АНАЛИЗА ЕФЕКАТА ЗАКОНА О ИЗМЕНАМА И ДОПУНАМА ЗАКОНА О ИНФОРМАЦИОНОЈ БЕЗБЕДНОСТИ

1) Који показатељи се прате у области, који су разлози због којих се ови показатељи прате и које су њихове вредности?

У области информационе безбедности показатељи који се прате односе се на:

- примену мера од безбедносних ризика у информационо-комуникационим системима и
- инциденте који значајно угрожавају информациону безбедност, а којима су изложени ИКТ системе под посебног значаја.

Наиме, Законом и информационој безбедности („Службени гласник РС“ бр. 6/16 и 94/17) (у даљем тексту: Закон) дефинисани су оператори ИКТ система од посебног значаја, као и мере заштите, односно техничке и организационе мере које су оператори ИКТ системи од посебног значаја у обавези да примењују, а у циљу одржавања адекватног нивоа безбедности система.

Сходно томе, оператори ИКТ система од посебног значаја дужни су да донесу акт о безбедности ИКТ система и дефинишу мере заштите, а нарочито принципе, начин и процедуре постизања и одржавања адекватног нивоа безбедности система, као и овлашћења и одговорности у вези са безбедношћу и ресурсима ИКТ система од посебног значаја.

Инспекцијским надзором над радом оператора ИКТ система од посебног значаја утврђује се да ли су оператори донели акт о безбедности и применили мере заштите, односно да ли је успостављен адекватан ниво безбедности система. Инспекцијски надзор до сада није вршен, будући да је први инспектор у новоформираној инспекцији за информациону безбедност запослен у другој половини 2018. године и, сходно томе, инспекцијски надзор се спроводи од 2019. године.

Оператори ИКТ система од посебног значаја у складу са Законом обавезни су да обавесте Надлежни орган, односно Министарство трговине, туризма и телекомуникација о инцидентима у ИКТ системима који могу да имају значајан утицај на нарушавање информационе безбедности.

На основу пријављених инцидената Национални центар за превенцију безбедносних ризика у ИКТ системима (у даљем тексту: Национални ЦЕРТ) реагује по пријављеним или на други начин откривеним инцидентима, тако што пружа савете на основу расположивих информација лицима која су погођена инцидентом и предузима друге потребне мере из своје надлежности на основу добијених сазнања. Национални ЦЕРТ на основу пријављених инцидената прати трендове у овој области и континуирано израђује анализе ризика и инцидената. Према извештајима Националног ЦЕРТ-а у 2017. години пријављено је 17 инцидената који значајно угрожавају информациону безбедност, а у 2018. години укупно 31 инцидент.

2) Да ли су уочени проблеми у области и на кога се они односе? Представити узроке и последице проблема.

Чланом 6. Закона дефинисани су ИКТ системи од посебног значаја и подељени су у три групе и то:

1) ИКТ системи који се користе у обављању послова у органима јавне власти;

2) ИКТ системи који се користе за обраду података који се, у складу са законом који уређује заштиту података о личности, сматрају нарочито осетљивим подацима о личности;

3) ИКТ системи који се користе у обављању делатности од општег интереса.

Међутим, током имплементације Закона утврђено је да наведеном дефиницијом обухваћен велики број органа јавне власти, чији системи по свом значају не спадају у ИКТ системе од посебног значаја. Будући да примена мера заштите подразумева примену техничких и организационих мера, за чију примену су потребна финансијска улагања, ови системи су били у обавези да своје системе унапреде, односно примене мере заштите, међутим, предложеном изменом Закона, предвиђено је смањење броја ИКТ системе који се користе у органима јавне власти, јер је утврђено да ти системи нису од посебног значаја за информациону безбедност у Републици Србији.

Током имплементације Закона утврђено је да ИКТ системи од посебног значаја не достављају информације о инцидентима који значајно угрожавају информациону безбедност, иако су обавезни да то чине. Услед тога Национални ЦЕРТ није у могућности да прати трендове у овој области, нити да израђује анализе ризика и инцидената на основу којих би се пружали савети и предлагале мере за отклањања потенцијалних инцидената.

У складу са Законом предвиђено је оснивање Националног ЦЕРТ, међутим, иако је Национални ЦЕРТ основан, потребно је и даље улагати у његове капацитете у смислу техничких, организационих и људских капацитета. Наиме, како би Национални ЦЕРТ био у могућности да пружа адекватну подршку ИКТ системима од посебног значаја у случају инцидената који значајно угрожавају информациону безбедност постојећи ресурси нису довољни, јер поред опреме, неопходно је да се Национални ЦЕРТ оснажи и запосли стручњаке у овој области. У супротном, може се наставити тренд непријављивања инцидената у ИКТ системима од посебног значаја, услед чега није могуће пратити кретања у овој области, нити предлагати мере за њено унапређење.

Како је у складу са Законом предвиђен рад како Националног ЦЕРТ, тако и ЦЕРТа републичких органа и ЦЕРТова самосталних оператора ИКТ система, у претходном периоду је констатовано да не постоји законски основ за њихову системску сарадњу која би омогућавала размену информација и међусобно пружање подршке у случају инцидената који значајно угрожавају информациону безбедност.

3) Која промена се предлаже и да ли је промена заиста неопходна и у ком обиму?

Измене Закона су инициране из разлога што је Закон ступио на снагу пре усвајања Директиве ЕУ о мерама за висок ниво безбедности мрежних и информационих система у Европској унији број 2016/1148 (у даљем тексту: НИС директива), која је усвојена у јулу 2016. године. Иако је био донет пре усвајања НИС директиве, Закон је у великој мери усклађен са овом директивом, будући да садржи решења која одговарају одредбама наведене директиве.

Међутим, изради Нацрта закона о изменама и допунама Закона о информационој безбедности (у даљем тексту: Нацрт закона) приступило се првенствено из два разлога: први је преостало усклађивање са одредбама НИС директиве ради постизања потпуне усаглашености Закона, а други је унапређење постојећих законодавних решења на бази потреба утврђених на основу досадашње примене.

Ради преосталих усклађивања са НИС директивом, у Нацрту закона извршене су следеће измене и допуне:

- допуна области у којима се користе ИКТ системи од посебног значаја, и то област дигиталне инфраструктуре и услуга информационог друштва (члан 6.);
- одређено је да се пре јавног објављивања обавештења о инциденту од стране надлежног органа изврше претходне консултације са оператором ИКТ система од посебног значаја који је доставио обавештење о инциденту (члан 11.);
- предвиђена је допуна одредаба о Националном ЦЕРТ-у које се односе на његову надлежност и потребне капацитете (члан 15.).

Током примене закона утврђена је потреба за изменом и допуном одређених норми, у циљу ефикаснијег спровођења закона у пракси. Сходно томе, Нацртом закона предвиђено је следеће:

- укључивање Народне банке Србије у рад Тела за координацију послова информационе безбедности (члан 5.);
- допуна области у којима се користе ИКТ системи од посебног значаја (производња и снабдевање хемикалијама, члан 6.);
- таксативно су набројане обавезе ИКТ система од посебног значаја (члан 6а);
- успостављање Евиденције оператора ИКТ система од посебног значаја (члан 6б);
- дефинисан је начин обавештавања о инцидентима који значајно угрожавају информациону безбедност преко портала Надлежног органа или Националног ЦЕРТ-а у јединствени систем за пријем обавештења о инцидентима (члан 11.);
- обавеза Народне банке Србије и РАТЕЛ-а да добијена обавештења о инциденту проследе Надлежном органу (члан 11.);
- достављање обавештења о инциденту који је повезан са значајним нарушавањем информационе безбедности, које има или може имати за последицу угрожавање националне безбедности, Безбедносно-информативној агенцији (члан 11.);
- дефинисани су инциденти који треба да се пријаве, а који могу да имају значајан утицај на нарушавање информационе безбедности (члан 11а);
- одређена је обавеза ИКТ система од посебног значаја да достављају статистичке податке о инцидентима који могу да имају значајан утицај на нарушавање информационе безбедности (члан 11б);
- дефинисана је сарадња ЦЕРТ-ова у Републици Србији (члан 15а);
- додате су одредбе о заштити при коришћењу информационо-комуникационих технологија (члан 19а).

Наведене измене закона допринеће бољој повезаности свих релевантних актера у области информационе безбедности, будући да се Нацртом закона предвиђа успостављање евиденције ИКТ система од посебног значаја. На тај начин Надлежни орган и Национални ЦЕРТ имаће могућност интензивније сарадње са свим операторима ИКТ система од посебног значаја, нарочито у случају када се дешава инцидент, али у смислу пружања подршке, препоруке и савета за заштиту ИКТ система од посебног значаја.

Значајно унапређење лежи и у чињеници да је Надлежни орган успоставио Јединствени систем за пријем обавештења о инцидентима, тако да их ИКТ системи од посебног значаја обавештења могу прослеђивати преко портала Надлежног органа и Националног ЦЕРТ-а. Ово решење доприноси ефикасности пријављивања инцидената, као и потпуној информисаности свих релевантних учесника (Надлежни орган, Национални ЦЕРТ) који потом могу да учествују у отклањању инцидента.

Такође, Нацрт закона предвиђа одредбе о Националном ЦЕРТ-у које се односе на јачање капацитета Националног ЦЕРТ-а, како би се успоставило благовремена и ефикасна подршка у случају инцидента, а за такву врсту подршке неопходно је стручно особље, одговарајућа инфраструктура у смислу опреме и просторија за рад, чије обезбеђивање је предвиђено Нацртом закона. Како Национални ЦЕРТ има и улогу превенције у области информационе безбедности, предвиђено је достављање статистичких података од стране ИКТ система од посебног значаја на бази којих ће Национални ЦЕРТ имати могућност израде адекватних анализа у области информационе безбедности и на основу чега ће припремати препоруке и савете за мере заштите у овој области.

С обзиром да је препозната потреба за континуираном сарадњом ЦЕРТ-ова у Републици Србији, предвиђене су одредбе којима се дефинише ова сарадња кроз организацију редовних заједничких састанака, а посебно у случају инцидената који значајно угрожавају информациону безбедност у Републици Србији.

Имајући у виду важност питања безбедности на интернету, Нацртом закона дефинисане су одредбе којима се предвиђају мере за безбедност и заштиту на интернету, као и генерално приликом коришћења информационо-комуникационих технологија.

4) На које циљне групе ће утицати предложена промена? Утврдити и представити циљне групе на које ће промена имати непосредан односно посредан утицај.

Измене и допуне Закона имаће непосредан утицај на:

- ИКТ системе од посебног значаја;
- Национални ЦЕРТ;
- нове ИКТ системе од посебног значаја у област дигиталне инфраструктуре и услуга информационог друштва
- ЦЕРТове самосталних оператора ИКТ система.

5) Због чега је неопходно постићи жељену промену на нивоу друштва? (одговором на ово питање дефинише се општи циљ).

Измене и допуне Закона су неопходне првенствено ради потпуног усклађивања са НИС директивом, а потом ради боље повезаности свих релевантних актера у области информационе безбедности, чиме се доприноси адекватнијем нивоу безбедности информационих система од посебног значаја у Републици Србији.

6) Шта се предметном променом жели постићи? (одговором на ово питање дефинишу се посебни циљеви, чије постизање треба да доводе до остварења општег циља. У односу на посебне циљеве, формулишу се мере за њихово постизање).

Изменама и допунама Закона постиже се успостављање евиденције о ИКТ системима од посебног значаја, што ће допринети бољој комуникацији између Министарства и Националног ЦЕРТа са једне стране и ИКТ система од посебног значаја са друге стране.

Такође се предвиђа јачање капацитета Националног ЦЕРТа и то технолошких, људских и организационих капацитета, што ће Националном ЦЕРТу омогућити прелазак са информативне и саветодавне улоге на оперативнију улогу. Пружајући адекватнију помоћ ИКТ системима од посебног значаја у случају пријављених инцидената, поспешиће се међусобна сарадња и створити поверење што ће последично довести до тога да ИКТ системи од посебног значаја пријављују инциденте у складу са Законом.

Обавезивањем ИКТ система од посебног значаја да достављају статистичке податке о свим инцидентима који се дешавају у њиховим системима, Национални ЦЕРТ ће бити у могућности да прати трендове у овој области и припрема анализе ризика и инцидената на основу којих би се пружали савети и предлагале мере за отклањање потенцијалних инцидената.

Предвиђена сарадња између ЦЕРТова у Републици Србији омогућиће размену информација и међусобно пружање подршке у случају инцидената који значајно угрожавају информациону безбедност.

7) Да ли су општи и посебни циљеви усклађени са важећим документима јавних политика и постојећим правним оквиром, а пре свега са приоритетним циљевима Владе?

Стратегијом развоја информационе безбедности у Републици Србији за период од 2017. до 2020. године („Службени гласник РС“ број 53/17) неки од предвиђених приоритетних области информационе безбедности у складу су са општим и посебним циљевима који се постижу изменама и допунама Закона, и то:

- безбедност информационо-комуникационих система, што се односи на ризике нарушавања функционисања органа власти, привреде и организација као последица инцидената у информационо-комуникационим системима и
- информациона безбедност Републике Србије, што се односи на ризике нарушавања националне безбедности путем информационо-комуникационих система.

8) На основу којих показатеља учинка ће бити могуће утврдити да ли је дошло до остваривања општих односно посебних циљева?

Основни показатељи учинка измена и допуна Закона огледају се у следећем:

- успостављена евиденција ИКТ система од посебног значаја
- успостављен систем доставе статистичких података од стране ИКТ система од посебног значаја
- успостављена сарадња између ЦЕРТова у Републици Србији.

9) Да ли је финансијске ресурсе за спровођење изабране опције потребно обезбедити у буџету, или из других извора финансирања и којих?

Средства потребна за реализацију обавеза из Нацрта закона није потребно обезбедити у буџету, будући да ће иста бити обезбеђена из средстава РАТЕЛа, за потребе подизања капацитета Националног ЦЕРТа.

10) Колики су процењени трошкови увођења промена који проистичу из спровођења изабране опције (оснивање нових институција, реструктурирање постојећих институција и обука државних службеника) исказани у категоријама капиталних трошкова, текућих трошкова и зарада и да ли је могуће финансирати расходе изабране опције кроз редистрибуцију постојећих средстава?

Будући да је НИС директивом предвиђено повећавање капацитета Националног ЦЕРТа у наредном периоду предвиђа се повећавање броја запослених као и куповина неопходне опреме. У том смислу трошкови повећања капацитета Националног ЦЕРТа би били следећи:

- 150.000 евра за набавку платформе за увежбавање сајбер напада ради промовисања информационе безбедности;
- 10.000 евра у периоду од три године за набавку форензичке лабораторије;
- 20.000 евра у периоду од три године за набавку софтвер за сајбер безбедност и пратеће лиценце;
- 15.000 евра у периоду од три године за набавку хардвера;
- 144.000 евра у периоду од три године дана износ зараде за 5 новозапослених (5 х запослених х 800 евра х 3 године);
- 90.000 евра у периоду од три године за обуке за запослене (10 запослених х 3.000 евра х 3 године)

11) Које трошкове и користи (материјалне и нематеријалне) ће изабрана опција проузроковати привреди, појединој грани, односно одређеној категорији привредних субјеката?

Нови ИКТ системи од посебног значаја у области дигиталне инфраструктуре и услуга информационог друштва који су предвиђени изменама и допунама Закона су у

обавези да примене мере заштите, односно техничке и организационе мере у циљу успостављања адекватног нивоа безбедности система.

Уколико су ти привредни субјекти већ успоставили систем управљања информационом безбедношћу у складу са међународним стандардима и добром праксом у овој области, не очекује се да примена закона изазове значајне трошкове. Међутим, привредни субјекти који представљају операторе ИКТ система од посебног значаја у складу са изменама Закона, а који до сада нису успоставили одговарајући систем управљања информационом безбедношћу имаће одређене трошкове за испуњење законских обавеза који се огледају у евентуалном додатном технолошком опремању, обуци запослених, ангажовању нових стручњака и слично. Прецизни износи додатних трошкова за наведене субјекте варирају у великом распону, будући да исти зависе од више фактора који могу да буду веома различити у различитим привредним субјектима. Наиме, колико ће финансијских средстава за примену закона издвојити ови привредни субјекти зависи од њихове величине, односно броја запослених, технолошке опремљености (поседовање рачунарске опреме, информационог система), обучености запослених за коришћење информационих технологија у домену информационе безбедности, и других фактора од којих функционисање информационе безбедности зависи у једном привредном субјекту. Сходно наведеном, није могуће дати ни тачне, ни оквирне износе по привредном субјекту.

12) Да ли је за спровођење изабране опције обезбеђена подршка свих кључних заинтересованих страна и циљних група? Да ли је спровођење изабране опције приоритет за доносиоце одлука у наредном периоду (Народну скупштину, Владу, државне органе и слично)?

Министарство трговине, туризма и телекомуникација је у 2018. години формирало радну групу за израду Нацрта закона о изменама и допунама Закона о информационој безбедности кога су чинили представници релевантних министарстава и институција.

Министарство трговине, туризма и телекомуникација спровело је јавну расправу о Нацрту закона о изменама и допунама Закона о информационој безбедности у периоду од 04. до 25. фебруара 2019. године, на основу закључка Одбора за привреду и финансије Владе 05 Број: 011-882/2019 од 31. јануара 2019. године. Нацрт закона је објављен на сајту Министарства трговине, туризма и телекомуникација www.mtt.gov.rs и порталу еУправа www.euprava.gov.rs. У оквиру јавне расправе, одржан је округли сто у Привредној комори Србије 20. фебруара 2019. године, који је био веома успешан и посећен. У јавној расправи учествовали су представници државних органа, привредног сектора, академске заједнице, невладиних организација и еминентни стручњаци у овој области. Министарство је по окончању јавне расправе путем Министарства за европске интеграције упутило Нацрт закона Европској комисији, ради давања мишљења.

Доношење Нацрта закона је приоритет имајући у виду чињеницу да се истим врши усклађивање са европском регулативом, односно НИС директивом.

13) Да ли су обезбеђена финансијска средства за спровођење изабране опције? Да ли је за спровођење изабране опције обезбеђено довољно времена за спровођење поступка јавне набавке уколико је она потребна?

Средства за реализацију законских обавеза обезбеђује РАТЕЛ, као организација у чијем се саставу налази Национални ЦЕРТ. Очекује се да ће у буџету наведене институције почев од 2020 године бити обезбеђена средства потребна за додатно запошљавање као и за куповину неопходне опреме.