До:
МИНИСТЕРСТВО ЗА ИНФОРМАТИЧКИ
ТЕХНОЛОГИИ И АДМИНИСТРАЦИЈА
Бул. „Св.Кирил и Методиј" бр.54
1000, Скопје

Предмет: Коментари за јавната расправа по Предлог-Законот за безбедност на мрежни и информациски системи и дигитална трансформација

Почитувани,

А1 Македонија со внимание го разгледа Предлог - Законот за безбедност на мрежни и информациски системи и дигитална трансформација објавен за јавна расправа на порталот ЕНЕР.

Пред се, ја поздравуваме иницијативата за унапрадување на заштитата од нападите на безбедноста и интегритетот на комуникациските и информатичките мрежи и системи и согласни сме дека кибербезбедноста е веќе еден од главните приоритети во процесот на дигитализација на општеството. Исто така, ги поздравуваме амбициите на Владата и Министерството за информатичко општество и администрација за зголемувањето на обемот на дигитализацијата на јавните установи и сервиси и како еден од клучните субјекти на пазарот на електронски комуникациски мрежи и услуги, подготвени сме на предизвиците кои ќе произлезат од понатамошните активности за дигитализација.

Во однос на јавната расправа по Предлог-Законот би сакале да вложиме неколку коментари кои веруваме дека ќе придонесат кон квалитетот на законското решение.

1. Пред се, би сакале да посочиме на внимание во однос на намерата за формирање на Агенцијата за безбедност на мрежни и информациски системи и дигитална трансформација, како независно регулаторно тело. Имено, функциите за заштита на општата јавна безбедност се во рамки на организационите структури на Министерствата за внатрешни работи и одбрана и вклучувањето на Агенцијата за безбедност на мрежни и информациски системи и дигитална трансформација би било, од една страна, додавање на потполно нов субјект во јавната администрација и, од друга страна, вклучување на ново Министерство во чиј домен се вклучуваат прашања на безбедноста. Сметаме дека кон ова прашање треба да се пристапи со исклучително внимание со оглед на тоа што како финансиски, така и организациски, сериозно влијае на ефикасноста на справувањето со предизивиците на кибербезбедноста.
2. Во член 12 се наведени условите кои треба да ги исполнуваат кандидатите за членови на комисијата на Агенцијата. Имајќи ја предвид одговорноста на Агенцијата лицата кои се ангажирани во кибербезбедноста, за обезбедување на повисоки гаранции за успешност, сметаме дека не се доволни само основни квалификации на членовите на Комисијата, туку и подлабоки познавања и искуство во областа на кибербезбедноста и дигиталната трансформација. Заради тоа, предлагаме членовите што ги предлагаат Министерствата за информатичко општество и администрација, Министерството за

одбрана и Министерството за внатрешни работи, покрај завршен VII/1 степен од областа на информатичкитеи комуникациските технологии, да поседуваат и серификати за безбедност на информатички мрежи и да имаат работно искуство во управување со информатички мрежи од најмалку 5 години. Исто така, за членовите кои ги предлагаат Министерството за правда и Министерството за финансии, покрај завршен VII/1 степен од областа на економијата и правото, да бидат со минимум 15 годишно искуство на истакнати позиции во домен на економијата и правото.

3. Во член 59 се утврдува принципот на спроведување на надзор од страна на Агенцијата. Притоа, во првиот став наведени се правата на Агенцијата за наметнување на одредени мерки при спроведувањето на надзорот. Согласно добрите практики на владеење сметаме дека мерката за покренување на прекршочна постапка наведена во алинеја i) не би требало да биде вклучена во мерките кои се предвидени при надзор, туку само кога ќе се констатира дека субјектот не постапил по мерки за кои претходно бил задолжен. Во понатамошните ставови од членот веќе има услови за покренување на прекршочна постапка во случај на непочитување на задолженијата и обврските.

4. Во домен на казнените одредби, би сакале да посочиме на неосновано високите казни како и нерамноправноста во третманот на индустријата и јавите установи. Имено, во член 68 се предвидуваат неколку основи за наметнување на казни до 2% за суштински оператори и 1.4% за важни оператори да дела кои објективно не предизвикуваат сериозни безбедносни ризици, освен во одредени исклучоци. Во исто време, се предвидува и казна во износ од 30% од одмерената глоба за одговорно лице во операторот. Сметаме дека казните за овие основи не треба да бидат поврзани со големината на субјектот бидејќи нарушувањето на кибербезбедноста како резултат на делата наведени во членот има ист степен на сериозност доколку е предизвикана од било кој субјект, без разлика дали е тоа субјект со големи или мали приходи, или е од јавниот или приватниот сектор. Во истиот член, се предвидува дека казната за одговорното лице во приватен субјект е 30% од одмерената глоба, а за функционерот кој раководи со органот на државната управа или со правното лице на кое со закон му е доверено да врши јавни овластувања на државно ниво е 1000 евра во противредност. Во услови кога имаме економски субјекти кои остваруваат годишни приходи на ниво од 100М евра годишно и повеќе, максималната казна која може да биде изречена за одговорното лице би била 660 илјади евра и повеќе, а во исто време, за ист престап функционер би бил одговорен само со 1000 евра.

   Предлагаме да се направи темелно преиспитување на казнените одредби и да се определат казни кои би имале соодветна ефикасност во превенцијата од прекршоци, но во исто време би биле споредливи со други области во економијата. Исто така, функционерите и одговорните лица на правните субјекти треба да имаат ист третман во однос на одговорноста за кибербезбедност.

А1 Македонија ви стои на располагање за евентуални понатамошни консултации во процесот на донесување на Законот.

Со почит,

А1 Македонија ДООЕЛ Скопје

Друштво за комуникациски услуги А1 Македонија ДООЕЛ Скопје, Плоштад Пресвета Богородица бр.1, 1000 Скопје,
Република Северна Македонија, ЕМБС: 7068310, Тел: +389 2 3100077, Факс: +389 2 3110077, e-mail: info@A1.mk