ИНФОРМАЦИОНА БЕЗБЕДНОСТ И ЗАШТИТА ТАЈНИХ ПОДАТАКА У ИНФОРМАЦИОНО-ТЕЛЕКОМУНИКАЦИОНИМ СИСТЕМИМА

Потпуковник *Марио Станковић,** мајор *Небојша Петровић,** потпуковник др *Ненад Димитријевић**

Интензивном применом информационих технологија које имају битну улогу у остваривању функција државних органа јављају се нови безбедносни ризици, који могу да доведу до угрожавања функционисања виталних система кроз деловање сајбер претњи. Због тога је неопходно континуирано унапређивати безбедност сајбер простора Републике Србије. Када су у питању подаци у електронском облику Република Србија је рад са тајним подацима у информационо-телекомуникационим системима уредила доношењем уредбе која прописује посебне мере заштите. Ова уредба дефинише и обавезе органа јавне власти и правних лица у току развоја и коришћења информационо-телекомуникационих система, ради одржавања њихове безбедности, а самим тим и безбедности тајних података.

* Аутори раде у Министарству одбране Републике Србије

Информациона безбедност подразумева очување тајности, интегритета и расположивости информација, а данас, у ери експанзије информационо-телекомуникационих система (ИТС), често је у употреби и термин информациона сигурност (Information assurance), који подразумева очување тајности, интегритета, доступности, непорецивости и аутентификације информација у сајбер простору.

Иначе, када је реч о безбедности информација, прво је настао појам комуникационе безбедности (COMSEC – *Communication Security*), са појавом рачунара настала је рачунарска безбедност (COMPUSEC – *Computer Security*), а касније се ова два појма обједињују у информациону безбедност (INFOSEC – *Information Security*).

Још увек не постоји јединствена (или опште прихваћена) дефиниција појмова информациона безбедност, сајбер простор, сајбер безбедност, сајбер криминал, сајбер тероризам, сајбер шпијунажа, сајбер ратовање. Полазиште за дефинисање ових појмова најчешће је америчка теорија информационог ратовања (*Information Warfare*).

Информациона безбедност данас поприма глобалне размере

Информациона безбедност примарно подразумева безбедност информација у ИТС, а секундарно безбедност рачунара (рачунарског система) и рачунарске мреже, чиме се посредно штите информације. Циљ информационе безбедности јесте заштита информационе имовине, односно заштита рачунара, рачунарских система, рачунарских програма и рачунарских мрежа ради очувања поверљивости, интегритета и расположивости информација.

Сајбер се дефинише као све што се односи на, или укључује, рачунаре или рачунарске мреже (као што је интернет). Сајбер простор често се поистовећује са интернетом. Међутим, он је више од тога и подразумева информациону имовину и друштвену интеракцију у оквиру мрежа. Међународна унија за телекомуникације (ITU *International Telecommunication Union*) под појмом „сајбер" подразумева системе и сервисе повезане било директно или индиректно на интер-

нет, телекомуникационе системе или рачунарске мреже. Међународна организација за стандардизацију (ISO – *International Standardization Organization*) под тим појмом подразумева комплексно окружење које резултира из интеракције људи, софтвера и сервиса на интернету и то посредством технолошких уређаја и мрежа са њима повезаним, који не постоји у било ком физичком облику.

Сајбер безбедност ИСО дефинише као очување тајности, интегритета и доступности информација у сајбер простору. ИТУ шире дефинише сајбер безбедност као колекцију алата, правилника, безбедносних концепата заштите, смерница, приступа у управљању ризицима, акција, обука, најбољих пракси, као и технологија које се могу користити ради заштите сајбер окружења, организација и корисничке имовине.

Сајбер одбрана, као појам, углавном се користи у војном контексту, али може се односити и на криминалне и шпијунске активности. НАТО дефинише сајбер одбрану као „способност да се осигура испорука и управљање сервисима у оперативним ИТС као одговор на потенцијалне, непосредне као и стварне злонамерне акције које долазе из сајбер простора".

Сајбер криминал се у домаћем законодавству дефинише кроз појам високотехнолошки криминал као вршење кривичних дела код којих се, као објекат или средство извршења кривичних дела, јављају рачунари, рачунарске мреже, рачунарски подаци, као и њихови производи у материјалном или електронском облику.

Сајбер тероризам – поље сајбер тероризма умногоме се поклапа са високотехнолошким криминалом или чак и са обичним тероризмом. У ужем смислу, сајбер тероризам представља са предумиш- љајем, политички мотивисан напад на информације, рачунаре, рачунарске системе, рачунарске програме и рачунарске мреже чији је резултат насиље над неборбеним (цивилним) циљевима од стране појединаца, група и/или

Пропусти у заштити информационих система могу имати несагледиве последице

организација. У ширем смислу, представља извођење нападних операција од стране појединаца, група или организација у сајбер простору искоришћавањем његових својстава које резултирају насиљем или претњом насиљем, ради стварања страха код власти државе и/или њених грађана, а све ради остваривања политичких или социјалних циљева.

НАТО дефинише сајбер шпијунажу као коришћење рачунарских система или информационих (информатичких) технологија да се нелегалним путем дође до поверљивих информација државе, приватног сектора или неке друге организације.

Сајбер ратовање представља облик асиметричног ратовања за који не постоји званична или генерално прихваћена дефиниција. Овај појам НАТО дефинише као борбене операције – обавештајне, нападне, одбрамбене, на високотехнолошком бојишту у којима супрот- стављене стране користе високотехнолошка средства, опрему и системе ради стицања предности за прикупљање, контролу и кориш- ћење информација. Више од 30 држава прихватило је доктрину и најавило развој специјалног програма офанзивних механизама сајбер ратовања. Према неким извештајима НАТО-а, око 120 земаља развија сопствене војне сајбер капацитете.

Република Србија је рад са тајним подацима у ИТС уредила доношењем Закона о тајности података, односно Уредбе о посебним мерама заштите тајних података у ИТС. Она дефинише и обавезе органа јавне власти и правних лица у току развоја и коришћења информационо-телекомуникационих система, ради одржавања њихове безбедности, а самим тим и безбедности тајних података који се у њима обрађују, чувају и преносе.

У овом раду дат је осврт на стање безбедности сајбер простора државних органа Републике Србије. Такође, предложене су мере за унапређење безбедности. Примена сваке од предложених мера – решења битно зависи од инфраструктуре којом се располаже, стручно- сти кадрова и финансијских могућности. Ни једно предложено решење само по себи не представља потпуну и довољну заштиту – по- требно је одабрати скуп оних која пружају баланс између сложености одржавања и нивоа заштите који је потребно постићи. У сваком тренутку треба имати у виду да је најслабија карика у сајбер простору управо човек. Овај рад има за циљ и да скрене пажњу на примере пропуста виђених у пракси и на тај начин допринесе смањењу грешака лица која битно утичу на функционисање система, а пре свега администратора ИТС.

СТАЊЕ БЕЗБЕДНОСТИ ИНФОРМАЦИОНО--ТЕЛЕКОМУНИКАЦИОНИХ СИСТЕМА ДРЖАВНИХ ОРГАНА

Информациона безбедност у Републици Србији још увек није на жељеном нивоу. Република Србија још увек није донела неопходна стратегијска и нормативна документа у области информационе и/или сајбер безбедности и једна је од малог броја земаља у Европи која није формирала национални тим за реаговање на рачунарске инциденте ЦЕРТ (CERT – *Computer Emergency Response Team*). Осим тога, проблем заштите информационе инфраструктуре представља и недостатак стручног кадра у тој области, недостатак неопходних техничких алата за одговор у случају напада, као и неумреженост са релевантним институцијама у окружењу.

Последица наведеног стања је неадекватна превенција у овој области. Са друге стране, нешто значајнији напредак остварен је у репресивном делу.

Са аспекта превенције значајно је то што је на националном нивоу препозната важност информационе безбедности, па је у Стратегији развоја информационог друштва до 2020. године читаво једно поглавље посвећено томе.

Стратегија посебно истиче неопходност унапређења правног и институционалног оквира, доношењем прописа којима ће се уредити стандарди и подручја информационе безбедности; надлежности и задаци појединих институција у овој области; формирање институције за послове верификације и сертификације метода, софтверских апликација, уређаја и система; истраживање и развој, као и формирање националног ЦЕРТ-а, с циљем да превентивно делује и координира решавање рачунарских безбедносних инцидената.

Значајна пажња посвећена је и борби против високотехнолошког криминала, као и научно-истраживачком и развојном раду у области информационе безбедности, што је, такође, у функцији унапређења стања информационе безбедности у земљи.

Израђен је Закон о информационој безбедности. Носилац израде било је Министарство за трговину, туризам и телекомуни- кације, а у посебној радној групи која припрема нацрт ангажована су и лица из више државних органа, академске заједнице и привредне коморе. Доношењем наведеног закона створио би се нормативни и институционални оквир за следеће области информационе безбедности у Републици Србији: акредитацију информационих система за рад са тајним подацима;

мере заштите информационих система који не садрже тајне податке; формирање националне институције за криптозаштиту; формирање националне институције за превенцију безбедносних инцидената у информационим системима; инспекцију поштовања примене мера информационе безбедности. Решења која овај закон нуди у складу су са решењима из Директиве Европске уније о заштити тајних података у информационим системима.

Област информационе безбедности делимично је уређена и *Законом о тајности података*, који дефинише посебне мере заштите ИТС. На основу тог Закона донета је *Уредба о посебним мерама заштите тајних података у ИТС*, а у Канцеларији Савета за националну безбедност и заштиту тајних података, која је уједно и национални безбедносни ауторитет за тајне податке, формирана је организациона целина за информациону безбедност.

Када се ради о репресивном делу, изменама и допунама Кривичног законика 2003. године, направљен је први значајан корак у кривично-правном уређењу борбе против високотехнолошког криминала. У КЗ су уврштена кривична дела из области безбедности рачу-

Законом о информационој безбедности побољшано је спровођење мераинформационе безбедности

нарских података. На основу искустава у примени тог закона, 2005. године донет је Закон о организацији и надлежности органа за борбу против високотехнолошког криминала, који је предвиђао формирање посебних државних органа са овом функцијом.

Такође, 2007. године извршене су и одговарајуће измене у другим прописима: Кривичном законику, Закону о кривичном поступку, Закону о посебним овлашћењима ради ефикасне заштите интелектуалне својине, као и другим законским и подзаконским актима у вези високотехнолошког криминала.

Органи за борбу против високотехнолошког криминала образовани су 2007. године, када је у оквиру МУП-а формирана посебна целина за борбу против високотехнолошког криминала.

Када се ради о сајбер одбрани битно је напоменути да је Канцеларија савета за националну безбедност и заштиту тајних података крајем 2012. године покренула иницијативу за израду концепта и стратегије сајбер одбране, али даље активности јиш увек нису започете.

РАЧУНАРИ ЗАПОСЛЕНИХ

Рачунари запослених, без обзира на то да ли садрже тајне податке или не, заслужују посебну пажњу. Најпре је потребно дефинисати програме и њихове верзије који се смеју користити на тим рачунарима. За употребу програма који се не налази на списку запослени може поднети захтев надлежном ИТ одељењу или администратору. На списку се никако не сме наћи програм, односно нека од његових верзија за који је познато да има велики број безбедносних пропуста.

Присуство антивирусног програма и заштитног зида (*Firewall*) неопходно је, за шта одлично решење представља бесплатни *Comodo Internet Security* или комерцијални *Kaspersky Internet Security*. Када се ради о бесплатним антивирусним програмима, попут *Avira, AVG, Avast* и *Panda,* они не представљају добро решење због тренутно ниског нивоа ефикасности.

Иако се рачунари запослених приликом приступа интернету обично налазе иза рутера, неопходно је на њима затворити све портове који нису неопходни, и обавезно потврдити успешност ове процедуре скенирањем одговарајућим програмом. Уколико пак одређени портови морају бити отворени, безбедност сервиса који их користе треба проверити алатом за скенирање. Поменуте провере треба спроводити из интранета и са интернета након сваке измене у конфигурацији програма рачунара и подешавању мрежних уређаја. У ИТС

од високе важности (нпр. који садрже тајне податке) провере треба спроводити чешће, ако је могуће и на дневном нивоу.

Опције за аутоматско ажурирање оперативног система треба да буду укључене на свим рачунарима корисника. За уобичајени рад са канцеларијским алатима за обраду текста и табела, у поређењу са *Windows* решењима, безбеднија за коришћење и знатно једноставнија за одржавање је нека *Линукс* дистрибуција и *Опен Офис*.

Код самосталних радних станица најважније је да обични корисници раде са налозима оперативног система ограничених права и могућности. Код *Windows* система такав налог онемогућује упис у *Program Files* и *Windows* директоријуме, што је најчешћи пут ширења вируса.

Програмски контролисана употреба УСБ портова треба да има превентивни карактер и има значајну улогу у спречавању крађе података од стране запослених, а препоручује се да ЦД/ДВД и *Флопи* уређаји физички ни не постоје. За приступ и размену датотека између запослених може се користити NAS (Network Access Storage) или, по потреби, мрежно дељење директоријума са рачунара корисника.

У институцијама високог значаја (одбрана, безбедност, правосуђе) сваком кориснику треба ускратити приступ интернету уколико му није неопходан. Тренутно, активности запослених у овим институцијама релативно је лако идентификовати на одређеним локацијама на интернету према ИП опсегу адресе и садржају *WHOIS* упита. До сада забележене активности огледају се у приступу играма, П2П размени садржаја који подлеже заштити од копирања (пре свега филмова), приступу интернет форумима и сл. Овакво понашање носи висок ризик од отицања информација, било циљаним нападом или ненамерним преузимањем злонамерних програма путем П2П мреже.

СЕРВЕРИ

Сервери електронске поште

Вероватно најлакши и најсигурнији пут за упад у рачунарски систем јесте *e-mail* сервер. Информациони системи који су у употреби изоловани су у интерне мреже, те им није могуће директно приступити са интернета. Због тога је електронска пошта највећи извор поверљивих информација до којих нападач може да дође. Употреба решења као што је *MDaemon* од стране више државних институција, и то старих верзија, битно нарушава безбедност садржаја.

Као најбоља решења у овој области намећу се *Postfix* (*UNIX*/*Linux* бесплатно решење отвореног кода са акцентом на безбедност) и *Microsoft Exchange Server* 2010 (комерцијално, скупо, једноставније за подешавање не и одржавање). У оба случаја посебну пажњу треба посветити и безбедности и ажурности самог оперативног система на којем се *и-мејл* сервер извршава, као и његовој стабилности у раду.

Без обзира на коришћено програмско решење, апсолутно је неопходно забранити приступ електронској пошти ван интерне мреже саме државне институције. Уколико је природа посла таква да захтева приступ е-пошти од стране већег броја запослених ван радног места, може се имплементирати ВПН (VPN *Virtual Private Network*) којем корисник приступа са посебно подешеног и обезбеђеног лаптоп рачунара, са хардверским или софтверским токеном.

Са аспекта безбедности система, коришћење POP3 протокола за пријем поште није безбедно, јер преноси податке преко мреже као чист текст без енкрипције. Успех код пресретања корисничког имена, лозинке и садржаја порука у хаб базираној мрежи (нпр. бежична мрежа) је 100%. Стога, намеће се употреба безбеднијих IMAPS и POP3S протокола и/или ВПН приступа.

За евентуалну удаљену администрацију сервера било које намене искључиво треба користити SSH тунеловање коришћењем јавног кључа за аутентификацију или, још боље, SSH кроз ВПН.

Такође, од изузетне важности је да се подразумеване лозинке за приступ свим мрежним уређајима промене!

Заштита информационих система на свим нивоима уз примену вишеструких технологија

Web сервери

У случају коришћења *Web* сервера, а ради спречавања ширења злонамерног кода и отицања података са других система, он треба да буде смештен на посебном хардверу или издвојеној виртуелној машини. Тиме се негативне последице напада на *Веб* сервер/презентацију неће одразити на перформансе и интегритет осталих сервиса. Нажалост, тренутно је дељење сервера између већег броја сервиса учестала пракса у државним институцијама и код ISP-а.

Оперативни систем на којем је сервер покренут мора бити редовно ажуриран најновијим закрпама, а сви портови осим неопходних (80 и евентуално 443) морају бити затворени. Ради већег нивоа безбедности, администрацију и ажурирање садржаја *Web* презентације треба обављати искључиво из локалне мреже. У до сада забележеним нападима које су најчешће извршавали тзв. албански хакери, мете напада су, после *Web* презентација, на другом месту били *Web* сервери домаћих ISP-а.

У случају употребе *Apache Web* сервера (најзаступљенији код нас), на интернету је доступно више упутстава за подешавање безбедносних опција, а препоручљиво је користити и *mod_securuty* модул. Овај модул филтрира све HTTP захтеве који су измењени ради извођења напада техником убризгавања SQL кода и XSS (*Cross Site Scripting*) напада и у великој мери их спречава.

DNS сервери

Најчешћи напади на DNS сервере имају за циљ преусмеравање саобраћаја на друге локације. Остали напади у овом домену огледају се у неовлашћеном трансферу DNS зоне и загушењима сервера ради ускраћивања услуге корисницима (Denial of Service).

Тренутно, BIND DNS сервер представља стандардно и одлично решење које примењују скоро сви ISP, мада је очигледан низак ниво заинтересованости администратора за његово напредније подешавање ради безбедности.

Када говоримо о државним органима може се закључити да Управа за заједничке послове републичких органа Владе Републике Србије, за разлику од скоро свих приватних ISP, квалитетно врши заштиту DNS сервера за gov.rs домене.

РАЧУНАРСКЕ МРЕЖЕ

Највећи број случајева крађе података обављен је изнутра или од заражених рачунара запослених злонамерним кодом који податке шаљу аутору. Овакви напади могу се ефикасно предупредити активним надзором локалне мреже. Мрежни администратор у свакој од државних институција морао би да користи неко софтверско решење за надгледање протока података у оквиру мреже и ка интернету. Такође, често је потребно пратити перформансе и статус сервера у мрежи. Запосленима је потребно забранити да приступају спољним адресама преко портова 443 (SSL) и 993 (IMAP), али и свим другим осим порта 80.

ИНТЕРНЕТ ПРЕЗЕНТАЦИЈЕ

CMS решења

Интернет презентације домаћих институција најчешће користе комерцијална и бесплатна CMS решења (*Joomla*, *Wordpress*, *BugAce*, *Drupal*). До сада су сви ови системи били подједнако успешно нападани, што због неадекватних лозинки и доступности страница за пријаву администратора, до неажурирања бесплатних CMS решења од стране администратора.

Употреба решења која нису написана ексклузивно за државне институције и која су распрострањена или доступна јавно није препоручљива уколико их администратор редовно не ажурира и одржава. У случају скромних захтева по питању функционалности, државна институција може користити класичне HTML странице чија би се интерактивност и модерни дизајн употпунио коришћењем *jQuery*.

Ради смањења информација о систему до којих нападач може доћи и отежавања приступа њима, изменама у изворном коду CMS-а треба прикрити верзију, назив и све друге податке које га идентификују.

Изнајмљивање ресурса и сервиса (Hosting)

Најчешће примењено решење за хостинг презентације институција је дељени hosting код домаћих ISP-а. Чињеница је да мали број

ISP-ова самоиницијативно предузима додатне мере заштите својих сервера и *Web* презентација на њима. Поред тога, општа карактеристика дељеног hosting-а је низак ниво безбедности због лаког ширења напада са рањиве презентације на остале на истом серверу, што код нас често експлоатишу албанске групе.

Презентације државних институција ни у ком случају се не смеју налазити на дељеном hosting-у нити серверима приватних ISP-а. Неопходно је издвојити посебан хардвер на којем би се оне извршавале, а због већег броја презентација финансијски адекватно решење била би виртуализација. У оквиру институције надлежне за њихово одржавање било би потребно оформити тим корисничке подршке за „објављиваче" садржаја презентација и тим за информациону безбедност.

Рачунари који се користе за администрацију и објављивање садржаја интернет презентација морају се користити само за ту намену и/или бити посебно заштићени.

Веома је чест метод крађе приступних лозинки са рачунара администратора путем тзв. *Keylogger* програма. Они се најчешће инсталирају на рачунар жртве кроз нелегалан или сумњив софтвер или жртвиним несвесним инсталирањем услед непажње. Поред тога, приступ датотекама на серверу се не сме вршити преко небезбедног FTP протокола, већ искључиво преко FTPS (*Wundows* или *UNIX server*) или SSH (*UNIX server*). Повезивање преко VPN везе је и овде препоручљиво.

МЕРЕ ЗАШТИТЕ ТАЈНИХ ПОДАТАКА У ИНФОРМАЦИОНО-ТЕЛЕКОМУНИКАЦИОНИМ СИСТЕМИМА

Република Србија је рад са тајним подацима у ИТС уредила доношењем Закона о тајности података, односно Уредбе о посебним мерама заштите тајних података у ИТС (Уредба). На самом почетку важно је објаснити кључне појмове на које се наведена уредба односи. То су појмови „тајни податак", „информационо-телекомуникациони систем" и „посебне мере заштите". Појам тајног податка одређује Закон о тајности података, према којем је тајни податак од интереса за Републику Србију који је законом, другим прописом или одлуком надлежног органа донесеном у складу са законом, одређен и означен одређеним степеном тајности.

Информационо-телекомуникациони систем означава било који систем који омогућава руковање подацима у електронском облику, а што нарочито обухвата сва средства потребна за функционисање система, укључујући рачунарске и комуникационе уређаје и инфраструктуру, софтверске ресурсе, организацију, особље и податке.

Коначно, „мере заштите" подразумевају мере које органи јавне власти и правна лица (у даљем тексту надлежни орган) предузимају како би тајни подаци који настају, чувају се и преносе у ИТС системима били сачувани од компромитовања, односно како их не би могла сазнати неовлашћена лица.

Уредба о посебним мерама заштите тајних података у ИТС дефинисала је:

– организационе и техничке мере заштите тајних података у ИТС;
– обавезу органа јавне власти да одреде овлашћена лица за упра вљање безбедношћу ИТС;
– услове које ИТС морају да испуне;
– безбедносни режими рада ИТС;
– потребу процене ризика безбедности ИТС;
– ISO 27001 као минимални стандард безбедности.

Дакле, посебне мере заштите тајних података у ИТС могу бити техничке и организационе. Техничке мере подразумевају примену свих метода, алата и знања која се употребљавају како би се тајни подаци заштитили од компромитовања. Организационе мере подразумевају такво устројство институција које располажу са ИТС, које омогућава ваљану заштиту тајних података у тим системима. Ове мере нису дате по принципу затвореног круга већ су дате карактеристичне мере техничке и организационе заштите тајних података у тим системима.

Као посебно значајне мере Уредбом је истакнута потреба примена криптозаштите када се подаци преносе изван безбедносних зона.

Уредба посебно третира и преносна ИТ средства. То има за последицу да се преносне меморије, дискете, ЦД-ови односно електронска и оптичка средства која се користе у ИТС такође сматрају тајним подацима. Пре њиховог коришћења за обраду, пренос и чување тајних података они морају бити проверени са аспекта могућег угрожавања (на пример, постојања злонамерног софтвера). Такве провере врше стручна лица, односно ако надлежни орган нема таква стручна лица провера се врши у органу који таквим лицима располаже. Њихово ангажовање врши се на основу међусобног споразума (на пример, уговор). Употреба приватних ИТ средстава за рад са тајним подацима је забрањена.

Поред наведених мера заштите у одредбама члана 6. Уредбе таксативно су наведени услови које ИТС мора да испуњава како би се у њему руковало тајним подацима.

Ради спровођења наведених мера надлежни орган дужан је да одреди овлашћено лице за управљање безбедношћу система. Дужности тог лица су да управља безбедношћу система, односно да прати и оцењује безбедносне карактеристике система. Уредба обавезује надлежни орган да приликом одређивања овлашћених лица за управљање безбедношћу система, обезбеде да једно лице не контролише све важне елементе безбедности система, као и да та лица поседују одговарајући сертификат за приступ тајним подацима. Такође, овлашћено лице за управљање безбедношћу система дужно је да прати и оцењује безбедносне карактеристике система.

Заштита преноса информација заузима посебно место у информационој безбедности

Техничке мере заштите

Техничке мере нарочито се односе на:

1) физичку заштиту објеката, простора, просторије, односно безбедносне зоне у којима се обрађују тајни подаци у систему, као и средстава и докумената из система (појам безбедносних зона у којима се обрађују тајни подаци уређује Уредба о посебним мерама физичко-техничке заштите тајних података. Тако, према одредби члана 2. став 1. наведене уредбе, тајни податак се чува, користи и обрађује у просторији, односно простору који је одређен као административна или безбедносна зона и има одговарајућу безбедносно техничку опрему, односно одговарајућа средства техничке заштите);

2) противпожарну заштиту (просторије у којима се чувају, користе, обрађују и уништавају тајни подаци обезбеђују се противпровалним и противпожарним системом, у сваком случају противпожарну заштиту

требало би обезбедити у складу са стандардима који уређују наведену област у Србији, као и на начин који ће омогућити да се тајни подаци сачувају по сваку цену и у случају у којем су исти угрожени пожаром);

3) обезбеђивање и заштиту опреме (избор одговарајуће и поузданe опреме, обезбеђивање опреме током њеног рада, редовно сервисирање и снабдевање резервним деловима) и докумената при њиховом коришћењу и чувању (ова одредба подразумева најпре да се опрема за обраду и чување података састоји од делова који су адекватни и од поузданог произвођача који обезбеђује њено функционисање током рада. Поред тога, то подразумева и адекватно обезбеђивање и заштиту и самих докумената који се користе у раду, односно који се у систему чувају);

4) заштиту програмске подршке (у фази пројектовања, развоја и коришћења програмског система). Програмску подршку, односно софтвер који се користи у систему требало би штитити у свакој фази, дакле у фази настанка, односно пројектовања и развоја за потребе система тако и за време његовог коришћења;

5) заштиту рачунарске мреже (приликом пројектовања и рада). Мрежа се штити како приликом пројектовања и инсталирања тако и приликом њеног рада.

Као техничку меру заштите можемо сматрати и одредбу Уредбе која говори о обавези заштите система од компромитујућег електромагнетног зрачења, а на основу процене ризика од тог зрачења.

Организационе мере заштите

Организационе мере нарочито се односе на сједињење људских и техничких потенцијала система који ће омогућити максималну заштиту тајних података и односе се на:

1) адекватну организацију технологије рада у систему при пројектовању. Пројектовање подразумева да се претходно изради студија којом се, поред осталог, утврђује и степен тајности података који се обрађују у систему и степен тајности самог система, идејног пројекта, главног пројекта, извођачког пројекта и увођења пројектованих решења, као и при оперативним раду система, што подразумева планирање рада и вођење евиденција о извршавању свих поступака у раду система и кретању документације;

2) утврђивање поступака у случају ванредних околности (то је најбоље учинити на основу Методологије израде Плана заштите тајних података за ванредне и хитне ситуације која је у надлежности Владе Републике, Србије);

3) остале услове за успешно функционисање система, при чему доносилац уредбе указује да то могу бити контрола приликом заснивања радног односа (на пример вршење одговарајућих безбедносних провера, утврђивање послова и задатака учесника у раду система и с тим у вези утврђивање степена тајних података са којима ће имати везе на одређеном радном месту, стручна обука запослених у вези са мерама заштите тајних података и др.).

Као организациону меру заштите можемо сматрати и одредбу Уредбе која инсистира да сва инсталирања у систему, која се односе на уређаје и на програме, врши једино овлашћено лице. То је, у крајњем, лице које поседује одговарајућа знања као и сертификат за приступ тајним подацима највишег степена тајности у конкретном систему.

Одржавање ИТС система

Уредба предвиђа да ИТС може да ради у једном од три безбедносна режима које Уредба означава као: неселективни, селективни и са више нивоа. Безбедносни режим подразумева одређивање лица која имају приступ тајним подацима, што је ближе објашњено у одредбама члана 8. Уредбе. Важно је нагласити да безбедносни режим рада ИТС одређује руководилац, односно одговорно лице у надлежном органу.

Одржавање безбедности система подразумева:

1) периодичну проверу система, свих његових делова и медија за чување и пренос тајних података, као и сагледавање достигнути услова за обезбеђење поверљивости, расположивости, интегритета и аутентичности тајних података у систему односно стално контролисање функционисања система;

2) чување података који се односе на систем, као и тајних података који се обрађују у систему на посебним документима, уз обавезно вођење резервних евиденција и примену мера заштите које су предвиђене за податке са највишим степеном тајности података који се налазе у систему (другим речима заштита тајних података о самом систему као и оних који се у систему обрађују и чувају);

3) инсталирање хардвера, софтвера и конфигурисање система од стране овлашћених лица (то подразумева да хардвер, софтвер и конфигурисање система не врше само овлашћена лица већ и лица која поседују сертификат за приступ тајним подацима одговарајућег степена тајности);

4) примењивање нових техничких и програмских средстава у систему у складу са одговарајућим техничким стандардима SRPS ICO/IEC 27001:2011 (овде се инсистира на томе да се у примени техничких и програмских средстава не сме ићи испод назначених стандарда);

5) сервисирање и поправку средстава из система на начин који не нарушава безбедност система (дакле сервис и поправка не смеју ни на који начин довести у питање тајне податке у том систему, као и тајност података који се односе на сам систем);

6) контролни преглед на средствима из система која су била на сервисирању и поправци изван органа јавне власти, односно правног лица од утицаја компромитујућег електромагнетног зрачења од стране стручних лица (надзор на сервисираним и поправљеним средствима је у функцији онемогућавања компромитовања тајних података у систему, као и тајних података који се односе на систем);

7) одговарајући поступак приликом неовлашћеног откривања тајности документа или губитка документа који садржи тајни податак (тај поступак подразумева предузимање мера дисциплинске и кривичноправне природе према лицима која су одговорна за компромитовање тајних података);

8) одговарајући поступак приликом откривања упада у систем (ово подразумева да постоје јасне и унапред одређене процедуре које се примењују у наведеним случајевима и имају за циљ да на најмању меру сведу штете по тајне податке од неовлашћеног упада у систем);

9) планирање мера безбедности у случају ванредних ситуација (то је у складу са Методологијом за израду Плана заштите тајних података у ванредним и хитним ситуацијама).

У одржавање безбедности ИТС можемо сврстати и одредбе које говоре о односу према носиоцима података (меморијски медијуми и модули). Тако, када се ради о тајним подацима степена „ДРЖАВНА ТАЈНА" и „СТРОГО ПОВЕРЉИВО" они се морају уништити након истека рока њихове употребе или након истека рока употребе система у којем су се користили, у складу са одредбама уредбе о посебним мерама физичко-техничке заштите тајних података.

Сервери захтевају посебне мере заштите

Према тим одредбама, тајни подаци, копије, радни нацрти, белешке, као и подаци који су физички оштећени и не могу се даље користити, осим тајних података стране државе и међународне организације, уништавају се на начин да се не могу препознати и обновити (хемијским разлагањем, спаљивањем, дробљењем и др.).

У случајевима у којима правно лице пружа услуге органу јавне власти које подразумева да се правно лице користи тајним подацима органа јавне власти, могуће је да дође до ситуација у којима је неопходно потребно да се повежу ИТС тих субјеката. Сматрамо да је форма у којој се споразум закључује уговор, али да треба да му претходи процена пре свега руководиоца органа јавне власти, у односу на то у којој би мери то повезивање угрозило сам систем органа јавне власти, односно заштиту тајних података. Такође, уговор би требало да укључи и мере заштите од компромитовања тајних података, било позивањем на одредбе ове уредбе и Уредбе о посебним мерама физичко-техничке заштите тајних података или и посебне аранжмане, односно мере, у зависности од специфичности сваког појединог уговарача и њихових потреба.

ПРОЦЕНА И УПРАВЉАЊЕ РИЗИКОМ У ИНФОРМАЦИОНО-ТЕЛЕКОМУНИКАЦИОНИМ СИСТЕМИМА

Надлежни органи могу користити ИТС само ако је испуњен услов који се састоји у томе да је потребно да се пре тога изврши процена могућег угрожавања безбедности тајних података од упада у систем, као и процена угрожавања употребе и уништавања тајних података који су обрађени и сачувани у систему (у даљем тексту процена ризика).

Процена ризика

Елементи процене ризика по безбедност система су следећи:

– утврђивање ризика,

– процена ризика који се не могу избећи,

– процена угрожености система,

– претње и могуће последице реализације претњи за систем, укључујући и ризике у вези са окружењем у којем се систем користи.

Процена ризика по безбедност система обухвата временски, плански и организациони фактор. Наиме, процена ризика се врши периодично (временски фактор), али обавезно у складу са планом за процену ризика система (плански фактор), који доноси руководилац, односно одговорно лице надлежног органа (организациони фактор).

Процена ризика безбедности система обавезна је за систем у којем се обрађују, преносе и чувају тајни подаци степена тајности од „ДРЖАВНА ТАЈНА" до „ПОВЕРЉИВО".

Када се ради о систему у којем се обрађују тајни подаци који су означени степеном тајности „ИНТЕРНО", надлежни орган обезбеђује одржавање одговарајућег нивоа безбедности тајних података (тајности, целовитости, аутентичности или доступности), у складу са прописима којима се уређује информациона безбедност. Међутим, сматрамо да ће надлежни орган често и за ове системе сачињавати процену ризика безбедности. У сваком случају, проверу спровођења нивоа безбедности система у којем се обрађују тајни подаци који су означени степеном тајности „ИНТЕРНО" врши надлежни орган, односно овлашћено лице за управљање безбедношћу система.

Смањењем ризика спречава се губитак и неовлашћени приступ тајним подацима

Поред обавезе вршења процене ризика, постоји и обавеза доношења акта којим прописује безбедносне процедуре, односно безбедносни поступак који се односи на: пријем, обраду, пренос, чување и архивирање тајних података у електронском облику, као и чување пројектне документације (прелиминарне студије о развоју система, идејни пројекат, главни пројекат и извођачки пројекат).

Управљање ризиком

Управљање ризиком је појам који, према ставу 1. члана 24. Уредбе, обухвата следеће материјалне елементе:

– трајно процењивање ризика (који су то ризици који могу угрозити тајност података у систему)

– обраду ризика (након уочавања ризика дати адекватан одговор како би се спречило њихово дејство на систем),

– циљ управљања ризиком безбедности (што подразумева спречавање уништења, отуђења, губитка и неовлашћеног приступа тајним подацима).

Формални елемент управљања ризиком је одлука о управљању ризиком безбедности система.

Обрада ризика представља активност у којој се за сваки процењени ризик утврђује степен прихватљивости ризика, ради његовог прихватања, смањења или избегавања. Ризик се сматра прихватљивим

ако би настала штета била мања од штете која би настала услед неспровођења безбедносних мера. Појам штете требало би посматрати у смислу одредбе члана 2. тачка 9. Закона о тајности података према којима је штета нарушавања интереса Републике Србије настала као последица неовлашћеног приступа, откривања, уништавања и злоупотребе тајних података или као последица друге радње обраде тајних података и страних тајних података.

Смањивање ризика подразумева примену безбедносних мера, којима је циљ спречавање уништења, отуђења, губитка и неовлашћеног приступа тајним подацима (спречавање компромитације тајних података).

Избегавање ризика подразумева предузимање мера, ради избегавање радњи које би могле изазвати ризик.

После доношења одлуке о управљању ризиком надлежни орган доноси акт о обради ризика којим се утврђује спровођење потребних безбедносних мера, односно процедура. Елементи за наведену одлуку дати су у одредбама чланова 25. и 26. Обавеза је надлежних органа да резултате процењивања и обраде ризика редовно ревидирају, при чему се то чини:

– у складу са потребама или

– на основу насталих унутрашњих или спољашњих промена система.

ЗАКЉУЧАК

Уколико је потребно изнети процену тренутног стања безбедности сајбер простора државних институција Републике Србије, у овом тренутку она би била између довољан и добар. Разлог за то лежи у многобројним пропустима који су довели до отицања података и „обарања" интернет презентација. Ипак, сви до сада забележени пропусти отклањани су у кратком року, што је похвално.

Међутим, боље решење од брзе реакције и сталног санирања последица је квалитетна превентива. Уредба о посебним мерама заштите тајних података у ИТС дефинише мере заштите тајних података и уједно корисника тих система.

У примени мера информационе безбедности требало би се искључиво ослањати на сопствене капацитете за деловање у сајбер простору, односно заштиту свог сајбер простора, које треба развија-

ти, проширити и ојачати, уз истовремено развијање сарадње у овој области на регионалном и глобалном нивоу. С тим у вези, сматрамо да би приступ у сајбер одбрани требало да буде одбрамбени из којег ће произићи и способности за офанзивни приступ.

Најзначајније људске и материјалне ресурсе за сајбер одбрану требало би да имају Министарство одбране, односно Војска Србије, МУП и службе безбедности (ВБА и БИА). Након дефинисања нормативних оквира сајбер одбране и одређивања критичне информационе инфраструктуре, ресурсе за сајбер одбрану требало би да имају јавне и приватне институције (нпр. Електропривреда, НИС, Телеком и други оператори електронских комуникација, железница, контрола летења, аеродроми, хитне службе, водоснабдевање, грејање, здравствене установе, финансијске установе, индустрија итд.), али и академске институције и специјализовани привредни субјекти из области информационих технологија, посебно информационе безбедности. Истовремено, изградња наведеног концепта требало би да утиче на подизање нивоа свести о сајбер безбедности.

Један од најважнијих предуслова за стварање одрживог концепта сајбер одбране је константно образовање и усавршавање кадра, због чега би требало предвидети мере за образовање и унапређење свести, како припадника система одбране, тако и целокупног друштва. Истовремено је неопходно иновирање и проширење наставних планова и програма у области информационе и сајбер безбедности и покретање научних пројеката за изградњу електронских система, технологија и решења у области сајбер безбедности.

На основу наведеног, на нивоу Републике Србије требало би предузети следеће активности:

– донети националну стратегију информационе безбедности и сајбер одбране;

– донети закон о информационој безбедности и друга подзаконска акта, којим би се регулисало постојање потребних државних тела и процедура у информационој безбедности;

– формирати национално тело за координацију сајбер одбране Републике Србије;

– дефинисати оквир за јавно-приватно партнерство у сајбер одбрани (ову улогу би требало да има министарство задужено за информационо друштво);

– формирати национални ЦЕРТ који би се бавио генералном превенцијом;

– формирати национални орган за криптолошку безбедност и заштиту од компромитујућег електромагнетног зрачења;

– формирати централно тело за планирање, имплементацију и превенцију безбедности информација у државним органима (ЦЕРТ државних органа);

– унапређивати наставне програме на свим нивоима школовања, са темама из информационе безбедности;

– унапређивати кадровске и материјалне капацитете постојећих институција, пре свега за борбу против високотехнолошког криминала;

– доследно примењивати одредбе Закона о тајности података и подзаконских аката донетих на основу овог закона и будућег закона о информационој безбедности.

Литература

1. IT Security Guidelines, BSI Germany, 2007.
2. Ruth A., Hudson K., Sertifikat Security+, Microsoft press, 2003.
3. Интернет презентације произвођача безбедносних програма и опреме
4. Службени гласник Републике Србије, број 53/11
5. Службени гласник Републике Србије, број 104/09
6. Службени гласник Републике Србије, број 97/11
7. Службени гласник Републике Србије, број 53/11
8. Синковски, С., Лучић, Б., „Информациона безбедност", Зитех, 2006.
9. Wamala F. „The ITU national cybersecurity strategy guide", ITU, 2011.
10. European Commission, „Cyber security Strategy of the European Union", 2013.
11. ITU „Cyber security Guide for developing countries", 2009.
12. Goodwin C.F., „Developing National Strategy for Cyber security", Microsoft, 2013.
13. ISO/IEC 27001:2005
14. ISO/IEC 27032