Систем управљања сигурношћу информација

У. Кондић,¹ Х. Анђелски²

System of Managing Health Safety of Informations

U. Kondic, H. Andjelski

Сажетак. *Превенција, као један од елемената управљања ризицима којима су изложене информације, подаци, може се посматрати као успостављење и примена поступака, процедура и алата у сврху детекције и спречавања нежељеног и неконтролисаног приступа информацијама, њихове неконтролисане обраде, уништавања, мењања садржине, злоупотреба, остваривања противправне користи, кроз нарушавања постулата сигурности информација.*

Сигурност информација се базира на три постулата сигурности и то: интегритет, поузданост, расположивост и на постојању елемената: непорецивости, доказивости, аутентичности и следивости.

Како су наведени постулати и елементи сигурности карактеристични за имовину, добра, неопходно је прихватити и посматрати информацију као имовину, заправо информационо добро.

Истовремено, како је за сваку имовину везан појам власништва, потребно је посебну пажњу посветити власништву над информацијама.

Правила, која дефинишу превенцију, саставни су део политике сигурности информација. Истовремено, политика сигурности предвиђа могућност успостављања система за детекцију напада и нарушавања постулата сигурности. Детекција и анализа реализованог напада захтевају регистровање што већег броја информација о: рањивостима, претњама, нивоима ризика, мера, инцидента и, исто тако, поступака, процедура, статистичких података рачунарских записа, података и информација који могу да

Summary. *The prevention, as an element of information and data risk managing, can be observed as restoring and applying of methods, procedures and tools for detection and obstruction of undesired or uncontrolled access to informations, their uncontrolled processing, destruction, changing, abusing, realization of illegal benefit – through disturbing of basic elements of information safety.*

Basic elements of safety are: integrity, reliability and availability.

The rules that define prevention are integral part of information safety politics. At the same time, the politics of safety anticipates possibility of restoring of system for detection of attack and disturbing of basic safety elements. Detection and analysis of the attack require to register great number of procedures, data and informations which can serve as proof elements for incident, but at the same time as proof elements for committer or cause of the incident.

The elements of information safety are: undeniability, proofability, authenticity, continuity.

Key words: *safety politics, basic safety elements, risks, incidents.*

¹ Урош Кондић, COMTEL D.O.O., Београд.

² Христо Анђелски, Градски завод за јавно здравље Београд.

послуже као елементи доказивости да је дошло до извршења дела, инцидента, али истовремено и као елементи утврђивања починиоца или узрочника инцидента.

Како у свим сферама у којима су присутни претње и ризици, постоји могућност преноса ризика на треће лице, то се поставља отворено питање да ли постоје релевантни елементи и фактори за увођење новог вида осигурања, осигурање сигурности информација.

Кључне речи: информација, политика сигурности, постулати и елементи сигурности, рањивости, претње, ризици, мере, инциденти, системски записи, власништво над информацијама, осигурање сигурности информација.

Увод

Политике сигурности информација (СИ) и њихове примене јесу основ, не само сигурности информација него и поузданости и управљања ризицима које собом носе информациона добра, а увећавају информационо-комуникационе технологије без којих се не може замислити функционисање модерних организација. Као такве, предмет су разматрања, размишљања и питања: да ли су довољно разумљиве; да ли су примењиве и прилагодљиве дневним потребама и дневним променама; да ли су дефинисане и креиране тако да буду прихваћене на лак и одговарајући начин; да ли су корисници информационе технологије (ИТ) упознати са политиком сигурности; да ли је ниво спознаје корисника довољан и да ли су свесни места и улоге политике сигурности; да ли се корисници придржавају правила организованости и функционисања који проистичу из препорука и процедура дефинисаних политиком сигурности?

Као такве су и темељ информисању друштва.

Са информатичког аспекта, сигурност информација је критична компонента управљања приступом локацији, месту, адреси, где се информације налазе у датом тренутку; начином обраде и коришћења информација са аспекта

контроле и управљања ризицима нарушавања, заправо управљања рањивостима које доносе информациона добра.

Постулати и елементи сигурности информација

Основни постулати сигурности информација су:

- **поверљивост:** постојање елемената који указују на потребу да информације, процеси и подаци не буду откривени, да не буду стављени на располагање лицима која на то немају право, нити имају овлашћења, или која покушавају да до њих дођу на недозвољен и противправни начин; **интегритет:** постојање елемената који указују на потребу да се на информацијама, процесима и подацима не могу вршити промене од стране неовлашћених лица или се не могу вршити на начин који није подложен контроли и надзору;
- **расположивост:** постојање елемената који указују на потребу да приступ информацијама, процесима и подацима буде омогућен, у датом тренутку, онима који на то имају право или су им дата права и овлашћења, сходно утврђеним правилима и усвојеним процедурама; уз уважавање присуства елемената;
- **аутентичност:** постојање елемената који указују на потребу провере идентитета лица заинтересованих за приступ информацијама,

информационим добрима, са предвиђеном намером;

- **непоречивост:** постојање елемената који указују на потребу постојања елемената који елиминишу могућност порицања, негирања да је нека активност, неки корак учињен, а односи се на информацију, информационо добро;
- **доказивост:** постојање елемената који указују на потребу постојања елемената којима се могу пратити и регистровати активности субјеката, а односе се на извршене радње по питању информација, информационих добара;
- **следивост:** постојање елемената који указују на постојање трагова о начину извршеног, урађеног дела које се односи на информацију, информационо добро, без обзира на форму у којој се налазе информације.

Постоји више узрочно-последичних веза које указују на могућности угрожавања поступата сигурности информација. То су, између осталог:

- **Одобрен приступ, одобрено коришћење** – остварен сходно дефинисаним идентификацијама, дозволама и дефинисаним правима и правилима који су саставни део политике сигурности – од стране особа које имају право приступа на бази дефинисаних и постојећих норми легалитета и легитимитета;
- **Одобрен приступ, одобрено коришћење** – остварен коришћењем дефинисаних норми легалитета и легитимитета, дозволама и дефинисаним правима и правилима који су саставни део политике сигурности – од стране особа која немају право коришћења истих;
- **Неодобрен приступ, није дозвољено коришћење** – противправни, противзаконит и недозвољен приступ, у сврху нарушавања поступата сигурности информација;
- **Непредвиђен случај** (нестанак напона, пожар, вода, ...) – неконтролисано уништавање имовине (информационог добра) на којем се налазе информисања и то;
- **писана документација** – уговори, упутства, документација општег типа, документација која садржи важне и поверљиве пословне резултате (информације или податке);

- **софтверске компоненте** – апликације; системски програми; развојни алати и алатке;
- **физичке компоненте** – компјутери и комуникациона опрема; магнетни медијуми (касете и дискови); друга техничка опрема (напајања, агрегати, клима уређаји), намештај;
- **средства везана за податке** – базе и фајлови са подацима, системска документација, упутства за кориснике, материјали за обуку, оперативне процедуре и процедуре за подршку, планови континуитета пословања;
- **људски фактор** – оперативно особље пословног лица, корисници;
- **продукти неког уложеног рада** – неки производи информације.

Информациона добра

- Информациона добра су елементи и компоненте информационо-комуникационог система и система, услуге, дистрибуције и реализације на тржишту;
- **психолошки елементи** (заштитни знак, ауторско дело, углед, поверење, репутација).

Како су, као што је већ напоменуто, информациона добра носиоци рањивости, а самим тим и потенцијални узрочници претњи и ризика реализовања претњи, управљање сигурношћу информација своди се на управљање сигурношћу информационих добара.

Сигурност информационих добара, изражена кроз основне постулате сигурности, кључни је фактор сигурности информација..

Власништво над информацијама

Како је информација, по напред изреченом, саставни део фамилије имовине, нема разлога да се власништво над информацијама не дефинише сходно дефиницијама власништва над било којом имовином, са пратећим правима и одговорностима које се односи на власништво.

Пренос на треће лице, нови видови осигурања

Исто тако, ако је информација имовина, а јесте, нема разлога да се по узору на осигуравање од ризика, која се односе на било коју имовину, не дерфинише и не уведе осигурање које се односи на сигурност информација.

Елементи система управљања сигурношћу информација

Издизање нивоа сигурности информација, сходно ISO/IEC 27000 фамилији стандарда, базира се на два кључна сегмента:

Организациона подршка која се заснива на дефинисању и успостављању управљачко-организационе структуре, одлучности примене политике сигурности информација и, сходно истој, дефинисању процедура, препорука, мера контрола, надзора и одређивања стриктних задужења и одговорности сваког појединаца за било који сегмент сигурности информација;

- Успостављање система управљања сигурношћу информација, који се ослања на скуп разумљивих информација прикупљених на основу праксе и позитивних искустава, врши контролу и надзор успостављене организованости и њеног функционисања, уз могућност надградње и прилагођавања новонасталим ситуацијама.
- Како је организованост, увођење и примена организационо-техничких мера увелико блиска окружењу и пословном свету, у даљем тексту ћемо акценат ставити на систем управљања сигурношћу информација.

Систем управљања сигурношћу информација се базира на класификацији и дефинисању основних елемената и то: рањивости; претње; нивои ризика; мера за снижавање нивоа реализација претњи; инцидената; процедура реаговања на спречавање извршења претњи.

Основни елементи, између осталог, јесу дефинисани и изражени кроз:

- Табелу извора рањивости везаних за информациона добра, поступке,

- Табелу претњи, сходно присутним рањивостима,
- Табелу нивоа ризика, који могу да произађу из претњи, уколико се стекну адекватни услови реализације,
- Табелу мера сигурности, превентивних и корективних, а планираних и предвиђених, сходно природи и нивоу ризика, вероватноћи реализације претње, финансијских ефеката улагања и финансијских ефеката изражених кроз негативне последице у случају реализације претњи,
- Табелу инцидената, реализованих претњи као последица деструктивних радњи и угрожавања постулата сигурности информација,
- Табелу процедура реаговања на инциденте и предузимање корака обезбеђивања континуитета функционисања, пословања,
- Табеле статистичких информација добијених из записа, журнализације, који се води на нивоу система, за потребе утврђивања извршиоца или узрочника инцидента, инцидентне радње.

Табеле су саставни део релационе базе која омогућава директан приступ систему за потребе: уноса и обраде информација и података везаних за рањивости, претње, ризике; мере и инциденте; реаговања на инциденте и континуитет пословања; контроле и надзора од стране надлежних институција и појединаца, али и упита и увида о стању система од стране руководеће структуре.

Дијалог са системом води се преко десктопа.

Тиме се омогућава:

- да информације система буду расположиве корисницима информационо-комуникационог система, сходно природи посла, правима и обавезама, али и одговорностима и ограничавајућим факторима дефинисаним политиком сигурности информација,
- да систем буде расположив за било коју врсту контроле, надзора и управљања елементима сигурности информација, од стране дефинисаних и предвиђених институција и појединаца, остручених у ту сврху.

Национална стратегија сигурности информација

Потреба дефинисања, доношења и усвајања **Националне стратегије сигурности информација** – као основице дефинисања и спровођења политике сигурности информација и успостављања система управљања сигурношћу информација, на бази домаћих знања и искустава, а у духу међународног ISO/IEC 27001:2005 стандарда, разматрана је на научно-стручном форуму: Сигурност информација, злоупотребе информационих технологија – СИЗИТ 09, који је одржан у Институту „Михајло Пупин“ у Београду, од 1. до 2. јула 2007. године, под покровитељством Министарства за телекомуникације и информационо друштво.

Организатори Форума били су: Институт „Михајло Пупин“, Удружење ИТ Ревизор и Comtel. Форуму су присуствовали представници Министарства одбране, Министарства за унутрашње послове, Криминалистичко-полицијске академије, Министарства спољних послова, Министарства за здравље, Градског завода за јавно здравље, Акредитационог тела за Србију, Ауторске агенције за Србију, Српске православне цркве, Електротехничког факултета Универзитета у Београду, РАТЕЛ-а, Републичког јавног тужилаштва, Окружног јавног тужилаштва, Општинског јавног тужилаштва, Компаније Дунав осигурање, Удружења банака Србије, Института „Михајло Пупин“, Удружења ИТ Ревизор, Информатике а.д., Comtela. Генерални спонзор Форума била је Компанија Дунав осигурање а.д.

Стварање платформе успостављања политике сигурности информација јесте добра основа за хармонизацију и усаглашавање са међународним стандардима, у сврху обезбеђивања предуслова сигурности информација и борбе против манипулација, злоупотреба и криминогених радњи које доносе информационе технологије.

На Форуму су биле обухваћене следеће теме: *Сигурност информација* (шта је сигурност информација, како издићи ниво сигурности информација), *Политика сигурности информација* (шта је политика сигурности информација, место, улога и одговорности организационе структуре по питању сигурности информација), *Међународни*

стандарди (фамилија ISO/IEC 27000 стандарда, други релевантни стандарди), *Искуства и праксе које указују на присуство злоупотреба и криминогених радњи*, *Место и улога класификације информација*, *Модалитети издизања нивоа сигурности информација* (глобалне мреже, манипулације, претње, ризици, финансијски ефекти, мере, организационо-технички и технолошки кораци и мере, праксе и позитивна искуства, едукација, издизање нивоа спознаје), *Правни аспекти и усаглашавање са законско-правним регулативама*, *Реаговање на инциденте и континуитет пословања* (база знања – регистровање познатих претњи, ризика, мера, планови рада у ванредним околностима, успостављање центра за обраду инцидената, рањивости и дефинисање ризика).

Полазећи од императива правовременог сагледавања проблематике сигурности информација, праћења светских збивања и предузимања корака припадности пословном свету, садржајност и рад Форума изражени су и дефинисани кроз Закључке Форума који су дати у Прилогу.

Прилог

Научно-стручни форум СИЗИТ 09 - Закључци

Полазећи од императива правовременог сагледавања проблематике сигурности информација, праћења светских збивања и предузимања корака припадности пословном свету, неопходно је иницирање доношења и дефинисања:

1. Националне стратегије сигурности информација.
 - 1.1. Национална стратегија треба да се базира на међународним и домаћим искуствима и позитивним праксама уз усаглашавање са међународним стандардима, домаћом правном регулативом, као и са међународним правом;
 - 1.2. Усклађивати дефиниције кључних појмова, као што су: место, улога и значај информација, карактеристике сигурности информација, модели класификације ин-

формација, власништво над информацијама и одговорности које следе, сходно основним карактеристикама сигурности информација (елементи кодификације, шифарника, основних елемената управљања сигурношћу информација: рањивости, претње, мере, инциденти);

- 1.3. Донети стандарде на српском језику који се односе на систем управљања сигурношћу информација (фамилија ИСО/ИЕЦ 27000 стандарда);
- 1.4. Стварати потребне услове, односно донети одговарајућа законска решења која ће прописати давање сертификација за: имплементацију елемената сигурности информација, издизања нивоа спознаје о месту и улози сигурности информација, примењених елемената сигурности информација, односно успостављеног система управљања сигурношћу информација, од стране акредитованих сертификационих тела.
2. Основе за увођење новог вида осигурања (пренос на треће лице), који се односи на сигурност информација.
3. Појмовника информационих технологија — једнозначност дефинисања значења појмова на српском језику (консензус). Дефиниције

значења појмова треба да буду усаглашене са дефиницијама значења са светским језицима и међународним стандардима који се односе на сигурност информација.

4. Основе за формирање фонда за промоцију потребе и оправданости примене елемената сигурности информација сходно карактеристикама сигурности и међународним стандардима.
5. Основе за дефинисање институције *ИТ ревизор* и, сходно томе, *Судски вештак за ИТ*.
6. Основе за одређивања институције за едукацију, оцену и сертификацију *ИТ ревизора* и *Судских вештака за ИТ*, сходно законској регулативи, компонентама и елементима сигурности информација
7. Јавних расправа по областима интересних групација (здравство, просвета, финансије, царина, банкарство, државне институције...) о месту и улози сигурности информација сходно потребама, искуствима и позитивним праксама.
8. Одлуке о једногодишњем одржавању Форума СИЗИТ, са могућношћу укључивања представника и институција земаља у региону, а по питању основне проблематике сигурности информација.