Acta oeconomica et informatica 1
Nitra, Slovaca Universitas Agriculturae Nitriae, 2009, s. 11–14

ANALÝZA BEZPEČNOSTI INFORMAČNÝCH SYSTÉMOV – SÚČASNÝ STAV V PODMIENKACH AGROREZORTU NA SLOVENSKU

ANALYSIS OF INFORMATION SYSTEMS SECURITY – ACTUAL SITUATION IN CONDITIONS OF AGROSECTOR IN SLOVAKIA

Milan KUČERA, Anton REPOVSKÝ, Milan FIĽA

Slovenská poľnohospodárska univerzita v Nitre

Information systems' security and information protection are becoming commonly used terms in the world. The need to increase the security comes from rising real and potential security threats. It is important to make information systems resist the forces they may be subjected to. Adequate degree of safety of information systems can guarantee every business continual development, as well as avoid undesirable loss of know-how. Information systems have markedly entered the management in Agrosector; however, Agrosector has in the field of IT a lot of drawbacks, which have to be analyzed and solved.

Key words: information system, audit of information systems, security of information systems, security

Pojem bezpečnosť sa stáva jedným zo základných aspektov analýzy dlhodobej spoľahlivosti informačných systémov. Rastúca závislosť tohto vzťahu je v súčasnosti výrazne stimulovaná vznikom bezpečnostných hrozieb vyplývajúcich z ilegálneho pôsobenia takzvaného kybernetického terorizmu. Ataky hrubej sily na informačné systémy nahrádzajú cielené, vysoko sofistikované útoky počítačových expertov smerujúce k zámernému poškodzovaniu systémov, alebo získavaniu informácií podporujúcich trestnú činnosť. V súčasnosti musí byť každá oblasť ekonomickej činnosti podporovaná požadovaným množstvom kvalitných informácií a informačných technológií podporujúcich ich spracovanie. V terajšom informačnom veku, v tomto kontexte, akékoľvek riziká ohrozujúce informácie súčasne priamo ohrozujú aj samotné podnikanie.

Témy bezpečnosti informačných systémov nachádzame v prácach Babinského (2004), Látečkovej (2007), Macka (2005), Lavrina (2000) a Naščákovej (2007).

Získavanie citlivých dát útočníkmi z počítača obete je považované zo strany odborníkov za jeden z hlavných problémov IT sektora. Tieto názory prezentujú aj Boyens a Gunther (2002), či Laclavík a Hluchý (2002).

K oblastiam hospodárstva, ktoré sú potenciálne ohrozené špecifikovanými rizikami, patrí aj agrorezort. Napriek relatívne nízkemu podielu poľnohospodárskej produkcie na celkovom hrubom domácom produkte v krajinách Európskej únie – menej ako 5 %, je nutné zdôrazniť, že bez vyprodukovania dostatočného množstva kvalitných potravín, pri čo najnižšej spotrebe nákladov, nie je možné garantovať potravinovú bezpečnosť regiónu. Aj v tejto oblasti hospodárstva začínajú plniť dôležitú úlohu progresívne prvky informatiky, a preto je zaistenie ich bezpečnosti pred možnými útokmi nevyhnutné, s ohľadom na budúci vývoj – kľúčové.

Vzhľadom na aktuálnosť témy bezpečnosti informačných systémov sa touto problematikou zaoberáme komplexne – – zhodnotením súčasného stavu bezpečnosti informačných systémov so zameraním na agrorezort, pomenovaním potenciálnych informačno-bezpečnostných hrozieb a rizík vo vybraných podnikoch a náčrtom možných návrhov riešení v tejto oblasti, s dôrazom na zaistenie čo najvyššieho stupňa ochrany dát i systému ako celku.

Materiál a metódy

Pri spracovaní príspevku boli ďalej použité poznatky získané z dostupnej literatúry, ako aj vlastné praktické skúsenosti s užívateľskou i administrátorskou prácou s informačnými systémami.

Za účelom získania dostatočných podkladových údajov pre vypracovanie príspevku sme uskutočnili výber poľnohospodárskych podnikov, na ktorých bol uskutočnený dotazníkový prieskum obsahujúci otázky bezpečnosti informačných systémov. Na 25 otázok dotazníkového prieskumu odpovedali manažéri poľnohospodárskych podnikov, v ktorých kompetencii je v danom dotazovanom subjekte problematika informačných systémov a informačnej bezpečnosti. V prieskume sme sa zamerali na poľnohospodárske podniky typu poľnonákup. Hlavným predmetom činnosti tejto skupiny právnických subjektov je výroba kŕmnych zmesí – premixov, koncentrátov a krmív, skladovanie poľnohospodárskych komodít rastlinného pôvodu, ako aj nákup a predaj krmív, kŕmnych komponentov a kŕmnych aditív.

Podľa zvoleného kritéria, prevádzkovateľa verejného skladu, sme z predmetnej skupiny podnikateľských subjektov vybrali 53 spoločností. Z vybraného súboru podnikov na dotazníkový prieskum reagovalo 19 poľnohospodárskych podnikov. Z celkového počtu zaslaných dotazníkov odpovedalo 36% subjektov.

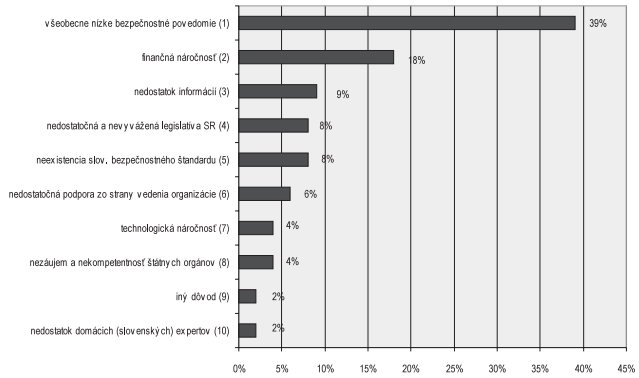
Pri skúmaní uvedenej problematiky boli použité metódy pozorovania, riadeného rozhovoru s administratívnymi i manažérskymi pracovníkmi z oblasti poľnohospodárstva, IS a aj IT, dotazníkový prieskum v reprezentatívnej vzorke poľnohospodárskych podnikov a taktiež boli použité metódy analýzy a syntézy podkladových materiálov a spracúvaných dát.

Výsledky a diskusia

Informačnú bezpečnosť môžeme vo všeobecnosti definovať ako určitý proces ochrany dát pred ich náhodným, alebo úmyselným zneužitím osobami v rámci organizácie alebo mimo nej. Jej chápanie len na úrovni technologickej záležitosti vedie čas-

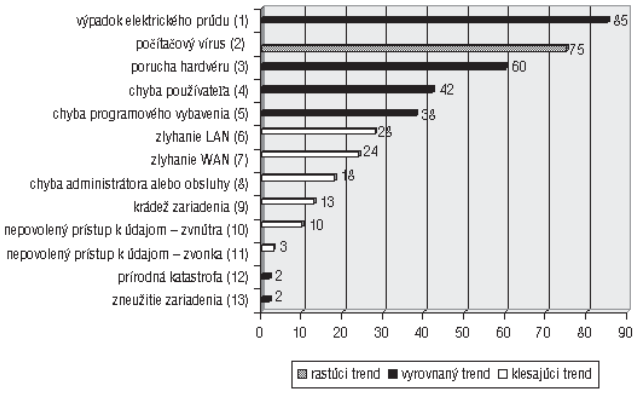
to k nesprávnemu stanovovaniu priorít a k podceňovaniu potenciálnych rizík. Mnohokrát sa stretávame s názorom, že odbor IT má vedieť určiť adekvátnu úroveň bezpečnosti v organizácii. Potreba zabezpečiť ochranu informácií je ale v prvom rade odvodená od dôležitosti a citlivosti samotných informácií pre jednotlivé podnikateľské činnosti, ktoré je primárne schopný posúdiť skôr používateľ údajov ako pracovník IT.

Podľa Laclavíka a Hluchého (2002) je bezpečnosť veľmi dôležitou požiadavkou všetkých systémov. Veľmi často sa objavujú bezpečnostné nedostatky a úspešné útoky hakerov, ktorí využívajú programové nedostatky a nedôslednosť ochrany dát užívateľov. Macko (2005) zdôrazňuje, že základným komunikačným prostriedkom počítačov je internet. Závažným problémom je škodlivý softvér, ktorý sa cez vysokorýchlostnú linku veľmi rýchlo dokáže dostať do počítača. Niektoré zistenia ukazujú, že správna funkčnosť nezabezpečeného počítača, pri vysokorýchlostnom pripojení na sieť Internet, trvá len niekoľko minút. Podľa odhadov laboratória McFee Avert Labs existuje pre rok 2007 viac ako 217 000 rôznych druhov doteraz známych bezpečnostných hrozieb. Napriek tomu, to veľká časť používateľov stále podceňuje.



Graf 1 Najväčšie prekážky informačnej bezpečnosti v SR
Zdroj: KPMG Slovensko

Chart 1 The most significant objection to information security supporting in Slovakia
(1) generally low security awareness, (2)high financial costs, (3) lack of information, (4) absence of Slovak security standart, (5) deficient legislation in Slovakia, (6) lack of management support in organisation, (7) incompetency of national institution, (8) factor intensity of technology, (9) others, (10) lack of IS security experts



Graf 2 Vyskyt bezpečnostných incidentov a trend ich výskytu
Zdroj: KPMG Slovensko

Chart 2 Security incident occurrence and ists trend
(1) electricity blackout, (2) computer viruses, (3) hardware failures, (4) mistake of user, (5) software failures, (6) crashes of computer network (LAN), (7) crashes of internet (WAN), (8) mistake of administrator, (9) steal / device abuse, (10) unauthorized access to data from Co. network, (11) unauthorized access to data from outside, (12) natural catastrophe, (13) abuse of company ICT

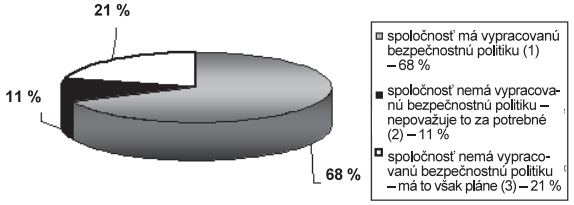
Informačná bezpečnosť v podnikoch v SR

Na prieskum stavu informačnej bezpečnosti sa zameral časopis DSM v spolupráci so spoločnosťou KPMG Slovensko, s.r.o. a Národným bezpečnostným úradom Slovenskej republiky. Z ich výsledkov vyplýva, že k najväčším prekážkam presadzovania informačnej bezpečnosti na Slovensku patria všeobecne nízke bezpečnostné povedomie (39 %), finančná náročnosť (18%), nedostatok informácií (9%) ako aj nedostatočná legislatíva a neexistencia slovenského bezpečnostného štandardu (8%). Čo sa týka výskytu bezpečnostných incidentov, k najčastejším patria paradoxne na prvý pohľad banálne výpadky elektrického prúdu a počítačové vírusy. Práve vírusy vo svojich rôznych formách zaznamenávajú ako jediné rastúci trend. Len 27–62 % respondentov (podľa segmentu, v ktorom pôsobia) sa domnieva, že sa bezpečnosti kladie adekvátna pozornosť, pričom však takmer všetci pripisujú bezpečnosti veľký význam.

Z výsledkov vlastného dotazníkového prieskumu realizovaného na súbore vybraných poľnohospodárskych podnikov vyplýva, že takmer tretina spoločností nemá vypracovanú komplexnú bezpečnostnú politiku a približne pätina respondentov to ani nepovažuje za potrebné (Graf 3). V tejto súvislosti je potrebné podotnúť, že je to tak aj napriek tomu, že spoločnosti sú aspoň v rozsahu zákona o ochrane osobných údajov povinné vypracovať bezpečnostný projekt s identifikáciou rizík a návrhom účinných opatrení.

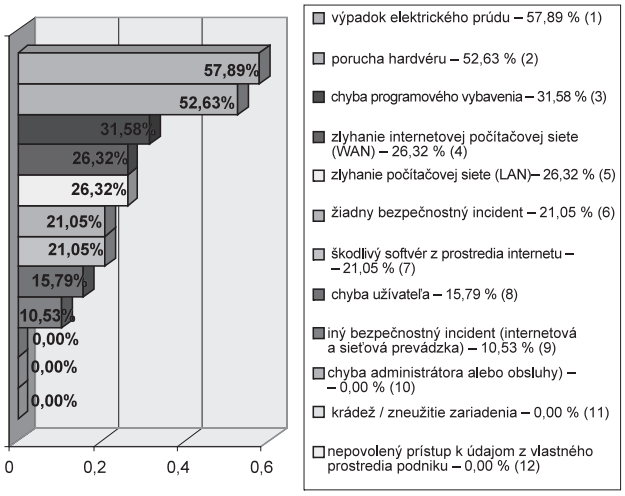
V rámci nášho výskumu sa často stretávame s názorom, že informačná bezpečnosť je drahá a spoločnosti sa ňou adekvátne nezaoberajú, pretože nemajú na ňu dostatok prostriedkov. Prieskum však potvrdil, že nie nedostatok financií, ale najmä podceňovanie rizík a nízke bezpečnostné povedomie sú hlavnou príčinou, nedostatočného záujmu o bezpečnosť informačných systémov. Výpadky systémov pritom môžu mať nepriaznivý dosah na fungovanie organizácie. Najčastejšími bezpečnostnými incidentmi sú zlyhania technologických prvkov, pričom až 5 zo 7 najčastejších incidentov priamo vedie k výpadku funkčnosti systémov (výpadok prúdu, zlyhanie počítačových sietí, porucha hardvéru a softvéru). Tieto najčastejšie incidenty boli zároveň respondentmi označené ako bezpečnostné incidenty s najzávažnejšími dosahmi. Napriek tomu, že škody spôsobené bezpečnostnými incidentmi sú často podceňované hoci môžeme konštatovať, že už len priame finančné škody často nie sú marginálne.

Najčastejšie sa vyskytujúcim bezpečnostným incidentom v cieľovej skupine podnikov je obdobne ako v celoslovenskom prieskume výpadok elektrického prúdu. K ďalším často sa vyskytujúcim incidentom patria porucha hardvéru, chyba programového vybavenia, i zlyhávanie siete (podrobne Graf 4).



Graf 3 Dokumentácia komplexnej bezpečnostnej politiky spoločnosti
Zdroj: vlastný výskum

Chart 3 Documentation on complex security policy of the company
(1) company uses security policy, (2) company has not security policy – it is considering as unnecessary, (3) company has not security policy – it is considering as necessary



Graf 4 Bezpečnostné incidenty v PIS za kalendárny rok 2007
Zdroj: vlastný výskum

Chart 4 Security incidents in company information system in 2007
(1) electricity blackout, (2) hardware failures, (3) software failures, (4) crashes of internet (WAN), (5) crashes of computer network (LAN), (6) no security incidens (7) malware from internet, (8) mistake of user, (9) other security incident, (10) mistake of administrator, (11) steal / device abuse, (12) unauthorized access to data from company network

Zo skúseností podnikov je možné vo všeobecnosti konštatovať, že pokiaľ je organizácia pripravená na prípadné havárie a neočakávané incidenty, dokáže prípadné škody výrazne eliminovať. Žiaľ až 54 % organizácií nemá vypracované plány obnovy funkčnosti informačného systému pre prípady mimoriadnych udalostí. Mnohé spoločnosti sa spoliehajú len na strohé zálohovanie dát, ktoré vo väčšine prípadov nestačí.

Bezpečnosť informácií a legislatíva SR

Slovenská legislatíva upravuje bezpečnosť informácií len okrajovo. Rámcové požiadavky na bezpečnosť spravovania údajov sa objavujú v legislatíve týkajúcej sa činnosti finančných inštitúcií, aj preto práve tieto riešia otázky bezpečnosti ako jednu zo svojich priorít.

V zmysle zákona č. 428/2002 Z. z. o ochrane osobných údajov v znení a doplnení ďalších zákonov č. 602/2003 Z. z., č. 576/2004 Z. z. a č. 90/2005 Z. z. je každá organizácia, ktorá spracúva osobné údaje a má viac ako 5 zamestnancov, povinná vypracovať tzv. Bezpečnostný projekt, ktorý musí obsahovať:

- bezpečnostný zámer,
- analýzu bezpečnosti informačných systémov,
- bezpečnostné smernice.

V rámci tohto projektu musí príslušná organizácia identifikovať všetky informačné systémy, ktoré spracúvajú osobné údaje fyzických osôb. Informačným systémom je pre účely príslušného zákona a bezpečnostného projektu napríklad kartotéka zamestnancov, register, papierový zoznam, záznam, prezenčná listina, digitálna databáza, alebo iná ľubovoľná sústava obsahujúca materiály napr. spisy, doklady, zmluvy, potvrdenia, posudky, hodnotenia, testy, ktoré obsahujú osobné údaje fyzických osôb. Účel spracovania určuje prevádzkovateľ s použitím automatizovaných, alebo neautomatizovaných prostriedkov spracúvania ešte pred jeho začatím, pričom k spracovaniu osobných údajov je potrebný súhlas dotknutej fyzickej osoby, ktorej osobné údaje sú predmetom spracovania.

Bezpečnostný projekt musí nevyhnutne obsahovať identifikáciu možných rizík vrátane určenia ich pravdepodobností výskytu a miery dopadov na informačný systém a samotné chránené osobné údaje. potrebné je tiež určiť návrh opatrení v prípade ich výskytu. Taktiež je dôležité určenie zvyškových rizík.

Celoslovenský prieskum zameraný na vplyv zákona č. 215/2004 Z. z. o utajovaných skutočnostiach a zákon č. 428/2002 Z. z. o ochrane osobných údajov ukázal, že vplyv tejto legislatívy je značný, pretože až polovica oslovených organizácií ich označila za tie, ktoré výrazne prispeli k úpravám v oblasti ochrany údajov. Zároveň priniesli do organizácií vedomie o tom, že citlivé informácie je potrebné chrániť pred odcudzením a najmä zneužitím.

Manažment informačnej bezpečnosti

Oblasť informačných technológií a bezpečnosť informácií patrí do prvej pätice najproblémovejších oblastí manažérov. Výskumy MET Group Gartner poukazujú na to, že priemerné výdavky na bezpečnosť v organizáciách skupiny Global 2000 prestavujú len 3–4% ich rozpočtu. Na základe mnohých celosvetových prieskumov je možné konštatovať, že na bezpečnosť informačných systémov sa z rozpočtu IT vyčleňuje v organizáciách len 5–8% v závislosti od veľkosti, regiónu a oblasti podnikania spoločností.

Boyens a Günther (2002) konštatujú, že súčasný stav bezpečnosti prenosu dát a ochrany privátnych údajov v počítačových sieťach je neuspokojivý. Väčšia časť poskytovaných služieb pracuje na báze dôvery. Aj keď je často mnoho dôvodov prečo dôverovať providerovi služieb, nesmie sa to považovať za pravidlo.

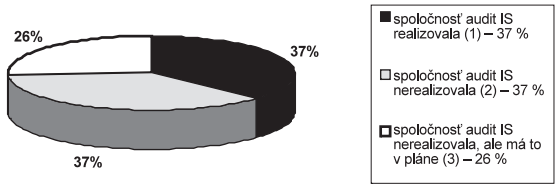
Pre stanovenie nákladov v oblasti bezpečnosti informácií je nutná identifikácia úloh a aktivít, ktoré sa čiastočne alebo úplne zahrnú do rozpočtu pre informačnú bezpečnosť. Pre každú z daných činností, hardvér, softvér, služby a kompletný personál by mali byť stanovené náklady.

V rámci zhodnotenia stavu investícií do bezpečnosti informačných systémov na Slovensku môžeme konštatovať, že väčšina spoločností preferuje prevažne vstupy do bezpečnosti sietí a do ochrany pred vírusmi. Prioritou je to až pre 28% podnikov. Na základe toho sa dá konštatovať, že väčší dôraz sa kladie na technologické opatrenia ako na rozvoj po stránke organizačnej, či personálnej. Zatiaľ len v malom počte spoločností sa zavádza systém manažmentu informačnej bezpečnosti. Taktiež sa nevytvára strategické smerovanie vedúce k pravidelným periodickým analýzam rizík. Pomocou v tejto oblasti by mohla byť podpora certifikácie organizácií v zmysle medzinárodného štandardu ISMS – ISO/IEC 27001:2005.

Audit informačných systémov

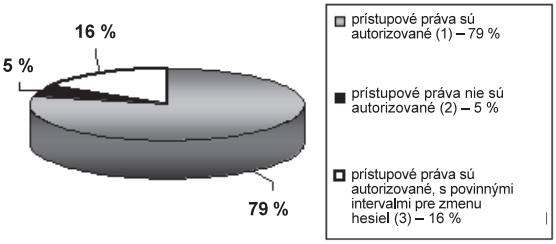
Podľa názoru Babinského (2004) musí mať každá firma, ktorá spracováva účtovníctvo a finančné podklady v elektronickej forme, zabezpečené údaje voči internému a externému úniku informácií. Celková úroveň bezpečnosti systému je daná jeho najslabším článkom. Jedným zo spôsobov nepriamej ochrany digitálnych údajov je audit informačných systémov, ktorého súčasťou je audit bezpečnosti počítačovej siete.

Samotné IS sa neustále modernizujú a prinášajú v sebe kombinované riešenia ochrany na viacstupňovej úrovni, ktorá zahŕňa napr. firewall, antivírusové programy, či detekcia útokov na systém. Audítor pritom analyzuje ich potrebu, funkčnosť a obmedzujúce faktory. Pre organizáciu je nevyhnutné, aby audítor hodnotil procesy spojené s riadením všetkých bezpečnostných komponentov. Lavrin (2000) tvrdí, že informačné technológie / informačné systémy predstavujú významný podiel na podnikových aktívach aj investičnom rozpočte. Z týchto dôvodov sa interný audítor musí zúčastňovať všetkých aspektov informačných technológií / informačných systémov s cieľom



Graf 5 Realizácia auditu IS v podnikoch
Zdroj: vlastný výskum

Chart 5 Realization of IS audit in companies
(1) company realized IS audit, (2) company did not realize IS audit, (3) company did not realize IS audit – audit is planned



Graf 6 Zabezpečenie modulov IS autorizovanými prístupovými právami
Zdroj: vlastný výskum

Chart 6 IS modules security by authorised access rules
(1) access rules are authorized, (2) access rules are not authorized – it is not important for company, (3) access rules are authorized with comlupsory intervals for passwords changing

uistenia, že podnikové aktíva sú chránené a že primerané interné kontroly podporujú ochranu informačných zdrojov.

V rámci analyzovanej skupiny podnikov sme zisťovali realizovateľnosť bezpečnostných auditov informačných systémov v uplynulých dvoch rokoch. Z výsledkov vyplýva, že až 63% oslovených spoločností deklaruje potrebu realizácie auditu informačného systému (podrobne Graf 5). Práve tu sa črtá priestor pre zverenie auditu informačných systémov do rúk certifikačného orgánu s cieľom identifikovať možné riziká, zabezpečiť ich elimináciu a v konečnom dôsledku nastaviť proces informačnej bezpečnosti na úroveň zodpovedajúcu príslušnej medzinárodnej norme ISO/IEC 27001:2005.

Vysoko účinným spôsobom ochrany dát a softvérových prostriedkov informačného systému je racionálny manažment prístupových práv jednotlivých podsystémov IS. Užívatelia IS musia byť zadelení do kategórií podľa problémových oblastí a práv na spracovanie informácií. Minimálnym požadovaným členením kategórií je kategória správy programu – modulu a kategória s právami na čítanie. Užívateľovi – členovi kategórie prislúchajú práva pridelené kategórii, ktorej je členom. Ak je užívateľ členom viacerých kategórií, práva sa mu zlučujú. Správny manažment prístupových práv predpokladá pravidelnú povinnosť zámeny prístupových hesiel do jednotlivých modulov systému zo strany zodpovednej osoby.

Z poznatkov získaných dotazníkovým prieskumom môžeme konštatovať, že až 95% spoločností autorizuje prístupové práva do jednotlivých podsystémov. Približne 17% z nich deklaruje aplikovanie autorizácií prístupových práv s povinnými intervalmi pre zmenu hesiel (Graf 6).

Stav bezpečnosti informačných systémov a samotných informácií v nich spracovávaných považujeme v súčasnosti na Slovensku za neuspokojivý. Napriek relatívne nízkemu počtu výskytu verejne známych útokov, ktoré by spôsobili výraznú škodu, v poslednom období rastie potenciálne riziko vzniku takýchto incidentov vo väčšom rozsahu. Nové hrozby už nie sú kódy začínajúcich programátorov, ktorí chcú zaujať, súčasný malvér (škodlivý softvér) je vo väčšine prípadov tvorený na objednávku pre organizované skupiny, s konečným cieľom vytvoriť finančný zisk. Zameraný je najmä na odcudzenie citlivých informácií. Z tohto dôvodu je potrebné pristupovať k ochrane informačných systémov komplexne. Investície do kvalitných firewallov a antivírusových softvérov už nie je postačujúce. Požaduje sa pravidelne vykonávať bezpečnostné audity a vytvárať systémy manažmentu bezpečnosti. Uvedené konštatovanie platí aj pre odvetvie agrorezortu, ktoré je v mnohých prípadoch známe nízkymi investíciami do prvkov zabezpečenia informačných systémov.

Súhrn

Bezpečnosť informačných systémov a informačná ochrana sa vo svete stávajú bežne používanými pojmami. Potreba zvýšenia bezpečnosti systémov a informácií vyplýva zo skutočných a potenciálnych bezpečnostných hrozieb. Je dôležité upravovať informačné systémy tak, aby bezpečne odolávali útokom, ktorým môžu byť vystavené. Ich dostatočná miera ochrany môže zabezpečiť kontinuálny priebeh i rozvoj podnikania, a tiež zabrániť nežiadanej strate know-how. Informačné systémy vstupujú čoraz výraznejšie i do riadenia v agrorezorte, kde sa zároveň objavujú aj značné nedostatky v dostatočnosti i spôsobe ich ochrany v podmienkach SR.

Kľúčové slová: informačný systém, audit informačných systémov, bezpečnosť informačných systémov, bezpečnosť

Literatúra

BABINSKÝ, R. 2004. Informačná bezpečnosť v malých a stredných firmách. In: Mladá veda 2004 : Zborník vedeckých prác. Nitra : SPU, 2004. s. 27. ISBN 80-8069-455-9

BOYENS, C. – GÜNTHER, O. 2002. Trust is not Enough: Privacy and Security in ASP and Web Service Environments. In: ADBIS 2002 – Advances in Databases and Information Systems: 6th East European Conference, Proceedings. Bratislava : Springer – Verlag Berlin Heidelberg New York, 2002. p. 8–22. ISBN 3-540-44138-7

LACLAVÍK, M. – HLUCHÝ, L. 2002. Agents as Key Elements for Information Security and Privacy. In: Electronic computers and informatics 2002 : Proceedings of the fifth international scientific conference. Košice – Herľany : University of technology Košice, Faculty of electrical engineering and informatics, 2002. p. 64–68. ISBN 80-7099-879-2

LÁTEČKOVÁ, A. 2007. Informačné systémy v riadení poľnohospodárskych podnikov. In: Acta oeconomica et informatica, roč. 10, 2007. č. 2, s. 49–51, ISSN 1335-2571

LAVRIN, A. 2000. Introduction to Information Systems Auditing. Košice : Elfa, s.r.o., 2000. s. 68. ISBN 80-88964-78-4

MACKO, O. 2005. Editorial. In: PC Revue roč. 8, 2005, č. 7. s. 1. ISSN 1335-0226

NAŠČÁKOVÁ, J. – KUŽDÁK, V. 2007. Manažment a informačné systémy. In: Trendy v systémoch riadenia podnikov : 10. medzinárodná vedecká konferencia, Vysoké Tatry – Štrbské Pleso, 15.–17. október 2007 : Zborník príspevkov v elektronickej forme. Košice : TU SjF, 2007. 5 s. ISBN 978-80-8073-885-3

Zákon NR SR č. 428/2002 Z. z. o ochrane osobných údajov, v zmysle zmien a doplnení vykonaných zákonom č. 602/2003 Z. z., zákonom č. 576/2004 Z. z. a zákonom č. 90/2005 Z. z.,

http://www.kpmg.sk/dbfetch/52616e646f6d49564b64792da8fc7c0542bf13af1bc9c94e/prieskum_ psib_ 2006.pdf – Prieskum stavu informačnej bezpečnosti v SR 2006, cit. [2007-12-12]

Kontaktná adresa:
doc. Ing. Milan Kučera, CSc., FEM, SPU v Nitre, Tr. A. Hlinku 2, 949 01, Nitra, ☎ +421 37 641 4191; e-mail: milan.kucera@fem.uniag.sk; Ing. Anton Repovský, ☎ +421 37 641 4191, e-mail: antonrepovsky@gmail.com; Ing. Milan Fiľa, ☎ +421 37 641 41 79, e-mail: milan.fila@fem.uniag.sk