



Съвет на
Европейския съюз

Брюксел, 2 декември 2020 г.
(OR. en)

13629/20

CYBER 263
TELECOM 248
COPEN 362
CODEC 1266
COPS 441
COSI 235
CSC 344
CSCI 86
IND 248
RECH 493
ESPACE 77

РЕЗУЛТАТИ ОТ РАБОТАТА

От:	Генералния секретариат на Съвета
Дата:	2 декември 2020 г.
До:	Делегациите

Относно:	Заклучения на Съвета относно киберсигурността на свързаните устройства
	– Одобряване на заключенията на Съвета чрез писмена процедура

Приложено се изпращат на делегациите заключенията на Съвета относно киберсигурността на свързаните устройства, одобрени от Съвета чрез писмена процедура на 2 декември 2020 г.

Заклучения на Съвета относно киберсигурността на свързаните устройства

Съветът на Европейския съюз,

КАТО ПРИПОМНЯ

- Заклученията на Съвета относно съвместното съобщение до Европейския парламент и Съвета „Устойчивост, възпиране и отбрана: изграждане на силна киберсигурност за ЕС“,
 - Заклученията на Съвета относно капацитета за киберсигурност и изграждането на способности в ЕС,
 - Заклученията на Съвета относно значението на 5G за европейската икономика и необходимостта от смекчаване на рисковете за сигурността, свързани с 5G,
 - Заклученията на Съвета относно бъдещето на една високо цифровизирана Европа след 2020 г. „Стимулиране на цифровата и икономическата конкурентоспособност в Съюза и цифровото сближаване“,
 - Заклученията на Съвета относно изграждането на цифровото бъдеще на Европа,
 - Заклученията на Европейския съвет относно COVID-19, единния пазар, промишлената политика, цифровите технологии и външните отношения,
 - Съобщението на Европейската комисия относно изграждането на цифровото бъдеще на Европа,
1. ПОДЧЕРТАВА, че Европейският съюз и неговите държави членки трябва да гарантират своя цифров суверенитет и стратегическата си автономност, като същевременно запазят отворената икономика. Това включва укрепване на способността да се вземат автономни технологични решения и да се създават устойчиви и сигурни инфраструктури, продукти и услуги като един от основните стълбове за изграждане на доверие в цифровия единен пазар и в европейското общество. Основните ценности на Европейския съюз са насочени най-вече към запазване на неприкосновеността на личния живот, сигурността, равенството, човешкото достойнство, върховенството на закона и отворения интернет като предпоставки за постигане на ориентирани към човека общество, икономика и промишленост, в които цифровите технологии са водещ фактор.

2. ПРИЗНАВА нарастващото значение на свързаните устройства и тяхната сигурност, включително машините, сензорите и мрежите, които съставляват интернета на предметите. Свързаните устройства ще играят ключова роля в по-нататъшното изграждане на цифровото бъдеще на Европа от промишлена и икономическа гледна точка, както и в ежедневието на потребителите на новото поколение технологии. Освен 5G изкуственият интелект, квантовата изчислителна технология, високоскоростните изчисления, компютърните услуги в облак, технологиите на разпределения регистър, а именно блоковата верига, и всички други нови приложения и възможности за устойчив икономически растеж и по-високо равнище на цифровизация на нашето общество могат да бъдат осъществени само чрез свързани устройства с гарантирана киберсигурност.
3. ОТБЕЛЯЗВА, че увеличеното използване на потребителски продукти и промишлени устройства, свързани с интернет, ще породи и нови рискове за неприкосновеността на личния живот, сигурността на информацията и киберсигурността, включително все повече потенциални въздействия върху интегритета и наличността на продуктите и данните, които могат да засегнат пряко сигурността. От съществено значение е тези рискове да бъдат сведени до минимум, за да се защитят потребителите, да се укрепи цялостната киберустойчивост на Европа и да се повиши доверието на гражданите в цифровите решения и технологии. Това ще стимулира и конкурентоспособността и капацитета за иновации на европейските доставчици на такива устройства. Киберсигурността и неприкосновеността на личния живот следва да бъдат признати като основни изисквания за продуктовете иновации, процесите на производство и разработване, включително на етапа на проектирането (сигурност още на етапа на проектирането), и следва да бъдат гарантирани през целия жизнен цикъл на продукта и по неговата верига на доставки.
4. ПОДЧЕРТАВА, че в допълнение към гарантирането на високо равнище на сигурност на свързаните устройства е също толкова важно да се повиши осведомеността на потребителите за потенциалните рискове на тези устройства, свързани със сигурността и неприкосновеността на личния живот. Това ще помогне да се сведат до минимум заплахите, произтичащи от засиленото използване на свързани устройства, да се повиши доверието в цифровия единен пазар и да се извлекат в максимална степен икономическите и обществените ползи, които технологиите на свързаните устройства предлагат.

5. ПОДЧЕРТАВА, че публичните инвестиции в научни изследвания и иновации, по-специално чрез програмите „Хоризонт Европа“ и „Цифрова Европа“, както и частните инвестиции, биха могли да създадат ценни стимули за повишаване на безопасността и сигурността на свързаните устройства, а оттам и на устойчивостта на интелигентните комуникационни мрежи. Инвестициите в необходимата цифрова инфраструктура и техника за внедряване на най-новите технологии на свързаните устройства също следва да бъдат ускорени, за да се постигне индустриално и цифрово лидерство и да се гарантира стратегическата автономност, като се запази отворената икономика.
6. ПОДЧЕРТАВА необходимостта от осигуряване на висока степен на взаимно допълване и съпоставимост на функционалните възможности за сигурност на ИКТ системите и компонентите, които се използват в много различни сектори на цифровия единен пазар.
7. ОТЧИТА текущите тенденции на равнището на Съюза за повишаване на нивото на киберсигурност на свързаните устройства, особено що се отнася до неотдавнашните инициативи на Комисията за включване в краткосрочен план на аспектите на киберсигурността в съответните правни актове, например актовете по Новата законодателна рамка (НЗР), по-специално Директива 2014/53/ЕС (Директивата за радиосъоръженията). ПОДЧЕРТАВА, че е важно да се оцени необходимостта от хоризонтално законодателство, като се определят и необходимите условия за пускането на пазара, за да бъдат обхванати в дългосрочен план всички съответни аспекти на киберсигурността на свързаните устройства, като например наличност, интегритет и поверителност. Във връзка с това ПРИВЕТСТВА дискусията за проучване на обхвата на това законодателство и връзките му с рамката за сертифициране на киберсигурността, както е определена в Акта за киберсигурността (АК), с цел повишаване на нивото на сигурност в рамките на цифровия единен пазар.
8. ПОДЧЕРТАВА, че изискванията за киберсигурност следва да бъдат определени в съответствие с релевантното законодателство на Съюза, включително АК, НЗР, Регламента за европейската стандартизация и евентуалното бъдещо хоризонтално законодателство, за да се избегне наличието на неяснота и разпокъсаност в законодателството.

9. ПРИЗНАВА важната роля на всички заинтересовани страни, по-специално на производителите, за повишаване на нивото на киберсигурност на свързаните устройства в цифровия единен пазар, поради което ПРИЗОВАВА за координация и тясно сътрудничество с всички заинтересовани страни от публичния и частния сектор, също и с оглед на евентуално бъдещо хоризонтално законодателство.
- 9а. ПРИВЕТСТВА текущата работа, ръководена от Агенцията на ЕС за киберсигурност (ENISA), за съставянето на първите схеми на ЕС за сертифициране на киберсигурността, а именно предложените общи критерии на Европейския съюз и предложените схеми за доставчиците на компютърни услуги в облак. Тези схеми ще бъдат подходяща основа за сертифициране на свързаните устройства.
10. ПОДЧЕРТАВА, че всяка допълнителна схема за сертифициране на свързаните устройства и услугите към тях, която ще бъде заложена в постоянната работна програма на Съюза и определена съгласно Акта за киберсигурността, следва да посочва как трябва да се спазват приложимите изисквания за сигурност на съответното ниво на увереност въз основа на специфични европейски и международно признати стандарти, независимо от сектора, в който ще се използва продуктът, както и кои спецификации за изпитване, сертификати и т.н. трябва да се прилагат.
11. ОТЧИТА, че сертифицирането на свързаните устройства ще изисква съответни норми, стандарти или технически спецификации за оценките на киберсигурността съгласно Акта за киберсигурността. Във връзка с това ИЗТЪКВА необходимостта от установяване на норми, стандарти или технически спецификации в областта на киберсигурността за свързаните устройства и ПРЕПОРЪЧВА да се увеличат усилията, предприети от европейските организации по стандартизация в тази област. Същевременно ОТБЕЛЯЗВА, че важна стъпка в тази насока е стандартът за киберсигурност на потребителските устройства, базирани на интернет на предметите – ETSI EN 303 645.

12. ПРИКАНВА Европейската комисия да разгледа искане за [...] проекти за схеми за сертифициране на киберсигурността за свързаните устройства и услугите към тях въз основа на постоянната работна програма на Съюза, която сега се изготвя, като отчита в максимална степен разработваните понастоящем хоризонтални европейски схеми за сертифициране на киберсигурността. Тези схеми ще дават възможност на производителите на въпросните продукти да популяризират на доброволна основа продукти с оценено ниво на увереност.
13. ПРИКАНВА да се обсъди как целта за киберсигурност би могла да се заложи в бъдещото хоризонтално законодателство, обхващащо рисковете за киберсигурността на свързаните устройства, и същевременно ОТБЕЛЯЗВА необходимостта да се обмисли по целесъобразност адаптирането на съществените изисквания на съответните директиви по НЗР.
14. НАСЪРЧАВА Комисията също да направи оценка дали е необходимо разработването на допълнителни секторни регламенти, които да определят на какво ниво на киберсигурност трябва да отговаря свързаното устройство, за да се гарантира, че са въведени специфични изисквания за сигурност и неприкосновеност на личния живот за устройствата с по-високи рискове за сигурността.
15. ПОДЧЕРТАВА необходимостта от подобряване на качеството на живот и благосъстоянието на европейските граждани и от насърчаване на доверието в цифровия единен пазар. Сигурността и неприкосновеността на личния живот в нашите общества са от съществено значение за съхраняване на основните ценности на Съюза. Във връзка с това ИЗТЪКВА необходимостта от надграждане върху рамката, предоставена от АК, за хармонизиране на изискванията за сигурност в съответствие с различните нива на увереност във всички сектори на НЗР, за да се избегне фрагментирането и многократните проверки на идентични изисквания и да се осигури равнопоставеност в Европейския съюз за конкуренцията и иновациите.

16. ПРИКАНВА Комисията, ENISA, Комитета за оценка на съответствието и за надзор на пазара в областта на далекосъобщенията и Европейската група за сертифициране на киберсигурността (ECCG) да участват активно в тази инициатива за укрепване на цифровия единен пазар и повишаване на доверието в продукти, услуги и процеси в сферата на ИКТ за свързаните устройства чрез гарантиране на неприкосновеността на личния живот и киберсигурността, както и да улеснят повишаването на глобалната конкурентоспособност на сектора на интернетa на предметите в Съюза чрез осигуряване на най-високите стандарти за устойчивост, безопасност и сигурност.
17. В този контекст ПОДЧЕРТАВА необходимостта от подкрепа за МСП като основен градивен елемент на европейската екосистема за киберсигурност и НАСЪРЧАВА МСП да участват във всички започнати обществени консултации, както и в дейностите по стандартизация, за да се вземе предвид техният ценен и важен принос за превръщането на киберсигурността не само в достижима цел, но и в конкурентно предимство на европейския пазар.
18. ОТБЕЛЯЗВА, че задължението за гарантиране на киберсигурността и неприкосновеността на личния живот през целия жизнен цикъл на даден продукт и по цялата му верига на доставки може да окаже положително въздействие върху екологичния отпечатък на технологичния сектор, напътствайки производителите към интелигентни и устойчиви процеси на разработване и производство, което пък ще намали количеството на електронните отпадъци, получени от изхвърлянето на свързани устройства.
-