ЕВРОПЕЙСКА
КОМИСИЯ

Брюксел, 13.9.2017 г.
COM(2017) 478 final

ДОКЛАД НА КОМИСИЯТА ДО ЕВРОПЕЙСКИЯ ПАРЛАМЕНТ И СЪВЕТА

относно оценката на Агенцията на Европейския съюз за мрежова и информационна сигурност (ENISA)

1. ВЪВЕДЕНИЕ

1.1 ИНФОРМАЦИЯ ЗА ENISA

Агенцията на Европейския съюз за мрежова и информационна сигурност (ENISA) първоначално е създадена през 2004 г. и мандатът ѝ периодично се подновява. Текущият мандат на ENISA е определен с Регламент (ЕС) № 526/2013[1] („Регламента относно ENISA)“ и ще изтече на 19 юни 2020 г.

Мандатът на ENISA е да допринася за високо ниво на мрежова и информационна сигурност в рамките на Съюза. В Регламента относно ENISA са определени специфичните цели на агенцията, според които тя:

- развива и поддържа високо ниво на експертни знания.
- подпомага институциите, органите, службите и агенциите на Съюза при разработването на политики за мрежова и информационна сигурност.
- подпомага институциите, органите, службите и агенциите на Съюза и държавите членки при изпълнението на политиките, необходими за спазването на правните и регулаторните изисквания на мрежовата и информационната сигурност съгласно действащите и бъдещите правни актове на Съюза, като по този начин допринася за правилното функциониране на вътрешния пазар.
- подпомага Съюза и държавите членки при укрепването и засилването на способността и подготвеността им за предотвратяване, установяване и реагиране на проблеми и инциденти, свързани с мрежовата и информационната сигурност.
- използва своите експертни знания и умения за стимулиране на широко сътрудничество между участниците от публичния и частния сектор.

В допълнение към това съзаконодателите на ЕС решиха чрез Директива (ЕС) 2016/1148[2] относно мерки за високо общо ниво на сигурност на мрежите и информационните системи в Съюза („директивата за МИС“) да възложат важни роли на ENISA в областта на прилагането на правото. По-специално Агенцията осигурява секретариат на мрежата на екипите за реагиране при инциденти с компютърната сигурност (CSIRT) (създадена за насърчаване на бързо и ефективно оперативно сътрудничество между държавите членки) като тя се призовава да съдейства на групата за сътрудничество за стратегическо сътрудничество при изпълнението на нейните задачи. В допълнение, съгласно директивата за МИС от ENISA се изисква да оказва подкрепа на държавите членки и Комисията като предоставя експертни познания и консултации, както и чрез улесняване на обмена на най-добри практики.

Агенцията се намира в Гърция, административното ѝ седалище е в Ираклион (Крит), а основните ѝ операции се извършват в Атина. Има 84 служители и годишен оперативен бюджет от 11,25 милиона евро. Тя се ръководи от изпълнителен директор, а управлението се извършва от управителен съвет, изпълнителен съвет и Постоянна група на заинтересованите страни. Неформална

[1] http://eur-lex.europa.eu/legal-content/BG/TXT/?qid=1495472820549&uri=CELEX:32013R0526

[2] http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv:OJ.L_.2016.194.01.0001.01.ENG&toc=OJ:L:2016:194:TOC

мрежа от национални служители за връзка улеснява контактите с държавите членки.

1.2 Цел на доклада

Съгласно член 32 от Регламента относно ENISA Комисията има задължението да извърши оценка на ENISA до 20 юни 2018 г. „*за оценяване по-специално на въздействието, ефективността и ефикасността на Агенцията и нейните работни практики*“ и да обмисли дали е необходимо текущият мандат на Агенцията да бъде удължен.

В светлината на значителните промени, настъпили в сферата на киберсигурността от 2013 г. насам, когато беше приет настоящият Регламент относно ENISA — като се има предвид постигнатото развитие на политическо, пазарно и технологично равнище — в своето съобщение относно укрепването на отбранителната способност на Европа срещу кибератаки от 2016 г.[3] Комисията съобщи, че ще постигне напредък в оценката и прегледа на ENISA. По-специално Комисията отбеляза, че прегледът на ENISA би дал възможност да се укрепят способностите и капацитетът на Агенцията да оказва на държавите членки последователна подкрепа за постигане на устойчивост срещу киберзаплахи.

Тази концепция е потвърдена и в Заключенията на Съвета от 2016 г.[4], в които се признава, че „заплахите и уязвимите места в кибернетично отношение продължават да еволюират и да стават все повече, което ще изисква непрекъснато и по-тясно сътрудничество, особено за справяне с мащабни трансгранични инциденти в сферата на киберсигурността“. В заключенията се потвърждава отново, че „Регламентът относно ENISA е един от централните елементи на рамката на ЕС за отбранителна способност срещу кибератаки“.

Резултатите от оценката на ENISA бяха използвани в оценката на въздействието, придружаваща предложението за Регламент на Агенция на Европейския съюз за мрежова и информационна сигурност (ENISA, „агенцията на ЕС за киберсигурност“) и за отмяна на Регламент (ЕС) № 526/2013, и относно сертифицирането за киберсигурност на информационните и комуникационните технологии („Акт за киберсигурността“).

Съгласно член 32 от Регламента относно ENISA Комисията изпраща доклада за оценка заедно със своите заключения на Европейския парламент, Съвета и управителния съвет. Този обобщен доклад се придружава от Работен документ на службите на Комисията относно оценката на Агенцията на Европейския съюз за мрежова и информационна сигурност (SWD(2017) 502).

2. Основни констатации от оценката

В съответствие с Насоките за по-добро регулиране на Комисията[5] при оценката бяха разгледани ефективността, ефикасността, съгласуваността, значението и

[3] Съобщение на Комисията „Укрепване на отбранителната способност на Европа срещу кибератаки и изграждане на конкурентен и иновативен сектор на киберсигурността“, COM/2016/0410 final.

[4] Заключения на Съвета относно укрепването на отбранителната способност на Европа срещу кибератаки и изграждането на конкурентен и иновативен сектор на киберсигурността — 15 ноември 2016 г.

[5] COM (2015)215 final SWD (2015)111 final;

добавената стойност за ЕС на Агенцията, отчитайки нейната работа, управление, вътрешна организационна структура и работни практики.

При анализа беше отчетен и измененият контекст, в който Агенцията функционира в момента, по-специално по отношение на: новата регулаторна и политическа рамка на ЕС (напр. директивата за МИС, Прегледът на стратегията за киберсигурност на ЕС); развиващите се нужди на общността от заинтересовани страни на Агенцията; и взаимното допълване и възможните взаимодействия с работата на други институции на ЕС и национални институции, агенции и органи, като например Екипите за реагиране при инциденти с компютърната сигурност на институциите, агенциите и органите на ЕС (CERT-EU) и Европейския център за борба с киберпрестъпността (EC3) към Европол.

За да оцени функционирането на Агенцията:

- Комисията възложи независимо изследване, проведено от ноември 2016 г. до юли 2017 г., което представлява основният източник на оценяване заедно с вътрешен анализ, извършен от Комисията.
- Дейностите от изследването включваха проучване на документи, събиране и анализ на данни, включително проучвания сред заинтересованите страни, задълбочени интервюта с ключови участници в сферата на киберсигурността, работен семинар със заинтересовани страни, съпоставителна оценка, дейност за позициониране на Агенцията и анализ на силните и слабите страни, възможностите и заплахите (SWOT).
- Комисията проведе също 12-седмична онлайн обществена консултация, която обхващаше както последващата оценка, така и бъдещето на ENISA, а също и целенасочени консултации с ключови заинтересовани страни.

Основните констатации от оценката според критериите за оценяване могат да бъдат обобщени, както следва:

1. **Уместност:** В контекста на технологични промени и развиващи се заплахи, както и на значителна нужда от засилване на мрежовата и информационната сигурност (МИС) в ЕС, беше доказано, че целите на ENISA са уместни. Всъщност държавите членки и органите на ЕС разчитат на експертните знания относно развитието на МИС, необходимо е в държавите членки да бъде изграден капацитет за разбиране и реагиране на заплахи, а заинтересованите страни трябва да си сътрудничат отвъд границите на конкретни тематични области и конкретни институции. МИС продължава да бъде ключов политически приоритет на ЕС, на който от ENISA се очаква да отговори; предназначението на ENISA като агенция на ЕС обаче, има фиксиран мандат: i) той не позволява дългосрочно планиране и устойчива подкрепа за държавите членки и институциите на ЕС в бързо развиващия се контекст на заплахи за киберсигурността; ii) той може да доведе до правен вакуум, понеже разпоредбите на директивата за МИС, с които са възложени задачите на ENISA, са с постоянен характер.

2. **Ефективност:** Като цяло ENISA е постигнала своите цели и изпълнила своите задачи. Допринесла е за повишаване на МИС в Европа чрез своите основни дейности (изграждане на капацитет, предоставяне на експертни знания, изграждане на общност, подкрепа за политиката). Показа потенциал

http://ec.europa.eu/smart-regulation/guidelines/docs/swd_br_guidelines_en.pdf

за подобрение по отношение на всяко от горепосочените. Заключението от оценката е, че ENISA е успяла ефективно да създаде стабилни и надеждни отношения с някои от своите заинтересовани страни, главно с държавите членки и общността на CSIRT. Намесите в областта на изграждането на капацитет са счетени за ефективни, по-специално за държавите членки, които не разполагат с достатъчно ресурси. Един от основните моменти беше стимулирането на широко сътрудничество, при което заинтересованите страни в голямата си част потвърдиха положителната роля на ENISA в обединяването на хората. ENISA обаче изпита трудности в постигането на голямо въздействие в обширната сфера на МИС. Това се дължеше на факта, че човешките и финансовите ѝ ресурси за осъществяването на нейния много широк мандат бяха сравнително ограничени. Друго заключение от оценката беше, че ENISA е постигнала частично целта за предоставяне на експертни знания, което се дължи на проблемите, свързани с набирането на експерти (вж. също по-долу в раздела относно ефикасността).

3. **Ефикасност:** Въпреки малкия си бюджет — едни от най-малките в сравнение с други агенции на ЕС — Агенцията успя да допринесе за постигането на конкретни цели, като показа цялостна ефикасност при използване на ресурсите си. От оценката беше заключено, че процесите като цяло са били ефективни, а ясното разграничаване на отговорностите в организацията е спомогнало за пълноценната работа. Едно от основните предизвикателства пред ефективността на Агенцията е свързано с трудностите на ENISA при набирането и задържането на висококвалифицирани експерти. Констатациите сочат, че това може да се обясни с комбинация от фактори, включително общите трудности на публичния сектор да се конкурира с частния в опита си да назначава високоспециализирани експерти, видовете договори (срочни), каквито Агенцията можеше главно да предложи, и донякъде ниското ниво на привлекателност, свързано с местоположението на ENISA, например свързано с трудността на съпрузите/съпругите да си намират работа. Разделеното между Атина и Ираклион местоположение наложи допълнителни усилия за координация и създаде допълнителни разходи, но с преместването в Атина през 2013 г. на основните дейности се повиши оперативната ефективност на агенцията.

4. **Съгласуваност:** Дейностите на ENISA като цяло са съгласувани с политиките и дейностите на нейните заинтересовани страни на национално равнище и равнището на ЕС, но е необходим по-координиран подход спрямо киберсигурността на равнището на ЕС. Потенциалът за сътрудничество между ENISA и другите органи на ЕС не е използван докрай. С развитието на правната и политическата ситуация в ЕС текущият мандат загуби част от съгласуваността си в днешно време.

5. **Добавена стойност от ЕС:** Добавената стойност на ENISA се дължи главно на способността на Агенцията да подобрява сътрудничеството главно между държавите членки, но и в свързаните общности в областта на МИС. Никой друг участник на равнището на ЕС не подпомага сътрудничеството на такова голямо разнообразие заинтересовани страни в областта на МИС. Предоставената от Агенцията добавена стойност варираще в зависимост от различните нужди и ресурси на нейните заинтересовани страни (напр. големи спрямо малки държави членки; държави членки спрямо

индустрията) и нуждата Агенцията да приоритизира своите дейности според работната програма. Заключение от оценката беше, че потенциалното преустановяване на дейността на ENISA би представлявало загубена възможност за всички държави членки. Без децентрализирана агенция на ЕС няма да е възможно да се гарантира същото ниво на изграждане на общност и сътрудничество в държавите членки в областта на киберсигурността. Ситуацията би била по-фрагментирана, ако мястото на ENISA бъде заето от двустранно или регионално сътрудничество.

3. ЗАКЛЮЧЕНИЯ/ПРЕПОРЪКИ

От оценката беше заключено, че по силата на регламента за нейното създаване на ENISA е възложен широк мандат, който позволява гъвкавост, но в някои случаи му липсва фокус, което затруднява Агенцията в постигането на значително въздействие, и целите ѝ за периода 2013—2016 г. са се доказали като уместни. Агенцията успя да постигне добро ниво на ефективност и показа добавената стойност на действията на равнището на ЕС, по-специално чрез ключови дейности, като например общоевропейските кибернетични учения, подкрепата за общността на CSIRT и анализите на контекста на заплахите. ENISA допринесе за повишаване на мрежовата и информационната сигурност в Европа главно чрез подпомагане на сътрудничество между държавите членки и заинтересованите страни в областта на МИС, както и чрез своите дейности за изграждане на общности и на капацитет.

Агенцията постигна тези резултати въпреки редицата предизвикателства, представени в предходните раздели на настоящия доклад и в приложения Работен документ на службите на Комисията. Едно от ключовите предизвикателства е свързано с ограничените ресурси, които не съответстваха на широкия мандат на Агенцията, особено с оглед на новите задачи, възложени ѝ с директивата за МИС, и с бързоразвиващия се контекст на заплахите. ENISA остава също и единствената агенция на ЕС с фиксиран мандат, въпреки че наред с другото изпълнява и задачи, свързани с директивата за МИС, както беше посочено по-горе.

Контекстът на заплахите за киберсигурността се развива бързо, и колкото повече Европа разчита на цифрова инфраструктура и услуги чрез не само свързани устройства, но вече и всеобща свързаност, толкова повече нови заплахи възникват. „Интернетът на нещата“ създава нови възможности, свързани с енергийната ефективност, опазването на околната среда, свързаната мобилност, системата за наблюдение на здравето в реално време и интелигентни и безпроблемни финансови транзакции в цифровата икономика и обществото. В комбинация тези стимули за бизнеса възникват и нови уязвими точки и методи на проникване, които позволяват компрометирани устройства да нарушават цифровия единен пазар.

От оценката беше направено заключението, че текущият мандат не осигурява на ENISA необходимите инструменти за справяне с текущите и бъдещите предизвикателства, свързани с киберсигурността.

Освен това е налице нарастващ риск от засилена разпокъсаност на равнището на ЕС поради множеството участници на равнището на ЕС в областта на киберсигурността и недостатъчната координация между тях. ЕС се нуждае от фокусна точка, за да преодолее новите заплахи, които по естеството си са хоризонтални и оказват въздействие върху множество сектори на промишлеността, както и за да отговори на нуждите на общността в областта на киберсигурността, и по-специално на държавите членки, институциите на ЕС и предприятията.

Оценката показва, че е необходима агенция на ЕС, организирана на междусекторна/хоризонтална основа със силен мандат.

Оценката сочи, че въпреки редицата въпроси, представляващи предизвикателство, ENISA има значителен потенциал, ако ѝ бъде възложен достатъчен мандат и ако бъде подпомогната с финансови и човешки ресурси, така че да допринесе за повишаване на киберсигурността в ЕС.

Има и ясна нужда от сътрудничество и координация между различните заинтересовани страни. Нуждата от орган за координация на равнището на ЕС за улесняване на потока от информация, свеждане до минимум на различията и избягване на припокриванията на ролите и отговорностите става все по осезаема. ENISA, като децентрализирана агенция на ЕС и като неутрален посредник, е в позицията да координира подхода на ЕС спрямо киберзаплахите.

На тази основа Комисията изготви предложение за реформиране на ENISA, при което да ѝ бъде възложен постоянен мандат, който надгражда върху ключовите силни страни, проявени от Агенцията, и новите приоритетни области за действие, например в областта на сертифицирането на киберсигурността. Този нов мандат следва да отразява променената реалност и да оправомощава Агенцията да оказва подходяща подкрепа на ЕС за в бъдеще.