ЕВРОПЕЙСКА
КОМИСИЯ

Брюксел, 4.10.2017 г.
COM(2017) 476 final

NOTE
This language version reflects the corrections done to the original EN version transmitted under COM(2017) 476 final of 13.9.2017 and retransmitted (with corrections) under COM(2017) 476 final/2 of 4.10.2017

СЪОБЩЕНИЕ НА КОМИСИЯТА ДО ЕВРОПЕЙСКИЯ ПАРЛАМЕНТ И СЪВЕТА

Максимално оползотворяване на МИС — за ефективно прилагане на Директива (ЕС) 2016/1148 относно мерки за високо общо ниво на сигурност на мрежите и информационните системи в Съюза

Въведение

Директива (ЕС) 2016/1148 относно мерки за високо общо ниво на сигурност на мрежите и информационните системи в Съюза[1] (наричана по-долу „директива за МИС“ или „директивата“), приета на 6 юли 2016 г., е първият хоризонтален законодателен акт на ЕС за преодоляване на предизвикателствата в сферата на киберсигурността, който променя из основи ситуацията в Европа по отношение на устойчивостта на киберзаплахи и сътрудничеството в тази посока.

Основните цели на директивата са три:

- подобряване на националните способности в областта на киберсигурността;
- изграждане на сътрудничество на равнището на ЕС; и
- насърчаване на култура на управление на риска и докладване на инциденти сред основни стопански субекти, и по-специално операторите, предоставящи основни услуги (ООУ) за поддържането на обществени или стопански дейности и доставчиците на цифрови услуги (ДЦУ).

Директивата за МИС представлява крайъгълен камък на реакцията на ЕС на нарастващия брой киберзаплахи и киберпредизвикателства, съпътстващи цифровизацията на нашия икономически и обществен живот и по тази причина нейното прилагане е съществена част от пакета за киберсигурността, представен на 13 септември 2017 г. Ефективността на реакцията на ЕС е възпрепятствана до пълното транспониране на директивата за МИС във всички държави — членки на ЕС. Това е признато като критична точка и в Съобщението относно укрепването на отбранителната способност на Европа срещу кибератаки от 2016 г.[2]

Новаторският характер на директивата за МИС и неотложната необходимост от противодействие в цялостния контекст на бързи промени при киберзаплахите обуславят специалното внимание върху предизвикателствата, пред които са изправени всички участници при осигуряване на навременното и успешното транспониране на директивата. С оглед спазването на крайния срок за транспониране, а именно 9 май 2018 г. и крайния срок за определяне на операторите на основни услуги, който е 9 ноември 2018 г., Комисията подкрепя процеса на транспониране в държавите членки и тяхната работа за тази цел в групата за сътрудничество.

Настоящото съобщение и приложението към него са основани на подготвителната работа и анализа на Комисията, свързани с прилагането на директивата за МИС до момента, на информацията от Агенцията на Европейския съюз за мрежова и информационна сигурност („ENISA“) и на обсъждания, провеждани с държавите членки на етапа на

[1] Директива (ЕС) № 2016/1148 на Европейския парламент и на Съвета от 6 юли 2016 г. относно мерки за високо общо ниво на сигурност на мрежите и информационните системи в Съюза. Директивата влезе в сила на 8 август 2016 г.
[2] COM(2016) 410 final.

транспониране на директивата, и по-специално в рамките на групата за сътрудничество[3]. То допълва значителните усилия, положени досега, по-специално чрез:

- Интензивната работа на групата за сътрудничество, която е одобрила работен план, насочен предимно върху транспонирането на директивата за МИС, и по-специално върху въпроса за определяне на операторите на основни услуги и техните задължения, свързани с изискванията за сигурност и уведомленията за инциденти. Макар и директивата да предвижда свобода на преценка по отношение на транспонирането на разпоредбите, свързани с операторите на основни услуги, държавите членки признават значението на прилагането на хармонизиран подход в това отношение[4].
- Създаването и бързата работа на екипите за реагиране при инциденти с компютърната сигурност (CSIRT) съгласно член 12, параграф 1 от директивата. От тогава насам, тази мрежа е започнала да поставя основите за структурирано оперативно сътрудничество на европейско равнище.

Както на политическото, така и на оперативното равнище, които тези две структури представляват, пълната ангажираност на всички държави членки е от съществено значение за постигане на целта за високо общо ниво на сигурност на мрежовите и информационните системи в Съюза.

Настоящото съобщение и приложението към него ще увеличат тези усилия, като обединят и сравнят най-добрите практики на държавите членки, които са от значение за прилагането на директивата, осигурят допълнителни насоки за това как следва да се прилага директивата, и чрез по-подробни разяснения във връзка с конкретни разпоредби. Основната цел е държавите членки да бъдат подкрепени за постигането на ефективно и хармонизирано прилагане на директивата за МИС в целия ЕС.

Настоящото съобщение ще бъде допълнено освен това и от предстоящия Регламент за изпълнение на Комисията относно допълнително конкретизиране на елементите и на показателите, свързани с изискванията по отношение на сигурността и уведомленията за инциденти за доставчиците на цифрови услуги съгласно член 16, параграф 8 от директивата за МИС. Регламентът за изпълнение ще улесни прилагането на директивата по отношение на задълженията за доставчиците на цифрови услуги[5].

---

[3] Механизъм за стратегическо сътрудничество между държавите членки съгласно член 11 от директивата за МИС.

[4] Понастоящем групата за сътрудничество работи по изготвянето на референтни документи с насоки, наред с другото, относно: критериите, определящи значението на даден оператор съгласно член 5, параграф 2 от директивата; обстоятелствата, при които от операторите на основни услуги се изисква да уведомяват за инциденти съгласно член 14, параграф 7 от директивата; и изискванията по отношение на сигурността за операторите на основни услуги в съответствие с член 14, параграф 1 и член 14, параграф 2.

[5] Проектът на регламента за изпълнение е достъпен за целите на обществената консултация на адрес: https://ec.europa.eu/info/law/better-regulation/have-your-say_en

В съобщението са представени основните заключения от анализа на въпросите, които се разглеждат като важни отправни точки и потенциален източник на идеи от гледна точка на транспонирането в националното законодателство. В него основният акцент е поставен върху разпоредби, свързани със способностите и задълженията на държавите членки по отношение на субекти, попадащи в приложното поле на директивата. В приложението се разглеждат по-подробно онези области, в които Комисията смята, че е най-важно да бъдат предоставени практически насоки за транспонирането чрез разяснение и тълкуване на определени разпоредби на директивата, както и чрез представяне на най-добри практики и натрупан опит с директивата до момента.

Път към постигане на ефективно прилагане на директивата за МИС

Целта на директивата за МИС е постигането на високо общо ниво на сигурност на мрежовите и информационните системи в ЕС. Това означава подобряване на сигурността на интернет и частните мрежи и информационни системи, което е от основно значение за функционирането на нашето общество и икономика. Първият важен елемент в това отношение е подготвеността на държавите членки, която следва да бъде гарантирана чрез наличието на национални стратегии за киберсигурност, както е описано в директивата, чрез работата на CSIRT и на компетентните национални органи.

Всеобхватност на националните стратегии

Важно е държавите членки да се възползват от възможността, която дава транспонирането на директивата за МИС, за да преразгледат своите национални стратегии за киберсигурност в светлината на пропуските, най-добрите практики и новите предизвикателства, разгледани в приложението.

Макар и по разбираеми причини директивата да се фокусира върху онези предприятия и услуги, които са от особена критична важност, необходимо е спрямо киберсигурността на икономиката и обществото като цяло да бъдат предприети комплексни и последователни мерки, предвид все по-засиленото използване на ИКТ. Следователно приемането на всеобхватни национални стратегии, които надхвърлят минималните изисквания, установени в директивата за МИС (т.е. обхващането на повече сектори и услуги от изброените съответно в приложения II и III към директивата) би повишило общото ниво на сигурност на мрежовите и информационните системи.

Тъй като киберсигурността все още е относително нова и бързоразвиваща се обществено-политическа област, в повечето случаи са необходими нови инвестиции, дори ако цялостното положение на публичните финанси налага ограничения и икономии. Поради това вземането на амбициозни решения за осигуряване на достатъчно финансови и човешки ресурси, които са необходими за ефективното прилагане на национални стратегии, включително набавянето на ресурси за националните компетентни органи и CSIRT, е от основно значение за постигане на целите на директивата.

Ефективност на прилагането и изпълнението

Необходимостта от определяне на съответни национални компетентни органи и единни звена за контакт е посочена в член 8 от директивата и е ключов елемент за гарантирането на ефективно прилагане на директивата за МИС и трансгранично сътрудничество. В тази връзка в държавите членки са били възприети по-централизирани и по-децентрализирани подходи. Когато държавите членки възприемат по-децентрализиран подход по отношение на определянето на национални компетентни органи, се оказва, че гарантирането на солидни договорености за сътрудничество между голям брой органи и единното звено за контакт е от съществено значение (*вж. таблица 1 в раздел 3.2. от приложението*). Това би повишило ефективността на прилагането и би улеснило изпълнението.

Натрупаният опит по отношение на защитата на критичната информационна инфраструктура (CIIP) може да спомогне за изготвяне на оптимален модел на управление за държавите членки, който гарантира както ефективно секторно прилагане на директивата за МИС, така и съгласуван хоризонтален подход (*вж. раздел 3.1. от приложението*).

Повишени капацитети на националните CSIRT

Без ефективни и разполагащи с достатъчно ресурси национални CSIRT в целия ЕС, както е определено в член 9 от директивата за МИС, ЕС ще остане твърде уязвим за трансгранични киберзаплахи. Поради това държавите членки биха могли да разгледат възможността за разширяване на обхвата на действие на CSIRT извън секторите и услугите, попадащи в приложното поле на директивата (*вж. раздел 3.3 от приложението*). Това би дало възможност на националните CSIRT да осигуряват оперативна подкрепа при възникване на киберинциденти в предприятия и организации, които не попадат в приложното поле на директивата, но също така са важни за обществото и икономиката. Освен това държавите членки могат да използват в пълна степен допълнителните възможности, предлагани от програмата за инфраструктурите за цифрови услуги (DSI) в областта на киберсигурността от Механизма за свързване на Европа (МСЕ), която има за цел да повиши способностите на националните CSIRT и сътрудничеството между тях (*вж. раздел 3.5 от приложението*).

Последователност на процеса на определяне на ООУ

Съгласно член 5 от директивата за МИС от държавите членки се изисква до 9 ноември 2018 г. да определят субектите, които ще бъдат считани за оператори на основни услуги. Във връзка с тази задача държавите членки биха могли да изберат последователно да използват определенията и насоките, включени в настоящото

съобщение, за да гарантират, че сходни субекти, които играят сходна роля на вътрешния пазар биха били определяни последователно като оператори на основни услуги в други държави членки. Освен това държавите членки биха могли да помислят за разширяване на приложното поле на директивата за МИС, така че да обхване публичните администрации предвид ролята, която те играят за обществото и икономиката като цяло (*вж. раздели 2.1. и 4.1.3 от приложението*).

Съгласуването в максимална степен на националните подходи към определянето на оператори на основни услуги, основно чрез следване на насоките, разработени от групата за сътрудничество (*вж. раздел 4.1.2 от приложението*) би било много полезно, тъй като би довело до по-хармонизирано прилагане на разпоредбите на директивата и така би намалило риска от разпокъсаност на пазара. В случаите, в които операторите на основни услуги предоставят основни услуги в две или повече държави членки, стремежът към постигане на споразумение между държавите членки в контекста на процеса на консултиране съгласно член 5, параграф 4 относно последователното определяне на субекти (*вж. раздел 4.1.7 от приложението*) е от съществено значение, тъй като по този начин би се избегнало различното регулаторно третиране на един и същ субект под юрисдикциите на различни държави членки.

Предоставяне на информация на Комисията относно определянето на ООУ

Съгласно член 5, параграф 7 от държавите членки се изисква да предоставят на Комисията информация относно националните мерки, позволяващи определяне на ООУ, списъка на основните услуги, броя на определените ООУ и значението на тези оператори за сектора. Освен това от държавите членки се изисква да предоставят информация за праговете, когато има такива, използвани в процеса на определяне на съответното равнище на доставките или значението на конкретния оператор за поддържането на достатъчно равнище на доставките. Освен това държавите членки биха могли да разгледат възможността за споделяне с Комисията, поверително, ако е необходимо, списъците на определените оператори на основни услуги, тъй като това би могло да помогне за подобряване на точността и качеството на оценката на Комисията (*вж. раздели 4.1.5. и 4.1.6. от приложението*).

Съгласувани подходи относно изискванията по отношение на сигурността и уведомленията за инциденти за ООУ

Във връзка със задълженията относно изискванията по отношение на сигурността и уведомленията за инциденти за операторите на основни услуги (член 14, параграфи 1, 2 и 3), един съгласуван подход във връзка с изискванията по отношение на сигурността и уведомленията за инциденти с цел улесняване на спазването на задълженията от ООУ през границите на държавите — членки на ЕС, би насърчил във възможно най-голяма степен ефект на единния пазар. В тази връзка източникът на информация остава работата на групата за сътрудничество по документ с насоки (*вж.раздели 4.2. и 4.3. от приложението*).

В случай на възникване на мащабен киберинцидент, засягащ няколко държави членки, много е вероятно задължително уведомление за инцидент да бъде подадено от ООУ или ДЦУ съгласно член 14, параграф 3 и член 16, параграф 3 или на доброволна основа, съгласно член 20, параграф 1, от друг субект, който не попада в приложното поле на директивата. В съответствие с Препоръката на Комисията относно координирана реакция на мащабни киберинциденти и кризи, държавите членки биха могли да разгледат възможността за съгласуване на своите национални подходи, за да могат да предоставят възможно най-бързо съответната информация, основана на тези уведомления, до компетентните органи или CSIRT на други засегнати държави членки. Предоставянето на точна и практическа информация би било от жизненоважно значение за намаляване на броя на заразяванията или отстраняване на уязвимите точки преди да бъдат атакувани.

В духа на партньорство за извличането на максимална полза от директивата за МИС, Комисията възнамерява да разшири обхвата на подкрепата по линия на Механизма за свързване на Европа с оглед включването на всички съответни заинтересовани страни съгласно това законодателство. Макар и фокусът да е бил поставян върху изграждане на капацитета на CSIRT и върху новаторска платформа за бързо и ефективно оперативно сътрудничество, чрез което да бъде укрепена мрежата на CSIRT, сега Комисията ще разгледа въпроса как от финансирането по линия на Механизма за свързване на Европа могат да се възползват също и националните компетентни органи, както и операторите на основни услуги и доставчиците на цифрови услуги.

Заключение

С оглед спазването на наближаващия краен срок за транспониране на директивата за МИС в националното законодателство до 9 май 2018 г. и крайния срок за определяне на операторите на основни услуги до 9 ноември 2018 г., държавите членки следва да предприемат подходящи мерки, за да гарантират, че разпоредбите и моделите на сътрудничество, предвидени в директивата за МИС могат да осигурят възможно най-добрите инструменти на равнището на ЕС за постигане на високо общо ниво на сигурност на мрежовите и информационните системи в целия Съюз. Комисията приканва в хода на този процес държавите членки да вземат предвид съответните информация, насоки и препоръки, които се съдържат в настоящото съобщение.

Настоящото съобщение може да бъде допълвано и от други действия, включително тези, които възникват в хода на текущата работа на групата за сътрудничество.