ФОРМИРАЊЕ ЦЕНТРА ЗА РЕАГОВАЊЕ НА НАПАДЕ НА ИНФОРМАЦИОНИ СИСТЕМ У МИНИСТАРСТВУ УНУТРАШЊИХ ПОСЛОВА РЕПУБЛИКЕ СРБИЈЕ

Небојша Јокић, Владан Бабић**

Подаци који се обрађују и чувају у информационим системима Министарства унутрашњих послова од велике су важности не само за оперативне линије рада, већ и за све грађане Србије. Министарство унутрашњих послова надлежно је за држављанство, јединствени матични број грађана, електронско вођење података о личности, пребивалиште и боравиште грађана, личне карте, путне исправе и мноштво других података о личности, од којих се велики део може окарактерисати као посебно осетљив. Због тога, Министарство унутрашњих послова мора посвећивати изузетну пажњу заштити ових података од свих облика злоупотребе, јер би, у супротном, последице могле бити катастрофалне. Ефикасни начини за реализацију оваквих циљева препознати су у свету кроз формирање посебних организационих целина које у надлежности имају заштиту информационих и телекомуникационих система, међу којима изузетно важну улогу имају CERT или CSIRT тимови.

* Аутори раде у Центру за реаговање на нападе на информациони систем Министарства унутрашњих послова Републике Србије

Интернет је почео да функционише у облику каквом га познајемо данас 1995. године, када су укинута последња ограничења по питању комерцијалног саобраћаја. Али, он није настао те године, већ је израстао из компјутерских мрежа које су настале раније и биле другачије конципиране.

НАСТАНАК ИНТЕРНЕТА

Мрежа која се сматра најранијом претходницом интернета звала се ARPANET[1] и била је пројекат агенције Министарства одбране америчке владе под именом DARPA[2]. Циљ овог пројекта био је да се кроз телефонску мрежу оствари повезивање рачунара и рачунарских мрежа на такав начин да се у случају нуклеарног сукоба подаци преносе телекомуникационим путем који је расположив или најмање оптерећен. Пројекат је започет крајем шездесетих година прошлог века, а прва два чвора мреже повезана су 1969. године. Пренос података између чворова ишао је преко телефонских жица коришћењем X.25 сета протокола, а тестирање је поверено неколицини престижних америчких универзитета.

Дигитална трансформација кроз дигиталну понуду и дигиталну потражњу

На истим принципима и уз употребу истих протокола, Национална научна фондација (NSF[3]) формирала је 1981. године мрежу CSNET[4] која је од почетка била повезана са мрежом ARPANET. Сврха мреже CSNET била је да повеже научне и истраживачке институције из области компјутерских наука које нису могле бити директ-

[1] Advanced Research Projects Agency NETwork
[2] Defense Advanced Research Projects Agency
[3] National Science Foundation
[4] Computer Science NETwork

но прикључене на ARPANET мрежу. До краја 1984. године на мрежу је повезано 84 сајта (укључујући и један у Израелу), а до краја самосталног рада повезивала је преко 180 сајтова, од којих су неки били у Аустралији, Канади, Француској, Немачкој, Кореји и Јапану.[1]

Упоредо са подизањем мреже CSNET, Национална научна фондација покренула је програм укључења суперкомпјутера у мрежу, али и програм помоћи у формирању суперкомпјутерских центара. Циљ ове иницијативе био је изградња нове, много брже мреже, која би повезала постојеће регионалне мреже, али и локалне ака- демске мреже. У том смислу, ова мрежа била би „мре́жа мрêжа[5]" или *internet* и омогућавала би корисницима да приступају било ком ресурсу у било којој мрежи из сопствене локалне мреже. Мрежа је названа NSFNET и почела је са радом 1986. године повезивањем пет универзитетских суперкомпјутерских центара, али, као што је то био случај са мрежом CSNET, сви академски корисници имали су отворену могућност за повезивање. Успех мреже био је запањујући и у првој години коришћења саобраћај је постао толико велики да је надоградња мреже постала неопходна. У Националној научној фондацији тада су проценили да је право време да се почне са уно- шењем комерцијалног фактора у мрежу на контролисан начин, јер су били свесни да би потенцијално неконтролисана, али неминовна комерцијализација могла потиснути академске институције на маргину.

Спроведена надоградња резултирала је мрежом која је постала оперативна у јулу 1988. године и повезивала 13 регионалних мрежа и суперкомпјутерских центара. Пренос података између чворова одвијао се преко T1 линкова капацитета 1.5 Mbps, што је био огроман напредак у односу на дотадашњих 56 kbps. Међутим, захтеви су одмах постали већи и коришћење мреже је почело да расте по стопи од 10 одсто месечно.[2]

Следећих неколико година радило се на комерцијализацији и униформности, па је тако мрежа ARPANET угашена 1990. године. Мрежа CSNET функционисала је до 1991. године, а након укидања ограничења по питању комерцијалног саобраћаја званично је, 30. априла 1995. године, угашена мрежа NSFNET. Али, оно што је нама посебно интересантно је појава првог „црва" на интернету у новембру 1988. године, само неколико месеци након надоградње мреже NSFNET.

[5] network of networks

„ЦРВ" MORRIS

Почетком новембра 1988. године на мрежу NSFNET било је повезано преко 60.000 компјутера, који су користили различите опера- тивне системе, али се међусобна комуникација одвијала коришћењем сета IP протокола. Мрежа NSFNET функционисала је претходних пар година без већих проблема, да би 2. новембра дошло до неконтролисаног ширења и аутоматског извршавања једног програма на ком- пјутерима који су користили BSD верзију UNIX оперативног система. Овај програм користио је безбедносне слабости оперативног система да самостално успостави мрежну конекцију, ископира себе на други компјутер и покрене извршавање своје копије на том компјутеру, при чему свака копија изнова понавља овај процес. Програм се брзо ширио и изазвао конфузију код корисника и администратора, који су приметили појаву нових фајлова и неуобичајених порука у *log* фајловима на својим компјутерима. Али, највећи проблем представљало је то што се овај програм непрестано извршавао, као и вишеструке копије које су стизале преко мреже. Како је време пролазило, ови про- цеси су толико оптерећивали заражене компјутере да они више нису могли да функционишу.

Генерално посматрано, ова врста програма, која користи пропусте у безбедносним протоколима да би се ширила и аутоматски извршавала, назива се *црв* (енглески: *worm*) и разликује се од вируса којима је потребан постојећи фајл за који ће се закачити. Без обзира на то што је то био први пут да се неки „црв" појавио на мрежи, на универзитетима у Америци одмах је започета анализа проблема и за мање од 12 сати од почетка инцидента Универзитет Беркли у Калифорнији објавио је начин како да се заустави ширење овог програма. На овом универзитету и на Масачусетском технолошком институту (MIT[6]) успели су да издвоје кôд програма, након чега је откривен и његов творац Роберт Морис, студент Универзитета Корнел, који је прво извршавање програма покренуо на једном од компјутера на Масачусетском технолошком институту. По свом творцу овај „црв" је добио и име.

Да би се систем вратио у стање пре инцидента, регионалне мреже су на неколико дана биле међусобно одвојене и од мреже NSFNET, како би се спречило поновно ширење „црва" и омогућило свима да очисте своје компјутере. Према проценама стручњака, од 60.000 компјутера који су у том тренутку били повезани на мрежу, „црв Morris" заразио је око 6.000, а штета је процењена на између 100.000 и

[6] Massachusetts Institute of Technology

„Syber" претње

10.000.000 америчких долара[7]. Роберт Морис осуђен је за компјутерску превару и злоупотребу на три године затвора условно, 400 сати добротворног рада и новчану казну. [5]

ПРВИ ЦЕРТ

Појава „црва Morris" и проблеми које је проузроковао покренули су обимну научну и јавну расправу о поступању са појединцима који узрокују инциденте, одговорности за унапређење софтвера и механизама заштите и генерално о безбедности на компјутерским мрежама. У сваком случају, овај инцидент иницирао је формирање првог тима за реаговање на компјутерске инциденте (CERT/CC[8]) у оквиру Института за софтверски инжењеринг (SEI[9]) на Универзитету Карнеги Мелон већ током новембра те године. Одмах после формирања овог тима, агенција DARPA овластила је SEI да успостави капацитет за брзу и ефикасну координацију комуникације између компјутерских експерата током инцидената у компјутерским мрежама. Осим овог примарног задатка, CERT/CC треба да изгради начине за рана упозорења интернет заједнице на безбедносне проблеме, анализира безбедносне слабости, проналази решења за безбедносне проблеме и о томе

[7] Процена портпарола Универзитета Харвард
[8] CERT Coordination Center
[9] Software Engineering Institute

информише ширу заједницу. У складу са добијеним задацима и овлашћењима, CERT/CC финансира се средствима америчке Владе.

Од мале групе људи у почетку, данас CERT/CC има више од 150 професионалаца из области сајбер безбедности. Поред тога што сарађују са владиним институцијама, индустријом, полицијом и академским институцијама, CERT/CC има посебно блиску сарадњу са Министарством државне безбедности (Department of Homeland Security) у областима прикупљања и анализе података, компјутерске и мрежне безбедности, управљања инцидентима и слично.

Након CERT/CC, широм света почели су да се формирају слични тимови са задатком да реагују у случају инцидената у компјутерским мрежама. У Европи данас има више од 100 оваквих тимова, а први је формиран у Холандији 1992. године (SURFnet-CERT). Ради боље координације и ефикасније размене информација, 1990. године формирана је организација FIRST[10] која окупља тимове за реаговање на компјутерске инциденте, која данас у свом чланству има преко 300 тимова широм света.

Занимљиво је да, без обзира на то што се CERT у целом свету означава као скраћеница од Computer Emergency Response Team, на Универзитету Карнеги Мелон сматрају да CERT не означава скраћеницу и чак су регистровали и заштитили права на овај назив, а тимовима

[10] Forum of Incident Response and Security Teams

са надлежностима у овој области препоручују назив Computer Security Incident Response Team (CSIRT). Овај назив је прецизнији и данас се користи претежно у Европи, а други термини који се користе за овакве тимове су IRT (Incident Response Team), IRC (Incident Response Center), CIRT (Computer Incident Response Team), SIRT (Security Incident Response Team) и SERT (Security Emergency Response Team).

ОСНОВНЕ ФУНКЦИЈЕ CSIRT (CERT) ТИМА

Оорганизације оснивају свој CSIRT због немогућности гарантовања потпуне заштите од упада или других злонамерних активности, чак и за најбоље обезбеђене информационе системе. Због заштите ресурса и података, од изузетне важности је да у случају инцидента детекција, анализа и реакција буду брзи и ефикасни, како би се спречиле веће последице, смањили трошкови и време опоравка. Запослени у CSIRT тимовима због тога морају проћи врхунске обуке, континуирано пратити дешавања у овој области и практиковати честе вежбе, како би били способни да одговоре на све изазове. Један од кључних фактора у успешној одбрани јесте и сарадња CSIRT тимова, јер се кроз међусобну комуникацију размењују информације о актуелним претњама и начинима одбране од њих.

Поред основног задатка да реагују на безбедносне инциденте у вези с компјутерима, готово сви CSIRT тимови баве се и превентивним активностима, као што су испитивање рањивости информационих система, едукација запослених и други видови подизања безбедносне свести. Ови тимови могу бити формално конституисани као организациона целина или се могу окупљати у случајевима инцидената или других догађаја. С тим у вези, један од предуслова за добро функционисање CSIRT тима је јасна дефиниција ситуација у којима се тим ангажује, односно тачна дефиниција термина „инцидент". За овај термин не постоји универзална дефиниција, тако да свака организација која формира CSIRT тим мора урадити своју дефиницију овог појма и тиме одредити праг ангажовања тима. Обично се под овим појмом подразумевају одређени штетни догађаји по безбедност информационих система, као и директна или посредна кршења безбедносних политика. Штетним догађајима по безбедност информационих система могу се сматрати, на пример, покушаји неауторизованих приступа информационом систему или подацима, догађаји који доводе до недоступности система или сервиса, неауторизовано коришћење ресур-

са система, неауторизоване измене на системском хардверу, фирмверу, софтверу или подацима и друго.

CSIRT тимови могу бити надлежни за системе целе државе, неке географске регије, појединих организација, као што су државне институције, академске мреже или компаније, а могу бити организовани и тако да нису везани за једну организацију већ пружају услуге за више клијената уз наплату. Неки CSIRT тимови врше координационе функције између више различитих CSIRT тимова како би се олакшало управљање инцидентом и слабљење напада.

У оквиру једне организације CSIRT тим може бити део сектора информационих технологија или телекомуникација, део сектора који се бави безбедношћу организације, али и независна целина директно подређена руководству. Без обзира на позицију у оквиру организације, подршка руководства и овлашћења за рад су од кључног значаја за успешно функционисање сваког CSIRT тима.

Заштита ИКТ система је обавеза сваког појединца а не само специјализованих служби

Програм рада CSIRT тима мора бити усклађен са овлашћењима за рад, а и овлашћења за рад и програм рада морају одговарати величини и комплексности, природи и обиму активности неке организације, као и осетљивости информација које се чувају и преносе у информационим и комуникационим системима те организације. Програм рада мора идентификовати разумно предвиђање унутрашњих и спољашњих ризика, као и процену да ли има довољно примењеног обезбеђења како би се ти ризици контролисали. Такође, програм рада мора обухватати редовно праћење и

тестирање ефикасности свих кључних контролних система и процедура. На крају, потребно је вршити вредновање и прилагођавање безбедносних програма према резултатима тестирања. У овом процесу веома је битно водити рачуна о великим променама на информационом систему које могу утицати на оперативне процесе или било које друге околности, јер могу имати озбиљан материјални удар на програм безбедности информација услед несагледавања целе ситуације.

ФОРМИРАЊЕ CSIRT ТИМА У МУП-у РЕПУБЛИКЕ СРБИЈЕ

Сајбер напади се дешавају свакодневно и имају мање или веће ефекте по податке, електронске сервисе и информационе и комуникационе системе. У случајевима када су напади усмерени на критичну инфраструктуру (електроенергетски систем, финансијске институције, транспорт итд.) може доћи до штете упоредиве са последицама традиционалног ратовања, па чак и до дестабилизације земље. Због тога је потребно да наша земља убрза и ојача напоре за подизање капацитета у одбрани од сајбер напада, пре свега користећи знање и стручност висококвалификованих професионалаца који су прошли одговарајуће обуке из области информационе безбедности. Нажалост, тренутне снаге нису довољне за све оно што нам је стварно потребно.

Имајући у виду значај својих информационо-комуникационих система за безбедност и функционисање земље и важност података који се у њима чувају или преносе, Министарство унутрашњих послова донело је одлуку да формира сопствени Центар за реаговање на нападе на информациони систем МУП-а. У наредном периоду овај центар ће имати велики задатак да достигне неопходан ниво капацитета за успешно управљање инцидентима, али и да учествује у подизању безбедности информационо-комуникационих система МУП-а на висок ниво. Већ израђени планови предвиђају више праваца у којима ће се кретати активности Центра за реаговање на нападе на информациони систем МУП-а Републике Србије, али најинтензивнији рад ће бити на пољу едукације и подизања свести, почевши од радника Центра за реаговање на нападе на информациони систем МУП-а и других радника који обављају послове везане за информациону безбедност, па до свих запослених који имају приступ информационо-комуникационим системима МУП-а.

Посебан акценат ставиће се на образовање запослених јер они својим поступцима, услед непознавања основних безбедносних правила, могу допринети нарушавању безбедности информационо-комуникационих система[9]. Потребно је избећи све већи степен неусаглашености (незнање, игнорисање, равнодушност, отпор и непослушност) а успоставити што је могући већи степен усаглашености (свест, послушност, посвећеност и безбедносна култура). Поред подизања нивоа знања, интензивно ће се радити и на подизању свести сваког појединца јер се показало да запослени упадају у ризик чак и када су свесни опасности, а разлог томе често буде недостатак одговорности појединца, немогућност системског праћења инцидента и одређивања одговорности, формални и практични проблеми приликом обезбеђивања правно одрживих доказа за спровођење поступка[10]. То је нешто што мора да се промени. Акценат на свим нивоима мора бити на знању и свести запосленог јер он представља прву линију одбране.

Баш зато што запослени представљају прву линију одбране они су и најугроженија и потенцијално најслабија карика у безбедносном ланцу. Ако се пажња обраћа само на помпезне наслове у медијима,

Социјални инжењеринг све више угрожава безбедност грађана

као што су: „Пробијена заштита информационог система", „Угрожени подаци грађана", „Хакери опљачкали банку" и слично, може се доћи до закључка да овакви напади морају укључивати изузетно образоване нападаче, високо софистицирани софтвер и врхунски хардвер. Овакво површно закључивање наводи и на изведене закључке да је заштита немогућа, јер ни велике компаније или институције најразвијенијих држава не могу да одбране своје информационе системе. Због таквих закључака радници на свим нивоима не обраћају претерану пажњу на своје поступке, јер сматрају да не могу да допринесу безбедности. Међутим, дубља анализа показује да готово сваки од напада почива на пропустима жртве напада по питањима елементарне безбедности (незаштићени системи, незакрпљене апликације, лоше лозинке, недостатак писаних процедура итд.). Због тога је први корак ка повећаној безбедности да се не дозволи неодговорно понашање радника који својим поступцима олакшавају посао потенцијалним нападачима, несвесни последица које ти напади могу да проузрокују.

На пример, велики број успешних сајбер напада одвија се преко и-мејла такозваним phishing нападима. Та врста напада искоришћава непажњу запосленог који је у журби, оптерећен гомилом обавеза и који не посвећује довољно времена да испита и-мејл (извор и-мејла, провера сертификата, провера линка итд). Phishing и даље представља једну од озбиљнијих спољњих претњи некој организацији. Анкета коју су радили Институт Ponemon и Wombat security показала је да организације које имају око 10.000 запослених троше годишње у просеку око 3,7 милиона долара на одбрану од phishing напада. Један од циљева које има Центар за реаговање на нападе на информациони систем је да сваки запослени у МУП-у пре отварања размисли о разлогу због којег је добио неки и-мејл, зашто у њему има додатак или зашто се од њега очекује да кликне на додатак. Сваки запослени треба да има свест да пријави сваки сумњиви и-мејл, чак и када је већ урадио нешто што може нанети штету информационом систему (кликнуо на линк, отворио додатак итд.), како би што пре могло да се одговори на инцидент и како би се што више смањила евентуална штета. Дакле, врло је јасно колико је потребно уложити труда како би се запосленима објаснило како да препознају phishing напад и како да одговоре на њега. У сваком случају, боље је улагати напоре у едукацију запослених по питању ове и било које друге теме, него у ублажавање и санирање последица успешног напада.

По питању експерата, планиране су интензивне обуке за едукацију радника који раде на пословима везаним за информациону безбедност, али и реализација програма привлачења младих стручњака у области информационих технологија. Јасно је да на тржишту постоји велики недостатак ових кадрова, као и да универзитети и факултети не прате довољно потребе тржишта које захтева све више квалификованих радника за борбу против сајбер напада. Због изражене разлике у платама, државне институције (укључујући МУП) не могу да конкуришу приватним компанијама у привлачењу стручњака овог профила, а извесно је да ће у наредном периоду доћи до повећања потребе за стручњацима из ове области. Једна од великих могућности нашег друштва је унапређење и промовисање високог образовања као мере за подизање капацитета одбране од сајбер претњи, јер је искуство показало да постоји велики потенцијал код наших студената. При томе, није довољно да се студенти само обуче за тражену вештину на тржишту, већ образовне установе треба да им понуде сертификацију и усавршавање у области сајбер безбедности кроз редовно студирање. То ће свакако помоћи студентима да већ на студијама изаберу уску професионалну оријентацију и започну своје каријере, али не само да би обезбедили каснији професионални успех, већ и да буду спремни да одговоре ако добију позив за помоћ. Поуздани, свесни и високообразовани кадрови најбоља су одбрана.

ЗАКЉУЧАК

Често се информациона безбедност посматра као дестинација, али она, у ствари, представља један дугачак процес коме нема краја. При томе, сам процес мора се спроводити свеобухватно, детаљно и пажљиво, имајући у виду да је сваки информациони систем специфичан и да не постоји безбедносно савршен систем, нити савршени људи. У том смислу није довољно ослањати се само на најбоље праксе и стандарде, већ је неопходно увидети све специфичности, анализирати ризике и успоставити ефикасан систем безбедности прилагођен конкретној организацији. Али, чак и достигнут висок ниво безбедности је ствар тренутка, јер нове претње и технолошки напредак терају на стално преиспитивање и унапређење примењених мера, технологија и процедура.

Дигитално доба у којем живимо приморава не само организације, већ и сваког појединца да се са овим темама ухвати у коштац.

Информациона безбедност захтева ангажовање шире друштвене заједнице

Потребно је озбиљно приступити његовом решавању, а едукација је кључна и примарна област у којој треба деловати. У едукацију треба укључити све слојеве друштва, јер свако од нас, хтео то или не, у данашње време има додира са неком од информационих или комуникационих технологија. Непажљиво опхођење према личним и корисничким подацима приликом коришћења информационих и комуникационих система може довести до крађе идентитета, новца, пословних и других информација, па чак и до угрожавања живота. Због тога је са подизањем свести о опасностима које вребају у сајбер простору и едукацијом о правилима којих се треба придржавати потребно започети кроз школске програме раније и озбиљније него што је то случај у овом тренутку. На тај начин нове генерације ће се боље припремити за свакодневни нормалан живот у сајбер свету, а сваки појединац биће спремнији да прихвати правила понашања на свом радном месту.

Литература

1. William Stewart: Internet History: CSNET (Internet book), www.livinginternet.com, 2000.

2. William Stewart: Internet History: NSFNET (Internet book), www.livinginternet.com, 2000.
3. Peter J. Denning, Anthony Hearn, C. William Kern: History and Overview of CSNET, ACM SIGCOMM symposium on data communications, 8.-9. март 1983.
4. Barry M. Leiner (Research Institute for Advanced Computer Science), Robert E. Kahn (CNRI), Jon Postel (USC IS), Vinton G. Cerf (Google), Leonard Kleinrock (UCLA), Larry G. Roberts (Anagran), David D. Clark (MIT), Daniel C. Lynch (CyberCash), Stephen Wolff (Cisco): A Brief History of the Internet, ACM SIGCOMM Computer Communication Review 22 Volume 39, Number 5, октобар 2009.
5. Eugene H. Spafford: The Internet Worm Incident, Purdue Univesity, Department of Computer Science, 1989.
6. „Computer Intruder is Put on Probation and Fined", John Markoff, New York Times, 5. maj 1990.
7. PART I: A basic collection of good practices for running a CSIRT, ENISA, WP2007/2.4.9/1 (CERT-D3.1)
8. A step-by-step approach on how to setup a CSIRT, ENISA, Deliverable WP2006/5.1(CERT-D1/D2)
9. Webinar: The Kick Inside – Dealing with Threats from Within Your Firm, октобар 2015., https://www.infosecurity-magazine.com
10. Webinar: Addressing the Security Risks of Negligent Insiders , јул 2015., https://www.infosecurity-magazine.com
11. https://www.wombatsecurity.com/press-releases/new-ponemon-research-shows-wombat-delivers-roi