ВИСОКА ПОСЛОВНА ШКОЛА
СТРУКОВНИХ СТУДИЈА – БЛАЦЕ
Часопис из области економије, менаџмента и информатике *„БизИнфо“*
Број 2/2010, стр. 161 - 169
Адреса: Краља Петра I, бр.70, 18420 Блаце

ЗАШТИТА ЛИЧНИХ ИНФОРМАЦИЈА У ИНФОРМАЦИОНИМ СИСТЕМИМА

PROTECTION OF PERSONAL INFORMATION IN INFORMATION SYSTEMS

Велимир Делетић, Милан Делетић
Висока пословна школа струковних студија, Блаце

***Резиме**: Мултиорганизациона транспарентност, легални и етички аспекти и одговорност, намећу сложене изазове не само у погледу технолошке архитектуре информационих система. При томе, технолошка архитектура мора бити усклађена са етичким и правним стандардима који често нису у сагласности са техничко-технолошким могућностима. Генерички механизми заштите треба да омогуће дефинисање стандарда и политике коришћења личних информација који ће бити технолошки скалабилни. Тиме се постиже максимално искоришћење технолошког развоја уз смањену опасност од појаве "рупа" у систему заштите које могу довести до злоупотреба.*
***Кључне речи**: информациони систем, заштита информација, контрола ризика, механизми заштите*

***Abstract**: Multiorganization transparency, legal and ethical aspects and the responsibility imposed on the complex challenges not only in terms of technological information systems architecture. In addition, technological architecture must be balanced with ethical and legal standards that often do not comply with technical and technological capabilities. Generic protection mechanisms should allow the definition of standards and policies the use of personal information that will be technologically scalable. This ensures maximum utilization of technological development with a reduced risk of developing the "hole" in the system of care that can lead to abuse.*

***Key words**: information system, information protection, risk control, protection mechanisms*

УВОД

Електронска документација садржи осетљиве личне информације које могу бити лако злоупотребљене. Са друге стране, широк приступ електронској документацији од стране корисника система и других професионалаца који треба да пруже одговарајућу услугу је предуслов за успешно пословање. Тако, са једне стране постоји потреба ограничења приступа подацима из електронске документације, док са друге постоји интерес корисника услуга да што више стручњака (из, по правилу, различитих организација) има увид у електронску документацију у циљу што бољег сагледавања статуса и тиме што квалитетнијег и ефикаснијег доношење одлука.

Многе организације развијају и уводе разне облике информационих система и система електронске документације. Саставни део набавке или сопственог развоја тих система је и процес обезбеђивања заштите информација као и процес дефинисања начина да се смање ризици и предупреде негативне последице које могу настати услед неадекватне заштите информација.

Приватност података се односи на жељу појединца да контролише публиковање (јавно изношење) личних и других информација. Поверљивост се односи на информације - у овом контексту, на могућност појединца да контролише начин на који пружалац услуге (организација или појединац) користи личне информације као и даље ширење тих информација (издавање другим појединцима или организацијама). Заштита омогућава осигурање приватности и поверљивости кроз избор стратегија, процедура и механизама заштите.

Информатичка безбедност се дефинише као "...скуп техничких и административних процедура установљених са циљем да се подаци заштите од неовлашћеног или ненаменског увида и отуђења, измене или уништења као и ради заштите функционалности самог информационог система"[1]. Посебни

циљеви у напору да се обезбеди сигурност односно пружи заштита информацијама, су:
• Очување интегритета података
• Једноставност приступа подацима од стране легитимних корисника
• Осигурање приватности личних података као и њиховог прикладног коришћења

Ови циљеви се у информатици посебно фокусирају на специфичне аспекте[2]:
• *Доступност* која обезбеђује тачну и ажурну информацију свакоме коме је потребна и на месту на којем је потребна.
• *Урачунљивост* помаже да су корисници одговорни за њихов приступ и коришћење информација по принципу потреба и права да одређену информацију знају.
• *Дефиниција периметра* омогућава да систем контролише границе поверљивог приступа, и физички и логички.
• *Приступ базиран на улогама* омогућава приступ корисника само оним информацијама које су важне за њихов посао чиме се ограничава и спречава искушење да неко неовлашћено приступи информацијама које су ван граница његових легитимних потреба.
• *Свеобухватност и контрола* обезбеђују да власник електронске документације (организација, особље укључено у процес пружања услуге), ИТ корисници и клијенти могу да разумеју и имају ефективну контролу над прикладним аспектима поверљивости и приступа информацијама.

Заштита података и једноставан, лак, приступ су често супротстављени захтеви: поједностављење приступа може угрозити сигурност података, ако софтверска апликација није пажљиво и адекватно пројектована и имплементирана, док превише робусни механизми заштите најчешће нарушавају ергономију апликације са становишта корисника.

Велики део лаика, али и информатичких професионалаца, нажалост, не респектује комплексност заштите информација чак и када разуме њен значај.

1. МЕТОДОЛОГИЈА

Уобичајена методологија за развој заштите личних информација у информационим системима се састоји од шест основних корака:
1. Идентификација информатичких ресурса који захтевају заштиту
2. Дескрипција архитектуре информационог система који се имплементира
3. Идентификација опасности по информације у склопу планиране архитектуре
4. Рангирање опасности по значају и потенцијалној штети
5. Дизајнирање решења која треба да смање ризике и последице
6. Спецификација имплементационих препорука.

Избор оптималне стратегије заштите представља компромис између нивоа и обима заштите и потенцијалних ризика и цене последица у случају грешке. Стога се често у овом процесу користе методологије анализе система, процеса и контроле ризика.

2. ИНФОРМАЦИОНИ РЕСУРСИ

Пре саме примене мера обезбеђења информација, потребно је идентификовати саме информације које је потребно штитити. Превише широка заштита која чува и информације које нису критичне (њихова (зло)употреба или неконтролисана измена не изазивају штетне последице) изискује непотребне ресурсе, компликује имплементацију и често деградира укупне перформансе система. Стога је важно наћи оптималан однос између критичног скупа информација и расположивих ресурса.

Информациони системи који садрже личне информације (медицинске, социјалне, демографске и друге) морају примењивати посебне мере опреза и заштите како би се спречиле потенцијалне злоупотребе које могу угрозити законска и људска права (приватност) појединца. Овде је веома важно разумети да се личне информације не односе само на случајеве директне везе једног скупа података за одређену особу (подаци о особи), већ и на случајеве када се укрштањем или анализом података ти подаци или информације могу довести у везу са разумно малим бројем

особа. Довођење у везу је често знатно сложенији аспект потенцијалног ризика од злоупотребе информација него сама заштита података.

3. АРХИТЕКТУРА СИСТЕМА

Информациони систем, или апликација, увек се појављује у контексту ширег система односно његове архитектуре. Размена информација, њихова дисеминација и коришћење у екстерним системима има значајну улогу у повећању ефикасности свих пословних процеса. У контексту потребе за што широм интеграцијом информационих система и апликација, све већим захтевима за слободном разменом информација и повезивање са другим изворима података, расте и ризик од злоупотребе или оштећења информација.

Архитектура информационог система представља план остварења визије будуће функционалности система кроз спровођење потребних набавки (што укључује и сопствени развој) и имплементације компоненти и елемената система. Процес набавке се спроводи кроз стандардну процедуру инвестиционог одлучивања која треба да обезбеди потребну технологију (технику - хардвер, софтвер и комуникације - али и људе који су способни да та средства на најефикаснији начин примене).

Неадекватна средства и/или нестручна употреба представљају највећи фактор ризика за функционалност система и безбедност података. Најчешће хаварије настају као последица потпуног одсуства свести о постојању нестручног приступа или импровизованих решења. Зато је професионално дизајнирање архитектуре и њено стриктно поштовање у основи планирања и спровођења механизама заштите.

4. ИДЕНТИФИКАЦИЈА РИЗИКА

Ризик је могућност да дође до материјалне или нематеријалне штете услед непланиране измене или губитка информација. Односи се на ситуацију људске грешке или намерне акције, као и на околности техничких или природних фактора који могу изазвати штету.

Први корак у контроли ризика је разумевање шта је то ризично (потенцијално опасно) по пословни процес, пословне циљеве или ресурсе организације. Након тога, спроводи се свеобухватна евалуација или истраживање ризика што доводи до идентификације ризика. Након почетне идентификације, врши се израда планова за умањење ризика који могу имати најштетније последице (одређивање приоритета). Овакав континуални процес идентификације ризика и развоја планова за њихово отклањање се дефинише као контрола (управљање) ризика.

Најчешће, организације не сагледавају све потенцијалне ризике и не формулишу целовиту и свеобухватну стратегију контроле ризика. Важно је разумети да само свеобухватан приступ, чак и са елементарним механизмима заштите, значи много више од парцијалног решавања проблема (чак и са најскупљим механизмима).

Једна од методологија евалуације ризика (OCTAVE - Operationally Critical Threat, Asset, and Vulnerability Evaluation) омогућава истраживање организационих и технолошких аспеката ради синтезе свеобухватне слике потреба информатичке безбедности. Основне фазе OCTAVE методологије обухватају[3]:

• Изградња профила опасности за ресурсе – Овде се евалуирају организациона својства система. Истражују се основни информатички захтеви по стручним сегментима организације, опасности по кључне информационе ресурсе који су везани за те домене, безбедносне мере које су потребне, тренутно примењене мере као и организационе слабости и рањивости у организационом смислу (организациона рањивост).

• Проналажење слабости у инфраструктури – Овде се евалуира информатичка инфраструктура. Кључне компоненте инфраструктуре (сервери, радне станице, мрежа, екстерне комуникације, оперативни системи, базе података итд.) се истражују ради проналажења слабости и "рупа" (технолошка рањивост) које могу довести до непланираних активности на нивоу информационог система.

• Развој сигуроносне стратегије и плана – У овој фази се анализирају сви уочени ризици. Информације сакупљене у организационој и технолошкој евалуацији (фазе 1 и 2) се

анализирају са аспекта идентификације ризика и да би се проценио значај сваког ризика на укупне интересе организације. Паралелно се развија стратегија заштите и планови за избегавање појединих опасности сагласно приоритету појединих ризика.

5. МЕХАНИЗНИ ЗАШТИТЕ

Механизми заштите су организационе и технолошке мере које се предузимају ради смањења ризика и отклањања узрока ризика. Врло често се, неправилно, сматра да су технолошки механизми заштите сами по себи довољни одбрамбени механизам. Већина штета које настају као последица злоупотребе информација (не губитка или оштећења) су последица људског фактора, или из разлога непрофесионалне примене технолошких механизама заштите или због организационих пропуста.

Организациони механизми заштите подразумевају планирање правила и процедура које се односе како на ИТ особље у свакодневном администрирању система тако и на корисничку политику тј. правила и права у коришћењу информација.

Технолошки механизми треба да обезбеде поуздану и контролисану функцију свих компоненти система и тиме система у целини. Примери технолошких механизама заштите (технологија заштите) су: антивирусни програми (апликација), RAID контролер (уређај), Firewall (сервис), Smart-картица (медијум), PKI (стандард), SSL (мрежни протокол) итд.

У склопу функционалности система се онда обезбеђују и потребни механизми за примену и спровођење организационих механизама заштите. Нагласимо да то значи да се спровођење организационе заштите информација базира на планској уградњи потребних функционалности система, односно да без правилног дизајна архитектуре, планирања и спровођење имплементације (која гарантује доследно испуњење свих дизајнираних функционалности) нема поуздане заштите.

Генеричке функционалности се могу реализовати, мање или више ефикасно, различитим технолошким механизмима односно решењима. Генеричке функционалности су веома стабилне, односно не мењају се радикално са променом тхенологије. То

омогућава да стратегија заштите базирана на генеричким механизмима не захтева сталне измене и ревизије процедура (организационих механизама) услед напретка технологије, већ технолошки напредак само стабилно подиже ниво и ефикасност заштите. Ово је веома важно јер у пракси највећи проблем и енергију захтева увођење процедура, односно привикавање корисника на доследно спровођење политике употребе система и располагања информацијама. Технику и технологију је лакше мењати него људске навике.

Већина савремених ICT инфраструктурних компоненти (OS, DBMS, мрежни уређаји итд.) обезбеђују генеричке заштитне функционалности. Зато је пре избора конкретних компоненти неопходно стручно проценити стварни ниво сигурносних механизама које генеричка функционалност уређаја подразумева. Сама генеричка функционалност не подразумева и стварну ефективну заштиту коју конкретна компонента омогућава. Лаички и непрофесионални приступ ствара илузију заштите док се у стварности појављу висок фактор ризика од "упада" управо кроз "сигурну" компоненту.

ЗАКЉУЧАК

Безбедност и заштита информација у информационим системима је веома важан аспект који треба посебно планирати и разматрати у имплементацији било ког система или апликације. Описана методологија рзвоја прикладне политике заштите информација је општа у начелу али је веома погодна за примену у актуелним пројектима који се спроводе у нашим установама. Посебан акценат је стављен на разумевање баланса између потреба, могућности и потенцијалних ризика. У условима ограничених средстава, што је свакако случај у нашим организацијама, правилно планирање безбедносне политике информационог система пре уласка у набавку опреме и апликативних решења је од суштинског значаја не само са аспекта рационализације трошкова набавке самих ресурса, већ и са аспекта смањења ризика од проблема и штета које ће се појавити у будућности.

ЛИТЕРАТУРА

[1] Lawrence O. Gostin et al., "*Privacy and Security of Personal Information in a NewHealth Care System*," Journal of the American Medical Association, 270(20), Nov. 24, 1993, p. 2487

[2] *Informatics*, Edward H. Shortliffe and Laslie E. Perreault, Springer, NY USA, 2001, p. 174

[3] *Managing Information Security Risks: The OCTAVE Approach*, Christopher Alberts and Audrey Dorofee, Addison Wesley Professional, 2002, p. 15