ЕВРОПЕЙСКА
КОМИСИЯ

Брюксел, 7.2.2013
SWD(2013) 31 final

РАБОТЕН ДОКУМЕНТ НА СЛУЖБИТЕ НА КОМИСИЯТА

ОБОБЩЕНИЕ НА ОЦЕНКАТА НА ВЪЗДЕЙСТВИЕТО

придружаваща

Предложение за директива на Европейския парламент и на Съвета

относно мерки за гарантиране на високо ниво на мрежова и информационна сигурност в рамките на Съюза

{COM(2013) 48 final}
{SWD(2013) 32 final}

РАБОТЕН ДОКУМЕНТ НА СЛУЖБИТЕ НА КОМИСИЯТА

ОБОБЩЕНИЕ НА ОЦЕНКАТА НА ВЪЗДЕЙСТВИЕТО

придружаваща

Предложение за директива на Европейския парламент и на Съвета

относно мерки за гарантиране на високо ниво на мрежова и информационна сигурност в рамките на Съюза

1. ОБХВАТ

Настоящата оценка на въздействието обхваща варианти на политиката, насочени към подобряване на сигурността на интернет и другите мрежи и информационни системи, залегнали в основата на услугите, поддържащи функционирането на нашето общество (например публични администрации, финансови и банкови услуги, енергетика, транспорт, здравеопазване и някои интернет услуги, имащи ключово значение за основните икономически и социални процеси, като платформите за електронна търговия и социалните мрежи). Общо този проблем е означен по-долу като „мрежова и информационна сигурност (МИС)“.

2. КОНТЕКСТ НА ПОЛИТИКАТА

Нарастващото значение на МИС за нашите икономики и общества беше признато от Комисията за първи път през 2001 г. За да се гарантира високото ниво и ефективността на МИС в ЕС, през 2004 г. Европейската общност взе решение да бъде създадена Европейска агенция за мрежова и информационна сигурност (ENISA). Подходът, практикуван до момента в Европейския съюз в областта на МИС, предвиждаше главно приемането на поредица от планове за действие и стратегии, в които се призоват държавите членки да увеличат своя капацитет в сферата на МИС и да си сътрудничат в борбата срещу трансграничните проблеми в тази област.

Със заинтересованите страни се проведоха консултации относно различни аспекти на инициативата (определяне на проблема и възможности за преодоляване на съществуващите недостатъци) посредством:

- **обществена консултация онлайн** на тема „Подобряване на МИС в ЕС“, която беше проведена от 23 юли до 15 октомври 2012 г. Общо 169 отговора постъпиха онлайн, а други 10 бяха получени от Комисията по пощата;
- обсъждания с **държавите членки** в контекста на Европейския форум за държавите членки (ЕФДЧ), на двустранни срещи и на конференцията на ЕС за киберсигурността, организирана от Комисията и Европейската служба за външна дейност на 6 юли 2012 г.;
- дискусии с фирми и асоциации от **частния сектор** в рамките на Европейското публично-частно партньорство за устойчивост (EP3R) и на двустранни срещи;
- дискусии с **ENISA и CERT-EU**;
- дискусии в контекста на **Асамблеята за цифрово развитие за 2012 г.**

3. ОПИСАНИЕ НА ПРОБЛЕМА

3.1. Определяне на проблема

Проблемът може да бъде описан като принципно ***недостатъчно равнище на защитата срещу инциденти, рискове и заплахи в областта на мрежовата и информационна сигурност в целия ЕС, което възпрепятства правилното функциониране на вътрешния пазар.***

Като се има предвид, че мрежите и информационните системи са взаимосвързани, и като се отчете глобалният характер на интернет, много от инцидентите в областта на МИС имат последствия, които излизат извън националните граници и вредят на функционирането на вътрешния пазар.

Може например да бъде нарушен достъпът до трансгранични услуги или те да бъдат прекратени или прекъснати поради нарушения на сигурността, както беше при атаките срещу eBay и PayPal. Необходимостта да се действа бързо при решаване на проблемите и да се обменя информация за значителни инциденти пролича при атаките срещу Diginotar, нидерландското дружество за интернет сертификати. В отговор на предишни инциденти държавите членки започват да въвеждат свои собствени регулаторни разпоредби. Некоординираните регулаторни интервенции могат да доведат до разпокъсаност на мерките и до възникване на бариери, което ще предизвика разходи за съвместимост за предприятията, работещи в повече от една държава членка.

Този проблем засяга всички елементи на обществото и икономиката (държавно управление, предприятия и потребители). По-специално, редица отрасли играят основна роля при предоставянето на ключови услуги за нашата икономика и общество и сигурността на техните системи е от особен интерес за функционирането на вътрешния пазар. Сред тези сектори са банковото дело, фондовите борси, производството, преносът и разпределението на енергия, транспортът (въздушен, железопътен, морски), здравеопазването, секторите, играещи съществена роля за ключовите интернет услуги и публичните администрации. Обществената консултация показа силната подкрепа от страна на заинтересованите страни за решаването на проблемите, засягащи МИС в тези сектори, и за предприемането на действия на равнище ЕС.

Ако не бъдат предприети допълнителни мерки за преодоляване на нарастващия брой инциденти, доверието на потребителите в онлайн услугите би могло да пострада и това може да попречи на постигането на целите на Програмата в областта на цифровите технологии.

3.2. Причини за възникването на проблема

Така определеният проблем се дължи на редица фактори.

На първо място е налице **нееднакво равнище на националния капацитет в ЕС**, което пречи между партньорите да възникне доверието, явяващо се предварително условие за сътрудничеството и обмена на информация.

На второ място **обменът на информация за инциденти, рискове и заплахи е недостатъчен**. Повечето инциденти, свързани с МИС, остават недекларирани и незабелязани главно поради нежеланието на предприятията да обменят такава информация поради страха да не навредят на репутацията си или да не дадат повод за искове за обезщетения. Обменът на информация в рамките на съществуващите публично-частни партньорства/платформи, като например ЕФДЧ и EP3R, се ограничава до обмен на най-добри практики.

4. ЕФЕКТИВНОСТ НА СЪЩЕСТВУВАЩИТЕ МЕРКИ

4.1. Пропуски в съществуващата регулаторна рамка

Съгласно настоящите правила не се изисква предприятията, работещи извън сферата на далекосъобщенията, да приемат мерки за управление на риска в областта на МИС и да докладват за инциденти, свързани с МИС. Всички участници, разчитащи на мрежови и информационни системи, обаче са изправени пред рискове за сигурността. Това води до неравнопоставеност, тъй като един и същ инцидент, засягащ например доставчик на далекосъобщителни услуги и предприятие, предоставящо услуги за предаване на глас по интернет, трябва да се докладва на националния компетентен орган в първия случай, но не и във втория.

Всички участници, които работят с данни (напр. банки или болници), са задължени от регулаторната рамка за защита на данните да въведат мерки за сигурност, които са пропорционални на рисковете, пред които са изправени. Те обаче са длъжни да докладват само за онези нарушения на сигурността, които са довели до компрометиране на лични данни.

Директива 2008/114/ЕО относно установяването и означаването на европейски критични инфраструктури обхваща само секторите на енергетиката и транспорта и към днешна дата държавите членки са идентифицирали само някои от европейските критични инфраструктури. С директивата не се предвиждат задължения за операторите да докладват за значителни нарушения на сигурността и не се установяват механизми, чрез които държавите членки да си сътрудничат и действат съвместно в отговор на инциденти.

Съзаконодателите понастоящем обсъждат предложението на Комисията за директива относно атаките срещу информационните системи[1]. Това предложение се отнася само до инкриминирането на определено поведение, но не се занимава с предотвратяването на рисковете и инцидентите по отношение на МИС, с ответните действия при инциденти, свързани с МИС, и ограничаването на последствията от тези инциденти.

4.2. Границите на доброволния подход

Доброволният подход, практикуван досега, доведе до нееднакви равнища на готовност и ограничено сътрудничество.

Мандатът на ЕФДЧ е ограничен, като се има предвид, че държавите членки не обменят информация за инциденти, рискове и заплахи нито пък си сътрудничат в борбата с трансграничните заплахи. ЕФДЧ не разполага с правомощия да изисква от своите членове да разполагат с минимален капацитет.

ENISA няма оперативни правомощия и не може да се намесва например, за да решава проблеми в сферата на МИС.

EP3R не е официална структура и не може да изисква от частния сектор да докладва за инцидентите на националните органи. В рамките на EP3R липсва схема за надежден информационен обмен и за разпространяване на информация относно заплахи, рискове и инциденти във връзка с МИС.

[1] COM(2010) 517, http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2010:0517:FIN:EN:PDF.

5. НУЖДА ОТ НАМЕСА НА ЕС, СУБСИДИАРНОСТ И ПРОПОРЦИОНАЛНОСТ

Обезпечаването на МИС е от жизненоважно значение за доброто функциониране на вътрешния пазар и за благосъстоянието на нашето общество. Член 114 от ДФЕС е подходящото правно основание за хармонизиране на изискванията относно МИС и за въвеждане на общо минимално ниво на сигурност в целия ЕС.

Намесата на Съюза в областта на МИС е оправдана от гледна точка на принципа на **субсидиарност** поради трансграничния характер на проблема и повишената в сравнение със съществуващите национални политики ефективност (и възникващата по този начин добавена стойност), до която би се стигнало в резултат на предприемането на действия на равнище ЕС.

За да се осигури взаимодействие, обхващащо всички държави членки, е необходимо да се гарантира, че техният капацитет е на изискваното минимално равнище. Освен това е ясно, че съгласуваните и съвместни политически действия в сферата на МИС могат да окажат изключително благоприятно влияние върху ефективната защита на основните права, и по-специално на правото на защита на личните данни и неприкосновеността на личния живот.

Мерките в предпочетения вариант са оправдани по отношение на принципа на **пропорционалност**, като се има предвид, че изискванията към държавите членки са определени на минималното равнище, необходимо за постигане на адекватна готовност и даване на възможност за сътрудничество, основаващо се на доверие, и че изискванията предприятията и публичните органи да осъществяват управление на риска и да докладват за инцидентите се отнасят само за критични икономически субекти, като налаганите мерки са пропорционални на рисковете и засягат инциденти със значително въздействие. Освен това мерките по предпочетения вариант няма да предизвикат прекомерни разходи.

6. ЦЕЛИ

Общата цел е да се повиши нивото на защита срещу инциденти, рискове и заплахи в целия ЕС, свързани с мрежовата и информационната сигурност. Конкретните цели са:

- **Цел 1** — да се въведе минимално общо ниво на МИС в държавите членки и по този начин да се повиши общото ниво на готовността и ответните действия;
- **Цел 2** — да се подобри сътрудничеството относно МИС на равнище ЕС с цел да се противодейства ефективно на трансгранични инциденти и заплахи;
- **Цел 3** — да се създаде култура на управление на риска и да се подобри обменът на информация между частния и публичния сектор.

7. ВАРИАНТИ НА ПОЛИТИКАТА

Вариантите на политиката, които бяха разгледани в настоящата оценка на въздействието, са: запазване на обичайната практика, регулаторен подход и смесен подход. Вариантът, предвиждащ прекратяване на всички дейности на ЕС в областта на МИС, беше отхвърлен.

7.1. Вариант 1 — запазване на обичайната практика („базисен вариант“)

Комисията, с помощта на ENISA, ще продължи работата по текущия доброволен подход, призовавайки държавите членки да изградят капацитет в областта на МИС на национално равнище (например екипи за незабавно реагиране при компютърни

инциденти, национални планове за действие при киберинциденти/в непредвидени ситуации, национални стратегии в областта на киберсигурността) и да си сътрудничат на равнище ЕС (напр. чрез мрежа, свързваща екипите за незабавно реагиране при компютърни инциденти в цяла Европа, и Европейски план за действие и сътрудничество при киберинциденти и в непредвидени ситуации).

7.2. Вариант 2 — регулаторен подход

Комисията ще изиска от всички държави членки да изградят своя национален капацитет поне до едно минимално равнище (екипи за незабавно реагиране при компютърни инциденти, компетентни органи, национални планове за действие при киберинциденти/в непредвидени ситуации, националните стратегии в областта на киберсигурността).

Съгласно този регулаторен вариант националните компетентни органи и екипите за незабавно реагиране при компютърни инциденти ще бъдат част от **мрежа** за сътрудничество на равнище ЕС. В рамките на мрежата органите и екипите за незабавно реагиране при компютърни инциденти ще обменят информация и ще си сътрудничат в борбата срещу заплахите и инцидентите в областта на МИС съгласно **Европейския план за действие и сътрудничество при киберинциденти и в непредвидени ситуации**, който ще трябва да бъде приет от държавите членки.

От предприятията (с изключение на микропредприятията) в конкретни критични сектори, т.е. банково дело, енергетика (електроенергия и природен газ), транспорт, здравеопазване, сектори, играещи съществена роля за ключовите интернет услуги и публичните администрации, ще се изисква да оценяват рисковете, пред които са изправени, и да приемат подходящи и пропорционални мерки за измерване на действителните рискове. Освен това от тези икономически субекти ще се изисква да докладват на компетентните органи за инцидентите, които нарушават сериозно функционирането на техните мрежи и информационни системи и по този начин оказват значително въздействие върху непрекъснатостта на услугите и доставката на стоки, основаващи се на мрежови и информационни системи. Тази схема следва посоченото в член 13а и 13б от Рамковата директива за електронните съобщения.

7.3. Вариант 3 — смесен подход

Комисията би могла да комбинира доброволни инициативи на държавите членки, насочени към изграждане или засилване на техния капацитет в сферата на МИС и към създаване на механизми за сътрудничество на равнище ЕС, с регулаторни изисквания по отношение на частните участници и публичните администрации, имащи ключова роля.

Доброволните инициативи по същество ще бъдат сходни с тези, предприети съгласно вариант 1, докато регулаторните изисквания ще бъдат същите като въведените съгласно вариант 2 както по отношение на избора на целеви предприятия, така и по отношение на същината на задълженията.

ENISA ще предоставя подкрепа и специализирани експертни познания на Комисията, държавите членки и частния сектор, например чрез издаването на технически насоки и препоръки.

8. АНАЛИЗ НА ВЪЗДЕЙСТВИЕТО

Освен нивото на сигурност оценката обхваща икономическото и социално въздействие на всеки от трите варианта. Тя разглежда също разходите, които биха възникнали при варианти 2 и 3.

Нито един от набелязаните варианти няма да има въздействия върху околната среда, които да могат да бъдат предвидени с точност.

8.1. Вариант 1 — запазване на обичайната практика („базисен вариант“)

Ниво на сигурност: Малко вероятно е всички държави членки да постигнат сравнимите равнища на националния капацитет и готовността, необходими, за да се подобри сигурността и да станат възможни сътрудничеството и обменът на доверителна информация на равнище ЕС. Няма да бъде постигната равнопоставеност по отношение на управлението на риска и повишаването на прозрачността относно инцидентите и поради това ще продължат да съществуват „вратички“ в нормативните уредби.

Икономически въздействия: Въздействието ще зависи от степента, в която държавите членки се придържат към препоръките на Комисията. Недостатъчното ниво на сигурността в по-слабо развитите държави членки ще подкопае тяхната конкурентоспособност и техния растеж и ще ги изложи на рискове и инциденти. С оглед на настоящите тенденции инцидентите, свързани с МИС, ще стават все по-осезаеми за предприятията и потребителите и ще възпрепятстват завършването на вътрешния пазар.

Социални въздействия: Ще продължат да възникват инциденти, рискове и заплахи, като се очаква тяхната сериозност да нараства, което ще има отрицателно въздействие върху доверието на гражданите в онлайн средата.

8.2. Вариант 2 — регулаторен подход

Ниво на сигурност: Задълженията, вменени на държавите членки, ще гарантират, че всички те са адекватно подготвени, и ще допринесат за създаването на климат на взаимно доверие, което е предпоставка за ефективно сътрудничество на равнище ЕС.

Въвеждането на изисквания за управление на риска в областта на МИС за публичните администрации и основните частни участници ще създаде силен стимул за управление и измерване на рисковете, свързани със сигурността. Общите допълнителни разходи, които ще възникнат в различни сектори в ЕС в отговор на тези изисквания, ще бъдат между **1 и 2 милиарда евро**. Разходите за привеждане в съответствие **на едно малко или средно предприятие** ще са от порядъка на **2500 до 5000 EUR**.

Икономическо въздействие: В резултат на повишеното ниво на сигурност ще бъдат намалени финансовите загуби, свързани с рискове и инциденти в областта на МИС. Доверието на предприятията и потребителите в цифровата среда ще бъде засилено и това ще донесе ползи за вътрешния пазар. Насърчаването на една подобрена културата на управление на рисковете също ще стимулира търсенето на сигурни продукти и решения на ИКТ.

Социално въздействие: По-високото ниво на сигурност ще подобри доверието на гражданите в онлайн средата и те ще могат изцяло да се възползват от възможностите на цифровия свят (напр. социални медии, електронно обучение, електронно здравеопазване).

8.3. Вариант 3 — смесен подход

Ниво на сигурност: Както при вариант 1, няма гаранция, че нивото на сигурност, постигнато въз основа на националния капацитет в областта на МИС, и сътрудничеството на равнище ЕС ще се подобрят в резултат на доброволни инициативи. От друга страна, въвеждането на изисквания за сигурност за публичните администрации и основните частни участници ще създаде силен стимул за управление и измерване на рисковете, свързани със сигурността. Тези механизми обаче ще бъдат неефективни в онези държави членки, които не следват препоръките на Комисията относно създаването на капацитет в областта на МИС.

Икономически въздействия: Темпото на развитие ще варира значително в различните държави членки. Недостатъчното ниво на сигурността в по-слабо развитите държави членки ще подкопае тяхната конкурентоспособност и техния растеж и ще ги изложи на отрицателното въздействие на рисковете и инцидентите.

Социални въздействия: Ще продължат да възникват инциденти, рискове и заплахи, като се очаква тяхната сериозност да нараства, което ще окаже отрицателно въздействие върху доверието в онлайн средата, особено в държавите членки, които не разглеждат МИС като приоритет.

9. СРАВНЕНИЕ НА ВАРИАНТИТЕ

Варианти 1 и 3 не се считат за подходящи за постигане на целите на политиката и поради това не се препоръчват, като се има предвид, че тяхната ефективност ще зависи от това дали доброволният подход ще доведе до постигането на едно минимално ниво на МИС, като при вариант 3 изграждането на капацитет и сътрудничеството с други държави ще зависи от добрата воля на държавите членки.

Вариант 2 е предпочетеният вариант, като се има предвид, че в рамките на този вариант защитата на потребителите, предприятията и правителствата в ЕС срещу инциденти, заплахи и рискове, свързани с МИС, ще се подобри значително. Освен това с решаването на собствените си проблеми ЕС ще бъде в състояние да разшири своето международно влияние и да се превърне в още по-надежден партньор за двустранно и многостранно сътрудничество. Също така ЕС ще бъде в по-добра позиция да насърчава съблюдаването на основните права и да популяризира своите основни ценности зад граница.

10. МОНИТОРИНГ И ОЦЕНКА

В глава 10 от доклада за оценката на въздействието е очертан набор от основни показатели за напредъка по постигането на целите. Сред тези показатели са например:

- за цел 1 — броят на държавите членки, определили компетентен орган за МИС и екип за незабавно реагиране при компютърни инциденти или приели национална стратегия в областта на киберсигурността и национален план за действие и сътрудничество при киберинциденти и в непредвидени ситуации
- за цел 2 — броят на компетентните органи и екипите за незабавно реагиране при компютърни инциденти от държавите членки, които участват в мрежата, и обемът на информацията, която се обменя в рамките на мрежата за рискове и инциденти в областта на МИС. За цел 3 — равнището на инвестициите в областта на МИС, направени от основните частни участници и публичните

администрации, и броят на съобщенията за инциденти в областта на МИС, имащи значително въздействие.