Bezpečnosť IS podniku – vybrané aspekty

Information system security of enterprises – selected aspects

Zuzana KORCOVÁ

Abstract
Security of information systems in enterprises are becoming increasingly importance. Information stored in computer memory, in the electronic documents sent via computer network are threatened from the outside and from inside of the company. information is very important for company and its damage or loss affect the profit. Enterprise security policy should be maintained and updated regularly. The paper deals with some aspects that are still relevant for the security of information systems in economic but also in the social sphere, and therefore the information systems of universities.

Keywords
information system, data protection, information security, software products, systems DLP

Úvod

Využívanie informačných a komunikačných technológií (ďalej IKT) vo všetkých oblastiach života spoločnosti, hlavne v hospodárskej, už dávno nie je len otázkou módy alebo prestíže, ale je už nevyhnutnou podmienkou existencie i rozvoja jednotlivých organizácií. S tým nutne súvisí prirodzená snaha o čo najefektívnejšie využívanie informačných systémov. Čím je informačný systém pre organizáciu efektívnejší, tým je činnosť organizácie, jej schopnosť plniť svoje poslanie, závislejšia na správnej a neprerušenej činnosti tohto systému. Bezpečnostná politika podniku by mala obsahovať riešenie problémov, ktoré môžu nastať pri využívaní informačných systémov. Cieľom príspevku je poukázať na niektoré problémy bezpečnosti IS a niektoré postupy a nástroje na ich riešenie. Použité zdroje sú materiály z odborných časopisov, dokumenty a správy odborníkov, odborné publikácie a niektoré výsledky prieskumov, ktoré boli uverejnené na Internete. Závery boli formulované prostredníctvom syntézy na základe poznatkov odborníkov z radov profesionálov IT v oblasti bezpečnosti IS, vyjadrenia vedúcich pracovníkov niektorých podnikov a na základe skúseností autorky príspevku z používania IS organizácie.

Výsledky a diskusia

Bezpečnosť – neustály proces

Každý podnik potrebuje definovať realizované procesy a premietnuť ich do bezpečnostnej politiky svojej organizácie. Ak chýba vypracovaná bezpečnostná politika alebo ju v podniku nedôsledne dodržiavajú dochádza k úspešným útokom proti informačnému systému. Vypracovať bezpečnostnú politiku je zložitý, ale nevyhnutný proces. Sú potrebné konzultácie s odborníkmi, ktorí majú v tejto oblasti bohaté skúsenosti a poznajú aj medzinárodné štandardy a rôzne normy. Spojenie odborníkov z IT a manažérov prispeje ku skvalitneniu procesu vypracovania bezpečnostnej politiky.

Zabezpečenie IS chápeme z rôznych hľadísk, ale najväčšiu hrozbu stále predstavujú vírusy a ďalší malware. Tieto sa šíria najmä prostredníctvom Internetu. Väčšina infiltrácií má zvyčajne ekonomické pozadie a slúži ako nástroj na kriminálnu činnosť. V súčasnosti má

kriminálna činnosť v oblasti IKT veľa podôb, spoločné majú infiltrácie to, že sú ziskové – výnosné. Sú také výnosné, že v celosvetovom rozsahu už dobiehajú aj drogovú oblasť. Túto kriminálnu činnosť už nevykonávajú iba jednotlivci, ale dobre organizované a finančne motivované skupiny.
Ďalší dôležitý prvok zabezpečenia je definovanie potrebných oprávnení každého používateľa vzhľadom na informačný systém podniku a jeho používateľov. Často sa stáva, že používatelia v rôznych pracovných pozíciách pracujú s právami administrátora.

Na prenosných počítačoch a dnes už aj na mobilných telefónoch sa ukladajú súbory, ktorých strata alebo poškodenie predstavuje väčšiu škodu ako cena ukradnutého notebooku alebo mobilného telefónu alebo strateného USB kľúča. Podniky si to uvedomujú, ale neimplementujú žiadne šifrovanie súborov a e-mailov. Nástroje na šifrovanie sú k dispozícií v každom operačnom systéme.
Najslabší kameň, na ktorý sa sústreďujú útočníci, je človek. Sociálne inžinierstvo nevyžaduje hlboké znalosti z oblasti IKT, orientuje sa na zneužívanie prirodzených ľudských vlastností, ktorými sú dôvera, lenivosť, strach alebo nevedomosť. Priamu zodpovednosť za vzniknuté škody prenáša útočník na používateľa, ak sa mu podarí ho presvedčiť na nežiaducu činnosť.

Ochrana dokumentov a citlivých informácií v IS podniku
Informácie, ktoré sú uložené v podnikových dokumentoch predstavujú riziko zneužitia, a toto riziko môže mať priamy vplyv na hospodársky výsledok podniku. Podniky však majú povinnosť ochraňovať dokumenty aj podľa platnej legislatívy, bez ohľadu na to, či to chcú alebo nechcú. Ochrana informácií v dokumentoch je teda nielen v záujme podniku samotného, ale aj povinnosť podniku. Má to veľký význam, pretože z hľadiska nákladov je vždy lacnejšie uskutočňovať preventívne opatrenie ako financovať vzniknuté škody vzniknuté stratou alebo únikom informácií v dokumentoch. Softvérové riešenia ochrany dokumentov poskytujú systémy Data Loss Prevention (DLP), ktoré umožňujú identifikáciu citlivých informácií na miestach uloženia i počas ich putovania po sieti.
Niektoré technológie DLP, ktoré poskytujú softvérové firmy:
Systémy Microsoftu Windows Server obsahujú technológiu, ktorá má ochraňovať elektronické dokumenty. Je to technológia Active Directory Right Management Services (AD RMS). V základnej konfigurácii zabezpečuje ochranu dokumentov Microsoft Office, e-mail a intranet. Ďalší vývoj AD RMS je zameraný na ďalšie produkty Microsoftu ako i produkty ďalších softvérových firiem.
Medzi technológie DLP patrí i riešenie networkbase DLP, ktoré je pomenované ako Cisco IronPort. Toto zariadenie umožňuje blokovanie správ s tajnými, prípadne s citlivými informáciami (rodné čísla, čísla účtov, čísla kreditných kariet, a pod). Medzi základné technológie v riešeniach DLP patrí šifrovanie. V prípade IronPortu je to vynútené automatické šifrovanie, ktoré môže predstavovať jedno z opravných riešení v takých situáciách, keď musia byť citlivé informácie doručené.
Technológia DLP, nazvaná Cisco Security Agent, umožňuje kontrolovať a následne povoliť alebo zakázať spúšťanie vybraných aplikácií. Ďalej môže kontrolovať kopírovanie citlivých informácií na prenosné médiá (USB kľúče, Bluetooth, CD, DVD, prenosné disky)
Aj keď mnohé riešenia DLP vedia už zabezpečiť veľa situácií, ochrana podnikových údajov je závislá od správania každého zamestnanca v podniku.

Informačná bezpečnosť na Slovensku

Prieskum stavu informačnej bezpečnosti v SR 2008 uskutočnil Ernst & Young v spolupráci s časopisom DSM – Data Security Management a Národným bezpečnostným úradom, pričom sa zameral na vybranú reprezentatívnu vzorku stredných a veľkých spoločností, pokrývajúcu všetky významné sektory ekonomiky.

Prieskum ukázal, že význam informačnej bezpečnosti v slovenských podnikoch rastie, pričom až 82 % organizácií hodnotí úroveň riešenia bezpečnosti optimisticky. Aj napriek tomu viac ako dve tretiny spoločností stále nemajú zamestnaného žiadneho špecialistu zaoberajúceho sa prioritne informačnou bezpečnosťou a naďalej pretrváva trend riadiť bezpečnosť iba v rámci IT oddelenia. Výsledky prieskumu ukázali tiež, že podniky si u svojich bezpečnostných pracovníkov najviac cenili vecné znalosti problematiky, IT technológií a flexibilitu a, naopak, najviac im chýbala znalosť finančného riadenia a schopnosť efektívnej komunikácie s vedením. Z prieskumu ďalej vyplýva, že väčšina podnikov zastavuje investície do nových IT riešení a funguje v udržiavacom režime. Hlavnou prioritou v oblasti informačnej bezpečnosti sa stáva riešenie už identifikovaných známych problémov. Najväčšími bezpečnostnými výzvami v minulom období boli prechod na euro a implementácia nových operačných systémov.

Záver

Informačné systémy a ich bezpečnosť neustále ovplyvňujú používateľov. Používateľ je často najslabší článok v bezpečnosti IS. Údaje v IS predstavujú najvyššiu hodnotu, ktorú treba chrániť, a to aj pred samotnými používateľmi. Práca v oblasti bezpečnosti IS je predovšetkým práca s ľuďmi a vyžaduje neustálu komunikáciu s nimi. Pracovníci nebudú prijímať bezpečnostnú politiku hneď a s nadšením. Aj toto je dôvod na konštatovanie, že bezpečnosť je proces, ktorý sa vyskytuje stále a nikdy sa nekončí.

Odborníci z oblasti IT tvrdia, že ochrana pred stratou alebo poškodením citlivých údajov má byť súčasťou podnikovej kultúry a má sa na nej podieľať každý zamestnanec.

Ochranu dokumentov a citlivých informácií v IS si podnik zabezpečí aj kvalitnými softvérovými produktmi, ktoré sú v súčasnosti dostupné v dostatočnom množstve..

Abstrakt

Bezpečnosť informačných systémov podnikov nadobúda čoraz väčší význam. Informácie uložené v počítači, na pamäťových médiách, v elektronických dokumentoch, posielané počítačovou sieťou sú ohrozené z vonku i z vnútra podniku. Pre podnik sú informácie veľmi dôležité a ich poškodenie alebo strata majú vplyv na hospodársky výsledok. Bezpečnostná politika podniku by sa mala dodržiavať a pravidelne aktualizovať. Príspevok sa zaoberá niektorými aspektmi, ktoré sú stále aktuálne pre bezpečnosť informačných systémov v hospodárskej, ale aj v spoločenskej sfére, a teda aj pre informačné systémy vysokých škôl.

Kľúčové slová

informačný systém, ochrana údajov, informačná bezpečnosť, softvérové produkty, systémy DLP

Literatúra

[1] HALEČKA, M.: Ochrana dokumentov vo firemnom prostredí, In: INFOWARE 10/2009, Bratislava, 2009, s. 19, ISSN: 1335-4787

[2] HENNYEYOVÁ, K.: Bezpečnosť digitálneho prostredia na Slovensku. In: Medzinárodné vedecké dni 2006 - Konkurencieschopnosť v EÚ - výzva pre krajiny V4 . 1. vyd. - Elektronický konferenčný zborník. - Nitra : Slovenská poľnohospodárska univerzita, 2006. - ISBN 80-8069-704-3. - S. 1510-1514. - 1 elektronický optický disk (CD-ROM).
[3] KORCOVÁ, Z.: Vybrané aspekty bezpečnosti IS v, CD-ROM mechanika. In: Aktuálne problémy riešené v agrokomplexe [elektronický zdroj] : zborník recenzovaných príspevkov, Nitra : SPU, 2008. - ISBN 978-80-552-0151-1. - S. 423-427
[4] RAJNOCH, M – MACKO, V.: Ochrana pred únikom citlivých informácií, In: INFOWARE 10/2009, Bratislava, 2009, s. 20, ISSN: 1335-4787
[5] TLAČOVÝ SERVIS PCR: Prieskum stavu informačnej bezpečnosti v SR 2008 23.1.2009 09:54, Dostupné na Internete: <http://www.itnews.sk/buxus_dev/generate_page.php?page_id=58195>
[6] ULÍK, B.: Bezpečnosť ako nikdy nekončiaci proces, In: INFOWARE 10/2009, Bratislava, 2009, s. 18, ISSN: 1335-4787

Kontakt

Ing. Zuzana Korcová, KI FEM, SPU v Nitre, Tr. A. Hlinku 2, 949 76 Nitra,
tel.: 037/641 4172, e-mail: Zuzana.Korcova@uniag.sk

Recenzent: Ing. Eva Oláhová, CIT FEM SPU v Nitre