Извештај радне групе за *CERT/SIRT*

Датум: 20.08.2015.

ОСНИВАЊЕ И ЦИЉ РАДНЕ ГРУПЕ

На основу одлуке Управног одбора Фондације од 02. априла 2015. и на основу правилника о формирању и раду радних група основана је радна група у следећем саставу:

Ненад Орлић – координатор
Бошко Радивојевић – члан
Ненад Крајновић – члан
Зоран Перовић – члан / представник УО

У раду радне групе у својству посматрача учествовао је и Душан Стојичевић, председник УО.

Циљ због којег је основана радна група је доношење препорука за формирање *CERT*/*SIRT* функције за доменски простор у оквиру РНИДС-а.

План рада радне групе је усвојен и одобрен од стране УО.

Радна група одржала је два састанка а између састанака комуникација се одвијала путем емаил-а. Ради прикупљања и размене информација чланови групе су комуницирали са особама и институцијама које се баве проблемом информационе безбедности у нашој земљи.

За сва кључна питања за која је дат закључак радне групе постигнут је консензус.

УВОД

Проблем информационе безбедности идентификован је као један од приоритета у држави на свим нивоима како због политичких дешавања односно процеса приступања ЕУ тако и због реалних животних потреба јер свакодневни раст употребе ИКТ у Србији није испраћен адекватном законском регулативом или организованим деловањем на сузбијању сигурносних инцидената.

РНИДС је организација са значајном улогом на домаћој информатичкој сцени где као регистар националних домена носи и део одговорности за информациону безбедност. Уз постојеће техничке и логистичке капацитете које РНИДС поседује логичан је закључак да се ова организација треба преузети и активну улогу у побољшању информационе безбедности односно да формира *CERT* који би се бавио безбедношћу унутар информационог простора националних домена Србије.

ПРЕТХОДНЕ АКТИВНОСТИ РНИДС-А НА ПОЉУ ИНФОРМАЦИОНЕ БЕЗБЕДНОСТИ И ФОРМИРАЊУ *CERT*-А

РНИДС је питање безбедности своје инфраструктуре увек озбиљно схватао тако да је и при пројектовању исте узета у обзир и безбедност података, редундантност и доступност сервиса која по природи функције коју РНИДС обавља мора бити изузетно висока.

УО је 2014. године идентификовао *CERT* као делатност којом би РНИДС требао да се бави и дао налог канцеларији да приступи прикупљању информација и изради докумената потребних за формирање *CERT*-а. У плану и програму УО за 2015. годину формирање *CERT*-а је постављен као један од циљева.

Радној групи су представљена документа која је канцеларија израдила по налогу УО:

- Преглед националних *CERT*-ова у Европи
- Коментари уз преглед националних *CERT*-ова у Европи
- Делатност РНИДС-СИРТ
- Кораци за формирање РНИДС-СИРТ

Половином 2015. године активности УО и канцеларије на ову тему су интензивиране и укључивале су

- Учешће на састанку у Петници у организацији Дипло фондације, где су учестовала сва релевантна министарства, службе безбедности, велики телекомуникациони оператери и други
- Учешће у јавној расправи одржаној 10. јула поводом предлога закона о информационој безбедности[1]
- Достављени су писани коментари на предлог Закона о информационој безбедности
- Пријава за учешће у оквиру програма Хоризон 2020[2]
- Одржавање неколико предавања из области сигурности и безбедности на интернету на факултетима

Поред ових активности предвиђено је и даље активно учешће на свим скуповима који се буду одржавали на ову тему као и активно учешће у активностима око креирања текста Закона о информационој безбедности.

Ове активности УО и директора представљале су почетни извор информација и креирале су оквир у којем је радна група радила, односно, утицале су на то да чланови радне групе могу да дођу до квалитетнијих закључака узимајући у обзир релевантне информације које су им стављене на располагање.

[1] http://mtt.gov.rs/vesti/javni-poziv-informaciona-bezbednost/
[2] http://ec.europa.eu/programmes/horizon2020/

ЗАКЉУЧЦИ РАДНЕ ГРУПЕ

У току свог рада, радна група је идентификовала основна питања и проблеме на које даје своје одговоре и препоруке.

- **Да ли током рада групе и у будућим актима треба користити скраћеницу *CERT*[3] или *SIRT*.** Иако је у досадашњем раду УО и канцеларије био уобичајен назив *SIRT* (*Security Incident Response Team*), радна група се определила да користи термин/скраћеницу *CERT* (*Computer Emergency Response Team*) из разлога што је тај термин предвиђен предлогом Закона о информационој безбедности чиме се постиже усклађеност са домаћим законодавством и смањује могућност забуне или погрешног тумачења сврхе и одговорности овог тела.
- **Да ли РНИДС треба да креира *CERT* и обавља послове из области информационе безбедности?**
  Препорука радне групе је да РНИДС као организација, која због функције коју обавља има значајну улогу у функционисању домаћег интернета и испуњава техничке и логистичке предуслове да се бави овим, треба да формира *CERT* за доменски простор Србије
- **Коју област би требао да покрије и којим активностима би *CERT* у оквиру РНИДС-а требао да се бави?**
  CERT у оквиру РНИДС-а би требао да се бави безбедношћу доменског простора Србије, пре свега .рс и .срб домена где би се власницима ових домена пружиле све услуге које *CERT* може да понуди од информисања и размене информација о безбедносним инцидентима до активне превенције и санације у случају безбедносних инцидената. До постизања већих техничких и људских капацитета, препорука је да се РНИДС *CERT* фокусира на рад ДНС сервиса и проблеме везане за ту област. Такав фокус би био у складу са задацима РНИДС-а док би у наредној фази област активности *CERT*-а требао да обухвати и друге сервисе у оквиру делатности РНИДС-а.
- **Коју правну форму би *CERT* требао да има?**
  Став радне групе је да је ради бржег формирања најбоље да се *CERT* формира као посебна организациона јединица у оквиру фондације. Почетно је потребно искористити то што РНИДС има сопствени простор и људство које може подржати административне функције *CERT*-а док је неопходно запослити барем једног човека који би имао функцију координатора активности *CERT*-а. Обавезе, овлашћења координатора и организациону структуру *CERT*-а унутар фондације потребно је да регулише УО посебним актом.
  Препорука је да након што ова функција успешно заживи у оквиру постојеће правне форме фондације, треба извршити припрему за одвајање *CERT*-а у посебан ДОО чији би РНИДС био власник капитала.
- **На који начин би се рад *CERT*-а финансирао?**
  У првих годину дана, рад *CERT*-а би се финансирао из постојећег буџета РНИДС-а односно прерасподелом прихода од основне делатности продаје домена. Потребно је тежити ка томе да до краја друге године постојања *CERT* може да функционише као финансијски независна целина односно да није потребно одвајати финансијска средства из прихода од продаје домена. Извори финансирања *CERT*-а могу бити: стручни курсеви и обуке, услуге провере безбедности информационих система, услуге санације инцидената и друге комерцијалне услуге везане за информатичку безбедност. *CERT* се може и финансирати из чланарина односно претплате, донација и спонзорстава компанија. У случају да се УО одлучи да постоји чланарина односно претплата за услуге *CERT*-а препорука радне групе је да од ње буду изузети суоснивачи РНИДС-а.

[3] https://en.wikipedia.org/wiki/Computer_emergency_response_team

- **Да ли постоји законски оквир који РНИДС мора поштовати при креирању *CERT*-а?**
  Тренутно не постоји законска регулатива која уређује рад *CERT*-а у Србији тако да поред опште регулативе не постоји посебна регулатива којом се треба руководити. Током рада радне групе, започела је јавна расправа о нацрту Закона о информационој безбедности. У оквиру овог закона предвиђено је и формирање Националног *CERT*-а као и других *CERT*-ова. Када Закон буде усвојен, РНИДС ће своје пословање и акте морати да прилагоди његовим одредбама. Такође, очекује се и измена Закона о електронским комуникацијама и то у делу који се односи на информациону безбедност те постоји могућност да и одређене одредбе овог закона такође уређују област рада *CERT*-а и евентуално друге активности РНИДС-а.
- **Да ли постоје други документи/препоруке којима се *CERT* треба руководити у раду?**
  Званично *CERT* нема за сада обавезу да се у раду руководи одређеним документима али је препоручљиво при раду узети у обзир следеће документе:
  - Стратегија развоја информационог друштва у Републици Србији до 2020. године
  - Препорука повереника за унапређење заштите података о личности у сфери интернета
  - ЕНИСА листа националних стратегија сајбер безбедности
- **Да ли је за успостављање *CERT*-а неопходна измена постојећих докумената РНИДС-а?**
  Да. Минимална неопходна измена укључује измену статута тако да укључи ову делатност и предвиди постојање посебне организационе јединце. Радна група је саставила и предлог измена статута које прилаже у прилогу уз овај извештај. Предложене измене односе се на минимум измена статута неопходних да се РНИДС бави овом делатношћу. Препорука Радне групе је да УО нађе начин и састави предлог измене статута у којем би се *CERT* предвидео као посебна целина унутар организације а на начин да се не нарушава постојећа организациона структура и да не долази до проблема надлежности унутар организације.

У односу на достављена документа од стране Канцеларије радна група је заузела став да су документи:
-Преглед националних *CERT*-ова у Европи,
-Коментари уз преглед националних *CERT*-ова у Европи,
-Делатност РНИДС-СИРТ
квалитетно урађени и могу да се користе и убудуће у целости како су достављени и да могу бити корисни у поступку формирања *CERT*-а. Став је да документ „Кораци за формирање СИРТ-а“ потребно изменити тако да он обухвати препоруке радне групе као и нову законску регулативу која се појавила након израде овог документа.

Чланови радне групе својим потписом потврђују своју сагласност са овим извештајем и његовим закључцима и препорукама.

_____
Ненад Орлић, координатор

_____
Ненад Крајновић, члан

_____
Бошко Радивојевић, члан

_____
Зоран Перовић, члан

ПРИЛОГ 1 - ПРЕДЛОГ ИЗМЕНЕ СТАТУТА РНИДС-А

Члан 2.

На крају постојећег члана додаје се следећа дефиниција:

„*CERT*“ (*Computer Emergency Response Team)* је тело које се бави информационом безбедношћу и то информисањем, едукацијом, превенцијом, детекцијом и санацијом безбедносних инцидената.

Члан3.

На крају члана 3, у став 3, додаје се ставка 4:

4) Активно деловање на повећању информационе безбедности у Србији

Члан 4.

У ставу 2. Члана 4. постојећа ставка 4. постаје ставка 5. а убацује се нова ставка 4. која гласи:

4) Управљање *CERT* телом за доменски простор Србије

Чланови радне групе својим потписом потврђују своју сагласност са овим извештајем и његовим закључцима и препорукама.

_____

Ненад Орлић, координатор

_____

Ненад Крајновић, члан

_____

Бошко Радивојевић, члан

_____

Зоран Перовић, члан