

## Коментари на нацрт Закона о информационој безбедности

Владимир Радуновић, Дипло фондација, [vladar@diplomacy.edu](mailto:vladar@diplomacy.edu)

Генерални коментари:

Позитивно је што су у Закон унете одредбе о формирању националног и Владиног ЦЕРТ тима, што је и позитивна пракса западних земаља. Можда треба нагласити као улогу Националног ЦЕРТ-а и подстицај оснивања ЦЕРТ при кључним провајдерима ИКТ услуга, као и приватних ЦЕРТ.

Члан 7:

- У ставу 1, додати
  - „преглед организационих и техничких полиса приступа подацима и сегментима ИКТ система“ после тачке 2),

и/или

- „мере заштите од социјалног инжињеринга“ после тачке 14)

Образложење:

Важно је прецизирати и дефинисање полиса јер су оне кључ у борби против социјалног инжињеринга, а који представља доминантни тип иницијалног напада у циљу крађе података

- У ставу 1, тачка 3. „технички опис ИКТ система“ додати „са описом критичних и редовних техничких и технолошких унапређења“

Образложење:

Важно је имати прецизну информацију у којој мери је систем „updateovan“ регуларно и у критичним моментима новим технолошким унапређењима (попут DNSSec, IPv6, ...)

Члан 8:

Став 3 „Одговорно лице... мора бити сертифицивано“ потребно је допунити спецификацијом на коју се сертификацију односи или да ће детаљи бити одређени подактом.

#### Члан 9:

Став 3 „Самостални руководиоци...“ треба да буде допуњен: иако се ради о службама/министарствима безбедности те је њихов План мера сам по себи тајна високог нивоа, тај План мера мора да постоји као што постоји и за остале. Можда не мора да се доставља Комисији (ако је процењено да би то био ризик) већ неке друге, али тај документ мора да постоји и да буде законски захтеван и од њих (тј. пре свега од њих).

#### Члан 10:

Став 4: „Акредитација ... важи 36 месеци“ треба да буде измењен:

Развој ИКТ је пребрз да би се безусловно оставила акредитација на тако дуг период. Док је са једне стране важно омогућити акредитованима лиценцу на дужи период, потребно је оставити могућност да Комисија затражи допуне/дораде Плана заштите и других мера у случају потребе (већих технолошких промена у том периоду - тренутни глобални пример је неопходност имплементације IPv6 и DNSSEC технологија, а могућа су и друга глобална унапређења која је хитно потребно испунити). Да би се избегла могућност манипулација (да се само неким од акредитованих тражи додатна документација, јер у поменутом случају кључних технолошких промена сви акредитовани би морали унапредити своје планове) можда нагласити да Комисија има могућност да од свих затражи ревидиране планове и ревидира акредитацију у случајевима неопходних критичних унапређења система, а о чему одлучује Влада или неко други. Ово може бити додато у став 6.

#### Члан 13:

Реална је бојазан да ће бити приличан број неакредитованих ИКТ система у органима јавне власти, који раде са приватним подацима грађана. Како они вероватно неће имати капацитета (организационог, финансијског, нити знања) потребно је помоћи екстерно; став 4 дакле може бити превише генералан и да остане недоречен. Познато је да системи падају на најслабијој карики - и ако се сви акредитовани системи покажу сјајнима, цео систем је слаб колико и најслабија карика а то може бити неки од неакредитованих система. План мера и стручна организациона и техничка помоћ је неопходна неакредитованима, и то треба прецизирати.

#### Члан 23:

Став 5:

Рок од 60 дана може бити предуг с обзиром на брз развој технологија. Нови модели опреме и верзије софтвера излазе готово на месечном нивоу, а готово свака нова верзија мора бити поново

проверена, те ће бити и неопходна је бржа провера од 60 дана (што је и реално предуго за такав посао).

Члан 24:

Службама од највишег значаја и са највећим евентуалним последицама цурења података дата је аутономија процене сопствене криптозаштите, што је потпуно у супротности са ризиком: управо ови органи морају имати највећи степен контроле уређаја и алгоритама, и опште одобрење може бити контрапродуктивно (начинити најслабију карику на најбитнијем месту).

Члан 25:

Став 5 „Седиште АМРЕС-а је у Београду“:

Иако тренутно технолошко стање опремљености академске мреже предпоставља да ће седиште АМРЕС бити у Београду, нема никаквог разлога законски онемогућити да се седиште АМРЕС (можда само административно ако не и техничко) не премести у неки други град у будућности. Стога овај став треба избрисати.

Члан 31:

Генерална примедба:

Од 5 чланова УО АМРЕС само је један биран испред академске заједнице. С обзиром да се ради о академској мрежи овај дисбаланс би требало променити. Такође, библиотеке би требало да такође имају директан утицај на одлучивање (јер ће мрежа омогућити промоцију културне баштине Србије у земљи и иностранству), можда и кроз свог представника у УО.

Треба претпоставити да постоји (макар теоретска) могућност да би нека наредна Влада могла бити мање демократска и утицати на коришћење академске мреже у смеру цензуре (политичке или макакве друге) и тиме обесмислити мрежу као средство за слободан проток информација. Ако Влада има већину представника у УО ова бојазан је реална. Стога је неопходан баланс владиних и не-владиних чланова.

Члан 43:

Став 2:

Поново се најбитнији сегменти националне безбедности остављају самоконтроли. Питање је да ли је то добра пракса; можда Инспекција није прави механизам контроле самосталних руковоаца ИКТ система, али неки систем треба прецизирати а не оставити самоконтролу.