

Поштовани г. Војводићу,

Надам се да мој прилог Нацрту закона о информатичкој безбедности није стигао касно до Вас. С једне стране, мисам могао да због обавеза на послу детаљно прочитам текст Нацрта, а с друге стране, желео сам да се упознам са другим коментарима, како не бих понављао већ речено. Сматрам да су коментари гг. Поповића, Петкова, Влаховића, Ћировића и Радојевоћа веома интересантни и корисни. Ја ћу покушати да дам коментаре и примедбе на нека друга питања која они у својим дискусијама нису поменули, а за која сматрам да би интересовала ширу информазичку јавност.

Лако је уочити да су аутори овог Нацрта желели да остану усаглашени са Законом о тајним подацима, па су тако наследили све пропусте које има овај Закон, а, може се рећи, дали и свој допринос— Овде пре свега мислим на несрећну класификацију података (зашто података, а не информација?) из поменутог Закона по степену осетљивости (sensitivity) у којој су „помешане бабе и жабе“, тако да уместо светски прихваћене класификације информација (јавне, за интерну употребу, поверљиве и строго поверљиве) имамо онакву каква је дата у Закону. Аутори овог Нацрта отишли су и корак даље, па су један од три кључна принципа безбедности информација, познат као „поверљивост“ (confidentiality), „прекрстили“ у „тајност“ (чл. 2 Нацрта и даље), о чему је дао коментар и г. Влаховић. Можда ја претерујем, али заиста не видим потребу „кумовања“ и измишљања нових термина уместо неких опште прихваћених у информатичкој заједници.

Оно што овом Нацрту недостаје, а недостаје и Закону о тајности података, јесте класификација информација (података) по власништву, и дефинисање појмова власника, корисника и чувара (custodian) информација. Да су ту термини дефинисани, лакше би било дефинисати, на пример, принцип поверљивости (или, ако хоћете, тајности). Тако би уместо непрецизне дефиниције тог принципа датој у члану 2 Нацрта, стајала кратка и јасна дефиниција да је то „принцип да информација може бити доступна само корисницима који имају одобрење власника те информације“.

Мислим да није на одмет рећи нешто о дефиницији појма „ризик“. Ово је кључни појам у информатичкој безбедности и, како је то лепо приметио г. Влаховић, управљању ризицима је у овом Нацрту посвећено неоправдано мало пажње. Па и сама дефиниција појма „ризик“ дата у члану 2 Нацрта, више одговара ономе што се зове „инцидент информатичке безбедности“. Ако аутори Нацрта нису хтели да прихвате дефиницију ризика из стандарда ISO 27005 – “Risk Management”, могли су да преузму неку од дефиниција ризика из других публикација о управљању ризицима. Чак и неформална дефиниција ризика као могућности да се реализује нека претња користећи слабости (рањивости) система чини ми се прикладнијом.

Да не бих само помињао појмове и дефиниције, хтео бих да нешто кажем и о поглављима 3 – 5 Нацрта, која се односе на Агенцију за криптолошку безбедност и заштиту од компромитујућег електромагнетног зрачења, њене надлежности и њен рад. Мислим да је таква институција потребна у овој земљи, и да ће ваљано радити свој посао. Познајем доста људи коју су радили још у некадашњем ИПМЕ у сматрам да су јако стручни за посао који им је овим Нацртом намењен. Моје питање је – зашто ова агенција треба да буде у саставу Министарства одбране? Не би ли било логично да буде у саставу министарства које се бави информационо–комуникационим технологијама, ма како се оно звало? Ако ће та агенција издавати атесте или сличне потврде за коришћење криптолошких производа, зар ће се ти производи користити само у војсци?

Имало би још подоста да се каже о овом Нацрту закона, али се и мени чини да је најбољи закључак дао г. Поповић – овај нацрт би требало поделити у два дела. Један део би заиста разматрао информатичку безбедност, али у знатно ширем обиму него што овај Нацрт то чини, док би други обухватио правно–организациона питања о Агенцији за КБ и КЕМЗ, националним мрежама и слично.

У овом коментару изражавам своје личне ставове, а не ставове институције у којој радим, па се зато потписујем без навођења назива те институције, да се не би сматрало да је то њен став.

С дубоким поштовањем,

Миодраг Р. Стефановић, дипл. инж. ел.

Слободана Јовановића 10/16

11060 Београд

Тел. 20 83 660