Закон за изменение и допълнение на Закона за киберсигурност

линк към консултацията

Информация

Откриване / Приключване: 04.07.2024 г. - 03.08.2024 г. Неактивна

Номер на консултация: #10433-K

Област на политика: Архив - Държавна администрация

Тип консултация: Закон

Вносител: Министерство на електронното управление

Тип вносител: Национално

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.

Отговорна институция

Отговорна институция

Министерство на електронното управление
Адрес: София, ул. Ген. Гурко №6
Електронна поща: mail@egov.government.bg

Документи

Пакет основни документи:

Доклад от вносителя - вер. 1.0 | 04.07.2024

Закон за изменение и допълнение на Закона за киберсигурност - вер. 1.0 | 04.07.2024

Решение на Министерския съвет - вер. 1.0 | 04.07.2024

Частична предварителна оценка на въздействието - НОИСРЕАУ - вер. 1.0 | 04.07.2024

Становище на ДМА - вер. 1.0 | 04.07.2024

Становище на „Домейн Менада“ ЕООД - вер. 1.0 | 01.08.2024

Становище на Фондация „Право и интернет“ - вер. 1.0 | 12.08.2024

Справка за отразяване на предложенията и становищата - вер. 1.0 | 04.09.2024

Консултационен документ:

Справка становища:

Коментари

Автор: Ясен Танев (03.08.2024 21:07)

Добавяне на нова алинея към чл. 27 преди чл. 27ж

Предложения за промяна в Закона за киберсигурност

Добавяне на нова алинея към чл. 27 преди чл. 27ж

„Националният компетентен орган утвърждава критерии за акредитация на независими органи по оценка на съответствието и одитори, които могат да извършват обективни и безпристрастни проверки за сигурност и редовни и целеви одити по този закон. Тези критерии трябва да включват изисквания за квалификация, опит и независимост на извършващите проверките, както и процедури за мониторинг и оценка на тяхната работа.“

Мотивация

1. На база на променените текстове в Закона за изменение и допълнение на Закона за киберсигурност и Директива (ЕС) 2022/2555 предлагаме да се въведат промени в закона, които да позволяват извършването на обективни и безпристрастни проверки и одити по този закон от трета страна. Очаква се това да подобри качеството и независимостта на проверките за киберсигурност, да подпомогне Компетентния орган при осъществяването на надзора за спазването на закона и да създаде стандарти за независимите одитори и органи.
2. Необходимо е да се внесе яснота по предложения чл. 27ж, ал. 1, т. 2 „да извършват редовни и целеви одити на сигурността, извършвани от независим орган или компетентен орган“.

Референция

Регламент ЕО 765/2008 на ЕП и на Съвета от 09 юли 2008 г. за определяне на изискванията за акредитация и надзор на пазара във връзка с предлагането на пазара на продукти и за отмяна на регламент ЕИД 339/3

Предложението е съгласувано с експерти от:

Европейски цифров иновационен хъб Тракия

Българска асоциация по киберсигурност

Български съюз на стандартизаторите

Автор: Stanimir Sotirov (02.08.2024 15:51)

Предложение за извеждане на ясни критерии за предвидените снакции по чл. 29

Имуществени санкции

Чл. 29.

(3) Съществен субект, който не изпълни задълженията по чл. 22 и чл. 24 се наказва с имуществена санкция от 200 000 лева до 2% от общия световен годишен оборот за предходната финансова година на предприятието, към което принадлежи съществения субект, но не по –малко от 20 000 000 лева.

(4) Важен субект, който не изпълни задълженията по чл. 22 и чл. 24 се наказва с имуществена санкция от 100 000 лева до 1,4% от общия световен годишен оборот за предходната финансова година на предприятието, към което принадлежи важния субект, но не по-малко от 14 000 000 лева.

Предложение за промяна - трябва да бъдат изведени ясни и точни критерии за размера на санкциите, които ще се налагат от съответния контролиращ орган, тъй като е предложено те варират в рамките на 1%-100%. В противен случай контролиращият орган ще бъде принуден да взима субективно решение относно размера на предвидените санкции, което от своя страна е предпоставка за корупция.

Автор: Stanimir Sotirov (02.08.2024 15:46)

Коментар относно чл. 29, секция (3) и секция (4) - размер на санкциите

Чл. 29

(3) Съществен субект, който не изпълни задълженията по чл. 22 и чл. 24 се наказва с имуществена санкция от 200 000 лева до 2% от общия световен годишен оборот за предходната финансова година на предприятието, към което принадлежи съществения субект, но не по –малко от 20 000 000 лева.

(4) Важен субект, който не изпълни задълженията по чл. 22 и чл. 24 се наказва с имуществена санкция от 100 000 лева до 1,4% от общия световен годишен оборот за предходната финансова година на предприятието, към което принадлежи важния субект, но не по-малко от 14 000 000 лева.

Предложение за промяна - трябва да бъдат изведени ясни и точни критерии за размера на санкциите, когато е заложено те да варират в рамките на 1%-100%. В противен случай, органът, който ще определя размера на санкциите ще бъде принуден да взема субективно решение относно размера на тези санкции, което от своя страна е предпоставка за навлизането на корупционни практики.

Автор: N S (01.08.2024 19:24)

Относно периодичните санкции и предвидената методика по чл. 16, ал. 3, т. 8

1. Предлагам да се измени или изцяло премахне §31, с който се създава чл. 30а.

Директивата представя единствено възможност за периодични санкции, поради което същата или трябва да се премахне изцяло, или следва да се намали значително размера ѝ, тъй като предвиденият в ЗИД размер от 5000 лв. на ден е прекомерен. Ако периодична санкция остане, то същата следва да се намали

значително или да се предвиди, че е най-малко за всеки месец. В нито един закон не се предвижда подобна огромна санкция, а ако такава санкция бъде наложена на практика - то тя би могла да доведе до несъстоятелност на почти всяко едно дружество в страната.

2. Предлагам в закона или методиката, която ще се приеме съгласно §31, да се предвиди изрично възможността, описана в преамбюл 16 от ?????????? ????

3. ? §40 следва да се направи промяна като референцията към чл. 4, ал. 3 се промени на чл. 16, ал. 3, т. 8

Автор: Божидар Божанов (01.08.2024 16:32)

Премахване на текстове от Закона за защита на класифицираната информация

Предлагам въвеждане на нов параграф в преходните и заключителни разпоредби, с който да бъде изменен Закона за защита на класифицирана информация, по отношение на Приложение 1, част II, като предлагам т. 14 да бъде отменена.

За постигане на високо ниво на киберсигурност, добрите практики изискват адекватна документация на процесите и практиките, конфигурациите, автоматизиране на дейностите. В допълнение, закупуването на решения (хардуерни и софтуерни) за киберсигурност следва да бъде максимално прозрачно и конкурентно.

Предложената за отмяна т. 14 съдържа пречки за ефективносто изпълнение на дейности, свързани с киберсигурността, поради особения режим на работа с класифицирана информация.

Сигурността на информационните системи се базира не на прикриването на информация, а на нейната навременна достъпност за експертните лица, поради което нейното класифициране следва да отпадне.

Алтернативно, може да бъде стеснен обхвата на информацията по т. 14, конкретно до информация за защита на криптографски ключове.

Автор: Christina Mercuriadi (25.07.2024 17:34)

Становище от Асоциацията на филмовите продуценти (MPA) - част 4

Становище по прилагане на Директивата NIS2: постигане на целта на член 28 за публичен достъп до надеждна информация за WHOIS (част 4)

- **Проверка:** Процедурите за проверка на данните от WHOIS трябва да бъдат надеждни и постоянно актуализирани, за да отразяват подобренията в технологиите и процесите. Както е посочено в съображение 111 от Директива NIS2, тези процедури следва да "предотвратяват и коригират неточни данни за регистрация" и следва да "отразяват най-добрите практики, използвани в индустрията [. . .], и напредъка, постигнат в областта на електронната идентификация" и следва да включват както "предварителни проверки,

извършвани по време на регистрацията, така и последващи проверки, извършвани след регистрацията".

Въпреки че регистрите на имена на ДПН може да не са в състояние да проверяват данните от WHOIS по време на регистрацията, тъй като първоначалното събиране на данните обикновено се извършва от регистраторите и/или услугите за защита на личните данни/прокси сървърите, те със сигурност могат да предприемат последващи процедури за проверка на данните от WHOIS. Препоръчваме законопроектът да направи задължителни предварителните и последващите процедури за проверка за регистрите на имена на ДПН.

Освен това следва да се предвидят последици за подаването на неправилни, неточни или непълни регистрационни данни. Ние категорично подкрепяме прилагането на този подход от страна на Белгия[5] при транспонирането на член 28 от Директива NIS2, както следва:

"*Ако данните за регистрация на име на домейн, изброени в параграф 1, точка 2 на име на домейн, са неправилни, неточни или непълни, регистрите на имена на домейни от първо ниво и организациите, предоставящи услуги за регистрация на имена на домейни, незабавно блокират работата на това име на домейн, докато притежателят на името на домейн не коригира данните за регистрация, така че те да станат правилни, точни и пълни*.

Ако регистрантът на име на домейн не направи това в рамките на срока, определен от регистъра на име на домейн от първо ниво или от организацията, предоставяща услуги за регистрация на имена на домейни, името на домейн се анулира.

Трансферът на блокирано име на домейн към друга организация, предоставяща услуги по регистрация на имена на домейни, е забранен."

- **Пълен регистър WHOIS (Thick WHOIS)**: Регистърът на единни имена на ДПН за .com и .net отговаря за повече от половината от всички регистрирани имена на домейни в световен мащаб и има договори с повече от 2000 регистратори по целия свят. Понастоящем правителствените агенции и други лица, които търсят законен достъп, са принудени да открият съответния регистратор, за да поискат данни от WHOIS. Трудният процес, който това налага, както и фактът, че регистраторът може да се намира в държава, която не сътрудничи по отношение на такива искания, напълно подкопават целта за повишаване на киберсигурността и вместо това служат за прикритие и защита на незаконните участници.

Поради това е от съществено значение този регистър, както и всички други регистри на имена на ДПН, да поддържат пълна, точна и независима база данни на WHOIS за **всички** имена на домейни, които администрират (наричана "дебела WHOIS"), като тези данни **трябва да включват** данните на действителния потребител на името на домейна, а не просто данните на доставчика на услуги за защита на личните данни или прокси, които може да са били използвани в процеса на регистрация (вж. по-горе). Това съществено изискване ще гарантира,

че правоприлагащите органи и други лица, законно търсещи достъп, разполагат с централизиран и единен източник, от който да черпят пълни и точни данни за всяко име на домейн, администрирано от регистъра на имена на ДПН.

Стан МакКой

Президент и Управляващ директор на MPA за Европа, Близкия изток и Африка

Автор: Christina Mercuriadi (25.07.2024 17:33)

Становище от Асоциацията на филмовите продуценти (MPA) - част 3

Становище по прилагане на Директивата NIS2: постигане на целта на член 28 за публичен достъп до надеждна информация за WHOIS (част 3)

Поради това при транспонирането на Директива NIS2 на национално равнище трябва да се вземе предвид популярността на услугите за прокси сървъри или за защита на личните данни сред лицата, извършващи незаконни и вредни дейности онлайн. Когато се подава законно искане за достъп, трябва да се разкрият основните данни на действителния клиент/ползвател на името на домейна, а не само данните на доставчика на услугата за защита на личните данни или прокси услугата, ако такава услуга за защита на личните данни или прокси услуга е била използвана в процеса на регистрация.

Ето защо приветстваме факта, че в българския проектозакон се пояснява, че понятието "доставчик на услуги за регистрация на имена на домейни" следва да се разбира като обхващащо доставчиците и препродавачите на услуги за защита на личните данни и прокси услуги. Въпреки това бихме препоръчали също така проектозаконът да включва изрично следната формулировка при прилагането на член 28 от Директивата NIS2: "*При предоставянето на данни в отговор на законни искания за достъп регистрите на имена на ДПН и организациите, предоставящи услуги за регистрация на имена на домейни, предоставят данните на действителния ползвател на името на домейна и не могат да предоставят вместо това данните на доставчика на услуги за защита на личните данни или данните на доставчика на прокси услуги за регистрация, които може да са били използвани в процеса на регистрация на името на домейна.*"

- **Третиране на въпроса за предотвратяване на мащабни злоупотреби с DNS:** Киберпрестъпниците често регистрират множество, понякога дори хиляди, имена на домейни за кратък период от време. Това се отнася особено за фишинг, разпространение на зловреден софтуер и съдържание, нарушаващо авторските права. Гарантирането, че търсещият законен достъп може да получи списък на всички имена на домейни, регистрирани с помощта на едни и същи данни за регистранта (обратна проверка на WHOIS), е от съществено значение, когато се подозират сложни и разпръснати незаконни дейности в такъв мащаб. Ето защо препоръчваме член 28 от Директива NIS2 да бъде транспониран така, че да позволява, че "*когато име на домейн е свързано с неправомерна или незаконна дейност и това се твърди от законно търсещо достъп лице, то регистрите на имена на ДПН и организациите, предоставящи услуги по регистрация на имена на*

домейни, трябва при поискване да предоставят на законно търсещото достъп лице списък на всички имена на домейни, които те администрират или са регистрирали със същите данни за регистранта".

- **Юридически лица:** Данните от WHOIS на юридическите лица (най-малко име и работещ/проверен телефонен номер и работещ/проверен имейл адрес за връзка) трябва да бъдат публично достъпни съгласно член 28, параграф 4 във връзка със съображение 112 от Директивата NIS2.

Стан МакКой

Президент и Управляващ директор на MPA за Европа, Близкия изток и Африка

Автор: Christina Mercuriadi (25.07.2024 17:31)

Становище от Асоциацията на филмовите продуценти (MPA) - част 2

Становище по прилагане на Директивата NIS2: постигане на целта на член 28 за публичен достъп до надеждна информация за WHOIS (част 2)

По-долу са посочени следните приоритети и препоръки за осигуряване на адекватно прилагане на член 28 и съображения 109-112 от Директива NIS2 и за значително увеличаване на достъпността и точността на данните от WHOIS:

- **Лица, законно търсещи достъп и данни**: Съображение 110 дефинира "законно търсещия(ите) достъп" до данните от WHOIS по смисъла на член 28 параграф 5 от Директива NIS2 като "всяко физическо или юридическо лице, което отправя искане съгласно правото на Съюза или националното право".

  Настоятелно призоваваме българският законодател да преразгледа обхвата на член 27в алинея 4, който е изключително тесен и задължава регистрите на имена на домейни от първо ниво (TLD/ДПН) и организациите, предоставящи услуги по регистрация, да си сътрудничат само с националните компетентни органи и органите на досъдебното производство. Обхватът следва да бъде разширен, така че да включва и всяко физическо или юридическо лице, което отправя искане за достъп до данни от WHOIS с цел разследване на правонарушение, включително, без ограничение, за установяване, упражняване или защита на киберсигурност, интелектуална собственост, защита на потребителите или други правни претенции в качеството си на лице, "законно търсещ(и) достъп". Това разширяване на кръга легитимирани лица е от решаващо значение за осигуряването на достъп до конкретни данни за регистрация на имена на домейни при законни и надлежно обосновани искания.

  Описаното съответства с наскоро публикуваната препоръка на Европейската комисия относно борбата с фалшифицирането, която насърчава субектите, предоставящи услуги по регистрация на имена на домейни в ЕС, да признават всички физически или юридически лица, които отправят искане за право на информация (ROI) съгласно Директива 2004/48/ЕО относно упражняването на права върху интелектуалната собственост (IPRED), за лица, законно търсещи

достъп.

Въз основа на изложеното предлагаме настоящата редакция на член 27в алинея 4 да бъде изменена така, че да задължи регистрите на имена на ДПН и организациите, предоставящи услуги за регистрация на имена на домейни, да сътрудничат на законно търсещите достъп, което следва да включва *всяко физическо или юридическо лице, което подава искане за достъп до данни от WHOIS за разследване на правонарушение, включително, без ограничение, за установяване, упражняване или защита на киберсигурност, интелектуална собственост, защита на потребителите или други правни претенции.*

Освен това достъпът до данни от WHOIS съгласно съображение 112 от Директива NIS2 трябва да бъде безплатен и тези данни трябва да се предоставят при поискване от законно търсещия достъп без неоправдано забавяне.

Бихме искали да обърнем внимание на неотдавнашното белгийско транспониране, което включва "**всяко лице в контекста на нарушения на права върху интелектуална собственост или сродни права**" в списъка на лицата, които се считат за лица, законно търсещи достъп за целите на исканията за предоставяне на достъп до данни за регистрация на имена на домейни. Ето защо, с уважение насърчаваме българските власти да приложат подобен подход, за да се даде възможност за ефективно наблюдение и борба с незаконните дейности онлайн.

- **Третиране на въпроса за използването на прокси услуги/ услуги за защита на личните данни:** В проучване на Службата на ЕС за интелектуална собственост (EUIPO) от 2021 г. се отбелязва, че "значителен процент от имената на домейни, използвани за извършване на незаконни или вредни дейности в интернет, са регистрирани чрез услуги за защита на личните данни или прокси услуги" и че след влизането в сила на Общия регламент за защита на данните обосновката на законното използване на услуги за защита на личните данни или прокси услуги "е поставена под въпрос".

Стан МакКой

Президент и Управляващ директор на MPA за Европа, Близкия изток и Африка

Автор: Christina Mercuriadi (25.07.2024 17:26)

Становище от Асоциацията на филмовите продуценти (MPA) - част 1

Становище по прилагане на Директивата NIS2: постигане на целта на член 28 за публичен достъп до надеждна информация за WHOIS (част 1)

The Motion Picture Association (MPA) служи като глобален глас и защитник на международната филмова, телевизионна и стрийминг индустрия. Наши членове са Walt Disney Studios Pictures, Netflix Studios, LLC, Paramount Pictures Corporation, Sony Pictures Entertainment Inc., Universal City Studios LLC и Warner Bros. Discovery. Компаниите, членуващи в MPA, продуцират и инвестират значителни средства в

производството на европейско аудиовизуално съдържание, което намира и глобална аудитория чрез тяхното разпространение.

MPA играе водеща роля в борбата с незаконното разпространение на защитено съдържание, което вреди на развитието на дигиталната екосистема. Целта на MPA е да намали и овладее ефектите от пиратството чрез ефективни стратегии за правоприлагане, насочени към операторите на незаконни сайтове и услуги, както и към посредниците, които предоставят технически условия за тяхната дейност.

MPA приветства предприетите действия по транспониране на преработената Директива относно сигурността на мрежовите и информационните системи (Директива NIS2), и по-специално разпоредбите на член 28 и съображения 109-112, свързани с услугите за регистрация на домейни. Осигуряването на достъп до надеждни данни за регистрантите ("WHOIS данни") е от съществено значение за борбата с незаконното и вредно съдържание онлайн, включително съдържанието, нарушаващо авторските права, и за защитата на здравето и сигурността на гражданите.

Следва да се отбележи, че проучването на Европейската комисия относно злоупотребите с DNS от 2022 г. посочва проверката на данните от WHOIS като една от основните препоръки за предотвратяване, откриване и намаляване на злоупотребите с DNS. Европейската комисия също така неотдавна призна в Препоръката за борба с фалшифицирането от 2024 г., че "точността и пълнотата на данните за регистрация на име на домейн също може да играе централна роля при прилагането на правата върху интелектуалната собственост", като допълнително подчерта необходимостта предоставените данни за регистрация да бъдат точни, проверени и да се отнасят до действителния ползвател на името на домейна, а не просто до доставчик на услуги за защита на личните данни или прокси.

По изложените причини приветстваме възможността да представим нашите коментари относно българския проектозакон и по-специално нашите опасения относно изключително ограничения обхват на проекта на член 27в алинея 4.

Стан МакКой

Президент и Управляващ директор на MPA за Европа, Близкия изток и Африка

Автор: Никола Петков (15.07.2024 13:09)

Производствени предприятия - част ОТ (Оперативни Технологии)

Здравейте,

Бих искал да обърна внимание на частта ОТ (Оперативни Технологии), които са съществени за производствените предприятия.

По своята същност ОТ се различават значително от ИТ, като тук специалистите по темата „Киберсигурност“ трябва същевременно да разбират в детайли и темата „Системи за Индустриална Автоматизация“.

Изискванията и добрите практики към ОТ са описани в стандарта **IEC 62443,** който покрива част от стандарта **ISO 27000** и от стандартите **IEC 61511 / IEC 61508** по отношение на функционалната сигурност. Този стандарт условно може да се раздели на три подраздела, които посочват различните изисквания, а именно:

- Подраздел отнасящ се към крайните потребители (Производствените предприятия), обект на проверка съгласно МИС2;
- Подраздел отнасящ се към фирмите Системи Интегратори (проектантски и инженерингови фирми), които проектират и внедряват Системи за Автоматизация и Задвижванията при горните и
- Подраздел отнасящ се към производителите на технологично оборудване, занимаващи се с развойна дейност и производство на софтуерни и хардуерни продукти

Както при ИТ, така и при ОТ обследването на съществуващата ситуация съгласно изискванията на IEC 62443 е началото на процеса по оценка на актуалното нивото сигурност, определящо последващите мерки за преминаване към по-високо ниво на сигурност.

Това са само част от особеностите в частта ОТ, поради което препоръчвам при производствените предприятия да се обърне допълнително внимание на оценката на частта ОТ.

С уважение,

Никола Петков

Автор: Никола Петков (15.07.2024 13:07)

Производствени предприятия - част ОТ (Оперативни Технологии)

Здравейте,

Бих искал да обърна внимание на частта ОТ (Оперативни Технологии), които са от съществено значение за производствените предприятия.

По своята същност ОТ се различават значително от ИТ, като тук специалистите по темата „Киберсигурност“ трябва същевременно да разбират в детайли и темата „Системи за Индустриална Автоматизация“.

Изискванията и добрите практики към ОТ са описани в стандарта **IEC 62443**, който покрива част от стандарта **ISO 27000** и от стандартите **IEC 61511 / IEC 6150**8 по отношение на функционалната сигурност. Този стандарт условно може да се раздели на три подраздела, които посочват различните изисквания, а именно:

- Подраздел отнасящ се към крайните потребители (Производствените предприятия), които са обект на проверка съгласно МИС2;

- Подраздел отнасящ се към фирмите Системи Интегратори (проектантски и инженерингови фирми), които проектират и внедряват Системи за Автоматизация и Задвижванията при горните;
- Подраздел отнасящ се към производителите на технологично оборудване, занимаващи се с развойна дейност и производство на софтуерни и хардуерни продукти.

Както при ИТ, така и при ОТ обследването на съществуващата ситуация съгласно изискванията на IEC 62443 е началото на процеса по оценка на актуалното нивото сигурност, определящо последващите мерки за преминаване към по-високо ниво на сигурност.

Това са само част от особеностите в частта ОТ, поради което препоръчвам при производствените предприятия да се обърне допълнително внимание на оценката на частта ОТ.

С уважение,

Никола Петков

Автор: Илия Христозов (07.07.2024 12:19)

Коригиране на технически грешки

1. На много места в изменените разпоредби на закона се правят препратки към „*чл. 4, **ал. 1**, т.…*“, но в изменения текст на разпоредбата на чл. 4 вече няма алинеи, а само точки. Затова **предлагам тези препратки да се коригират на** „***чл. 4, т.…***“.

2. Предлагам в разпоредбата на § 17, т. 3, буква е) от проекта **думите „*т. 6 и 7*“ да се заменят с думите „*т. 6, 7 и 8*“**,

защото се създава и нова т. 8.

3. Предлагам **разпоредбата на § 40, т. 1 от проекта да се измени във вида:**

*„1. в срок до три месеца от влизането в сила на закона определя с решение административните органи по чл. 16, ал. 1 и приема методиката по **чл. 16, ал. 3, т. 8**;“*

защото приемането на тази методика вече ще е регламентирано в чл. 16, ал. 3, т. 8 от закона.

4. Предлагам в разпоредбата на § 41 от проекта **думите *„решението по § 41, т. 1“* да се заменят с думите *„решението по § 40, т. 1“***

за да е точна препратката.

5. За по-добра прецизност **предлагам разпоредбата на § 42, т. 2 от проекта да се измени във вида:**

„2. В чл. 30, ал. 1, т. 22 думите „като при необходимост си съдейства с компетентните органи по чл. 244а, ал. 3“ ***и запетайката пред тях*** *се заличават.“*

6. В разпоредбата на § 42, т. 4 от проекта предлагам да се коригира думата „*петнад**а** сета*“ с думата „*петнадесета*“.

Автор: Илия Христозов (05.07.2024 18:07)

За изменение на § 42, т. 1 от проекта

Така предложеният текст на разпоредбата на **§ 42, т. 1 от проекта:**

§ 42. В Закона за електронните съобщения се правят следните изменения и допълнения:

*1. В чл. **16**, се създава **ал. 2а**:*

*„(**2а**) Национален компетентен орган за субектите по чл. 4, **ал. 1,** т. 3, буква а) и б) е Комисията за регулиране на съобщенията.“*

е неточен и непълен, защото е ясно, че не може да става въпрос за чл. 16 от ЗЕС, който регламентира дейностите на министъра на транспорта и съобщенията, а и няма алинеи в него. Освен това, така написана в ЗЕС, тази разпоредба реферира към разпоредбите на чл. 4, ал. 1, т. 3, буква а) и б) от ЗЕС, но в тях не става въпрос за субекти, а за целите на закона. Един внимателен анализ показва, че вероятно се имат предвид изменените разпоредби на чл. 4, т. 3, буква а) и б) от самия Закон за киберсигурност.

За преодоляване на горепосочената грешка, **предлагам разпоредбата на § 42, т. 1 от проекта да се измени в един от двата варианта:**

Вариант **1**:

1. В чл. 21 се създава ал. 6:

„(6) Комисията изпълнява функциите на национален компетентен орган за субектите по чл. 4, т. 3, буква а) и б) от Закона за киберсигурност.“

или Вариант **2**:

1. В чл. 30, ал. 1 се създава т. 30:

„30. изпълнява функциите на национален компетентен орган за субектите по чл. 4, т. 3, буква а) и б) от Закона за киберсигурност.“

в зависимост от това, за кое място в ЗЕС се прецени, че е по-подходящо за тази разпоредба.

Вероятно горепосочената грешка в разпоредбата на § 42, т. 1 от проекта се е допуснала, защото на някакъв по-ранен етап от изготвянето на проекта, тази разпоредба е била предвидена като нова алинея 2а на чл. 16 от самия Закон за киберсигурност, **в което също има логика и смисъл**. Затова, ако се прецени, че е необходимо, **предлагам да се добави като § 17, т. 3 от проекта разпоредбата във вида:**

3. В чл. 16 се създава ал. 2а:

„(2а) Национален компетентен орган за субектите по чл. 4, т. 3, буква а) и б) е Комисията за регулиране на съобщенията.“

и следващите точки в § 17 да се преномерират.

История

Начало на обществената консултация - 04.07.2024

Приключване на консултацията - 03.08.2024

Справка за получените предложения - 04.09.2024

Справка за отразяване на предложенията и становищата

Окончателен акт на Министерския съвет
