Фондација „Регистар националног интернет домена Србије“
Жоржа Клемансоа 18а/I, Београд, Србија
ПАК 101147 | телефон: 011.7281.281
kancelarija@rnids.rs
rnids.rs | рнидс.срб

Министарство трговине, туризма и телекомуникација
Париска 7, 11000 Београд

– г-дин Милан Војводић –

ПРЕДМЕТ: Коментари на нацрт Закона о информационој безбедности

Поштовани господине Војводићу,

Фондација „Регистар националног интернет домена Србије” поздравља намеру Министарства трговине, туризма и телекомуникација да унапреди ниво информационе безбедности у Србији, путем Закона о информационој безбедности.

Полазећи од заједничког интереса и одговорности за стабилно и поуздано функционисање националне информационе инфраструктуре, као и за стварање услова за њен даљи развој, шаљемо Вам наше коментаре на нацрт закона, за које верујемо да могу допринети његовој бољој практичној примени.

Коментари су дати у прилогу овог дописа, на вашем обрасцу.

Захваљујемо Вам на могућности да учествујемо у јавној расправи и стојимо Вам на располагању за све додатне информације и будућу сарадњу у примени закона.

У Београду,
23. јула 2015.

Душан Стојичевић
председник Управног одбора
dusan.stojicevic@rnids.rs

Име и презиме: Душан Стојичевић

Име организације и институције (ако постоји): Фондација „Регистар националног интернет домена Србије" (РНИДС)

Контакт телефон: 064-1452-171

Е-пошта: dusan.stojicevic@rnids.rs

Датум: 22. 7. 2015.

1. Општи коментари и сугестије у односу на Нацрт закона као целину

1. Врсте критичне инфраструктуре требало би да буду дефинисане у самом закону, како би били јасни опсег надлежности, обавезе, дубина заштите и реакције на инциденте законом формираних тела.
2. Нису испраћене смернице ENISA.
3. Законом је предвиђено доношење великог броја подзаконских аката, па би у тај посао требало укључити, осим надлежног министарства и Тело за координацију.

2. Конкретан део Нацрта закона чију измену предлажете и Ваш предлог за измену

Члан 1. – После речи „системима" додати запету и речи „управљање безбедносним инцидентима".

Члан 2. – *Тачка 1:* уместо „може бити" треба „јесте"; такође, дефиницију треба допунити тако да покрива cloud системе и виртуелне приватне мреже. *Тач. 3-8, 18, 20*: уместо „података" треба „података и информација". *Тачка 9:* брисати све после прве запете. *Тачка 24:* ова дефиниција не би требало да буде дата кроз набрајање примера, већ би требало једнозначно да опише појам (нпр. „информациона добра су производи чија се вредност базира на информационом садржају" и сл.). Треба додати нову тачку у којој би био дефинисан појам „CERT".

Члан 3. – *Тачка 2:* уместо „целовите" треба „свеобухватне".

Члан 4. – Пре „безбедност" уметнути „информациону". Уместо „информационог друштва" ставити „телекомуникација" или „телекомуникација и информационог друштва".

Члан 5. – У састав Тела за координацију додати Повереника за приступ информацијама од јавног значаја и заштиту података о личности и Заштитника грађана, као и представнике професионалних удружења произвођача опреме, софтвера и оператора електронских комуникација, као и организација цивилног

друштва које се баве информационом безбедношћу. Прецизирати какве одлуке доноси ово тело и да ли су оне саветодавне или обавезујуће.

Члан 7. – Уместо „стави на располагање" треба „обезбеди приступ" или „стави на увид". Треба строже прецизирати услове под којима државни органи могу тражити приступ подацима у контексту овог закона, посебно имајући у виду да „подаци од значаја за информациону безбедност" нису нигде дефинисани (нпр. додати став 2. који гласи „Органи из става 1. овог члана могу остварити приступ подацима, који су у непосредној вези са обавезама руковаоца ИКТ система из овог закона, само ради спречавања тешких последица по националну и јавну безбедност, животну средину и здравље људи, основна људска и грађанска права, економски систем и пословање привредних субјеката."). Такође, додати да су државни органи дужни да обезбеде заштиту тајности података означених као пословна тајна и размотрити успостављање механизма судске контроле захтева за приступ подацима.

Члан 13. – Уместо „Надлежни орган", треба „Национални CERT". Евентуално додати нови став који каже да „Национални CERT обавештава Надлежни орган о инцидентима у ИКТ системима, њиховим последицама и предузетим мерама".

Члан 14. – Брисати цео члан.

Члан 15. – У ставу 1. уместо „Надлежни орган" треба „Национални CERT". После „пружи" додати запету и речи „Надлежном органу и руковаоцима ИКТ система, односно јавности".

Члан 16. – Уместо „ЦЕРТ", овде и на даље треба писати „CERT". Текст у загради заменити следећим речима „на енглеском језику 'Computer Emergency Response Team, CERT', у даљем тексту: Национални CERT". Дефиницију појма „CERT" требало би преместити у члан 2.

Члан 17. – *Тачку 1* заменити текстом „прикупља информације о ризицима и инцидентима на националном и интернационалном нивоу". Додати нову тачку: „7) успоставља и остварује међународну сарадњу у области размене информација и знања о безбедносним инцидентима, као национална тачка за контакт".

Члан 18. – Након речи „Надзор над радом Националног ЦЕРТ-а" ставити запету и речи „у смислу закона којим се уређује државна управа". Брисати запету и речи „његова овлашћења". Пре речи „учинак" уметнути речи „какав је".

Члан 19. – Речи „Ближе услове за упис" заменити речима „Поступак уписа".

Члан 20. – Додати нову тачку: „4) успоставља и остварује сарадњу у области размене информација и знања о безбедносним инцидентима са Националним CERT-ом, посебним CERT-овима и руковаоцима ИКТ система". У последњем ставу уместо „министарства надлежног за послове информационог друштва" треба „Надлежног органа".

Члан 22. – Након речи „зрачења" додати речи „у органима јавне власти, Војсци Србије и код руковалаца тајних података".

Члан 31. – Додати опис стручних квалификација које мора да поседује инспектор, нпр. „Инспектор за информациону безбедност мора имати најмање диплому основних академских студија у трајању од четири године, односно 240 ESPB, као

и четири године радног искуства на пословима у вези са информационом безбедношћу". Додати одредбу о спречавању сукоба интереса: „Инспектор не може да врши надзор информационе безбедности ИКТ система, ако је претходно учествовао у његовом пројектовању или реализацији". Додати одредбу о ангажовању стручних лица за непосредан приступ ИКТ системима: „У вршењу инспекцијског надзора, за обављање послова непосредног приступа ИКТ системима, инспектор може ангажовати лица овлашћена или сертификована за тај конкретан ИКТ систем".

Члан 33. – *Тачка 3:* уместо „достављање" треба „приступ" или „на увид". Потребно је додати и нови став који би прецизирао да су инспектори дужни да обезбеде заштиту тајности података означених као пословна тајна.

Члан 34. – Потребно је прописати казне за непридржавање свих обавеза које су прописане овим законом, при чему их је неопходно таксативно пописати у овом члану. Нпр. казниће се правно лице за прекршај ако: „не предузме одговарајуће мере заштите ИКТ система (члан 6); не достави податке од значаја за информациону безбедност (члан 7); не предузме одговарајуће мере заштите ИКТ система од посебног значаја (члан 9)" итд. Даље, потребно је извршити градацију прекршаја и казни – на пример, не може бити исто третирано непримењивање мера заштите обичних ИКТ система (члан 6) и ИКТ система од посебног значаја (члан 9). Такође, потребно је прописати могућност изрицања заштитних мера забране обављања делатности (за правна лица) и одређених послова (за одговорна лица) у случају тежих или поновљених кршења обавеза прописаних законом.

Члан 35. – Размотрити могућност да се рок за доношење подзаконских аката смањи на 6 месеци.

Члан 35а – Додати нови члан који би прописао рок за формирање и почетак рада свих CERT-ова из овог закона (националног, републичког и CERT-ова самосталних руковалаца). Рецимо, годину дана од ступања на снагу закона.

3. Образложење упућеног предлога за измену Нацрта закона

Члан 1. – Овај члан недовољно прецизно описује предмет закона, пошто се базира само на мерама заштите. Како и сама дефиниција појма Националног CERT-а каже да се ради и о радњама у току и након настанка „штете", изостављено је у набрајању све везано за мере које подразумевају реакцију на инциденте.

Члан 2. – *Тачка 1:* непрецизна дефиниција може довести до тешкоћа у примени закона, како од стране власника ИКТ система, тако и од инспекција и правосудних органа. *Тач. 3-8, 18, 20*: имајући у виду да је предмет закона заштита информација, требало би допунити дефиниције тако да се односе и на информације, а не само на податке. *Тачка 9:* информациона безбедност је већ дефинисана у тачки 3, тако да је ово понављање сувишно. *Тачка 24:* отворене дефиниције су подложне различитим интерпретацијама и зато могу створити велике проблеме у примени закона. Додавање нове тачке са дефиницијом појма „CERT" неопходно је имајући у виду неконзистентне дефиниције у чл. 16, 19. и 20.

Члан 4. – Није дефинисан појам „безбедност ИКТ система”, па га треба заменити појмом који јесте дефинисан („информациона безбедност”). Имајући у виду је законом РАТЕЛ одређен као Национални CERT, његов рад би требало да буде првенствено у ресору телекомуникација (и информационог друштва).

Члан 5. – Не би требало пропустити прилику да се институционализује вишепартнерски модел сарадње државних институција и приватног сектора, под чијом контролом се налази највећи део критичне информационе инфраструктуре и без чијег учешћа није могуће обезбедити домаће ИКТ системе и мреже.

Члан 7. – Стављање на *располагање* података је превише широко овлашћење. Такође, ако већ нису дефинисани „подаци од значаја за информациону безбедност” треба строже дефинисати услов за приступ подацима и директније их повезати са обавезама које проистичу из овог закона. Такође, треба имати у виду да прикупљање података на овај начин потенцијално крши одредбе уговора о чувању поверљивости (Non-Disclosure Agreement, NDA), који су уобичајени у области ИКТ и информационе безбедности. Потребно је размотрити успостављање судске контроле над захтевима за приступ подацима, имајући у виду да је податке о информационој безбедности често тешко одвојити од података о личности, података о комуникацији и садржаја комуникације.

Члан 13. – Поставља се питање капацитета ресорног министарства за оперативно деловање у вези са безбедносним инцидентима, па је овај посао боље препустити Националном CERT-у, који онда може обавештавати Надлежни орган (а он даље друге надлежне органе, као што су Савет за националну безбедност, Тужилаштво, Повереник за заштиту података о личности и сл.).

Члан 14. – Требало би раздвојити доношење правила од њиховог спровођења, па је, с тим у вези, предлог да се провера поступања руковалаца ИКТ система врши преко надлежне инспекције (уређено чл. 31-33), чиме члан 14. постаје сувишан.

Члан 15. – Исто као и образложење уз члан 13.

Члан 16. – Уместо „ЦЕРТ” треба писати „CERT”, јер се ради о скраћеници која има значење само у енглеском језику. Премештање дефиниције појма „CERT” у члан 2. Неопходно је ради конзистентне употребе овог појма у чл. 16, 19. и 20.

Члан 17. – Предложено је у складу са препорукама ОЕБС-а и предлогом NIS директиве ЕУ.

Члан 18. – Треба имати у виду да је РАТЕЛ независно регулаторно тело, које врши јавна овлашћења поверена законом и, с тим у вези, самостално планира и располаже сопственим буџетом (на који сагласност даје Влада). Надзор може бити једино у смислу Закона о државној управи (надзор над законитошћу и сврсисходношћу рада).

Члан 19. – Нема разлога додатно условљавати упис посебних CERT-ова у регистар. Довољно је да испуњавају основни услов из закона (да су основани ради обављања послова из става 1. овог члана). Са друге стране, може се прописати поступак уписа у регистар.

Члан 20. – Од кључног је значаја обезбедити сарадњу, размену информација и искустава између CERT-а републичких органа и других CERT-ова.

Члан 22. – Потребно је додати предложени текст, како би било јасно да се побројане обавезе односе само на државне органе, Војску Србије и лица који се сматрају руковаоцима тајних података према Закону о заштити тајности података, а не на сва (правна и физичка) лица и њихову употребу криптографских средстава и крипто-материјала.

Члан 31. – Додавање описа квалификација инспектора неопходно је како би се обезбедио адекватан стручни ниво инспекције, будући да се ради о приступу комплексним продукционим ИКТ системима. Из истог разлога предложена је могућност инспектора да ангажује сертификоване стручњаке за сваки конкретни ИКТ систем, имајући у виду велики број и разноликост ИКТ платформи. Напокон, неопходно је обезбедити непристрасност инспектора у обављању надзора, па је предложено да он не може обављати надзор над ИКТ системом који је пројектовао или учествовао у његовој реализацији.

Члан 33. – Исто као и образложење уз члан 7.

Члан 34. – Садашња формулација овог члана је неадекватна и захтева темељну прераду на предложени начин.

Члан 35. – Имајући у виду хитност примене мера информационе безбедности на свим нивоима, предложено је да се убрза процес доношења подзаконских аката, без којих примена закона није могућа.

Члан 35а. – Потребно је оснажити прописане обавезе конкретним роковима за њихово извршење.