Место и улога сигурности информација: модел управљања сигурношћу информација – намењено власницима информација

Х. Анђелски¹, В. Ђерковић², У.Кондић³

Place and Role of Information Security: Information Security Management Model - For Owners Information

Hristo Anđelski, Veljko Đerković, Uroš Kondić

Сажетак: Дугогодишње искуство у раду на пољу приступа информацијама и схватања места и улоге њихове сигурности уверава нас да многи прописи, многа законско-правна регулатива и многи закони, који се односе на исте, нису донети на адекватан начин.

Приступ проблематици се у највећем броју случајева односио на имплементације међународних ISO/IEC 27001 стандарда.

Кроз процедуре, протоколе и препоруке заговарају потребу дефинисања мера сигурности, чијом применом се снижава ниво ризика угрожавања сигурности, врше контроле и надзори мера ефикасности, као и прилагођавања, сходно променама које утичу, или могу да утичу, на сигурност информација.

Само један интегрални, свеобухватни, холистички приступ изналажења начина дефинисања конкретних мера сигурности може дати стварни допринос издизању нивоа сигурности информација. Такав приступ, користећи праксу и позитивна искуства, уважавајући препоруке, протоколе и процедуре међународних стандарда и директиве ЕУ, резултира моделом управљања сигурношћу информација, који инсистира на практичним применама процедура, препорука, прописа и њиховом безрезервном поштовању у реалном времену, уз присуство високог степена одговорности.

Кључне речи: сигурности информација: модел управљања сигурношћу информација - намењено власницима информација.

Summary: Many years of experience working in the field of information and understanding of the place and role of their security, assures us that many regulations, many legal-regulatory framework and many of the laws relating to the same, did not bring in an adequate manner.

Approach to the problem in most cases related to the implementation of the international ISO / IEC 27001 standard.

Procedures, protocols and recommendations advocate the need to define measures of safety, the application of which lowers the risk of endangering safety, exercise control and supervision measures of efficiency and ability to adjust according to changes that affect or may affect the safety information.

Only one integrated, comprehensive, holistic approach to finding ways of defining specific security measures, can make a real contribution to the elevation of the level of information security.

Such an approach, using the practices and positive experiences, taking into account the recommendations, protocols and procedures of international standards and EU directives, resulting in a model of information security management, which insists on the practical applications of procedures, recommendations, regulations, and their unqualified respect in real time, with the presence of a high degree of responsibility.

Key words: information security, information security management model, owners information.

1 Доц. др Христо Анђелски, Стоматолошки факултет Панчево.

2 Прим. др Вељко Ђерковић, Градски завод за јавно здравље, Београд.

3 Урош Кондић, ИТ Ревизор, Београд.

Увод

Дугогодишње искуство у раду на пољу приступа информацијама и схватања места и улоге њихове сигурности уверава нас да многи прописи, многа законско-правна регулатива и многи закони, који се односе на исте, нису донети на адекватан начин. Као такви су тешко разумљиви, прихватљиви и готово неприменљиви у пракси. Овде мислимо на информације опште форме и карактера, независно од садржајности, вредности, значења, на проблематику угрожавања њихове сигурности, као превенције и саставног дела злоупотреба и криминогених радњи које прате информационо-комуникационе технологије. Приступ проблематици се у највећем броју случајева односио на имплементације међународних ISO/IEC 27001 стандарда, стандарда који се баве пословним информацијама и базирају на дефинисању и успостављању организационо-управљачких структура и система управљања сигурношћу информација. Кроз процедуре, протоколе и препоруке заговарају потребу дефинисања мера сигурности, чијом применом се снижава ниво ризика угрожавања сигурности, врше контроле и надзор мера ефикасности, као и прилагођавања сходно променама које утичу, или могу да утичу, на сигурност информација. Нажалост, овакав приступ није указивао на изналажење адекватног начина одабира и примене конкретних и ефикасних мера сигурности. Често се сводио на формалне захтеве релевантних међународних стандарда и директива ЕУ, поготову у фирмама чија се имплементација мера декларише сертификацијама неких од међународних стандарда (пре свих ISO/IEC 27001). Постоје читава брда папирне документације о креираним политикама, процедурама и оперативним упутствима, која никад нису примењена у практичном раду.

Угрожавање сигурности информација

Имајући у виду да проблематика угрожавања сигурности информација ескалира брзим променама, које доносе информационо-комуникационе технологије, то и не треба да чуди.

Али, како такав приступ не даје потпуна решења, изналежења начина одабира и примене конкретних мера сигурности и контрола њихове ефикасности, постаје прави изазов. Поготову што се мере и контроле базирају на идентификовању информационих добара, која у датом тренутку одређују информацију; њихових рањивости; претњи, које проистичу из рањивости, са ризиком да се реализују када се стекну одговарајући услови и угрози сигурност информација. Истовремено, ако се узме у обзир да је људски фактор у великом проценту (око 80%) узрочник угрожавања сигурности информација, на видно место долази значај издизања нивоа свести о месту и улози сигурности информација, одабира и примене мера сигурности, њиховог поштовања и спровођења у дело, али и одговорности, како опште тако и појединачне, за појаву било каквог вида угрожавања сигурности, било какву манипулацију, злоупотребу или криминогену радњу.

Само један интегрални, свеобухватни, холистички приступ изналажења начина дефинисања конкретних мера сигурности може дати стварни допринос издизању нивоа сигурности информација. Такав приступ, користећи праксу и позитивна искуства, уважавајући препоруке, протоколе и процедуре међународних стандарда и директиве ЕУ, резултира моделом управљања сигурношћу информација, који инсистира на практичним применама процедура, препорука, прописа и њиховом безрезервном поштовању у реалном времену, уз присуство високог степена одговорности. Овај материјал се бави баш таквим моделом.

Процедуре, протоколи, препоруке, као саставни делови међународних стандарда и директива ЕУ, које се односе на издизање нивоа сигурности информација, у великом броју случајева се, као што је већ речено, не спроводе у дело на прави начин, у виду одабира и примене одговарајућих и конкретних мера сигурности; административних, техничких и технолошких, које истински издижу ниво сигурности, штите принципе сигурности и спречавају манипулације, злоупотребе и/или криминогене радње било какве природе. Обично је то „мртво слово на папиру“, исказано писаним про-

цедурама, протоколима, препорукама и имплементацијом оног дела истих, који испуњава контролно надзорне провере садржане у поступцима сертификација. Сертификација које се свODE на извођење доказа постојања организационих и контролно надзорних механизма, примењених за издизање нивоa сигурности, имплементираних уз усаглашавање са међународним стандардима, односно на испуњавање захтева оних у чије име се и врше сертификације. Све док мере сигурности не постану саставни део средине и амбијента, примене и поштовања процедура протокола и препорука, све док одговорност за очување принципа сигурности информација, како општа тако и појединачна, не буде издигнута на највиши могући ниво, присуство опасности од угрожавања сигурности информација, злоупотреба и криминогених радњи биће све изражајније. Све док свест о месту и улози сигурности информација не буде дигнута на задовољавајући ниво, никакви закони, никакве санкције, као ни било каква законско-правна регулатива, неће имати ефикасно дејство, како по питању сигурности информација, тако и по питању заштите података о личности.

Да би се обезбедила практична, одговорна и ефикасна примена мера сигурности, потребно је начинити додатне кораке. Ти кораци би се могли огледати у додатним процедурама, протоколима и препорукама, усаглашеним са међународним стандардима и директивама ЕУ, заснованим на пракси и позитивним искуствима. Као такви, били би усмерени ка правним лицима и сакупљачима информација - власницима информација, у намери њиховог мотивисања да, када је реч о питању издизања нивоa сигурности информација, пређу са теорије на праксу. Да креирају и примене сопствене системе управљања сигурношћу информација који ће, кроз одабир и примену конкретних мера сигурности, сходно утврђеним и прихватљивим нивоима ризика: отклонити рањивости, спречавати или елиминисати услове за реализације претњи, успоставити контролно надзорне механизме функционалности и ефикасности система, те сходно њима вршити сталну надградњу и прилагођавање, зависно од природе нових претњи, у духу процесно оријентисаног

система. То изискује много дубља разматрања проблематике угрожавања сигурности информација, узимајући у обзир њену хетерогеност и комплексност, уз покушај изналажења минимума заједничког интереса који би могао да послужи као показатељ изналажења правог начина приступа проблематици, креирању и успостављању система, израженог кроз одабир и примену конкретних и јасно дефинисаних мера сигурности. Баш због комплексности и хетерогености проблематике, јако је тешко изнаћи, или бар имати визију, такве платформе. Поготову из разлога што се одабир и примена мера сигурности врши од случаја до случаја, зависно од намене и вредности информација; информационих добара која их у датом тренутку одређују, њихове рањивости, и ризика да претње коришћења рањивости буду реализоване, са несагледивим негативним последицама. У духу напред изнетог, а засновано на минимуму заједничког интереса - потреби превенције и борбе против манипулација, злоупотреба и криминогених радњи, неопходно је поћи од праксе и позитивних искустава и покушати дефинисати модел управљања сигурношћу информација, који би садржавао минимум заједничких елемената, алате и алатке који би могли да помогну власницима информација при креирању и имплементацији сопственог система управљања сигурношћу информација. Модел се заснива на елементима сигурности информација (информациона добра, рањивости, претње, мере сигурности) који би по дефиницији, садржајности и значају, а у духу хармонизације, могли да буду прихваћени од свих власника информација, али и од надлежних институција које се баве сигурношћу информација. Као такви, елементи би били дефинисани и евидентирани у табелама БАЗЕ СИГУРНОСТИ. То би практично била евиденција свих познатих угрожавања сигурности, манипулација, злоупотреба и криминогених радњи (у даљем тексту инцидената), чији су узроци, узрочници; рањивости; претње, откривени, јасно дефинисани и отклоњени конкретним мерама сигурности, уважавајући прихватљив ниво ризика. Међусобно повезани, у датом тренутку могли би да послуже при изналажењу начина предузимања конкретних ко-

рака издизања нивоа сигурности информација, као помоћи при доношењу одлуке о одабиру и примени конкретних и ефикасних мера сигурности. Кључни чиниоци модела би били: модалитет израчунавања нивоа ризика, процедуре, протоколи, препоруке инцијалног одабира мера сигурности, примењених од случаја, у зависности од нивоа ризика, као и свеукупна финансијска средства која су неминовно присутна. Како је приступ проблематици угрожавања сигурности информација процесно оријентисан, примењене мере, поступци и кораци стално се контролишу и надзиру, преиспитују, мењају и надграђују, сходно променама окружења и информационо-комуникационих технологија које угрожавају, или могу да угрозе, сигурност информација. Модел је својом садржајношћу усмерен ка управљању инцидентима, где се под управљањем подразумева: детектовање инцидента, повратак у стабилно стање које је постојало пре инцидента, а потом анализа свих релевантних фактора, лоцирање узрока, узрочника и његово елиминисање. Модел је по својој природи управљачки, зато што је процесно оријентисан и, прилагођавајући се променама и срединама у којима функционише, кроз контроле и надзор, инсистира на вршењу промена које се односе на кључне елементе система, а доприносе стабилности и ефикасности самог система, практично управљања истим. У даљем тексту ћемо модел управљања сигурношћу информација означавати као модел.

Власници информација

У духу напред изреченог, анализе и дискусије намењене су, пре свега, власницима информација, да би се скренула пажња на свакодневно присуство проблематике, са основним циљем издизања: заинтересованост за те проблеме, осећаја значаја и улоге мера сигурности, као и свести о сопственим обавезама и одговорностима. Не малим успехом сматрало би се изналажење модалитета који би могли да помогну при одређивању начина доношења одлуке о одабиру и примени конкретних мера сигурности и њихове примене. Исто тако и

начина управљања инцидентима. И све то у духу истинског снижавања нивоа угрожености сигурности информација, обезбеђивања поштовања принципа сигурности и смањења манипулација, злоупотреба и криминогених радњи. Исто тако, анализе и дискусије би требало да укажу на значај, место и улогу одговорности по питању непоштовања принципа сигурности информација, са акцентом на урушавање безбедности података о личности. Требало би да дају одговор на питања: како присуство одговорности може да утиче на модел, његову садржајност, његову примену и његову ефикасност, какав би и колики би допринос одговарајућа законско-правна регулатива могла дати придржавању прописаних и препоручених процедура, протокола и директива, као и колико би санкције допринеле одвраћању од покушаја чињења или самог чињења; манипулација, злоупотреба и/или криминогених радњи. У овом тексту, између осталог, коришћени су материјали који су садржани у Директивама 95/46/ЕЦ, Европског парламента објављених 24. октобра 1995. године (погледати Директиве 2002/58/ЕЦ од 12. јула 2002. године), у којима је акценат стављен на заштиту података о личности, као и међународни ИСО/ИЕЦ 27001 стандард.

Као што је већ напоменуто, заједнички интерес власника информација могао би да буде стварање платформе очувања принципа сигурности информација (власништво, интегритет, поверљивост, расположивост), као превенције и саставног дела борбе против манипулација, злоупотреба и криминогених радњи које доносе ИКТ, при чему је, у духу хармонизације, неопходно приступити усаглашавању терминологије, дефинисању елемената и принципа сигурности и што бољег начина одабира конкретних мера сигурности и њихове примене. То се свакако односи и на спровођење контроле и надзора њихове ефикасности, потребе прилагођавања и надградње, сходно новонасталим условима и регистрованим догађајима, детектованим констатованим инцидентима, реализованих претњи или угрожавања принципа сигурности, препорукама и процедурама реаговања на инциденте и, да не буде заборављено, повратка у претходно стабилно стање

(претходно у односу на време појаве инцидента, ако је исти довео до дестабилизације). Платформа би могла да буде прихватљива за јавни и цивилни сектор и појединце, укључујући све власнике информација, са акцентом на заштиту података о личности.

Имајући у виду чињеницу да се ни процедуре ни препоруке међународних стандарда, ни директиве ЕУ не баве начином одабира конкретних и ефикасних мера сигурности, обавеза аутора овог текста јесте да укажу на потребу да садржајност и примењивост модела буде таква да може дати допринос и бити на располагању власницима информација при осмишљавању свог система управљања сигурношћу информација, при изналажењу начина предузимања конкретних корака и одабира конкретних мера сигурности, реаговања на инциденте и истинског стављања под контролу узрока и/или узрочника инцидента.

Са тог аспекта, препоруке, протоколи и процедуре да се спроводе у дело уз инсистирање на одабиру потребних, довољних и одговарајућих сигурносних мера, њиховој примени и ефикасности, од случаја до случаја, као и демонстрацији ефикасности и функционалности, сходно потреби и/или захтеву надлежних контролно-надзорних тела и/или институција. У пракси то значи постојање, евидентирање и статистичко праћење елемената сигурности, као основице модела и саставног дела базе сигурности, и иницијалног одабира и примене конкретних мера сигурности, сходно постојећим информационим добрима, њиховим рањивостима, претњама и ризицима њиховог реализовања, уз уважавање прихватљивог нивоа ризика.

Модел управљања сигурношћу информација

Са тог аспекта, сврха овог текста јесте да пружи основне информације о моделу.

Први део се односи на: терминологију, дефинисање елемената сигурности, принципа сигурности, модалитета израчунавања и прихватања толерантних нивоа ризика, заснованих на дефинисаности елемената: 1. организацио-

но-управљачких структура и 2. контролно-надзорних механизма примењивости, функционалности и ефикасности техничко-технолочких мера саигурности, на бази процесног приступа, преиспитивања, промена, измена, надградње и прилагођавање новонасталим условима регистрација и појаве нерегистрованих рањивости, претњи, инцидента и нивоа детектованих и прихватљивих нивоа ризика. Евидентирање и праћење елемената сигурности, као саставни део модела, јесте дефинисани скуп процедура, препорука и директива, које од случаја до случаја, указују на одабир корака које треба предузети и мере које треба одабрати и применити.

Други део се односи на опис, дефинисање и стварање БАЗЕ ЗНАЊА, евидентирање елемената сигурности информација; информациона добра, рањивости, претње, мере сигурности, процедуре, препоруке и протоколи функционисања модела. Други део се, исто тако, бави модалитетима израчунавања нивоа ризика као неизоставног дела опредељења, одабира и примене мера сигурности, као и методолошким приступом детекцији, констатовању и препознавању инцидента, њихове природе, извештавања и обавештавања о њиховој појави, као и предузимања корака обезбеђивања континуитета пословања, враћања стабилног стања које је постојало пре појаве инцидента. Након тога, анализи узрока и/или узрочника појаве инцидента, мерама и поступцима њиховог елиминисања, регистрацијом нових, нерегистрованих, информационих добара, рањивости, претњи, мера сигурности, уколико су као такве везане за констатовани инцидент, и њиховим праћењем уписом у базу знања. Даље, други део се односи на одређивање места, улоге и значаја извештавања и обавештавања о појавама инцидента и инцидентних радњи, како унутар власника информација, тако и на нивоу окружења, јавности, државе и друштва, сходно масовности појава инцидента и тежини негативних последица које из њих произилазе.

Трећи део се односи на место и улогу општих и појединачних права, одговорности, законско-правне регулативе, и санкција као мера одвраћања од реализације претњи и спречавања стварања услова реализације претњи.

Литература

1. Директива 95/46/ЕЦ, Европског парламента, објављено 24. октобра 1995. године.
2. Директива 2002/58/ЕЦ од 12. јула 2002. године.
3. ИСО/ИЕЦ 27001 стандард.
4. Кондић У., Анђелски Х.: Систем управљања сигурношћу информација. Здравствена заштита, Београд, 2009; XXXVIII 4: 61–66.