Съвет на
Европейския съюз

Брюксел, 17 май 2016 г.
(OR. en)

Междуинституционално досие:
2013/0027 (COD)

5581/1/16
REV 1 ADD 1

TELECOM 7
DATAPROTECT 6
CYBER 4
MI 37
CSC 15
CODEC 84
PARLNAT 154

ИЗЛОЖЕНИЕ НА МОТИВИТЕ НА СЪВЕТА

Относно:	Позиция на Съвета на първо четене с оглед приемането на ДИРЕКТИВА НА ЕВРОПЕЙСКИЯ ПАРЛАМЕНТ И НА СЪВЕТА относно мерки за гарантиране на високо общо ниво на сигурност на мрежите и информационните системи в Съюза — Изложение на мотивите на Съвета — Приемане от Съвета на 17 май 2016 г.

I. ВЪВЕДЕНИЕ

1. На 12 февруари 2013 г. Комисията представи предложението си за директива на Европейския парламент и на Съвета относно *мерки за гарантиране на високо общо ниво на мрежова и информационна сигурност в Съюза* (по-нататък „Директивата“), имащо за правно основание член 114 от ДФЕС.

2. Европейският икономически и социален комитет гласува становището си на 22 май 2013 г., а Комитетът на регионите — на 3—4 юли 2013 г.

3. Европейският парламент гласува законодателната си резолюция на първо четене на 13 март 2014 г.[1], като прие 138 изменения.

4. През октомври 2014 г. Съветът и Европейският парламент започнаха преговори с оглед на бързото постигане на споразумение на второ четене. Преговорите приключиха успешно на 7 декември 2015 г. с постигането на предварително споразумение между Европейския парламент и Съвета по компромисен текст.

5. На 18 декември 2015 г. Комитетът на постоянните представители потвърди компромисния текст на директивата, договорен от двете институции.

6. На 28 януари 2016 г. председателят на Комисията на Европейския парламент по вътрешния пазар и защита на потребителите (IMCO) изпрати писмо до председателя на Комитета на постоянните представители, в което се посочва, че ако Съветът изпрати официално на Европейския парламент своята одобрена позиция, след проверка от юрист-лингвистите, председателят на IMCO ще препоръча на пленарното заседание позицията на Съвета да бъде приета без изменения по време на второто четене в Парламента.

7. На 29 февруари 2016 г. Съветът потвърди политическото си съгласие по компромисния текст на директивата.

---

[1] Законодателна резолюция на Европейския парламент от 13 март 2014 г. относно предложението за директива на Европейския парламент и на Съвета относно мерки за гарантиране на високо общо ниво на мрежова и информационна сигурност (МИС) в Съюза.

II. ЦЕЛ

8. Резултатите от преговорите показват, че с директива се установяват мерки с цел постигане на високо общо ниво на сигурност на мрежите и информационните системи в рамките на Съюза, така че да се подобри функционирането на вътрешния пазар.

III. АНАЛИЗ НА ПОЗИЦИЯТА НА СЪВЕТА НА ПЪРВО ЧЕТЕНЕ

А. Общо положение

9. След гласуването на пленарното заседание Европейският парламент и Съветът проведоха преговори с цел да сключат споразумение на второ четене въз основа на позицията на Съвета на първо четене, която Парламентът да бъде в състояние да одобри. Текстът на позицията на Съвета на първо четене отразява напълно компромиса, постигнат между двата законодателни органа.

Б. Ключови въпроси

10. Основните елементи на компромиса, постигнат с Европейския парламент, са изложени по-долу:

a. *Национални способности*

11. В рамките на постигнатия компромис държавите членки имат определени задължения по отношение на националните си способности в областта на киберсигурността. Първо, от държавите членки се изисква да приемат национална стратегия, в която да са определени стратегическите цели и подходящата политика, както и регулаторни мерки за постигане и поддържане на високо ниво на сигурност на мрежите и информационните системи.

12. Второ, държавите членки определят един или повече национални компетентни органи по сигурността на мрежите и информационните системи, които да наблюдават изпълнението на директивата на национално равнище.

13. Трето, от държавите членки се изисква да определят и единно национално звено за контакт по сигурността на мрежите и информационните системи, което да изпълнява функцията на връзка, така че да се осигури трансграничното сътрудничество между органите на държавите членки, съответните органи в други държави членки, групата за сътрудничество и мрежата на ЕРИКС. Единното звено за контакт ще представя и годишен доклад до групата за сътрудничество относно получените уведомления.

14. Накрая, държавите членки определят един или повече екипи за реагиране при инциденти с компютърната сигурност (ЕРИКС), които отговарят за предприемането на действия при инциденти и рискове. В приложение I към компромисния текст се предвиждат изисквания и задачи за ЕРИКС.

б. *Сътрудничество*

15. С цел да се подпомага и улеснява стратегическото сътрудничество между държавите членки, да се изгражда доверие и увереност и с оглед постигането на високо общо равнище на сигурност на мрежите и информационните системи в Съюза, с компромисния текст се създава група за сътрудничество. Групата ще се състои от представители на държавите членки, Комисията и Агенцията на Европейския съюз за мрежова и информационна сигурност (ENISA) и ще има конкретни задачи, изброени в текста, като обмен на най-добри практики и информация по редица въпроси или обсъждане на способностите и готовността на държавите членки.

16. Освен това с компромисния текст се установява мрежа от националните ЕРИКС с цел да се допринесе за изграждане на доверие и увереност между държавите членки и да се стимулира бързото и ефективно оперативно сътрудничество. Мрежата ще се състои от представители на ЕРИКС и CERT—ЕС на държавите членки, а Комисията ще участва в нея като наблюдател. ENISA ще изпълнява ролята на секретариат и ще подкрепя активно сътрудничеството между ЕРИКС. Текстът представя списък със задачите, които ще бъдат изпълнявани от мрежата, като обмен на информация относно услугите, операциите и капацитета за сътрудничество на ЕРИКС, подкрепа на държавите членки за справяне с трансгранични инциденти или, при определени условия, обмен и обсъждане на информация, свързана с инциденти, и отнасящите се до това рискове.

в. *Изисквания за сигурност и уведомяване*

17. Директивата установява някои задължения за две групи участници на пазара: операторите на основни услуги и доставчиците на цифрови услуги.

18. В приложение II към директивата са изброени редица важни за обществото и икономиката сектори, а именно енергетиката, транспорта, банковото дело, инфраструктурите на финансовия пазар, здравеопазването, доставката и снабдяването с питейна вода и цифровата инфраструктура. В рамките на тези сектори държавите членки ще определят операторите, които предоставят основни услуги, въз основа на определени в директивата точни критерии.

19. В приложение III към директивата се изброяват три вида цифрови услуги, доставчиците на които ще трябва да спазват изискванията на директивата: онлайн места за търговия, онлайн търсачки и компютърни услуги „в облак“. Всички доставчици на изброените цифрови услуги ще трябва да спазват изискванията на директивата, с изключение на микропредприятията и малките предприятия.

20. От двете групи участници на пазара ще се изисква да предприемат организационни и технически мерки за управление на рисковете, пред които е изправена сигурността на мрежите и информационните системи, както и да предотвратяват и намаляват до минимум въздействието на инциденти, засягащи сигурността на тези системи. Освен това националните компетентни органи или ЕРИКС ще трябва да бъдат уведомявани за инцидентите с определено ниво на въздействие върху въпросните услуги. В директивата се предвиждат критерии за определяне на степента на въздействие на подобни инциденти.

21. В директивата е възприет диференциран подход по отношение на двете категории участници. Изискванията за сигурност и уведомяване са по-леки за доставчиците на цифрови услуги от тези за операторите на основни услуги и съответстват на степента на риска, на който нарушаването на техните услуги може да изложи обществото и икономиката. Освен това, като се има предвид, че доставчиците на цифрови услуги често работят в много държави членки и с цел да се гарантира висока степен на хармонизация, директивата не позволява на държавите членки да налагат допълнителни изисквания за сигурност и уведомяване на тези доставчици.

22. В компромисния текст се предвижда също, че субектите, които не са били определени като оператори на основни услуги и не са доставчици на цифрови услуги, могат да уведомяват за определени инциденти на доброволна основа.

г. *Транспониране*

23. Държавите членки ще трябва да транспонират директивата не по-късно от 21 месеца след датата на влизането ѝ в сила и ще разполагат с още 6 месеца, за да определят своите оператори на основни услуги.

IV. ЗАКЛЮЧЕНИЕ

24. Позицията на Съвета отразява напълно компромиса, който беше постигнат в преговорите между Европейския парламент и Съвета със съгласието на Комисията. Компромисът се потвърждава от писмото на председателя на Комисията по вътрешния пазар и защита на потребителите до председателя на Комитета на постоянните представители от 28 януари 2016 г.