад на Комитета за Европейския съюз към Камарата на лордовете относно плана за действие за ЗКИИ се посочва, че ЕФДЧ „*е успех и отговор на действителната нужда на лицата, определящи политическите насоки, от възможности за обмяна на опит*“.

дългосрочни ориентири и приоритети за паневропейски широкомащабни учения в областта на мрежовата и информационната сигурност.

– Освен това ЕФДЧ ще участва и в дискусии относно приоритетите на международното сътрудничество за сигурност и устойчивост, особено във връзка с дейността на Работната група ЕС—САЩ за кибернетична сигурност и компютърни престъпления.

– Приоритетните области за бъдещи инициативи на ЕФДЧ, които ще се ползват от пряката помощ на ENISA, включват[37]: изработване на методи за ефективно сътрудничество между националните/правителствените CERT; установяване на минимални изисквания по отношение на обществени поръчки с цел да се увеличи кибернетичната сигурност; определяне на икономически и регулаторни стимули за сигурност и устойчивост (като същевременно се спазват приложимите правила за конкуренцията и държавните помощи); оценяване на състоянието на кибернетичната сигурност“ в Европа.

2. Откриване и реагиране

Европейска система за информационен обмен и предупреждаване (ЕСИОП)

Постижения

– Два проекта за създаване на прототипи (FISHAS и NEISAS) бяха финансирани от Комисията и вече дават първи резултати.

– Въз основа на своя доклад за осъществимостта[38] от 2007 г. и на анализ на подобни проекти на национално и европейско равнище, ENISA изготви план на високо равнище за развитието на ЕСИОП до 2013 г.[39]

Предстоящи стъпки

– През 2011 г. ENISA ще подкрепя държавите-членки при прилагането на плана за ЕСИОП, като разработва „базовите услуги“, от които те се нуждаят за създаването на своите национални системи за информационен обмен и предупреждаване (СИОП) въз основа на съответните национални/правителствени CERT.

– През 2012 г. ENISA ще разработи „услугите за оперативна съвместимост“, позволяващи всяка национална СИОП да бъде интегрирана в ЕСИОП. ENISA ще подпомага държавите-членки също при изпитването на тези услуги посредством постепенното интегриране на националните системи.

– В течение на 2011—2012 г. ENISA ще изиска от националните/правителствените CERT да интегрират СИОП в своите услуги.

3. Смекчаване на последиците и възстановяване

Национални планове за действие при непредвидени ситуации и учения

[37] COM(2010) 251.

[38] Вж. http://www.enisa.europa.eu/act/cert/other-work/files/EISAS_finalreport.pdf.

[39] http://www.enisa.europa.eu/act/cert/other-work/eisas_folder/eisas_roadmap.

Постижения

– В края на 2010 г. 12 държави-членки бяха разработили национален план за действие при непредвидени ситуации и/или организирали учения за широкомащабно реагиране на инциденти по мрежовата сигурност и за възстановяване след бедствия.[40]

– Въз основа на опита, събран на национално и международно равнище, ENISA разработи ръководство за добри практики във връзка с национални учения[41]; организира с държавите-членки и със CERT от целия свят мероприятия, посветени на националните учения; и издаде неотдавна препоръки относно разработването на национални стратегии, в които на националните/правителствените CERT/CSIRT (Computer Emergency Response Teams/Computer Security Incident Response Teams) е отредена водеща роля при ученията и изпитанията съгласно националните планове за действие при непредвидени ситуации с участието на заинтересовани страни от частния и публичния сектор.[42]

Предстоящи стъпки

– ENISA ще продължи да подкрепя усилията на държавите-членки за разработване на национални планове за действие при непредвидени ситуации и за организиране на редовни учения за реагиране на широкомащабни инциденти по мрежовата сигурност и за възстановяване след бедствия като стъпка към паневропейска координация.

Паневропейско учение за реагиране на широкомащабни инциденти по мрежовата сигурност

Постижения

– На 4 ноември 2010 г. се проведе първото паневропейско учение за широкомащабни инциденти по мрежовата сигурност (*Cyber Europe 2010*), в което се включиха всички държави-членки, като 19 от тях участваха активно, а също така Швейцария, Норвегия и Исландия. Организацията и оценката[43] на ученията бяха извършени от ENISA с активното участие на осем държави-членки в екипа по планирането и с технологичната подкрепа на Съвместния изследователски център (СИЦ).

Предстоящи стъпки

– През 2011 г. ще се проведат дискусии между държавите-членки относно целта и обхвата на следващото паневропейско кибернетично учение, планувано за 2012 г. Ще бъде разгледан вариант за постепенен подход, при който се провеждат по-задълбочени учения с участието на по-малък брой държави-членки и с възможност за включване на международни участници. ENISA ще продължи да подпомага този процес.

---

40 Вж. http://www.enisa.europa.eu/act/res/policies/good-practices-1/exercises/national-exercise-good-practice-guide/at_download/fullReport.

41 Вж. http://www.enisa.europa.eu/act/res/policies/good-practices-1/exercises/national-exercise-good-practice-guide/at_download/fullReport.

42 Вж. http://www.enisa.europa.eu/act/cert/support/files/baseline-capabilities-of-national-governmental-certs-policy-recommendations.

43 Вж. http://www.enisa.europa.eu/.

– Комисията подкрепя финансово проекта EuroCybex, в чиято рамка през втората половина на 2011 г. ще бъде проведено организационно учение.

– Кибернетичните учения са важен компонент на една съгласувана аварийна стратегия за планиране при кибернетични инциденти както на национално, така и на европейско равнище. Поради това в бъдеще паневропейските учения от такъв характер следва да се провеждат въз основа на Европейския план за действие при кибернетични инциденти, който е създаден въз основа на националните планове за действие в непредвидени ситуации и осъществява връзката между тях. Този план следва да предоставя базови механизми и процедура за връзка между държавите-членки и не на последно място да подпомага определянето на обхвата и организацията на бъдещи паневропейски учения. ENISA ще си сътрудничи с държавите-членки при разработването на Европейския план за действие при кибернетични инциденти до 2012 г. Всички държави-членки следва да разработят в същия срок редовни планове за действие при непредвидени ситуации и учения за предотвратяване и реагиране. Необходимата за постигането на този резултат координация ще бъде поета от ЕФДЧ.

Засилено сътрудничество между националните/правителствените екипи за незабавно реагиране при компютърни инциденти (CERT)

Постижения

– Сътрудничеството между националните/правителствените CERT стана по-интензивно. Работата на ENISA по базовите способности на националните/правителствените CERT, ученията на CERT и националните учения, както и по управлението на кибернетичните инциденти допринесе за насърчаването и подпомагането на засилено паневропейско сътрудничество между националните/правителствените CERT.

Предстоящи стъпки

– ENISA ще продължи да подкрепя сътрудничеството между националните/правителствените CERT. За тази цел през 2011 г. тя ще изготви анализ на изискванията и ще предостави насоки за създаване на подходящ канал за сигурни комуникации със CERT, включително план за изграждане и бъдещо развитие. Освен това тя ще анализира оперативните пропуски на европейско равнище и ще докладва за възможностите за засилване на трансграничното сътрудничество между CERT и съответните заинтересовани страни, по-специално с оглед на координирането на реакциите при инциденти.

– В програмата DAE държавите-членки се призовават да създадат добре функциониращa мрежа от CERT на национално равнище **до 2012 г.**

4. Международно сътрудничество

Устойчивост и стабилност на интернет

Постижения

– Въз основа на извършената в ЕФДЧ работа бяха разработени Европейски принципи и насоки за постигане на устойчив и стабилен интернет[44].

Предстоящи стъпки

– През 2011 г. Комисията: ще популяризира и обсъжда принципите както на двустранна основа с международни партньори, особено със САЩ, така и в многостранни дискусии в рамките на Г-8, ОИСР, Meridian и Международния съюз по далекосъобщения; ще проведе консултации със заинтересовани страни, по-конкретно с частния сектор, на европейско (чрез ЕПЧПУ) и международно (чрез Форума за управление на интернет или други подходящи форуми) равнище; ще насърчава дискусиите с ключови за интернет участници/организации.

– През 2012 г. международните партньори ще работят за превръщането на принципите и насоките в общоприета рамка за съвместни международни ангажименти в областта на дългосрочната устойчивост и стабилност на интернет.

Учения на световно равнище по възстановяване от широкомащабни инциденти в интернет и смекчаване на последиците от тях

Постижения

– Седем държави-членки[45] взеха участие като международни партньори в кибернетичното учение на САЩ Cyber Storm III. Комисията и ENISA участваха като наблюдатели.

Предстоящи стъпки

– В рамките на Работната група ЕС—САЩ за кибернетична сигурност и компютърни престъпления през 2011 г. Комисията ще разработи съвместно със САЩ обща програма и план за съвместни/съгласувани трансконтинентални кибернетични учения през периода 2012—2013 г. Ще бъдат разгледани също възможности за контакти с други региони или държави, работещи по сходни въпроси, с цел да бъдат определени съвместни подходи и сродни действия.

5. Критерии за европейски критични инфраструктури в сектора на ИКТ

Специфични секторни критерии за установяване на европейските критични инфраструктури в сектора на ИКТ

Постижения

– Техническата дискусия в ЕФДЧ относно специфичните секторни критерии за ИКТ доведе до разработването на проект за критерии за стационарните и мобилните комуникации и за интернет.

Предстоящи стъпки

[44] Вж. http://ec.europa.eu/information_society/policy/nis/index_en.htm.

[45] Франция, Германия, Унгария, Италия, Нидерландия, Швеция и Обединеното кралство.

– Техническата дискусия в ЕФДЧ относно специфичните секторни критерии за ИКТ ще продължи, като се очаква да приключи в края на 2011 г. Успоредно с това от някои държави-членки и на европейско равнище (чрез ЕПЧПУ) се плануват консултации с частния сектор по проекта за критерии в сектора на ИКТ.

– Комисията ще обсъди с държавите-членки специфичните за сектора на ИКТ елементи, които трябва да бъдат взети под внимание в рамките на преразглеждането на Директива 2008/114/ЕО относно установяването и означаването на европейски критични инфраструктури през 2012 г.

–