Съвет на
Европейския съюз

Брюксел, 16 септември 2022 г.
(OR. en)

Междуинституционално досие:
2022/0272(COD)

12429/22
ADD 6

CYBER 298
JAI 1181
DATAPROTECT 254
TELECOM 369
MI 665
CSC 388
CSCI 133
CODEC 1310
IA 133

ПРИДРУЖИТЕЛНО ПИСМО

От:	Генералния секретар на Европейската комисия, подписано от г-жа MARTINE DEPREZ, директор
Дата на получаване:	15 септември 2022 г.
До:	Генералния секретариат на Съвета
№ док. Ком.:	SWD(2022) 283 final
Относно:	РАБОТЕН ДОКУМЕНТ НА СЛУЖБИТЕ НА КОМИСИЯТА РЕЗЮМЕ НА ДОКЛАДА ЗА ОЦЕНКАТА НА ВЪЗДЕЙСТВИЕТО, на Законодателния акт за киберустойчивост, придружаващ Предложение за Регламент на Европейския парламент и на Съвета относно хоризонтални изисквания за киберсигурност за продукти с цифрови елементи и за изменение на Регламент (ЕС) 2019/1020

Приложено се изпраща на делегациите документ SWD(2022) 283 final.

Приложение: SWD(2022) 283 final

ЕВРОПЕЙСКА
КОМИСИЯ

Брюксел, 15.9.2022 г.
SWD(2022) 283 final

РАБОТЕН ДОКУМЕНТ НА СЛУЖБИТЕ НА КОМИСИЯТА

РЕЗЮМЕ НА ДОКЛАДА ЗА ОЦЕНКАТА НА ВЪЗДЕЙСТВИЕТО,

на Законодателния акт за киберустойчивост,

придружаващ

Предложение за Регламент на Европейския парламент и на Съвета

относно хоризонтални изисквания за киберсигурност за продукти с цифрови елементи и за изменение на Регламент (ЕС) 2019/1020

{COM(2022) 454 final} - {SEC(2022) 321 final} - {SWD(2022) 282 final}

Резюме (максимум 2 страници)

Оценка на въздействието на Законодателния акт за киберустойчивост

А. Необходимост от действия

В какво се изразява проблемът и защо той се разглежда на равнището на ЕС?

Хардуерните и софтуерните продукти често са обект на успешни кибератаки, поради което годишните разходи във връзка с киберпрестъпността в световен мащаб се оценяват на 5,5 трилиона евро до 2021 г. Тези продукти имат два основни проблема, които увеличават разходите на ползвателите и обществото: 1) ниско ниво на киберсигурност, което се изразява в широко разпространени уязвимости и недостатъчно и непоследователно предоставяне на актуализации на сигурността за справяне с тях, и 2) недостатъчно разбиране и достъп до информация от страна на ползвателите, което им пречи да избират продукти с подходящи функции за киберсигурност или да ги използват по сигурен начин.

Киберсигурността на продуктите с цифрови елементи има силно трансгранично измерение, тъй като продуктите, произведени в една държава, често се използват в целия вътрешен пазар. Освен това инцидентите, които първоначално засягат един субект или една държава членка, често се разпространяват в рамките на минути на целия вътрешен пазар.

Въпреки че действащото законодателство в областта на вътрешния пазар се прилага към някои продукти с цифрови елементи, повечето хардуерни и софтуерни продукти понастоящем не са обхванати от законодателство на ЕС, занимаващо се с тяхната киберсигурност. По-специално в настоящата правна рамка на ЕС не се разглежда киберсигурността на невградения софтуер, въпреки че атаките срещу киберсигурността все по-често са насочени към уязвимости в тези продукти, което води до значителни обществени и икономически разходи. Скорошни примери са шпионският софтуер Pegasus, който използва уязвимости в мобилни телефони, или криптовирусът червей WannaCry, който използва уязвимост на Windows, засягаща компютри по целия свят.

Какво следва да бъде постигнато?

Поставени бяха две основни цели, които да осигурят правилното функциониране на вътрешния пазар: 1) създаване на условия за разработване на защитени продукти с цифрови елементи, като се гарантира, че на пазара се пускат хардуерни и софтуерни продукти с по-малко уязвимости, както и че производителите се отнасят сериозно към защитата през целия жизнен цикъл на продукта; и 2) създаване на условия, които позволяват на ползвателите да вземат предвид киберсигурността при избора и използването на продукти с цифрови елементи. Определени бяха четири специфични цели**:** i) да се гарантира, че производителите подобряват защитата на продуктите с цифрови елементи още от етапа на проектиране и разработване и през целия жизнен цикъл; ii) да се осигури съгласувана рамка за киберсигурност, която улеснява спазването на изискванията от производителите на хардуер и софтуер; iii) да се повиши прозрачността на характеристиките за защитата на продуктите с цифрови елементи и iv) да се даде възможност на предприятията и потребителите да използват продуктите с цифрови елементи по безопасен начин.

Каква е добавената стойност от действия на равнището на ЕС (субсидиарност)?

Силно изразеният трансграничен характер на киберсигурността и нарастващият брой инциденти, които се разпространяват в други държави, сектори и продукти, означават, че целите не могат да бъдат постигнати ефективно само от държавите членки. Предвид глобалния характер на пазарите на продукти с цифрови елементи, държавите членки са изправени пред едни и същи рискове за

един и същ продукт с цифрови елементи на тяхна територия. Възникващата разнородна рамка от потенциално различаващи се национални правила също създава риск да попречи на отворения и конкурентен единен пазар за продукти с цифрови елементи. Следователно са необходими съвместни действия на равнището на ЕС, за да се повиши доверието на ползвателите и привлекателността на продуктите с цифрови елементи, пуснати на пазара в ЕС. Те ще бъдат от полза и за вътрешния пазар, тъй като ще осигурят правна сигурност и равнопоставеност на производителите на продукти с цифрови елементи.

Б. Решения

Какви са различните варианти за постигане на целите? Има ли предпочитан вариант? Ако няма такъв, каква е причината?

Бяха анализирани четири варианта на политиката и свързани с тях подварианти, излизащи извън настоящото положение: 1) подход на незадължително право и доброволни мерки, 2) специфична за продукта допълнителна регулаторна намеса за киберсигурността на материални продукти с цифрови елементи и съответния вграден софтуер, 3) смесен подход, включващ хоризонтални задължителни правила за киберсигурност на материални продукти с цифрови елементи и съответния вграден софтуер и поетапен подход за невградения софтуер, с два подварианта за оценяване на съответствието, и 4) хоризонтална регулаторна намеса, с която се въвеждат изисквания за киберсигурност за широк набор от продукти с цифрови елементи, включително невграден софтуер, с подварианти относно набора, и за оценяването на съответствието.

В оценката на въздействието се стига до заключението, че предпочитаният вариант е вариант 4, който обхваща всички продукти с цифрови елементи и предвижда задължителна оценка от трета страна за критични продукти въз основа на оценката на ефективността спрямо конкретните цели, ефикасността на разходите спрямо ползите и съпоставимостта.

Какви са позициите на различните заинтересовани страни? Кой подкрепя отделните варианти?

Когато бе поискано да оценят ефективността на политическите намеси, участниците в обществената консултация се съгласиха, че вариант 4 би бил най-ефективната мярка (4,08 по скалата от 1 до 5). В това число влизат организациите на потребителите (5,00), респондентите, определящи себе си като ползватели (4,22), нотифицираните органи (4,17), органите за надзор на пазара (5,00) и производителите на продукти с цифрови елементи (3,85), включително малките и средните предприятия (4,05).

В. Въздействия на предпочитания вариант

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

Предпочитаният вариант би донесъл значителни ползи за различните заинтересовани страни. За предприятията той би предотвратил различаващи се правила за сигурността за продукти с цифрови елементи и би намалил разходите за привеждане в съответствие със свързаното законодателство в областта на киберсигурността. Той би намалил броя на киберинцидентите, разходите за действията при инцидент и накърняването на репутацията. За целия ЕС се смята, че инициативата би могла да доведе до намаляване на разходите от инциденти, засягащи предприятията, с около 180—290 млрд. евро годишно. Освен това инициативата би довела до увеличаване на оборота поради нарастващото използване на продукти с цифрови елементи. Тя ще подобри и репутацията на

дружествата в световен мащаб, което ще доведе до увеличаване на търсенето извън ЕС. За крайните потребители предпочитаният вариант би повишил прозрачността на свойствата за сигурност и би улеснил използването на продукти с цифрови елементи. Потребителите и гражданите ще се възползват и от по-добрата защита на основните си права, като неприкосновеност на личния живот и защита на личните данни.

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

Предпочитаният вариант ще увеличи разходите за спазване и прилагане на законодателството за предприятията, нотифицираните органи и публичните органи, включително нотифицираните органи и органите по акредитация и надзор на пазара. За разработчиците на софтуер и производителите на хардуер той ще увеличи преките разходи за спазване на новите изисквания за киберсигурност, оценка на съответствието, документация и задължения за докладване, което ще доведе до съвкупни разходи за спазване на изискванията, възлизащи на приблизително 29 млрд. евро при приблизителна пазарна стойност на продуктите с цифрови елементи с оборот от 1485 млрд. евро. Крайните потребители, включително крайните бизнес потребители, потребителите и гражданите, може да се сблъскат с по-високи цени на продуктите с цифрови елементи. Те обаче следва да се разглеждат на фона на значителните ползи, описани по-горе. За нотифицираните органи се очаква допълнителните разходи да бъдат компенсирани от увеличаване на оборота.

Какво е въздействието върху МСП и конкурентоспособността?

МСП ще бъдат засегнати от новите изисквания както като производители, така и като крайни потребители. По отношение на разходите за привеждане в съответствие МСП по принцип ще бъдат засегнати в по-голяма степен в сравнение с големите дружества, които обикновено имат по-добри икономии от мащаба и по-голяма осведоменост в областта на киберсигурността. МСП обаче ще имат голяма полза от инициативата, тъй като киберсигурността, вградена в продуктите с цифрови елементи, би довела до сериозна възможност за спестяване на разходите за МСП като ползватели. Като производители МСП ще се възползват от по-голямо доверие на крайните потребители и на новите клиенти. Безпроблемният достъп до вътрешния пазар и намаляването на разпокъсаността на пазара може да донесат дори още по-големи ползи за МСП, които са по-слабо подготвени да се справят с различни нормативни изисквания. Въпреки че подчертават необходимостта от пропорционален подход и придружаващи мерки, МСП като цяло подкрепят равнопоставеността между всички дружества и не считат, че биха били в неравностойно положение в сравнение с по-големите дружества в случай на сценарий на задължителни хоризонтални изисквания.

Ще има ли значително въздействие върху националните бюджети и администрации?

Инициативата ще засегне националните органи, като например националните нотифициращи органи, органите по акредитация и надзор на пазара, които имат отговорности да наблюдават и прилагат предложените мерки. Тези органи ще имат допълнителни разходи за приспособяване (напр. обучение и човешки ресурси) и прилагане, за да действат с оглед на новите изисквания. Ресурсите, изразходвани от органите по акредитация, обаче се компенсират и поемат до голяма степен от органите за оценяване на съответствието чрез закупуване на услуги по акредитация.

Ще има ли други значителни въздействия?

Не се очакват други значителни неблагоприятни въздействия. Предпочитаният вариант на политиката би спомогнал за намаляване на броя и сериозността на инцидентите, включително

нарушения на сигурността на личните данни, и би имал положително социално въздействие, като например намаляване на киберпрестъпността. Търсенето на специалисти по сигурността вероятно ще нарасне, а информационната асиметрия в областта на киберсигурността ще намалее.
Пропорционалност?
Предпочитаният вариант не надхвърля необходимото за задоволителното постигане на специфичните цели. Тази намеса ще гарантира, че продуктите с цифрови елементи са защитени през целия си жизнен цикъл и пропорционално на рисковете, пред които са изправени.
Г. Последващи действия
Кога ще се извърши преглед на политиката?
В срок до [36 месеца] след датата на прилагане на инициативата и на всеки четири години след това Комисията представя на Европейския парламент и на Съвета доклад относно оценката и прегледа на инициативата.