Българска асоциация по киберсигурност (БАК)
София, България

До: Членовете на парламентарната Комисия по електронно управление и информационни технологии Народно събрание на Република България

Относно: Становище по Проекта на Закон за изменение и допълнение на Закона за киберсигурност – Необходимост от прецизиране на разпоредбите относно Координираното разкриване на уязвимости (CVD)

Уважаеми народни представители,

От името на **Българската асоциация по киберсигурност (БАК)**, част от Европейския цифров иновационен хъб "Тракия" и Съюза за стопанска инициатива, обединяваща едни от най-големите и утвърдени компании и организации в сферата на киберсигурността, явяваща се национален партньор на водещите европейски мрежи за киберсигурност, изразяваме своята **подкрепа** за предложения проектозакон за изменение и допълнение на **Закона за киберсигурност**, който цели привеждане на националното законодателство в съответствие с **Директивата NIS2**. Законодателната инициатива е **необходима и навременна стъпка** за укрепване на киберсигурността в България.

Въпреки това, намираме за необходимо да подчертаем няколко възможности за оптимизация:

I. Относно координираното оповестяване на уязвимости

Макар проектозаконът на Министерския съвет да предвижда въвеждането в българското законодателство на вече утвърдени другаде в Европа мерки като приемането на **общи разпоредби относно координираното оповестяване на уязвимости (CVD)**, те остават **недостатъчно детайлни и не осигуряват ясен механизъм за прилагането на тази практика**. В този контекст, **Белгийският модел** предлага значително по-прецизирани и ефективни законови решения.

1. Значението на координираното разкриване на уязвимости (CVD)
Директивата NIS2 и **Насоките на ENISA относно прилагането на национални политики за координирано разкриване на уязвимости (NIS Cooperation Group, 2023)** насърчават държавите членки да изградят правна рамка за етичното изследване на сигурността и отговорното докладване на уязвимости - както от засегнатите организации, така и от добросъвестни трети страни - изследователи на кибер-уязвимости (cybersecurity researchers), познати в медийното пространство и с популярния етикет на "етични хакери". **CVD играе жизненоважна роля в противодействието на киберзаплахите, тъй като позволява на изследователите на сигурността да докладват уязвимости без страх от правни последици, гарантирайки тяхното отстраняване преди да бъдат експлоатирани от злонамерени субекти.**

2. Недостатъците в настоящия законопроект
Въпреки че проектозаконът на Министерския съвет съдържа текстове, свързани с **координираното оповестяване на уязвимости (CVD)**, той **не предлага достатъчно ясни правила, процедури и гаранции за участниците в процеса**. Липсата на конкретика може да доведе до:

- **Правна несигурност за изследователите на кибер-уязвимости**, които няма да имат категорична защита при добросъвестно изследване и докладване на уязвимости на системи на трети страни;
- **Ограничена ефективност на докладванията**, поради липсата на ясно дефинирани задължения за компетентните органи;
- **Неефективна координация между публичния и частния сектор** в процеса на разкриване и отстраняване на уязвимости.

3. Приложимост на Белгийския модел

Белгия е сред водещите страни в ЕС по отношение на киберсигурността, като през 2023 г. въведе законодателство, което **ясно защитава добросъвестните изследователи на киберсигурността** и **осигурява механизми за ефективно координирано разкриване на уязвимости от външни експерти**. Според **Глобалния индекс по киберсигурност 2024**, Белгия постига **96.81/100**, докато **България е с 74.73/100**, което показва необходимостта от по-прецизна регулаторна рамка. **БАК счита, че прилагането на ключови елементи от Белгийския модел, както са разписани в приложения законопроект на БАК, би осигурило по-ефективна защита на критичната инфраструктура и цифровите услуги в България.**

4. Нашите препоръки

БАК **призовава Народното събрание** да внесе **по-прецизирани разпоредби** относно CVD преди второто четене на закона, като се осигурят:

- **Ясна правна защита** за специалистите по киберсигурност при отговорно докладване на уязвимости, разкрити в системи на трети страни - компании и институции;
- **Подробни процедури за CVD**, дефиниращи задълженията на всички участници в процеса, които не се ограничават до компетентния държавен орган и засегнатата организация;
- **Интегриране на CVD процедури в Националния екип за реагиране при инциденти с компютърната сигурност (НЕРИКС)**, но с ясно разписани срокове и механизми за реакция.

5. Заключение

България има възможност да **се изравни с водещите европейски практики в областта на киберсигурността** чрез **по-прецизирано законодателство относно CVD. Настоящите разпоредби в проектозакона са добра основа, но без допълнителна яснота и детайлизация те рискуват да останат неефективни.**

Призоваваме **Комисията по електронно управление и информационни технологии** да въведе по-ясни и конкретни текстове, основаващи се на **Белгийския модел**, за да гарантира ефективно и правно защитено координирано разкриване на уязвимости в България.

Оставаме на разположение за допълнителни дискусии и експертни консултации.

С уважение,

Милчо Еврогиев

Председател, Българска асоциация по киберсигурност (БАК)

ПРОЕКТ!

ЗАКОН ЗА ИЗМЕНЕНИЕ И ДОПЪЛНЕНИЕ НА ЗАКОНА ЗА КИБЕРСИГУРНОСТ

(обн., ДВ., бр. 94 от 2018 г., изм. и доп., бр. 69 и 85 от 2020 г. и бр. 15 и 25 от 2022 г.)

§ 1. Създава се чл. 19а:

Чл. 19а (1) Всяко физическо или юридическо лице може да докладва на националния екип за реагиране при инциденти с компютърната сигурност (НЕРИКС) за наличието на потенциална уязвимост по смисъла на § 3. т. 34, установени в рамките на юридическо лице от частния или публичен сектор. Докладът се подава писмено, съгласно процедура, описана на уебсайта на НЕРИКС.

(2) НЕРИКС може да наблюдава, изучава или тества сигурността на мрежова и информационна система, за да определи наличието на потенциалната уязвимост или да провери методите, използвани от лицето, което подава доклада. Когато става въпрос за оператор на основни услуги или доставчик на цифрови услуги, НЕРИКС уведомява компетентния секторен орган, че възнамерява да предприеме мерки на тази основа, както и резултатите от тези мерки.

(3) НЕРИКС запазва цялостността, целостта, дългосрочното съхранение и конфиденциалността на информацията, предадена чрез доклада, както и самоличността на лицето, което е подало предаването, при условие че това лице го поиска и спазва условията, посочени в чл. 19а, ал. 5. Достъпът до тази информация е ограничен до лица, упълномощени от ръководителя на НЕРИКС, освен ако споделянето на тази информация не е необходимо за изпълнението на задачите, възложени на НЕРИКС по този закон.

(4) Ръководителят на НЕРИКС гарантира, чрез приемане на вътрешни процедури, спазването на условията, посочени в този член.

(5) В рамките на процедурата по координирано докладване на уязвимости, авторите на доклада не извършват престъпление за фактите, необходими за доклада, при условие че:

1. те са действали без измамно намерение или намерение да причинят вреда;

2. те са уведомили организацията, отговорна за системата, процеса или контрола, възможно най-скоро и не по-късно от момента на докладването на НЕРИКС, за откриването на потенциална уязвимост;

3. те не са действали извън това, което е било необходимо и пропорционално за проверка на съществуването на уязвимост;

4. те не са разкрили публично информацията, свързана с откритата уязвимост, без съгласието на НЕРИКС.

(6) Когато лица докладват информация за потенциална уязвимост, за която са узнали в професионален контекст, те не се считат за нарушили задължението за професионална тайна и не понасят никаква отговорност във връзка с предаването на информация, необходима за докладването на потенциална уязвимост на НЕРИКС.

(7) Всяка друга възможна отговорност на докладващите лица, произтичаща от действия или бездействия, които не са необходими за изпълнение на процедурата, описана в чл. 19а, ал. 1-4, и не отговарят на условията на чл. 19а, ал. 5, продължава да се урежда от приложимото законодателство.

МОТИВИ:

Законодателната инициатива за регламентиране на етичното хакерство в България (изследването на уязвимости в киберсигурността) е в унисон с позицията на Агенцията на Европейския съюз за киберсигурност (ENISA), която в свой скорошен доклад препоръчва на страните членки, в навечерието на влизането в сила на NIS2 директивата за мрежова и информационна сигурност, да изградят такава законова рамка, която да предоставя закрила от съдебно преследване на изследователи на кибер-уязвимости, съблюдаващи съответните етични стандарти и установените протоколи за координирано разкриване на уязвимости (CVD), въведени от Националните екипи за реагиране при инциденти във връзка с компютърната сигурност (НЕРИКС).

Предложението на експертите по киберсигурност от БАК е НЕРИКС (или CERT България) към Министерството на електронното управление да стъпи на процедурата по етично и координирано докладване на уязвимости в киберсигурността, въведена през 2023 г. в Белгия, доколкото белгийското законодателство, уреждащо въпросите на етичното хакерство, е това, на което БАК се позовава като на добра и съвременна практика в областта. Само преди броени дни бе публикуван международният „Global Cybersecurity Index 2024" на International Telecommunication Union, спрямо който Белгия, с резултат от 96.81/100, се нарежда сред водачите в глобалната киберсигурност. България с общ резултат от 74.73 се нарежда в третото от пет нива на глобалната киберсигурност и отстъпва най-вече в сфери като мерките за изграждане на капацитет – област, която би била подпомогната най-силно от ангажирането на изследователите на уязвимости в киберсигурността („етичните хакери") при защитата на бизнеса и държавата от настъпване на кибер инциденти.

Според Докладите за дейността на МВР и ДАНС през периода 2018-2023 г. се отчита висока честота на киберпрестъпления в България. За по-ефективно противодействие на нарастващите киберпрестъпления и на престъпните структури, използващи високотехнологични методи и средства, през март 2023 г. отдел „Киберпрестъпност" в ГДБОП-МВР е преструктуриран в самостоятелна дирекция, чиято дейност е насочена към борба с кибер- и киберсвързани престъпления, извършвани от организирани престъпни групи (ОПГ) и отделни лица, разкриване и документиране на престъпления, при които обект на нерегламентиран достъп са компютърни системи или мрежи, както и престъпления, чието извършване е практически невъзможно без кибер-пространството. Създаден е Екип за реагиране при инциденти с компютърната сигурност на МВР, който поддържа готовност за координирана съвместна реакция с аналогичен национален екип към МЕУ. Съвместно с партньори от гражданския сектор като Българската асоциация по киберсигурност и Европейския цифров иновационен хъб „Тракия" се организират превантивни кампании за образование, включващи лекции и презентации пред ученици и студенти.

Въпреки тези комплексни и споделени усилия, докладът за развитието на Интернет в България, изготвен по рамката на индикаторите за интернет универсалност на ЮНЕСКО, показва ръст на атаките и измамите, извършвани спрямо държавни институции, фирми и частни лица, свързани с използването на спам или т.нар. фишинг атаки, кибератаки от типа „отказ от услуга", нерегламентиран достъп и хакерски атаки посредством използването на „бот-нет" мрежа, присвояването на акаунти в социалните мрежи, използването на т.нар. вирус „ransomware" и др. Зачестяват и кампаниите за дезинформация, създадени с цел умишлено разпространение на невярна информация. Все повече са сигналите, свързани с инвестиционни измами и неправомерен достъп до акаунти на лица, използващи интернет банкиране. Измамни сайтове за търговия стават инструмент за атаки, засягайки стотици български потребители.

Обобщено, оценката на развитието на Интернет в България показва, че киберпрестъпленията в страната през последните години са в нарастваща тенденция, която засяга широк спектър от сектори и институции. Извършвани са различни видове нарушения, включително използване на зловреден код, спам, DDoS атаки, кражби на лични данни, финансови измами и разпространение на противоправно съдържание. Подчертаната нужда от поддържане на високо ниво на информационна сигурност не може да се обезпечи само с институционалните усилия и ресурси на МЕУ, МВР и ДАНС, нито посредством проактивното поведение на сравнително малкия процент напредничави юридически лица, обръщащи се превантивно към корпоративните услуги на специализираните компании от сектор киберсигурност. Необходимо са нови мерки за изграждане на капацитет в системата на киберсигурност като законовото регламентиране на дейността на изследователите на уязвимости в киберсигурността, т.нар. „етични хакери", по подобие на указанията на ENISA (Guidelines on Implementing National Coordinated Vulnerability Disclosure Policies, NIS Cooperation Group, 2023) и на най-добрите практики на лидерите в киберсигурността измежду страните-членки на Европейския съюз, за да може хиляди обучени експерти по мрежова и информационна сигурност, да започнат да допринасят пълноценно за неутрализирането на киберзаплахи чрез етичното и координирано докладване на установени от тях уязвимости в активи, мрежи и информационни системи на трети страни без риск от наказателно преследване по повод на изследователската им работа.