**Коментари на Македонски Телеком АД Скопје по**

**предлог ЗАКОН ЗА БЕЗБЕДНОСТ НА МРЕЖНИ И ИНФОРМАЦИСКИ СИСТЕМИ И ДИГИТАЛНА ТРАНСФОРМАЦИЈА**

|  |  |  |
| --- | --- | --- |
| **Цели****Член 2** | Цели на овој закон се обезбедување на:   1. високо ниво на сајбер безбедност со цел заштита и понатамошен развој на општеството, 2. градење и проширување на ИТ инфраструктурата, односно поефикасна и поефективна дигитална трансформација на јавниот сектор, 3. повисок степен на отвореност со цел да се обезбеди развој на иновативни софтверски решенија, 4. обуки за сајбер безбедност и дигитални вештини за вработените во јавниот сектор и граѓаните на Република Северна Македонија | Во целите на овој закон акцентот е поставен на јавниот сектор и генерално општеството и граѓаните. Понатамошното вклучувањето на индустриите кои припаѓаат на приватниот сектор во понатамошните членови од законот се чини дека излегува од делокругот на овие цели. |
| **Дефиниции**  **Член 3** | “Oператори на суштински услуги”  “Oператори на важни услуги’’ | Во законот за првпат се воведуваат ново карактизирање на правните лица како ’’оператори на суштински услуги” и “оператори на важни услуги’’ без да се обебеди дефиниција за тоа што се подразбира под овие категории.  Со оглед дека овие називи и групи не се познати потребно е нивно дефинирање и прецизирање.  Освен овие дефиниции потребно е законодавецот да предвиди и дефиниции за одредени градации со цел обврските на субјектите да бидат конкретни и јасни. Така ревидираната ЕУ директива ги класифицира субјектите кои работат во секторите опфатени со NIS2 во две категории: суштински и важни. Оваа поделба се заснова на критичност на субјектите од аспект на сајбер безбедност кои работат во опфатените сектори, како и степенот на зависност од други сектори или услуги на специфичниот сектор.  По правило, сите средни и големи субјекти ќе мора да се усогласат со безбедносните правила за управување со ризик и известување на NIS2 директивата. Сепак, директивата ја прилагодува класификацијата на суштински и важни ентитети врз основа на нивната големина.  Средно големите и големите субјекти би се дефинирале според бројот на вработени и нивниот годишен обрт по препораката на ЕУ Комисијата 2003/361/ЕC.   |  |  |  | | --- | --- | --- | | **Големина на компаниите** | **Број на вработени** | **Годишен обрт** | | Средно големи | Помеѓу 50 and 250 | Помеѓу €10m до €50m | | Големи | Повеќе од 250 | Повеќе од €50m |   Само ентитети со големи димензии активни во секторите опфатени со Анекс I од директивата, како што се управувани давателите на услуги (MSPs) или давателите на услуги во облак (CSPs) се класифицираат како суштински ентитети.  Исклучок е направен за телекомуникацискиот сектор, телекомуникациските оператори со средна големина, исто така, се сметаат за суштински субјекти.  Без оглед на нивната големина, субјектите класифицирани во согласност со eIDAS регулацијата (Regulation on electronic identification and trust services for electronic transactions in the internal market), на TLD (Top-Level Domains) регистрите на имиња и на давателите на услуги на DNS (Domain name system), подеднакво ќе се класифицираат како суштински ентитети.  Субјекти со средна големина опфатени во Анекс I, како и големите и средно големите субјекти опфатени во анекс II од директивата (на пр. онлајн услуги и пребарувачи) се класифицираат како важни субјекти.  NIS2 директивата им овозможува на државите да го рекласифицираат секој ентитет опфатен во анекс I и II како суштински, по национална проценка на ризикот и врз основа на збир на критериуми наведени во директивата. Таков би бил случајот доколку нарушување на услугата обезбедена од одреден субјект има значително влијание врз јавната безбедност. |
|  | 6) „инцидент“ е настан што ја загрозува достапноста, веродостојноста, интегритетот или доверливоста на складираните, пренесените или обработените податоци или на услугите што ги нудат или до кои може да се пристапи преку мрежните и информациските системи; | Низ текстот постои терминот “сајбер безбедносни инциденти” додека во делот дефиниции освен општо појаснување на инцидент нема јасно појаснување за овој термин. Доколку точка 6 е за сајбер инциденти или да се преформулира или терминолошки се појасни со нова точка затоа што во точка 7 има дефиниција за “сајбер безбедносни инциденти” од големи размери.  Сметаме дека треба да се даде јасна дефиниција на поимот инцидент, притоа да се има предвид разликата меѓу инцидент и безбедносен инцидент.  Дополнително, потребно е да се дефинираат јасни прагови за одредување на големината/значајноста на инцидентот, на пример во член 34. |
| **Член 28**  **Оператори на суштински услуги и оператори на важни услуги** | (5) Агенцијата води Регистар на оператори на суштински услуги и оператори на важни услуги согласно ставот (3) на овој член. Регистарот не е јавно достапен и истиот редовно се ажурира. | Сметаме дека регистарот на оператори на суштински услуги и оператори на важни услуги треба да биде јавно достапен. Ова од причина што доколку субјектите од тој регистар имаат потреба од соработка со некој друг субјект потребно да се знае кои се неговите се обврски и статус. |
| **Член 28**  **Оператори на суштински услуги и оператори на важни услуги** | (10) Пред да го донесе подзаконскиот акт од ставот (8) на овој член Агенцијата е должна да да се консултира со субјектите од ставот (3) на овој член и да ги земе предвид нивните мислења и забелешки | Предлагаме наместо општата предложена одредба да се вметне попрецизна одредба како што следи:  (10) Пред да го донесе подзаконскиот акт од ставот (8) на овој член Агенцијата е должна да објави јавна расправа за период не пократок од 30 дена, за да можат сите сите заинтересирани субјекти да ги достават своите коментари. Сите пристигнати коментари треба да бидат објавени на веб страната на агенцијата. Стручните служби на Агенцијата треба да се произнесат по доставените коментари со напомена дали се прифатени и образложение доколку не се прифатени. |
| **Член 39**  **Задачи на MKD-CSIRT** | 1. MKD-CSIRT може да спроведува проактивно неинтрузивно скенирање на јавно достапни мрежни и информациски системи на операторите на суштински услуги и операторите на важни услуги. Скенирањето се врши со цел да се откријат ранливи или несигурно конфигурирани мрежни и информациски системи и како би се информирале засегнатите субјекти. Ваквото скенирање не треба да има негативно влијание врз функционирањето на услугите кои ги обезбедува операторот | Сметаме дека скенирањето на јавно достапни мрежни и информациски системи на операторите на суштински услуги и операторите на важни услуги треба да се прави со претходна навремена најава (информација ) до операторот. |
| **Член 43**  **Обврски за известување** | (4) Со цел исполнување на обврските од ставовите (1) и (2) на овој член, операторите на суштински услуги и операторите на важни услуги се должни на MKD-CSIRT, да ѝдостават:  a. во рок од 24 часа од дознавањето за значителниот инцидент, рано предупредување во коешто доколку е соодветно, ќе се наведе дали постои сомневање дека значителниот инцидент е предизвикан од незаконско или злонамерно дејствување или може да има прекугранично влијание; | Во теоријата и пракса постојат пријави по инциденти и инциденти по кои е потребно да се постапи и истражи во рок поголем од 24 часа за да се направи дистинкција дали се работи за инцидент или не. Роковите и према други државни органи се подолги од 24 часа на пример 72 часа кон АЗЛП. Од таа причина 24 часа е многу краток рок, независно од препораките во NIS2 директивата, националната регулатива треба да ги земе во предвид и локалните специфичности.  Истиот коментар важи и за став 5 од истиот член. |
|  | (7) Доколку значителниот инцидент се однесува на повеќе држави, единствената точка за контакт, односно Агенцијата, е должна без непотребно одложување да ги извести засегнатите држави и да им ги достави оние информации што се примени согласно ставот (4) на овој член, притоа, водејќи сметка за заштита на безбедноста и комерцијалните интереси на операторот на суштински услуги или на операторот на важни услуги, како и за доверливоста на доставените информации. | Во текстот на предлог Законот во неколку наврати се споменува “значителен инцидент” но нема дефиниција за тоа во законот. И покрај тоа што се наведува дека ќе биде дефинирано во подзаконскиот акт, сметаме дека е потребно да се дефинира значителен инцидент и да се направи градација за да се разграничува значителен од незначителен и сл...Овие градации и категоризации се посебно важни во процесите на дефинирање на мерки за управување со сајбер безбедносни ризици согласно член 42. |
| **Член 45** | (1) Со цел да се докаже усогласеноста со одредени обврски од членот 42 од овој закон, Агенцијата може да бара од операторите на суштински услуги или од операторите на важни услуги користење на одредени ИКТ-услуги, ИКТ-системи и ИКТ-производи кои ги развил самиот оператор или се набавени од трета страна кои се сертифицирани врз основа на европски програми за сајбер безбедносна сертификација. | Сметаме дека за ИКТ производи кои ги развил самиот оператор нема потреба од сертификација ако операторот ги почитува обврските од овој закон и европските и меѓународни стандарди и технички спецификации за безбедност на мрежни и информациски системи, што се утврдува со редовните надзори од страна на агенцијата.  Примена на европски програми за сајбер безбедносна сертификација како што е наведено во член 45 од овој закон може да има за одредени ИКТ продукти кои треба да се дефинираат прецизно во подзаконските акти. |
| **Член 46**  **Стандардизација** | (2) Агенцијата со релевантните засегнати страни изготвува совети и упатства во однос на техничките области од ставот (1) на овој член, како и во однос на веќе постојните меѓународни и национални стандарди. | Пред да го упатствата од став 2 на овој член Агенцијата е должна да објави јавна расправа за период не пократок од 30 дена, за да можат сите сите заинтересирани субјекти да ги достават своите коментари. Сите пристигнати коментари треба да бидат објавени на веб страната на агенцијата. Стручните служби на агенцијата треба да се произнесат по доставените коментари со напомена дали се прифатени и образложение доколку не се прифатени. |
| **Член 59**  **Мерки кај операторите на суштински услуги** |  | Сметаме дека точката а. од член 59 треба да се измени на следниот начин:  а. Доколку Агенцијата при вршење на надзор утврди дека оператор при своето работење не е усогласен со еден или повеќе од условите утврдени со овој закон, прописите донесени врз основа на него, обврските наметнати од страна на Агенцијата, таа за тоа писмено ќе го извести операторот и ќе му даде рок не пократок од 3 месеци од денот на приемот на писменото известување да ја отстрани утврдената неусогласеност. Ваквиот рок е потребен бидејќи усогласувањето со одредбите од овој закон може да подразбира јавна набавка, објавување на тендер и оперативна работа за кој е потребно поголем временски период.  Доколку операторот не постапи по обврските од став а) агенцијата може да преземе и други мерки кои точно треба да се дефинираат во кој случај која мерка ќе се примени. Покренување на прекршочна постaпка пред надлежен суд од став i) сметаме дека треба да се избрише. |
| **Член 68 Прекршоци** | (1) Глоба во износ од 2% од вкупниот годишен приход на операторот на суштински услуги, односно глоба во износ од 1,4% од вкупниот годишен приход на операторот на важни услуги (изразена во апсолутен износ) остварен во деловната година што и претходи на годината кога е сторен прекршокот или од вкупниот приход остварен за пократок период од годината што му претходи на прекршокот, доколку во таа година операторот на суштински услуги, односно операторот на важни услуги започнал да работи, ќе му се изрече за прекршок на операторот на суштински услуги со исклучок на органите на државната управа и правнитене лица на кои со закон им е доверено да вршат јавни овластувања на државно ниво, како и на операторот на важни услуги ако: | Оваа одредба не е во согласност со NIS 2 директивата каде нема вакви ригорозни глоби односно глоби со фиксен износ, туку во зависност од тежината на прекршокот глобата може да биде и помала од **2%** односно **1,4%.**  Предлагаме глобата да се определува во износ **до 2%** од вкупниот годишен приход на операторот на суштински услуги, односно глоба во износ **до 1,4%** од вкупниот годишен приход на операторот на важни услуги (изразена во апсолутен износ) остварен во деловната година што и претходи на годината кога е сторен прекршокот.  Дополнително треба да се усогласат глобите во овој предлог закон со глобите во Законот за електронски комуникации кои се однесуваат на неисполнување на обврските за безбедност и интегритет на електронски комуникациски мрежи и услуги. |
| **Член 76** | Комисијата на Агенцијата ќе ги усвои подзаконските акти кои произлегуваат од овој Закон, во рок од девет месеци од денот на влегување во сила на овој закон | Сметаме дека треба да се има во предвид дека NIS2 директивата ќе стапи на сила на 18 октомври 2024 година а до тогаш треба да се усвои и да стапи на сила и Draft EU Cyber Resilience Act (CRA), кој моментално е во фаза на усвојување на забелешки (преговири ) на EU Commission со European Parliament (EP) и Council of the EU. Во CRA се предвидува и преоден период за имплементација на одредбите од актот од најмалку 18 месеци од стапување на сила, а според European Commission предлогот е 2 години.  Во преодните одредби на овој закон сметаме дека треба да се имаат во предвид и роковите за имплементација на одредбите од NIS2 директивата и Draft EU Cyber Resilience Act (CRA), за да не дојдеме во ситуација Македонија да ја транспонира NIS2 директивата и придружните акти пред да се донесат и применат од земјите членки на Унијата. |
| **Член 77** | Законот за електронски документи, електронска идентификација и доверливи услуги, Законот за електронски услуги и електронско управување и Законот за централен регистар на население ќе се усогласат со одредбите од овој закон во рок од две години од денот на влегување во сила на овој закон | Потребно е и во овој член да се напомене дека ќе се направи усогласување и со Законот за електронски комуникации поради тоа што надлежностите на MKD-CIRT се дефинирани во овој закон, како и усогласување со другите членови од ЗЕК кои се однесуваат на безбедност и интегритет на електронски комуникациски мрежи и услуги.  Услогласување со Законот за електронски комуникации е потребно и тоа со членовите 166-а, 166-б, 166-г, 166-д кои се однесуваат на безбедно управување, работа и мониторирање на електронските комуникациски мрежи кај операторите односно обврските од Законот за електронски комуникации се повторуваат во предлог Закон за безбедност на мрежни и информациски системи и дигитална трансформација. Истото важи и за прекршочните одредби од ЗЕК кои се однесуваат на членовите 166 -д каде глобата за неисполнување на обврските е 7-10% од вкупниот бруто приход. За да избегнеме двојна регулација предлагаме пред да стапи на сила овој закон да се направат измени на ЗЕК. |