Съвет на
Европейския съюз

Брюксел, 14 септември 2017 г.
(OR. en)

Междуинституционално досие:
2017/0225 (COD)

12183/17
ADD 2

CYBER 127
TELECOM 207
ENFOPOL 410
CODEC 1397
JAI 785
MI 627
IA 139

ПРИДРУЖИТЕЛНО ПИСМО

От:	Генералния секретар на Европейската комисия, подписано от г-н Jordi AYET PUIGARNAU, директор
До:	Г-н Jeppe TRANHOLM-MIKKELSEN, генерален секретар на Съвета на Европейския съюз
№ док. Ком.:	SWD(2017) 501 final
Относно:	РАБОТЕН ДОКУМЕНТ НА СЛУЖБИТЕ НА КОМИСИЯТА ОБОБЩЕНА ОЦЕНКА НА ВЪЗДЕЙСТВИЕТО придружаващ Предложение за РЕГЛАМЕНТ НА ЕВРОПЕЙСКИЯ ПАРЛАМЕНТ И НА СЪВЕТА относно ENISA — Агенцията на ЕС за киберсигурност, и за отмяна на Регламент (ЕС) № 526/2013, както и относно сертифицирането на киберсигурността на информационните и комуникационните технологии („Акт за киберсигурността“)

Приложено се изпраща на делегациите документ SWD(2017) 501 final.

Приложение: SWD(2017) 501 final

ЕВРОПЕЙСКА
КОМИСИЯ

Брюксел, 13.9.2017 г.
SWD(2017) 501 final

РАБОТЕН ДОКУМЕНТ НА СЛУЖБИТЕ НА КОМИСИЯТА

ОБОБЩЕНА ОЦЕНКА НА ВЪЗДЕЙСТВИЕТО

придружаващ

Предложение за РЕГЛАМЕНТ НА ЕВРОПЕЙСКИЯ ПАРЛАМЕНТ И НА СЪВЕТА

относно ENISA — Агенцията на ЕС за киберсигурност, и за отмяна на Регламент (ЕС) № 526/2013, както и относно сертифицирането на киберсигурността на информационните и комуникационните технологии („Акт за киберсигурността“)

{COM(2017) 477 final}
{SWD(2017) 500 final}
{SWD(2017) 502 final}

A. НУЖНО Е ДЕЙСТВИЕ

Какъв е проблемът и какво е неговото естество?

Цифровите технологии и интернет представляват гръбнака на икономиката и обществото на ЕС. Жизнено важни сектори като транспорта, енергетиката, здравеопазването или финансите зависят все повече от мрежови и информационни системи, за да упражняват своите основни дейности. Интернетът на нещата свързва обекти и хора чрез съобщителни мрежи. Тази нова реалност създава безпрецедентни възможности, но е също така уязвима. Наблюдава се истински бум на киберинцидентите. Тяхната сложност, тяхната честота и мащабът на въздействието им — от смущения на достъпа до услуги от основно значение до нарушаване на демократичните процеси — се очаква да нараснат още.

В тази връзка бяха установени следните взаимосвързани проблеми:

- Разнородност на политиките и подходите към киберсигурността във всички държави членки.
- Разпръснати ресурси и подходи към киберсигурността в институциите, агенциите и органите на ЕС.
- Недостатъчна осведоменост на гражданите и дружествата относно киберзаплахите и недостатъчна информация относно свързаните със сигурността характеристики на ИКТ продуктите и услугите, които закупуват, съчетани с нарастващ брой национални и секторни схеми за сертифициране.

Тези проблеми оказват въздействие върху цялостната киберустойчивост на ЕС и ефективното функциониране на вътрешния пазар.

Какви цели се преследват?

Конкретните цели на инициативата са следните:

1. Увеличаване на способностите и подготвеността на държавите членки и предприятията, особено за защита на критични инфраструктури.
2. Подобряване на сътрудничеството и координацията между държавите членки и институциите, агенциите и органите на ЕС.
3. Увеличаване на способностите на равнище ЕС за допълване на действията на държавите членки, особено в случай на трансгранични кризи на киберсигурността.
4. Повишаване на осведомеността на гражданите и предприятията по въпроси, свързани с киберсигурността.
5. Повишаване на цялостната прозрачност на обезпечаването на киберсигурността на ИКТ продукти и услуги, с цел да се укрепи доверието в цифровия единен пазар и в цифровите иновации.
6. Избягване на разпокъсаност на схемите за сертифициране в ЕС и свързаните с тях изисквания за сигурност и критерии за оценка в различните държави членки и сектори.

Каква е добавената стойност от предприемането на действия на равнището на ЕС?

Тъй като цифровизацията и взаимната свързаност на икономиката и обществото са факт в глобален мащаб, измерението на проблема надхвърля границите на всяка отделна държава членка. Ето защо това изисква намеса на равнището на Съюза. В актуалния контекст и с оглед бъдещите сценарии става очевидно, че индивидуалните действия на държавите членки и разпокъсаният подход към киберсигурността, особено в нейното ясно изразено трансгранично измерение, не могат да повишат киберустойчивостта на Съюза.

В. РЕШЕНИЯ

Какви са различните варианти за постигане на целите? Има ли предпочетен вариант сред тях?

Оценката на въздействието разглежда конкретен набор от варианти на политиката, които обхващат преглед на Агенцията на Европейския съюз за мрежова и информационна сигурност (ENISA) и сертифициране на сигурността на ИКТ продуктите и услугите.

Преглед на ENISA

Вариант 0 — Базов сценарий — този вариант разглежда запазването на статуквото. Мандатът на ENISA ще бъде разширен и целите и задачите на Агенцията ще останат до голяма степен непроменени, като ще се вземат предвид задачите, възложени на ENISA от последващото законодателство на ЕС (напр. Директивата за МИС).

Вариант 1 — Изтичане на мандата на ENISA (разформироване на ENISA). Този вариант ще доведе до разформироване на ENISA в края на мандата ѝ (юни 2020 г.) и вероятно до преразпределение на компетенциите/дейностите на равнището на ЕС и/или на национално равнище.

Вариант 2 — „реформиране на ENISA“. Този вариант ще се основава на текущия мандат на ENISA с оглед на приемането на избирателни промени, които да вземат под внимание контекста на киберсигурността. Агенцията ще придобие постоянен мандат на основата на следните ключови елементи: подкрепа за разработването и прилагането на политиките на ЕС; изграждане на капацитет; познания и информация; свързани с пазара задачи; научни изследвания и иновации; оперативно сътрудничество и управление на кризи.

Вариант 3 — Създаване на агенция на ЕС за кирберсигурност с пълна оперативна способност. Този вариант означава реформиране на ENISA чрез обединяване на три основни функции: 1. Политическа/консултативна функция; 2. Център за информация и експертен опит, и 3. Екип за незабавно реагиране при компютърни инциденти (CERT). До голяма степен този вариант би означавал същата промяна в обхвата на мандата, както и при вариант 2. Ще бъдат добавени обаче допълнителни задачи в областта на реагирането на инциденти и управлението на кризи, така че Агенцията да обхваща целия жизнен цикъл на киберсигурността и да се занимава с предотвратяване, откриване и отговор на киберинциденти.

Сертифициране

Вариант 0 — Базов сценарий — Не се променя нищо. При този вариант Комисията запазва статуквото и не предприема никакви политически или законодателни действия.

Вариант 1 — Незаконодателни мерки (актове с незадължителен характер). При този вариант Комисията ще използва незадължителни инструменти на политиката (напр. тълкувателни съобщения, подкрепа на инициативите за саморегулиране и дейностите по стандартизация на равнище ЕС) с цел да се подобри прозрачността и да се намали разпокъсаността.

Вариант 2 — законодателен акт на ЕС за разширяване на споразумението на Групата на висшите служители по сигурността на информационните системи (SOG-IS), за да обхване всички държави членки. При този вариант на политиката Комисията ще предложи законодателен акт, за да разшири по законов път членството върху всички държави членки.

Вариант 3 — обща рамка на ЕС за сертифициране на киберсигурността в сектора на ИКТ. Този вариант предполага създаването на европейска рамка за сертифициране на сигурността на ИКТ (включително експертна група, съставена от национални органи) чрез надграждане върху съществуващите схеми за сертифициране на сигурността на ИКТ, доколкото е възможно. По същество рамката ще спомогне за създаването на схеми за сертифициране на ЕС, които ще бъдат приети във всички държави членки.

Предпочетеният вариант е комбинация от вариант 2 за ENISA и вариант 3 за сертифицирането.

Кои са различните заинтересовани страни? Кой подкрепя отделните варианти?

Огромното мнозинство от заинтересованите страни във всички категории (държавите членки, промишлеността, институциите на ЕС, научноизследователската общност), които участваха в консултациите, изглежда приветстват предпочетения вариант, тъй като изразяват подкрепа за укрепването на ENISA и създаването на европейска рамка за сертифициране на сигурността на ИКТ.

Налице е по-специално консенсус относно необходимостта от (най-малко) добре функционираща агенция на ЕС с постоянен мандат и достатъчни ресурси и правомощия за посрещане на настоящите и бъдещите предизвикателства пред киберсигурността. Има също така широко съгласие сред заинтересованите страни за създаването на доброволна европейска рамка с възможност за допълнително разширяване.

От страната на промишлеността това решение за сертифицирането се подкрепя от предприятията, които вече са задължени да отговарят на изисквания за сертифициране, и които биха имали полза от механизъм за целия ЕС на основата на взаимното признаване на сертификати. То се подкрепя и от МСП, които ще пострадат най-много, ако вече им се налага или им се наложи занапред да започнат различни процедури на сертифициране в различните държави членки. Някои държави членки, особено тези с по-малко ресурси, и някои представители на промишлеността и институциите на ЕС, изразиха положителни становища и по отношение на вариант 3 за ENISA.

C. ВЪЗДЕЙСТВИЕ НА ПРЕДПОЧЕТЕНИЯ ВАРИАНТ

Какви са предимствата на предпочетения вариант (ако има такъв, в противен случай — на основните варианти)?

Съгласно предпочетения вариант, ЕС ще има агенция, съсредоточена върху осигуряване на подкрепа за държавите членки, институциите на ЕС и предприятията в области, където това ще донесе най-голяма добавена стойност. Те обхващат: подпомагане на изпълнението на Директивата за МИС; разработване и изпълнение на политики; информация, познания и осведоменост; научни изследвания; оперативно сътрудничество и управление на кризи; пазар. По-специално, ENISA ще подкрепя политиката на ЕС в областта на сертифицирането на сигурността на ИКТ, като осигурява административна поддръжка и техническо управление на европейската рамка за сертифициране на сигурността на ИКТ. Такава рамка ефективно ще въведе набор от правила за управлението на сертифицирането на сигурността на ИКТ в ЕС, които ще насърчат утвърждаването на система за взаимно признаване на сертификати, издадени в различни държави членки. Решението за комбиниране на тези варианти се смята за най-ефективният начин ЕС да постигне набелязаните цели, а именно: увеличаване на капацитета в областта на киберсигурността; подготвеност; сътрудничество; осведоменост; прозрачност; избягване на разпокъсаност на пазара. Този вариант също така е най-добре съгласуван с приоритетите на политиката, тъй като е залегнал в стратегията за киберсигурността и свързаните с нея политики (напр. Директивата за МИС) и в стратегията за цифровия единен пазар. Освен това с този вариант ще бъдат постигнати целите чрез разумно използване на ресурси.

Какви са разходите за предпочетения вариант (ако има такъв, в противен случай — за основните варианти)?

Макар че е натоварена с нови функции, „реформираната ENISA“ ще си остане гъвкава организация. Нужният финансов принос от бюджета на ЕС ще бъде по-висок, отколкото в момента, но въпреки това ще остане под този за други агенции, работещи в критични области.

Създаването на европейска рамка за сертифициране на сигурността на ИКТ не предполага допълнителни първоначални разходи за промишлеността (включително МСП). То по-скоро би довело до значителни спестявания за тези предприятия, които вече сертифицират своите продукти или са готови да проведат сертифициране на сигурността, като ще има и положителен ефект върху конкурентоспособността им в световен план. От друга страна, това ще включва някои бюджетни задължения, с които да се гарантира поддържането на рамката, осигурявано предимно от модела на „реформираната ENISA“, що се отнася до техническите задачи и работата на секретариата.

Ще има ли значително отражение върху националните бюджети и администрации?

Не. Разходите, свързани с укрепването на ENISA, ще се поемат предимно от бюджета на ЕС, а държавите членки все така ще могат да предоставят доброволни финансови вноски към Агенцията. В областта на сертифицирането основното въздействие върху

националните бюджети ще произтече от създаването на орган за сертифициране, когато това е уместно.

Ще има ли друго значително въздействие?

Не.

Пропорционалност

Предпочетеният вариант включва балансирани мерки, които се считат за необходими за постигането на поставените цели без да се налага прекомерна тежест на съответните заинтересовани страни. Предвид гореизложеното настоящата инициатива се счита за съответстваща на принципа на пропорционалност.

D. ПОСЛЕДВАЩИ ДЕЙСТВИЯ

Кога ще се извърши преглед на политиката?

Предлага се първата оценка да се направи пет години след влизането в сила на правния акт. Впоследствие Комисията ще докладва на Европейския парламент и на Съвета за неговата оценка, придружена при необходимост от предложение за неговото преразглеждане. Допълнителни оценки ще бъдат извършвани на всеки пет години.