**Генерални суштински забелешки кон Нацрт Законот за безбедност на мрежи и информациски системи**

Покрај конкретните и детални забелешки, предлози за подобрување и технички исправки на текстот од Нацрт законот за безбедност на мрежи и информациски системи кои се дадени со трага на промени и коментари во приложениот документ со назив „2\_2015596024 Нацрт - закон\_ за безбедност на мрежи забелешки од Народна банка.docx “, во продолжение ги резимираме суштинските забелешки кон нацрт Законот:

1. Согласно Законот за Народната банка на Република Македонија, Народната банка е надлежна за надзор на платните системи. Подзаконската регулатива која ја има донесено Советот и гувернерот на Народната банка за остварување на оваа задача е следната: Политика за надзор на платните системи, Одлука за критериуми и стандарди за работењето на платни системи, Одлука за начин и методологија на надзор на платните системи и Упатство за известување од операторите на платните системи за спроведување на посреден надзор. Притоа, оваа регулатива е во согласност со меѓународните стандарди за надзор на платните системи: Принципите за инфраструктура на финансиските пазари и Рамка за обелоденување и методологија за проценка на Комитетот за системите за плаќање и порамнување при Банката за меѓународно порамнување и Одборот на Меѓународната организација на комисиите за хартии од вредност.

Во рамки на подзаконската регулатива, како и во наведените меѓународните стандарди, е опфатен оперативниот ризик кај платните системи кој, меѓу другото, го покрива и делот за безбедност, интегритет и опоравување на мрежи и информациски системи. Дополнително, со меѓународните стандарди, покрај платните системи е опфатена и останатата инфраструктура на финансиски пазари (депозитари на хартии од вредност, системи за порамнување на хартии од вредност, централни договорни страни и друштвата за регистрација на финансиски трансакции), за чијшто надзор од аспект на усогласеноста со овие стандарди во иднина се планира да биде назначена Народната банка. Во таа насока, во подготовка се соодветни измени на Законот за Народната банка.

Исто така, Народната банка е надлежна за супервизија на банките, штедилниците, друштвата за издавање на електронски пари и други финансиски институции, а Советот и гувернерот на Народната банка за спроведување на оваа задача има издадено бројна подзаконска регулатива како на пример: Одлука за методологијата за управување со ризиците, Одлука за методологијата за сигурност на информативниот систем на банката, Одлука за сигурноста на информативниот систем на штедилница, Одлука за начинот на вршење супервизија и надзор, Одлука за консолидирана супервизија и сл.

Според погоре наведеното, предлагаме во членот 3 од Нацрт законот за безбедност на мрежи и информациски системи да се додаде нов став (4), во кој ќе се пропише дека одредбата од ставот (2) алинеја 1 од членот 16 нема да се применува на банките, штедилниците, друштвата за издавање на електронски пари, другите финансиски институции, операторите на платните системи и операторите на останата инфраструктура на финансиските пазари за кои надзорен орган е (или ќе биде во иднина) Народната банка, а одредбата од постојниот став (4) би станала став (5). Притоа, согласно рециталот од релевантната директива на ЕУ и мислењето од ЕЦБ, Народната банка како надзорен орган за платните системи (во иднина, и за останатата инфраструктура на финансиски пазари) и супервизорски орган за банкарскиот сектор, е подготвена да разменува искуства за прашања поврзани со безбедноста на мрежните и информациските системи со надлежните органи согласно со овој Нацрт закон.

2. Заради правилно разбирање на Законот во однос на субјектите што треба да го применуваат овој закон, како и заради утврдување на надлежните CSIRT-ови за секој сектор поодделно, предлагаме во законот точно да се определи кои потсектори и правни лица припаѓаат во секторите дефинирани во Членот 3, слично како што тоа е напишано во Анекс 2 од ЕУ Директивата ((EU) 2016/1148), или да се напише одредба во која ќе се определи дека министерот за МИОА ќе ги пропише во подзаконски акт.

Исто така, сметаме дека од примената на овој закон не треба целосно да се исклучуваат операторите на јавна електронска комуникациска мрежа определени со Законот за електронските комуникации и давателите на доверливи услуги определени со Законот за електронски документи, од причина што тие се даватели на суштински услуги на давателите на суштински услуги од другите сектори. Размената на информации во врска со инцидентите кај операторите на јавната електронска комуникациска мрежа и давателите на доверливи услуги ќе биде од полза за останатите сектори доколку постои ризик инцидентот да зафати други сектори или пошироко географско подрачје. Оттука, нашиот предлог е во насока на вклучување и на овие оператори и даватели на доверливи услуги во примена на законот во делот кој се однесува на обврските за рано предупредување, известувања, соопштенија и пренос на информации до засегнатите страни од ризиците и инцидентите.

3. Во однос на тимовите за одговор на компјутерски безбедносни инциденти (CSIRT) предлагаме тие, како посебни организациски единици да се формираат во рамките на Дигиталната агенција, а не како посебни организациски единици во различни надлежни органи како што е пропишано во членот 2 и членот 3 од нацрт Законот.

Имено воспоставувањето на националните CSIRT-ови од страна на државата е потребно заради воспоставување ефикасен систем на координирана одбрана од сајбер и хибридни закани кои подразбираат мултидимензионални активности во кои се користат конвенционални и неконвенционални методи на напад, кои можат да бидат од дипломатска, воена, економска или технолошка природа и во кои, како учесници можат да се јават државни или приватни актери кои користат различни методи на координиран напад за да постигнат специфични цели.

Исто така, видно од Анексот 1 (ANNEX I REQUIREMENTS AND TASKS OF COMPUTER SECURITY INCIDENT RESPONSE TEAMS (CSIRTs)) од ЕУ Директивата, барањата кои треба да ги исполнат CSIRT-овите подразбираат ангажирање на значителен обем на финансиски средства и човечки ресурси, што во случајот со МК сметаме дека ќе биде економски неоправдано наместо еден централно поставен, да се воспостават десетина посебни CSIRT-ови во рамки на повеќе “надлежни органи за секторите“. Од одредбите наведени во нацрт Законот, исто така, не е јасно кој треба да ги формира и финансира секторските CSIRT-ови. Понатаму, покрај обврската на земјите членки да осигураат дека CSIRT-овите имаат ангажирано адекватни ресурси за ефикасно справување со задачите, во членот 9 од ЕУ директивата е пропишана и обврска, дека земјите членки треба да осигураат дека CSIRT-овите имаат пристап до соодветна, безбедна и флексибилна комуникациска и информациска инфраструктура на национално ниво и дека државите можат да побараат помош на ENISA во развојот на националните CSIRT-ови. Оттука, сметаме дека е порационално со помош на ENISA да се развие еден соодветно опремен и екипиран CSIRT, во рамките на кој ќе се воспостават стручни тимови за поддршка на различните сектори кои нудат суштински услуги.

Во прилог кон овој предлог се и воспоставените CSIRT-ови од нашето опкружување, каде како пример ги земавме Албанија, Бугарија, Црна Гора, Хрватска и Словенија. Имено, во овие држави има воспоставено еден до два CSIRT-ови, сите на ниво на влада и/или на национално ниво:

|  |  |
| --- | --- |
| **Држава/Конституент** | **Број на конституенти** |
| **Albania** | **1** |
| Government |  |
| **Bulgaria** | **1** |
| Government |  |
| **Montenegro** | **1** |
| National |  |
| **Croatia** | **2** |
| Government |  |
| NREN, National research and education network), National |  |
| **Slovenia** | **2** |
| Government |  |
| NREN (National research and education network), National |  |

Извор:ENISA - CSIRTs by Country - Interactive Map, <https://www.enisa.europa.eu/topics/csirts-in-europe/csirt-inventory/certs-by-country-interactive-map>

Согласно погоре наведеното, предлагаме државата да обезбеди адекватни ресурси со цел ефикасно извршување на задачите од страна на CSIRT-овите, пристап на CSIRT-овите до флексибилна комуникациска и информациска инфраструктура на национално ниво и ресурси кои ќе бидат неопходни за задоволување на барањата што се дефинирани во точката 1 од Анексот 1 на ЕУ директивата.

4. Во однос на идентификувањето на операторите на суштински услуги, предлагаме тие да се идентификуваат однапред од страна на Владата на Република Северна Македонија, а не како што е одредено во нацрт Законот од страна на CSIRT-овите од причина што државата треба да определи кои се тие критични општествени или економски активности во државата кои зависат од оператори кои даваат одреден вид на услуга што зависи од мрежни и информациски системи и доколку настане инцидент, тој може да предизвика значителни подривачки ефекти врз обезбедувањето на услугата од страна на операторот. Поткрепа на овој наш предлог наоѓаме и во членот 5 од ЕУ Директивата, каде е пропишано дека земјите членки треба да извршат идентификување на операторите на суштински услуги, дека Групата за соработка на ЕУ ќе ги поддржува земјите-членки во процесот на идентификација на операторите на суштинските  услуги, дека земјите-членки треба да доставуваат извештаи до Комисијата со потребните информации за да и се овозможи на Комисијата да го процени спроведувањето на директивата, а особено конзистентноста на пристапите на земјите-членки во процесот на идентификација на операторите на суштинските услуги и дека заради идентификување на операторите на суштинските услуги, секоја земја членка треба да воспостави листа на услуги коишто се од суштинско значење за одржување на критични општествени и / или економски активности.

5. Во Нацрт Законот за безбедност на мрежи и информациски системи недостасуваат преодни и завршни одредби, во кои ќе се пропишат рокови за донесување на подзаконските акти, за усогласување со законот и за негова примена.