ЕВРОПЕЙСКА
КОМИСИЯ

Брюксел, 16.12.2020 г.
SWD(2020) 344 final

РАБОТЕН ДОКУМЕНТ НА СЛУЖБИТЕ НА КОМИСИЯТА

РЕЗЮМЕ НА ДОКЛАДА ЗА ОЦЕНКАТА НА ВЪЗДЕЙСТВИЕТО,

придружаващ

Предложение за Директива на Европейския парламент и на Съвета

относно мерки за високо общо ниво на киберсигурност в Съюза и за отмяна на Директива (ЕС) 2016/1148

{COM(2020) 823 final} - {SEC(2020) 430 final} - {SWD(2020) 345 final}

Резюме

Оценка на въздействието относно *прегледа на Директива (ЕС) 2016/1148 от 6 юли 2016 година относно мерки за високо общо ниво на сигурност на мрежите и информационните системи в Съюза (наричана по-нататък „Директивата за МИС“)*

А. Необходимост от действия

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

Независимо от забележителните постижения на Директивата за МИС, която проправи пътя за значителна промяна в нагласите, институционалния и регулаторния подход към киберсигурността в редица държави членки, проличаха и нейните ограничения. Цифровата трансформация на обществото (ускорена от кризата с COVID-19) разширява картината на заплахите и поражда нови предизвикателства, изискващи съобразени и новаторски реакции. Броят на кибератаките продължава да нараства, като все по-комплексни атаки идват от широк кръг от източници в ЕС и извън него.

Въз основа на оценката за функционирането на Директивата за МИС оценката на въздействието установи следните проблеми: ниското равнище на киберустойчивост на предприятията, извършващи дейност в ЕС; нееднаквите равнища на устойчивост сред държавите членки и секторите, както и ниското равнище на съвместна ситуационна осведоменост и липса на съвместна реакция при кризи. Например в резултат от някои от тези проблеми и движещи сили са налице ситуации, при които главни болници в една държава членка не попадат в обхвата на Директивата за МИС и поради това от тях не се изисква да прилагат произтичащите мерки за сигурност, докато в друга държава членка почти всяка болница в страната е обхваната от изискванията за сигурност на МИС.

Какво следва да бъде постигнато?

С прегледа на МИС се предвиждат три главни цели:

1. **Да се повиши нивото на киберустойчивост на широкообхватен набор от предприятия, извършващи дейност в Европейския съюз във всички относими сектори,** като се въведат правила, гарантиращи, че от всички публичноправни и частноправни субекти във вътрешния пазар, изпълняващи значими функции за икономиката и обществото като цяло, се изисква да предприемат адекватни мерки за киберсигурност.
2. **Да се намалят несъответствията в устойчивостта в рамките на вътрешния пазар във вече обхванатите от директивата сектори,** като допълнително се съгласуват 1) фактическият обхват, 2) изискванията за сигурност и докладване за инциденти, 3) разпоредбите, уреждащи националния надзор и правоприлагане, и 4) способностите на компетентните органи в държавите членки.
3. **Да се подобрят равнището на съвместна ситуационна осведоменост и колективната способност за подготовка и реакция,** като се предприемат мерки за повишаване на нивото на доверие между компетентните органи, обменя се повече информация и се определят правила и процедури в случай на мащабен инцидент или криза.

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

Устойчивостта на киберсигурността в Съюза не може да бъде ефективна, ако подходът към нея е различен при отделните национално или регионално обособени системи. С Директивата за МИС

тази слабост се преодолява, като се установява рамка за сигурността на мрежите и информационните системи на национално равнище и на равнището на Съюза. Транспонирането и прилагането ѝ обаче разкриха също така присъщи недостатъци на някои разпоредби или подходи, като например неясното определяне на обхвата на Директивата за МИС. Освен това, от началото на кризата с COVID-19 зависимостта на европейската икономика от мрежите и информационните системи нарасна още повече, а секторите и услугите стават все по-взаимосвързани. Ето защо първият периодичен преглед на Директивата за МИС създаде възможност за допълнителни действия от страна на ЕС. Намесата на ЕС отвъд настоящите мерки по Директивата за МИС е обоснована главно от: i) трансграничния характер на проблема; ii) потенциала на действията на ЕС за подобряване и улесняване на ефективните национални политики; iii) значението на съгласувани и съвместни действия на политиките в областта на МИС за ефективната защита на данните и поверителността.

Б. Решения

Какви са различните варианти за постигане на целите? Има ли предпочитан вариант сред тях? Ако не, защо?

При оценката на въздействието бяха анализирани четири варианта на политиката: 0) запазване на съществуващото положение; 1) незаконодателни мерки за съгласуване на транспонирането; 2) ограничени промени в Директивата за МИС с цел допълнителна хармонизация; 3) системни и структурни промени в Директивата за МИС. Вариант 1 бе отхвърлен на ранен етап, тъй като не се различава значително от съществуващото положение. В оценката на въздействието се заключава, че **предпочитаният вариант** е вариант 3 (т.е. **системни и структурни промени в уредбата за МИС**), тъй като при него се предвижда по-основно изменение на подхода към обхващането на по-широк сегмент от икономиките в Съюза, при това с по-фокусиран надзор, насочен пропорционално към големите и ключовите дружества, като същевременно ясно се определя приложното поле. Той също така би оптимизирал и допълнително хармонизирал свързаните със сигурността задължения за дружествата, би създал по-ефективна среда за оперативните аспекти и би установил ясна основа за споделени отговорности и отчетност на съответните действащи лица и би насърчил обмена на информация.

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

По-голямата част от компетентните органи и предприятия изразиха подкрепа за преработването на Директивата за МИС. В рамките на няколко консултации те посочиха, че преработената Директива за МИС следва да обхваща допълнителни (под)сектори, да съгласува или оптимизира допълнително мерките за сигурност и задълженията за докладване. Заинтересованите страни изразиха подкрепа и за нови концепции или свързани с политиките мерки, които са налични единствено в предпочитания вариант (напр. политики за сигурност на веригите за доставка, институционализация на рамката на ЕС за оперативно управление на кризи).

В. Въздействие на предпочитания вариант

Какви са ползите от предпочитания вариант (ако има такъв, в противен случай — на основните варианти)?

Предпочитаният вариант би довел до значителни ползи: прогнозите, основани на икономическо моделиране, разработено в рамките на проучване в подкрепа на прегледа на МИС, показват, че предпочитаният вариант може да доведе до намаляване на разходите за инциденти с

киберсигурността с 11,3 милиарда евро. Секторният обхват би бил значително по-широк съгласно рамката за МИС, но наред с горепосочените предимства, тежестта, която може да породят изискванията за МИС, особено от гледна точка на надзора, също би се уравновесила както за новите субекти, които ще бъдат обхванати, така и за компетентните органи. Причината за това е, че с новата рамка за МИС би се установил подход на две нива, с фокус върху големите и ключовите субекти, и разграничаване при режима на надзор, позволяващо само последващ надзор (т.е. реактивен и без общо задължение за систематично документиране на изпълнението) за голям брой от тях, особено за считаните за „значими“, но не и за „съществени“. Като цяло предпочитаният вариант на политика би довел и до ефикасни съгласувания и полезни взаимодействия и разполага с най-добрия потенциал от всички анализирани варианти на политиката за осигуряване на повишено и съгласувано равнище на киберустойчивостта на ключови субекти в Съюза, което в крайна сметка би довело до икономия на разходи както за предприятията, така и за обществото.
Какви са разходите за предпочитания вариант (ако има такъв, в противен случай — за основните варианти)?
Предпочитаният вариант на политика би довел до някои разходи за изпълнение и правоприлагане за съответните органи на държавите членки (прогнозирано е общо увеличение на ресурсите с около 20—30 %). Независимо от това новата рамка би донесла съществени ползи също и посредством подобряване на обзора върху ключовите предприятия и взаимодействието с тях, подобрено трансгранично оперативно сътрудничество, както и механизми за взаимопомощ и партньорска проверка. Това би довело до цялостно повишаване на способностите в областта на киберсигурността сред държавите членки. За дружествата, които биха попаднали в обхвата на рамката за МИС, се прогнозира, че би било необходимо увеличение с най-много 22 % на настоящите им разходи за сигурността на ИКТ за първите години след въвеждането на новата рамка за МИС (стойността би била 12 % за дружествата, които вече попадат в обхвата на настоящата Директива за МИС). Това средно увеличение на разходите за сигурността на ИКТ обаче би довело до пропорционални ползи от тези инвестиции, особено поради значителното намаляване на разходите за инциденти с киберсигурността (прогнозирани на 11,3 милиарда евро за десет години).
Какво е въздействието върху МСП и конкурентоспособността?
Малките предприятия и микропредприятията биха били изключени от обхвата на рамката за МИС съгласно предпочитания вариант. За средните предприятия може да се очаква увеличение в нивото на разходите за сигурността на ИКТ през първите години след въвеждането на новата рамка за МИС. Същевременно, повишаването на равнището на изискванията за сигурността по отношение на тези субекти би стимулирало и техните способности в областта на киберсигурността и би спомогнало за подобряване на управлението на риска при ИКТ.
Ще има ли значително въздействие върху националните бюджети и администрации?
Предпочитаният вариант би оказал въздействие върху националните бюджети и администрации: съгласно прогнозите може да се очаква увеличение на ресурсите с приблизително 20—30 % в краткосрочен и средносрочен план.
Ще има ли друго значително въздействие?

Не се очакват други съществени неблагоприятни въздействия. Очаква се предпочитаният вариант на политика да доведе до по-солидни способности в областта на киберсигурността и поради това той би имал по-съществено ограничаващо въздействие върху броя и тежестта на инцидентите, включително нарушенията на сигурността на данните. Вероятно е той да има положително въздействие и върху гарантирането на условията на равнопоставеност в държавите членки на всички субекти, попадащи в обхвата на МИС, и да намали информационната асиметрия в областта на киберсигурността.
Пропорционалност?
Предпочитаният вариант не надхвърля необходимото за задоволителното постигане на конкретните цели. Предвиденото съгласуване и оптимизиране на мерките за сигурност и задълженията за докладване е свързано с исканията на държавите членки и предприятията за подобряване на настоящата рамка.
Г. Последващи действия
Кога ще се извърши преглед на политиката?
Първият преглед ще се извърши 54 месеца след влизането в сила на правния инструмент. Комисията ще представи доклад пред Европейския парламент и Съвета за прегледа. Прегледът ще бъде изготвен с подкрепата на ENISA и групата за сътрудничество.