Ниво на конфиденциалност 1
[TLP-GREEN]

Р Е П У Б Л И К А Б Ъ Л Г А Р И Я
М И Н И С Т Ъ Р Н А Е Л Е К Т Р О Н Н О Т О У П Р А В Л Е Н И Е

Проект!

ДО
МИНИСТЕРСКИЯ СЪВЕТ НА
РЕПУБЛИКА БЪЛГАРИЯ

ДОКЛАД
от
Валентин Мундров – министър на електронното управление

ОТНОСНО: *Проект на Решение на Министерския съвет за одобряване на проект на Закон за изменение и допълнение на Закона за киберсигурност*

УВАЖАЕМИ ГОСПОДИН МИНИСТЪР-ПРЕДСЕДАТЕЛ,
УВАЖАЕМИ ГОСПОЖИ И ГОСПОДА МИНИСТРИ,

На основание чл. 31, ал. 2 от Устройствения правилник на Министерския съвет и на неговата администрация, внасям за разглеждане от Министерския съвет проект на Решение на Министерския съвет за одобряване на проект на Закон за изменение и допълнение на Закона за киберсигурност.

Законопроектът е изготвен в изпълнение на ангажиментите на Република България като държава членка на Европейския съюз, която следва да въведе в националното си законодателство до 17.10.2024 г. разпоредби и да създаде организация за изпълнението на Директива (ЕС) 2023/2555 на Европейския парламент и на Съвета от 14 декември 2022 година, относно мерки за високо общо ниво на киберсигурност в Съюза, за изменение на Регламент (ЕС) № 910/2014 и Директива (ЕС) 2018/1972 и за отмяна на Директива (ЕС) 2016/1148 (ОВ L 333, 27.12.2022г.), наричана по-нататък Директивата МИС 2.

Директивата (ЕС) 2016/1148, транспонирана в българското законодателство чрез Закона за киберсигурност, е първото всеобхватно законодателство в областта на мрежовата и информационна сигурност на ниво ЕС и предоставя хармонизирана правна

основа за борба с киберинцидентите в целия ЕС. В България до приемане на Директива (ЕС) 2016/1148 нямаше съществуващ единен принцип на взаимодействие при киберинциденти и инциденти в мрежовата и информационната сигурност (МИС), както и цялостна система за взаимодействие на междуинституционално ниво и между държавите членки на ЕС при случаи на инцидент с трансгранично значение и измерение.

Директивата осигури завършването на националните рамки относно сигурността на мрежовите и информационните системи чрез създаването на национални стратегии за сигурност на мрежовите и информационните системи и създаването на национални способности.

Същият ефект/резултат се констатира и в България след приемането на Закона за киберсигурност, както следва:

– създаде се организацията, управлението и контролът на киберсигурността, определиха се компетентните органи в областта на киберсигурността, както и техните функции и правомощия, регламентираха се дейностите по предприемане на необходимите мерки за постигане на високо общо ниво на сигурност на мрежите и информационните системи, като един основен стълб на киберсигурността, така че да се подобри функционирането на вътрешния пазар;

– създаде се институционалната рамка в областта на киберсигурността, превенцията и противодействието на кибератаките, насочена към по-голяма ефективност и по-добра координация между съществуващите органи и звена в публичната администрация;

– създаде се Национално единно звено за контакт, регламентираха се управлението и организацията на националната система за киберсигурност, Националният координатор по киберсигурност, секторни екипи за реакция при инциденти в киберсигурността – ЕРИКС, както и Национален ЕРИКС, регламентираха се въпросите за междуинституционална взаимосвързаност и сътрудничество;

– регулацията на мрежовата и информационна сигурност на административните органи, изискванията към тях да осигуряват и отговарят за мрежовата и информационната сигурност на използваните от тях информационни системи, също така изискванията и стандартите за сигурност, на които трябва да отговарят информационните системи за въвеждане, изпращане, обработка, достъп, обмен, съхраняване и архивиране на данни, както и общите мерки за сигурност, които трябва да предприемат;

– определен бе статутът и функционирането на операторите на съществени услуги (ОСУ) и на доставчиците на цифрови услуги (ДЦУ).

Прегледът на Директива (ЕС) 2016/1148 обаче разкрива, че независимо от тези постижения, тя има и присъщи слабости, които пречат на намирането на ефективни решения за настоящите и възникващи предизвикателства в областта на киберсигурността. С Директива МИС2 се осъвременява съществуващата правна рамка, като се отчитат повишената цифровизация на вътрешния пазар през последните години и развиващата се картина на заплахите за киберсигурността и се разширява обхватът ѝ.

Основните разлики между предходната и новата Директива за NIS се състоят в:

- отстраняване на разграничението „Оператори на основни услуги (OES)“ и „Доставчици на цифрови услуги (DSP)“, залагайки на обектите като „Съществени“ или „Важни“;
- разширение на обхвата на директивата с цел да се включат нови сектори в зависимост от степента им на критичност по отношение на тяхната индустрия или на вида услуга, която предоставят;

- основаване на Европейска мрежа за връзка при киберкризи (EU-CyCLONe), за да се подпомогне управлението на киберсигурността при широкомащабни инциденти и кризи;
- определянето на един ЕРИКС като координатор за целите на координираното оповестяване на уязвимости, обмена на служители, обединяването на взаимодействието между EU-CyCLONe и мрежата CSIRTs, определянето на повече от един НКО, отговорен за изпълнението на задачите, свързани със сигурността на МИС на съществени и важни субекти съгласно директивата, широкото сътрудничество с академични и изследователски институции, въвеждането на механизъм за партньорска проверка, позволяващ оценка от експерти, определени от държавите членки, на прилагането на политиките за киберсигурност, включително нивото на способностите на държавите членки и наличните ресурси и други, са все мерки, които изискват наличие на заявен политически модел на взаимодействие, на една развита и работеща в пълен обем национална киберсистема;
- осигуряване на непрекъснатост на бизнеса при засягането му от киберинциденти и бързото докладване след анализа им;
- промяна на сроковете за докладване на инцидент и последващ доклад;
- промяна във вида и размера на административно-наказателните разпоредби.

Необходимо е транспониране на Директива (ЕС) 2022/2555 (Директива МИС2) поради непълно съответствие на действащата нормативна уредба и действащите разпоредби в тази област на политиката.

За да се преодолее недостатъчната законова уредба от гледна точка на разгръщане на секторите, създаване на нови регулаторни функции, както и правила за управление на риска, свързан с ИКТ, в т.ч. за да се осигурят мерки по прилагането на Директива (ЕС) 2022/2555 и да се въведат предвидените изменения в националното законодателство, е необходимо в срок до 17 октомври 2024 г., да се измени действащият Закон за киберсигурност.

Законопроектът, в съответствие с Директивата МИС2, осигурява възможност за постигането на общата цел да се повиши нивото на защита срещу инциденти, рискове и заплахи за мрежовата и информационна сигурност в ЕС. Това би довело до смекчаване на потенциалните загуби на приходи поради кибератаки и би намалило големите разходи за смекчаване на заплахите ad hoc. Подобни ползи вероятно ще надделеят над необходимите инвестиционни разходи. Намаляването на фрагментирането на вътрешния пазар би подобрило и условията на равнопоставеност сред операторите.

Общата цел е да се обезпечи правната интеграция на българската киберсигурност с европейската, в т.ч. посредством въвеждането на подобрените европейски изисквания във връзка с оценката на риска например.

Конкретната цел е да се запълнят констатираните празноти и отстранят несъответствията в действащото българско законодателство чрез въвеждането на правила за капацитета за оценка на риска, докладването на инциденти, тестването, повишаването на осведомеността и осъзнатостта на факта, че киберинцидентите и липсата на адекватен отговор могат да застрашат стабилността както на публичните, така и на частните субекти.

Оперативната цел на предложените промени в националното законодателство е в него да се въведат мерки за прилагането на Директива (ЕС) 2022/2555.

Една от основните цели на Директива (ЕС) 2022/2555 е именно осигуряването на високи гаранции и възможности за по-добра устойчивост на киберпространството и по-ефективни мерки за противодействие на кибератаките, особено по отношение на основните икономически субекти и държавните органи. В този смисъл новите регулации целят гарантиране на справедливо третиране на субектите, повишаване на тяхната

информираност и осигуряване на надежден и ефективен надзор за спазване на правата и законните им интереси. Това може да се осъществи чрез възлагане на допълнителни правомощия в полза на компетентните в областта органи и усъвършенстването на съществуващата нормативна уредба, което ще подсигури постигането на следните конкретни цели:

• регламентиране на процедури за сътрудничество и обмен на информация между компетентните органи и НЕРИКС, ЕРИКС;

• промяна в сроковете за докладване на инциденти;

• да се въведат условия за управление и противодействие на рисковете, касаещи съществените и важни субекти, както и отговарящите на зададените критерии, попадащи в определените сектори в Приложение 1 и 2;

• на компетентните органи се предоставят широки пълномощия по управление и надзор политиките по киберсигурност по отношение на определените субекти – съществени и важни. Компетентните органи следва да бъдат оправомощени да прилагат санкции, състоящи се в спиране на сертифициране или разрешение относно част или всички услуги пропорционално на тежестта на нарушението, само като ultima ratio, което означава само след изчерпване на другите съответни действия по прилагане, за времето, докато субектите, спрямо които се прилагат, предприемат необходимите действия за отстраняване на недостатъците;

• да се установи рамка за координирано оповестяване на уязвимости и изискване държавите членки да определят ЕРИКС, като координатор за целите на координираното оповестяване на уязвимости и да улесняват взаимодействието между докладващите субекти и производителите или доставчиците на ИКТ продукти и услуги;

• да се въведе национална рамка за управление на кризи в областта на киберсигурността, по-специално чрез определяне на национални компетентни органи, отговарящи за управлението на мащабни инциденти и кризи в тази област;

• да се развие международното сътрудничество като се участва активно в създадената Европейска мрежа за връзка на организациите при кибер кризи (EU – CyCLONe) с цел подпомагане на координираното управление на мащабни инциденти и кризи, свързани с киберсигурността, и осигуряване на редовния обмен на информация сред държавите членки и институциите на ЕС;

• управление на риска, свързан с киберсигурността;

• от компетентните органи се изисква да упражняват надзор върху субектите, попадащи в обхвата на директивата, и по-специално да гарантират спазването от тяхна страна на изискванията за сигурност и уведомяване за инциденти. Разграничава се между режим на предхождащ надзор (ex-ante) за съществените субекти и режим на последващ надзор (ex-post) за значимите субекти, като във втория случай от компетентните органи се изисква да предприемат действия, когато са получили доказателства или индикации, че значим субект не спазва изискванията за сигурност и уведомяване за инциденти.

Със промяната на закона се разширяват секторите на въздействие, а именно:

1. Енергетика
2. Транспорт
3. Банков сектор
4. Инфраструктури на финансовия пазар
5. Здравеопазване
6. Питейна вода
7. Отпадъчни води
8. Цифрова инфраструктура
9. Управление на услуги в областта на ИКТ (между предприятия)
10. Публична администрация

11. Космическо пространство

Други критични сектори:

12. Пощенски и куриерски услуги

13. Управление на отпадъците

14. Производство, изготвяне и дистрибуция на химикали

15. Производство, преработка и разпространение на храни

16. Производство

17. Доставчици на цифрови услуги

18. Научни изследвания

Като резултат от приемането на предлаганите изменения се очаква:

- създаване на условия за изграждане на ефективна система за превенция и борба с кибератаките;
- ограничаване на мащаба, честотата и въздействието на инцидентите;
- противодействие на инцидентите, които причиняват значителни финансови загуби, подкопават доверието на потребителите и причиняват сериозни вреди на икономиката на държавата;
- ограничаване на транснационалния характер на инцидентите;
- установяване на условия за равнопоставеност по отношение на контрола на съществените и важни субекти, и административните органи;
- улесняване на достъпа до надлежна информация, касаеща услуга, която е от съществено значение за поддържането на особено важни обществени и/или стопански дейности;
- повишаване на сигурността чрез създаване и поддръжка на непубличен регистър на определените субекти в кръга на законопроекта, както и на самите съществени услуги;
- въвеждане на ясна йерархична структура в управлението и организацията на националната система за киберсигурност;
- подобряване на надеждността, устойчивостта и ефективността на мрежите и информационните системи на всички субекти в обхвата на закона.

С транспонирането на Директивата МИС 2 и реализиране на поставените цели ще се опрости и ускори процесът по взаимодействието и разрешаването на трансгранични и национални инциденти в ЕС, като това ще става бързо и без никакви допълнителни формалности, което ще допринесе за своевременното преодоляване на атаките и намаляване на негативните последици от тях.

С уеднаквяването на процедурата и процесите по взаимодействие на местно и европейско ниво ще се намали документацията, ще се ускори времето за взаимодействие, ще се въведе единен стандартен формуляр за докладване на инциденти, с който органите да изискват помощ при нужда, което, от своя страна, ще доведе до намаляване на административната тежест.

Приемането на законопроекта ще има за резултат хармонизирането и привеждането в съответствие на националното с европейското законодателство.

Съгласно чл. 26, ал. 2-4 от Закона за нормативните актове проектът на Решение на Министерския съвет за одобряване на проект на Закон за изменение и допълнение на Закона за киберсигурност е публикуван на интернет страницата на Министерството на електронното управление и на Портала за обществени консултации на Министерския съвет за срок от 30 дни.

Проектът на Решение е съгласуван в съответствие с разпоредбите на чл. 32 от Устройствения правилник на Министерския съвет и на неговата администрация. Направените бележки и предложения са отразени, съгласно приложената справка.

Предложеният проект на Решение не води до въздействие върху държавния бюджет, поради което към него е приложена финансова обосновка, съгласно приложение № 2.2 към чл. 35, ал. 1, т. 4, буква „б“ от Устройствения правилник на Министерския съвет и на неговата администрация.

Проектът съдържа разпоредби, свързани с въвеждане на изисквания на европейското право, поради което е приложена справка за съответствие.

УВАЖАЕМИ ГОСПОДИН МИНИСТЪР-ПРЕДСЕДАТЕЛ,
УВАЖАЕМИ ГОСПОЖИ И ГОСПОДА МИНИСТРИ,

Предвид гореизложеното и на основание чл. 8, ал. 4, т. 1 от Устройствения правилник на Министерския съвет и на неговата администрация, предлагам Министерският съвет да разгледа и приеме предложения проект на Решение на Министерския съвет за одобряване на проект на Закон за изменение и допълнение на Закона за киберсигурност.

ВАЛЕНТИН МУНДРОВ

Министър на електронното управление