КОРПОРАТИВНА ИНФОРМАЦИОНА БЕЗБЕДНОСТ
(Позивни реферат)

Проф др. Драган Триван, е-маил: dtrivan.trivan@fpsp.edu.rs
Факултет за пословне студије и право
Универзитет „Унион-Никола Тесла“, Београд

Сажетак: Циљ рада је указивање на значај корпоративне информационе безбедностии емпиријско истраживање цурења поверљивих пересналних информација у 2015. гоидни у свету, из комерцијалних и некомерцијалних државних организација, до којих је дошло злонамерним или немарним деловањем запослених или спољних нападача и њихово процентуално учешће према утврђеним критеријумима. Истраживање је засновано на бази података креираној на основу јавних саопштења о случајевима цурења поверљивих информација.Студија обухвата мање од 1% случајева претпостављеног укупног броја цурења. Критеријуми категоризације цурења изабрани су тако да истраживање категорија садржи довољно елемената како би формирање поља истраживања омогућило теоријско разматрање узорка, а резултати и уочени трендови генерализацију закључака. Резултати су показали да је у 2015. години регистровано 1505 случајева цурења информација, од чега 965,9 персоналних. 32,2% је узроковао спољашњи злонамерник, а 65,4% запослени. Персонални подаци и финансијске информације су најчешћи објекти напада – 90,8%. Мреже су најчешћи канали цурења информација – 45,6%. Највећи проценат цурења информација је у комерцијалним средњим предузећима, а најпривлачнија привредна грана за нападе је у области високих технологија, трговине и транспорта.
Кључне речи: Корпоративна безбедност, информатичка заштита, информациона безбедност, цурење поверљивих персоналниих информација

CORPORATE INFORMATION SECURITY
(Keynote paper)

Abstract: The aim of this paper is to show the importance of corporate information security and empirical research of leaks of confidential personal information in 2015 in the world of commercial and non-commercial state organizations, which occurred because of malicious or careless employees' operation or external attackers, and their percentage according to established criteria. The research is based on a database created on the basis of public statements on cases of leaks of confidential information. The study covers less than 1% of the assumed total number of leaks. Criteria for the categorization of leakage are chosen so that study category contains enough elements to allow the formation of fields of research theoretical consideration of the sample, and the results and conclusions of the observed trends enable generalization of conclusions. Results showed that 1,505 cases of information leaks were registered in 2015, of which 965.9 personnel. 32.2% were caused by external malicious person, and 65.4% by employees. Personal data and financial information are the most frequent object of attack - 90.8%. Networks are the most common channels of information leakage - 45.6%. The highest percentage of information leaks in commercial medium-sized enterprises, and the most attractive economic sector for attacks is in the area of high technology, trade and transport. Data of trading, transportation and high-tech organizations are most often attacked from outside, while the financial, medical and educational organizations were, as a rule, attacked by insiders. For all the data theft is less likely the use of e-mail, removable media, services for instant messaging, because the control of these channels is high. Selection of hackers are closed uncontrolled channels whose protection systems either do not work or are inefficient.
Keywords: Corporate security, information protection, information security, leakage of confidential personal information

1. Увод

Информатичка заштита, односно информациона безбедност, предмет је општег интересовања како државних институција тако и корпорација и других привредних субјеката. У том смислу, од кључног значаја је разрада и имплементација поузданих метода и средстава заштите информација, као и тражење системских решења и средстава заштите применом ефективних алгоритама и метода пројектовања средстава заштите информација – инструмената информационе безбедности (Триван, 2012).

За област информатичке заштите је веома значајно превазићи конзервативизам који може постојати у делу менаџмента корпорација, а који се испољава у потцењивању претњи интегритету информационог система, непознавању основне структуре ИС, па и избегавању комуникације са особљем које ради на пословима заштите тог система. Као образложења и изговори за неулагање у заштитне мере често се помињу њихова висока цена и неисплативост на кратак рок. (Родић, Ђорђевић, 2004).

Информациони системи су данас за свет оно што су нервни систем и крвоток за људски организам, а слом светског информационог система би довео до пада савремене цивилизације и вратио живот човека на ниво из далеке прошлости. На микронивоу корпорације, уништавање базе података или унутрашњег информационог система значило би пословну катастрофу коју многе компаније не би преживеле. Проблем је, међутим, што све већа сложеност, величина и важност информационих система повећава њихову осетљивост на све врсте напада и угрожавања и што последице њихове деструкције постају утолико теже (Јаворовић, Биланџић, 2007).

2. Дефиниција и историјски развитак информатичке заштите

Информатичка заштита јесте заштита информационих система од неауторизованог приступа или модификација информација у складиштењу, обради и преносу и заштита ауторизованих корисника, укључујући неопходне мере детекције, документовања и отклањања таквих претњи. (National Information Systems Security Glossary, 2000).

Како истиче Волф, развој информационе безбедности је започео 60-их година XX века преко комуникациона безбедности (COMSEC – Communication Security) (Wolf, 2003). Са првим компјутерима, почетком 70-их година, настала је компјутерска безбедност (COMPUSEC – Computer Security). Крајем 80-их година COMSEC и COMPUSEC су обједињене у информациону безбедност (INFOSEC - Information Security), која је покушала да интегрише раније одвојене дисциплине као што су безбедност персонала, компјутерска безбедност, комуникациона безбедност и оперативна безбедност.

3. Штетни утицаји на информациону инфраструктуру

Информациона инфраструктура може бити изложена различитим штетним утицајима који могу директно или индиректно угрозити њено функционисање - кваровима, инцидентима и нападима (Ellison et all. 1997). Кварови су потенцијално штетни догађаји, изазвани унутрашњим дефектима система или дефектима спољњих елемената нужних за његово функционисање. Они могу бити и последица грешака у пројектовању софтвера, као и последица кварова хардвера, људских грешака и др. Инциденти

укључују све случајне догађаје попут природних непогода и катастрофа. За разлику од кварова, узроци инцидената се налазе изван система (Петковић, 2009). Напади на информационе системе представљају директне акције против мрежа или информационих система с циљем да неовлашћено пресретну или прекину операције, преузме контрола и униште, промене или корумпирају њихови подаци (Stallings, 1995). По неким ауторима, постоје три врсте напада на информационе системе: физички напад (Marlin, Darvey, 2004), електронски напад и сајбер напад (Петковић, 2009).

Нападачи су полазна тачка сваког напада на рачунарски систем, иако се они разликују по томе ко су или одакле су, по способностима, те да ли су унутар или ван система који нападају. По томе се нападачи деле на пет категорија: хакери, шпијуни, терористи, организовани нападачи и професионални криминалци (Родић, Ђорђевић, 2004).

Према Р. Игену, од унутрашњих безбедносних претњи информационим системима, најчешће су материјалне штете, оштећења и дисфункције које настају случајно, услед нерада и немара запослених, одговорних и руководећих лица (Eagan, 2005). Спољна угрожавања информационих система такође могу бити различита, од имовинског, преко политичког до различитих форми високотехнолошког криминала.

Као извори и врсте угрожености информационих система помињу се и: софтверски извори угрожености, хакерски напади, пиратерија (бесправно умножавање и продаја пиратског софтвера), физички напади на информационе системе (интерне и екстерне крађе података и информација, крађа информатичке опреме, онеспособљавање сервера, уништавање информатичке опреме, намерно изазивање пожара и терористички напади на информационе системе), угрожавање из окружења, унутрашњи организациони проблеми,информациона и пословна шпијунажа, недолично и криминално понашање корисника информационих система и мрежа, техничке погрешке у компонентама информационе и комуникационе технологије (Јаворовић, Биланџић, 2007).

4. Методе и средстава заштите информација

Мере информационе безбедности су општа правила заштите података на физичком, техничком или организационом нивоу. Стандарди информационе безбедности су организационе и техничке процедуре и решења намењени системском и унификованом спровођењу прописаних мера информационе заштите (Триван, 2012). Мерама и стандардима информационе безбедности се утврђују минимални критеријуми за заштиту поверљивих података у пословним субјектима (Ивандић и др. 2011).

Најважнија међународна норма за управљање информационом безбедношћу је стандард ISO/IEC 27001:2005, којим се дефинишу захтеви за успостављање, одржавање и континуирано побољшавање система управљања информационом безбедношћу. Појам информационе безбедности се овде не посматра искључиво са информатичког аспекта већ се предвиђа и примена других елемената корпоративне безбедности, као што су физичка и техничка безбедност, управљање људским ресурсима, правна заштита и др. Тај стандард садржи смернице и спецификације за помоћ организацијама у развоју система управљања информационом безбедношћу (ISMS – Information Security Management System) односно безбедношћу информација које се налазе у поседу организације (Ивандић и др. 2011).

Мере заштите информационих система корпорација обухватају: нормативно-правне мере (пре свега доношење Правилника о информационој и комуникационој заштити), организационе мере (организациона јединица за информациону и комуникациону безбедност, организациона решења за спровођење одређених заштитних мера), програмске (софтверске) мере, техничко-технолошке мере (коришћење заштитних могућности саме информационе технологије, примена техничких средстава заштите), кадровске мере, образовне мере (безбедносна обука и усавршавање запослених), мере надзора, санкције, физичке мере заштите, контраобавештајне мере на софтверском, хардверском, техничком и физичком нивоу, те заштитно уређење пословног окружења (Јаворовић, Биланџић, 2007).

Према неким ауторима, заштита информационих система од неауторизованог приступа обухвата четири подручја од значаја за информациону безбедност: безбедносну проверу, физичку безбедност, безбедност података и безбедност информационог система (Ивандић и др. 2011). Тако се ауторизацијом кориснику и после приступа систему ограничавају акције и манипулације са подацима и информацијама. У том смислу, свака спроведена акција над подацима и /или информацијама треба да буде регистрована, а нарочито промене уколико је до њих дошло (Родић, Ђорђевић, 2004).

Напредак у рачунарској техници и појава мрежа (пре свега Интернет), проширила је листу својстава информација, пред које се постављају безбедности захтеви. То су првенствено аутентичност (authentication) и непорицљивост (non-repudiation). Важно је уочити да та разлика није само терминолошке природе (Stephenson, 2010). Утврђивање аутентичности је доказивање да је корисник информационог система заиста тај за кога се издаје. Провера аутентичности је способност система да верификује идентификатор (или више њих) које предочава корисник, односно утврђује да ли систему приступа онај корисник чији је идентификатор предочен систему (Родић, Ђорђевић, 2004).

Важне одлике информационе безбедности су оперативност и осетљивост на време, што изражавају термини детекција и реакција. То су дефанзивне оперативне могућности за које се, заједно са традиционалним информатичко-заштитним активностима, од краја XX века користе изрази теорија информационог ратовања и одбрамбене информационе операције (Field Manual, 2010). Према документу Министарства одбране САД из 2002. године, информациону сигурност чине „информационе операције заштите и одбране информација и информационих система, којима се обезбеђује њихова расположивост, интегритет, аутентичност, поверљивост и непорицљивост, а што подразумева рестаурацију информационих система инкорпорираним могућностима заштите, детекције и реакције“ (Department of Defense Directive No. 8500.1, 2002).

5. Упоредна пракса информатичке заштите у најзначајнијим савременим корпорацијама

Према Здравку Баздану, информациони системи корпорација се деле на: информационе системе за прикупљање и обраду података, системе информисања, системе информација, те на интегралне информационе системе. Главни део информационог система - информатичка оперативна јединица, често се назива и оперативно-информатички центар (ОИЦ). На врху информационог система корпорације се налази

информатички менаџмент, коме су подређене стручне службе за изградњу и развој информационог система, истраживање информатичких потреба, корисничку обраду и припрему информација, пословно-обавештајну делатност и за питања безбедности и надзора. Сматра се да од савремених транснационалних корпорација, најсложенијим информационим системима располажу General Electric, Royal Dutch Shell, General Motors, Toyota Motors, Exxon Mobil, British Petroleum (BP) и JP Morgan Chase, које су и по другим параметрима међу најмоћнијим компанијама на свету (Bazdan, 2009).

Неке претње информационим системима корпорација се никад и не открију, због чега се ангажују посебне службе које откривају или процењују могућност претње. Истовремено, рањивост система је обрнуто сразмерна степену његове брањености. Значај самог информатичког система зависи од његове финансијске, материјалне или политичке вредности. Анализа претњи, рањивости и значаја система, расположивости противмера и односа цене ризика и цене коштања, помаже у вођењу и одређивању потребних активности руководства компаније и приоритета у раду са ризицима у заштити информација, као и код увођења контрола одабраних да би штитиле од тих ризика. У неким ситуацијама је потребно да се поступак оцењивања ризика и одабирања контроле понове неколико пута како би се обухватили различити делови корпорације или појединачни информациони системи (Родић, Ђорђевић, 2004).

Савремене корпорације третирају информациону безбедност као један од приоритета у вођењу пословања. У складу са тим, евидентне су радикалне промене у организацији служби информационе безбедности у таквим компанијама, које не само да се одвајају од службе за развој и примену информационих технологија, већ често уводе и функције директора и менаџера за информациону безбедност. То показује да су питања информационе безбедности и проблеми заштите пословних информација доспели у позицију да буду делокруг интересовања самог топ-менаџмента (Муравјева, 2006).

6. Емпиријско истраживање цурења поверљивих информација у свету

Методологија

Последњих година су водеће медијске куће непрестано обавештавале о цурењу поверљивих информација светских корпорација. Реч је о великим и значајним именима корпорација, жртвама крађе поверљивих информација: Anthem, Apple, AT&T, British Airways, DreamWorks, Electronic Arts, Equifax, FIA, Google, HBO, HSBC, HTC, JP Morgan Chase, Kia Motors, Lenovo, Lufthanse, Microsoft, Morgan Stanley, NVIDIS, PayPal, PwC, Samsung, Starbucks, Tele2, Toyota, Twitter, Uber, United Airlines, Yahoo. Тако је 2014. године у свету регистровано 1395 случајева цурења поверљивих информација, што је 22% више него 2013. (извор: http://bis-expert.ru/bis-summit).Највише цурења повезано је са личним подацима – 92%. Више од 767 милиона личних података било је компромитовано због грешака или намерног деловања унутрашњих нападача. 2014. забележено је 14 великих случајева – исцурило је више од 10 милиона персоналних података, што је 89% свих компромитованих записа. Банке, интернет сервиси и медицинске установе били су најчешће мете напада. У 55% случајева виновници цурења поверљивих информација били су запослени, а у једном случају то је био високо позиционирани руководилац организације (извор: http://bis-expert.ru/bis-summit).

Једанаест и по милиона докумената процурило је из једне од главних агенција за оснивање офшор фирми „Mossack Fonseca“, откривајући имена низа политичара, криминалца, бизнисмена и других личности који су се скривале иза компанија основаних у пореским рајевима. У овом истраживању, учествовало је више од 100 редакција широм света (извор:https://www.krik.rs/najvece-curenje-informacija-iz-ofsor-zona-u-istoriji/#sthash.X1CstAty.dpuf).

Полазећи од наведеног, предмет истраживања је цурење поверљивих персоналних информација. У раду су комбиновани квалитативни и квантитативни методолошки приступ, тзв. метода триангулације. Технике и инструменти бирани су у оквиру дескриптивног истраживачког метода. Примењени су аналитичко-синтетички и статистички метод, као и контент анализа. Истраживање је засновано на бази података креираној на основу јавних саопштења о случајевима цурења поверљивих информација (различити отворени извори) из комерцијалних и некомерцијалних државних организација, до којих је дошло злонамерним или немарним деловањем запослених или спољних нападача. Приликом креирања базе свако цурење података класификовано је по следећим критеријумима: величина организације, привредна грана, степен оштећења, тип цурења (према намери), канал цурења, тип информација.

7. Узорак

Студија обухвата мање од 1% случајева претпостављеног укупног броја цурења. Ипак, критеријуми су изабрани су тако да истраживање мноштва категорија садржи довољно елемената како би формирање поља истраживања омогућило теоријско разматрање узорка, а резултати истраживања и уочени трендови генерализацију закључака. Да би узорак био што уједначенији, из истраживања су искључени тзв. „мега цурења“ (више од 10 милиона информација) персоналних информација, као и она са мање од 100.

Случајеви нарушавања поверљивости информација и слични инциденти који нису довели до цурења информација, као и они са нејасним извором података (када се не зна којој организацији су припадале информације) нису ушли у узорак истраживања. Чињеница је да су ови велики инциденти само врх леденог брега. У 2015. години забележено је много случајева цурења поверљивих информација из медицинских и финансијских установа и то најчешће због грешке или непажње запослених.

Циљ истраживања је да се утврди број цурења поверљивих персоналних информација у 2015. години у свету, на основу основу јавних саопштења о случајевима цурења поверљивих информација (средства информисања, блогови, интернет форуми, други отворени извори) из комерцијалних и некомерцијалних државних организација, до којих је дошло злонамерним или немарним деловањем запослених или спољних нападача и њихово процентуално учешће према различитим критеријумима: величина организације, привредна грана, степен оштећења, тип цурења, канал цурења, тип информација. На основу предмета и циља истраживања постављени су следећи **задаци**:
1. Истражити јавна саопштења о случајевима цурења поверљивих информација у свету.
2. Креирати базу података на основу истраживања саопштења о случајевима цурења поверљивих информација у свету.
3. Класификовати цурење података према критеријумима: величина организације, привредна грана, степен оштећења, тип цурења, канал цурења, тип информација.

4. Издвојити уочене трендове.

Хипотезе
X0 Цурење поверљивих информација је у порасту.
X1 Унутрашњи напади су најчешћи тип деловања.
X2 Запослени су најчешћи извор цурења информација.
X3 Персонални подаци и финансијске информације су најчешћи објекти напада.
X4 Мреже су најчешћи канали цурења информација код случајних цурења информација.
X5 Мреже су најчешћи канали цурења информација код намерних цурења информација.
X6 Средње компаније су најчешће мете напада на поверљиве персоналне информације.
X7 Највећи проценат цурења информација је у комерцијалним пословним субјектима.
X8 Најпривлачнија привредна грана за нападе је у области високих технологија, трговине и транспорта.

8. Резултати истраживања са дискусијом

У 2015. години регистровано је 1505 случајева цурења поверљивих информација, од чега је 965,9 милиона персоналних – бројеви социјалног осигурања, банковне картице и друге поверљиве и важне информације.

Табела 1. Цурење информација по вектору деловања

Регистровано је 48 (32,2%) цурења информација чији узрок је спољашњи злонамерник. У 984 (65,4%) случаја до цурења поверљивих информација дошло је кривицом запослених. Спољашњи напади забележени су у 15 од 21 случаја мега цурења. Овим смо доказали X1 хипотезу **Унутрашњи напади су најчешћи тип деловања.** Цурење поверљивих информација узроковано спољашњим нападима одликује се већим обимом компромитованих података. У просеку, по једном спољашњем нападу компромитује се око 1,26 милиона података, док је у случају унутрашњег напада то 0,34 милиона. Ово, наравно, не значи да је цурење до којег је дошло изнутра мање разорно и опасно од оног до којег је дошло услед спољашњег напада.

Табела 2. Цурење информација према извору

У 2015. години у 51,2% случајева виновници цурења информација били су садашњи или бивши запослени (48,9% и 2,3%). У више од 1% случајева забележена је кривица руководилаца организације (топ менаџмент, руководилац департмана и сл.), што потврђује нашу хипотезу **X2 Запослени су најчешћи извор цурења информација.** Веома је висок проценат цурења који се догодио од стране спољних сарадника који имају приступ заштићеним информацијама, чак 3,5%.

Табела 3. Цурење информација према типу података

Највећи проценат цурења поверљивих информација је у домену персоналних и финансијских података – 90,8%, следе комерцијални са 5%, државна тајна са 1,7% и

2,5% je neopredeljenih, čime smo potvrdili našu treću pomoćnu hipotezu **X 3 Personalni podaci i finansijske informacije su najčešći objekti napada.**

Tabela 4. Incidenti prema karakteru

Kao glavni trend uočili na globalnom uzorku uočen je visok stepen curenja informacija prouzrokovan zlonamernim upadima spolja. Skoro 2/3 kompromitovanih personalnih informacija u 2015. godini dogodilo se kao rezultat napada spolja. Izdvajaju se incidenti koji se odnose na nezakonite aktivnosti hakera, penetraciju u infrastrukturu kompanije, krađu informacija o klijentima i zaposlenima. U 2015. godini najčešći kanali curenja informacija bili su: gubitak opreme, elektronska pošta, papirni dokumenti, prenosivi medijи, mobilni uređaji, tekst/video poruke i društvene mreže. U poređenju sa podacima iz 2014. godine, uočavamo trend smanjenja curenja informacija zbog gubitka opreme, elektronske pošte i papirnih dokumenata. Uz to, veoma je veliki broj slučajeva u kojima ne može tačno da se odredi kanal curenja (procenat ovakvog gubljenja informacija je čak 21,3%).

Tabela 5. Kanali curenja informacija

Postoji pogrešno mišljenje da su slučajevi slučajnog curenja informacija manje štetni za kompaniju od zlonamernih. Praksa je pokazala da posledice ne zavise od tipa curenja niti od izvora delovanja nego od karaktera izgubljene informacije.

Tabela 6. Slučajni i namerni slučajevi curenja informacija

Mreže su se pokazale kao najkritičnijи kanali slučajnih i namernih curenja informacija, što potvrđuje hipotezе **X4** i **X5.** Mrežno curenje informacija karakteriše visok nivo kritičnosti podataka i veliki obim kompromitujućih informacija. Rezultat spoljnjih napada je velikи finansijski gubitak za kompaniju, a samo jedan incident može drastično izmeniti njenu budućnost. Inače, 45% mrežnih incidenata tiče se finansijskih podataka – brojevi računa, bilansi, platne kartice.

Tabela 7. Curenje finansijskih podataka po kanalima

Mali procenat namernih curenja informacija putem mobilnih uređaja, prenosivih medija, elektronske pošte i papirnih dokumenata može se objasniti činjenicom da se za zlonamerne upade sve manje koriste ti kanali. Počiniоci su svesni da se savremenim sredstvima kontrole mogu uspešno presresti preноsi poverljivih informacija ovim kanalima te ne rizikuju neuspeh. Dominacija mrežnih kanala i kod slučajnih i kod namernih curenja informacija svedoči o nagло rastućem značaju ovog kanala za biznis. Zbog toga raste i broj slučajnih curenja informacija prilikom širenja informacija mrežom, objavljivanja podataka na vebu i dr. Sa druge strane, zlonamernici sve ređe koriste one kanale u kojima je kontrolisan prenos informacija – elektronsku poštu, servise za brza saopštenja i slično.
Prema tipu organizacija najveći procenat curenja informacija dešava se u komercijalnim – 72,8%, zatim u državnim – 17%, a 10,2 % je neopredeljeno, što čime smo potvrđuje našu sedmu pomoćnu hipotezu **X7 Najveći procenat curenja informacija je u komercijalnim poslovnim subjektima**. Prema privrednim

гранама, највећи проценат цурења је у трговини – 63,9%, затим у високо-технолошким гранама – 63,2%, следи производња и транспорт са 61,6%, банке и финансије са 51,3%, те медицина – 26,1%, нафта и гас – 25,9%, образовање 24%, јавна и државна управа 7,8%, што потврђује нашу осму помоћну хипотезу **X8 Најпривлачнија привредна грана за нападе је у области високих технологија, трговине и транспорта.**

Привлачност привредне гране за нападе условљена је ликвидношћу података које компанија поседује, што потврђује број забележених намерних цурења информација. Претпоставка нападача о нивоу заштите података у привредној грани обрнуто пропорционално утиче на привлачност. Један од основних разлога високог процента крађе информација у медицинским и финансијским институцијама је низак ниво културе коришћења информација ограниченог доступа и висока ликвидност података. Према величини компанија такође постоји разлика. Највећи проценат цурења информација забележен је у средњим – 85%, затим у великим – 8,7% и најмањи у малим субјектима – 6,3%. Тиме смо потврдили хипотезу **X6 Средње компаније су најчешће мете напада на поверљиве персоналне информације.** Важно је напоменути да је ово тренд уназад две до три године и то најпре у медицинским и трговачким компанијама. За намерне нападе најпривлачније су привредне гране: делови виске технологије, трговина, транспорт. Највећи обим компромитујућих података, без мега-цурења, уочен је у високотехнолошким компанијама и у образовним институцијама. Трговина, транспорт и високотехнолошке компаније најчешће се нападају споља, а банке, медицина и осигуравајуће куће уз помоћ запослених. Средњи бизнис подвргнут је цурењу персоналних података у много већем степену него велики.

9. Закључак

Када у интернет претраживач укуцате кључне речи „цурење поверљивих информација“ у року од неколико секунди појави се 2.860 резултата, што само сведочи о величини проблема којим се бави овај рад.

Након уводног разматрања у раду је дефинасана информатичка заштита и дат је њен историјски развитак, са освртом на најрецентније ауторе који се овом проблематиком баве код нас и у иностранству. Даље се у раду говори о штетним утицајима на информациону инфраструктуру (кварови, инциденти и напади), те се наводе могуће методе и средства заштите информација. Последњи део теоријског разматрања у раду посвећен је упоредној пракси информатичке заштите у најзначајнијим савременим корпорацијама, с обзиром да откривање осетљивих пословних података, може да има озбиљне последице по пословање једне компаније, њену репутацију или чак опстанак.

За адекватан приступ решавању овог проблема потребно је схватити његове узроке, било да су технички или припадају људској природи и понашању. Последице губитака података могу бити директне или индиректне. Директне последице се могу сагледати на конкретан финансијски начин. Оне настају након губитка личних и финансијских података клијената. Индиректне последице је теже сагледати јер се јављају током дужег периода и њихову финансијску тежину не можемо увек прецизно да одредимо. Ове последице настају након губитка критичних пословних података и интелектуалне својине а узрокују нарушавање репутације компаније, окретања клијената ка

конкурентим компанијама и смањивање обима пословања. С тим у вези, превенција цурења података треба да буде усмерена ка најризичнијим аспектима пословне праксе.

Емпиријски део рада бави се најзначајнијим инцидентима у 2015. години у вези са незаконитим активностима хакера, пенетрацијом у инфраструктуру компаније, крађом информација о запосленима и клијентима. Истраживање је показало да за крађу података све мање користе електронска пошта, преносиви медији, сервиси за брзе поруке, будући да је контрола ових канала велика. Избор хакера су све више затворени неконтролисани канали чији системи заштите или не раде или су неефикасни.

Најатрактивнији за нападаче су компаније у области високих технологија, трговине и транспорта. Подаци трговачких, транспортних и високотехнолошких организација најчешће су нападнути споља, док су финансијске, медицинске и образовние организације, по правилу нападнуте од инсајдера. Истраживање је показало да су средња предузећа чешће жртве цурења персоналних података од великих.

Подаци добијени истраживањем потврдили су све постављене хипотезе. Тема цурења података постаје све транспарентнија, што је веома добро и корисно. Надамо се да ће се у будућности говорити не само о цурењу, типовима података, особености канала, него и о оцени заштите, о реалним финансијским губицима конкретних компанија услед цурења одређеног типа информација, те о нивоу инцидента.

Литература

[1] Баздан, З. (2009). *Менаџери морају знати: пословно обавјештајна дјелатност креира најважнији ресурс управљања*, Пословна изврсност, год. III, бр. 2, Хрватски институт за квалитету, Загреб, стр. 62.
[2] Ellison R.J., Fisher D.A., Linger R.C., Lipson H.F., Longstaff T., Mead N.R., (1997).*Survivable Network Systems: An Emerging Discipline, Technical Report (CMU/SEI-97-TR-013.ESC-TR-97-013),* CERT, Pittsburgh PA
[3] Field Manual No. 3-13, FM 3-13 (FM 100-6), in: Information operations: Doctrine, Tactics, Techniques and Procedures, Department of the Army, Washington DC, November 2003.
[4] Ивандић Видовић Д., Карловић Л., Остојић А. (2011). Корпоративна сигурност, Удруга хрватских менаџера сигурности – УХМС, Загреб
[5] Јаворовић Б., Биланџић М. (2007). Пословне информације и бизнис интелигенце, Голден маркетинг, Техничка књига, ЗагребMarlin, S., Darvey M. (2004). *Disaster-Recovery Spending on the Rise*“, Information Week, Manhasset NY, Avgust 2004., p. 26.
[6] Муравъева И. (2006). *Новый взгляд на службу информационной безопасности компании*, (http: www.bre.ru/security/20033.html). доступан 14. 08. 2016.
[7] National Information Systems Security Glossary, NSTISSI No 4009, National Security Agency, Fort Meade MD, September 2000.
[8] Петковић, Т. (2009). Пословна шпијунажа и економско ратовање, Protexi Group System, Нови Сад
[9] Родић, Б., Ђорђевић Г. (2004). Да ли сте сигурни да сте безбедни, Продуктивност, Београд
[10] Триван, Д. (2012). Корпоративна безбедност, Досије студио, Београд

[11] Stallings, W. (1995).*Network and Internetwork Security – Principles and Practice*, Prentice Hall, Englewood Cliffs, New Jersey
[12] Stephenson, P. (2010). *Authentication: A pillar of information assurance*, SC Magazine, Vol. 21, No. 1, New York, January 2010., p. 55.
[13] Wolf G. D. (2003).*Statement before the House Select Committee on Homeland Security Subcommittee on Cybersecurity, Science and Research & Development*,National Security Agency US, Fort Meade MD.
[14] http://bis-expert.ru/bis-summit

Додатак:

Табела 1. Цурење информација по вектору деловања

Р.бр.	Вектор деловања	Проценат
1.	Спољашњи напади	32,2
2.	Унутрашњи напади	64,4
3.	Неопредељено	2,5

Табела 2. Цурење информација према извору

Р.бр.	Извор цурења	Проценат
1.	Руководилац	1,1
2.	Систем администратор	1,4
3.	Запослени	48,9
4.	Бивши запослени	2,3
5.	Спољни сарадник	7,6
6.	Спољашњи злонамерник	32,2
7.	Неопредељено	6,5

Табела 3. Цурење информација према типу података

Р.бр.	Тип података	Проценат
1.	Персонални подаци и финансијске информације	90,8%
2.	Комерцијална тајна, ноу-хау	5%
3.	Државна тајна	1,7
4.	Неопредељено	2,5

Табела 4. Инциденти према карактеру

Р.бр.	Карактер инцидента	Проценат
1.	Цурење информација	82
2.	Превара коришћењем података	10,3
3.	Прекорачење права доступа информацијама	7,7

Табела 5. Канали цурења информација

Р. бр.	Канал цурења информација	Проценат
1.	Крађа/губљење опреме	7,6
2.	Мобилни уређаји	0,2
3.	Преносиви медији	3,6
4.	Мрежа (браузер, клауд...)	45,6
5.	Електронска пошта	7,5
6.	Папирни документи	14
7.	Видео материјали	0,3
8.	Неопредељено	21,3

Табела 6. Случајни и намерни случајеви цурења информација

Р. бр.	Канал цурења информација	Проценат	
		Случајни	Намерни
1.	Крађа/губљење опреме	1,5	0,4
2.	Мобилни уређаји	0,3	0,2
3.	Преносиви медији	5,5	0,4
4.	Мрежа (браузер, клауд...)	27,4	73

5.	Електронска пошта	12,1	2,1
6.	Папирни документи	21,9	2,1
7.	Видео материјали	10,3	0,1
8.	Неопредељено	21	21,7

Табела 7. Цурење финансијских података по каналима

Р. бр.	Канал цурења информација	Проценат
1.	Крађа/губљење опреме	7,57
2.	Мобилни уређаји	0,63
3.	Преносиви медији	3,56
4.	Мрежа (браузер, клауд...)	45,57%
5.	Електронска пошта	7,49
6.	Папирни документи	14%
7.	Видео материјали	0
8.	Неопредељено	21,27