Bezpečnostné aspekty využívania IKT v podnikoch

Security aspects in the use of ICT in enterprises

Klára HENNYEYOVÁ (SR)

ABSTRACT

Information and communication technologies and information systems in enterprises must be able to provide managers current and reliable information in real time and these must be adequate secure. Information security is a very important task for all users of ICT and IS. Information security is defined as the ability of the network and information system as a whole to withstand with a certain level of confidence against of accidental events, or unlawful or malicious actions that compromise the availability, authenticity, integrity and confidentiality of stored or transmitted data and related services offered by these networks and systems.

KEY WORDS

information and communication technologies (ICT), informatization of the society, information security, information system

ÚVOD

Informačná spoločnosť je charakteristická využívaním digitálneho spracovávania, uchovávania a prenosu informácií. Technologickou základňou tejto zmeny je využívanie prvkov moderných informačných a komunikačných technológií. Hlavnými znakmi informačnej spoločnosti sú prevaha práce s informáciami, interaktivita, integrácia a globalizačné trendy. Z technologického pohľadu potom možno informačnú spoločnosť označiť ako spoločnosť, ktorá vo vysokej miere využíva IKT založené na prostriedkoch výpočtovej techniky a s tým spojenú digitalizáciu.

S rozvojom informačných technológií v posledných desaťročiach, ako aj s globalizáciou svetového informačného priestoru súvisí nárast množstva zaznamenaných, ale aj nezaznamenaných informácií. Pre akýkoľvek podnik je dnes jednou z kľúčových úloh efektívne získavať, využívať a chrániť informácie z okolitého, ako aj z vnútorného prostredia. Úlohu úspešne sa orientovať v tomto rozsiahlom informačnom priestore berú na seba informačné systémy.

Informačná bezpečnosť je proces ochrany dát pred ich náhodným alebo úmyselným zneužitím osobami v rámci alebo mimo organizácie, vrátane zamestnancov, alebo aj obávaných hackerov. Narušenie bezpečnosti môže zahŕňať rôzne činnosti, napr. poškodenie vzhľadu webovej stránky, napadnutie počítačovým vírusom, zlyhanie zamestnanca, ktorý neúmyselne prezradí svoje heslo, a pod. Informačná bezpečnosť v tomto kontexte je vyváženie rizík výhodami v podobe vykonávania činností elektronicky.

MATERIÁL A METÓDY

Hlavnou úlohou v oblasti informačnej bezpečnosti je vytvoriť jednotnú platformu budovania informačnej spoločnosti postavenú na právnych základoch so zabezpečením primeranej ochrany a dôveryhodnosti digitálneho priestoru Slovenska. Nevyhnutnosťou pre úspešné plnenie tejto úlohy je vytvorenie *Národnej stratégie pre informačnú bezpečnosť (NSIB) v SR*, ako základného dokumentu štátu. NSIB v SR je koncipovaná na obdobie 5 rokov (2008 – 2013). Z nej vyplývajú aj úlohy pre podnikovú sféru a riešenie informačnej bezpečnosti.

Informačná bezpečnosť má podľa materiálu *Národná stratégia pre informačnú bezpečnosť v SR* multilaterálny charakter, t. j. musí zohľadňovať záujmy vlastníkov IKT systémov, potreby ich používateľov, ako aj práva fyzických a právnických osôb, ktorých údaje sa v systémoch spracovávajú. Z hľadiska vlastníkov a prevádzkovateľov je najdôležitejší spoľahlivý prístup k informačným zdrojom s prístupom on-line a ich zabezpečenie pred únikom informácií, neoprávneným použitím a narušením integrity údajov, ako aj autorita a dobré meno vlastníka systému.

Ako vyplýva z prieskumu informačnej bezpečnosti vo verejnej správe v SR v roku 2011, informačnej bezpečnosti sa stále nevenuje dostatočná pozornosť. Je to spôsobené jednak neznalosťou problematiky IB a nedocenením hrozieb a rizík, ale aj zlou ekonomickou situáciou podnikov, v dôsledku čoho nie sú vyčlenené finančné zdroje na zabezpečenie informačnej bezpečnosti.

Z hľadiska používateľov je pri spracovávaní informácií najdôležitejšie účel a obsah informácií, presnosť, aktuálnosť, prístupnosť, autenticita, usporiadanie a kvalita informácií.

Existuje množstvo činiteľov, ktoré môžu spôsobiť znefunkčnenie IKT systémov a znehodnotenie údajov, ktoré sa v nich spracovávajú. Sú to napr. prírodné vplyvy, technické poruchy, ľudské chyby a omyly, škodlivý softvér, cieľavedomé útoky, počítačová kriminalita a medzinárodný terorizmus.

Ako sa uvádza v materiáli Národná stratégia pre informačnú bezpečnosť v SR, ucelená koncepcia informačnej bezpečnosti SR zatiaľ nebola prijatá. Napriek tomu existujú čiastkové oblasti, v ktorých je informačná bezpečnosť rozpracovaná (legislatívne, kompetenčne, organizačne aj metodicky). Sú to najmä:

Informatizácia spoločnosti a informačná bezpečnosť verejnej správy spadajúca do kompetencie MF SR, ktoré činnosť v oblasti informačnej bezpečnosti zabezpečuje prostredníctvom Komisie pre informačnú bezpečnosť. V pôsobnosti tejto komisie je odborná príprava návrhov a stanovísk pre oblasť informačnej bezpečnosti, v rámci čoho komisia o. i. navrhuje zavedenie bezpečnostných štandardov, zmenu alebo zrušenie existujúcich platných bezpečnostných štandardov pre informačné systémy verejnej správy.

Ochrana utajovaných skutočností z hľadiska informačnej bezpečnosti predstavuje klasifikovanú informáciu a systémy pracujúce s klasifikovanou informáciou. Napriek tradičnej terminológie použitej v legislatíve, utajované skutočnosti nie sú klasifikované len z hľadiska dôvernosti, ale bezpečnostné požiadavky na ich ochranu sú komplexné a zohľadňujú aj potrebu zaistenia integrity, autentickosti a dostupnosti. Vo vzťahu k utajovaným skutočnostiam, ktoré sú obsahom kybernetického priestoru a tej časti digitálneho priestoru SR, v ktorom sa nepracuje s klasifikovanou informáciou, sa uplatňuje dvojaký systém riadenia. V záujme ochrany digitálneho priestoru SR bude preto potrebné rozvinúť bližšiu spoluprácu v oblasti ochrany klasifikovanej informácie (utajovaných skutočností) a informačnej bezpečnosti celého digitálneho priestoru SR.

Ochrana osobných údajov a *používanie elektronického podpisu*, tieto oblasti sú upravené zákonmi a príslušné inštitúcie zabezpečujú dohľad nad dodržiavaním zákona.

Elektronický obchod upravuje Zákon č. 22/2004 Z. z. o elektronickom obchode, do ktorého bola transponovaná smernica Európskeho parlamentu a rady o elektronickom obchode, ktorá tvorí spoločný právny rámec elektronického obchodovania pre všetky členské štáty.

Autorské právo a práva súvisiace s autorským právom sú ošetrené autorským zákonom.

Bezpečnosť IT sa stala najdôležitejším stavebným kameňom vývoja, údržby, prevádzky a využitia spoľahlivých, dobre dostupných a dôveryhodných IT systémov a služieb, a to vo firmách, vládnych inštitúciách a úradoch, ako aj v súkromnom sektore. Toto vedomie významu bezpečnosti IT sa však nevyvinulo na základe všeobecného záujmu poskytovateľov služieb alebo užívateľov služieb o tému bezpečnosti, ale na základe zintenzívnenej potreby ochrany.

VÝSLEDKY A DISKUSIA

Bezpečnosť informačných systémov predstavuje v súčasnosti komplexný systém technických a organizačných opatrení. Predstavuje kompromis medzi otvorenosťou dnešných informačných systémov a ich ochranou pred napadnutím, prípadne zneužitím citlivých dát organizácie. Podniky potrebujú takú informačnú bezpečnosť, ktorá zodpovedá ich obchodným a prevádzkovým potrebám ako aj rizikám ich informačných aktív. Vždy ide o nájdenie istého rovnovážneho stavu. Najväčšiu hodnotu v každom podniku tvoria jeho informácie a ich ochrana je prioritou.

Finančné prostriedky vynaložené v podnikoch na zlepšenie stavu informačnej bezpečnosti nemajú priamo vyčísliteľnú návratnosť. Implementácia bezpečnostných riešení však znižuje pravdepodobnosť vzniku bezpečnostných incidentov, ktoré takmer vždy znamenajú straty v dôsledku zneužitia informácií alebo znefunkčnenia informačného systému.

S rozvojom technológií sa preto jednak zdokonaľujú súčasné metódy zabezpečenia, jednak vyvíjajú nové, účinnejšie, bezpečnejšie, ale na každodenné použitie čoraz komplikovanejšie metódy. Pritom použitá metóda by mala byť vždy adekvátna tomu, čo má byť zabezpečené.

V podnikoch by mala byť vypracovaná bezpečnostná politika a smernice na jej dodržiavanie.

Na zlepšenie úrovne informačnej bezpečnosti na podnikovej úrovni navrhujeme:

A. Definovanie prístupových práv používateľov IT a IS:

Na zabezpečenie IB v oblasti spracovania informácií je dôležitým bodom v bezpečnostnej politike odoberanie a pridávanie prístupových práv používateľom. Každý zamestnanec by mal mať len také prístupové práva, ktoré potrebuje pre plnenie svojich pracovných úloh podľa pracovného zaradenia (t.j. odlišné prístupové práva bude mať IT manažér podniku, ktorý musí mať prístup do celého IS a iné prístupové práva bude mať pracovníčka mzdového oddelenia, ktorej stačí prístup len do podsystému MZDY).

Za prideľovanie prístupových práv môže byť zodpovedný len priamy nadriadený, ktorý posúdi ich opodstatnenosť. V prípade odchodu zamestnanca z pracovného pomeru mu musia byť odobraté všetky prístupové práva, aby neprišlo k úniku a zneužitiu informácií.

B. Definovanie zodpovednosti používateľov IT a IS za vznik a riešenie bezpečnostných incidentov:

V tejto súvislosti je potrebné, aby mal podnik vypracované pravidlá využívania prostriedkov IT (napr. zákaz využívania prostriedkov IT na súkromné účely), pravidlá a zásady pre bezpečnú prácu v lokálnej podnikovej sieti i sieti Internet, pravidlá pre využívanie a aktualizáciu antivírusových programov, ako aj pravidlá pre prácu s osobnými údajmi a pod.

Do smerníc by mali byť zahrnuté aj povinnosti používateľov pri nahlasovaní vzniknutých bezpečnostných incidentov, dodržiavanie mlčanlivosti o podnikových informáciách, s ktorými zamestnanec pracuje, ako aj riešenie zodpovednosti používateľa za úmyselné porušenie bezpečnosti, alebo porušenie bezpečnosti z nedbanlivosti.

C. Klasifikácia informácií v podniku podľa citlivosti:

Informácie by mali byť rozdelené do kategórií podľa ich citlivosti a požadovanej úrovne ochrany. Informácie môžeme z tohto pohľadu deliť na:

- *verejné* – prístupné širokej verejnosti (napr. informácie zverejnené na www stránkach podnikov),
- *interné* – prístupné len zamestnancom, ktoré sú určené na interné využitie v podniku,
- *chránené* – slúžia iba pre oprávnené osoby v podniku a vyžadujú najvyššiu mieru ochrany (napr. osobné údaje o zamestnancoch a pod.).

Pre každú kategóriu informácií by sa mali vytvoriť zásady využívania, spracovávania a ich uchovávania. Zásady práce s informáciami by mal mať podnik vo forme internej smernice.

D. Odhalenie a riešenie bezpečnostných incidentov:

Pre nahlasovanie a riešenie incidentov by mali byť vypracované zásady procesu riešenia vzniknutých bezpečnostných incidentov. Ak má podnik manažéra pre IB, rieši túto problematiku v spolupráci s IT manažérom. Ak podnik nemá vytvorenú pozíciu manažéra pre IB ani IT manažéra, zodpovednosť za riešenie incidentov preberá vedenie podniku a ním poverení zamestnanci. Ich úlohou je identifikovať incident, zhodnotiť situáciu a riešiť problém, ktorý nastal (napr. zlyhanie IS, únik informácií a pod.). Po vyriešení incidentu je potrebné prijať opatrenia, aby sa podobné škody následkom iného bezpečnostného incidentu neopakovali.

E. Vypracovanie bezpečnostných smerníc:

V podniku by mali byť vypracované bezpečnostné smernice, ktoré by obsahovali všetky práva a povinnosti zamestnancov v oblasti informačnej bezpečnosti. Mali by obsahovať zásady dodržiavania fyzickej a personálnej bezpečnosti, bezpečnosti počítačov zapojených do siete, bezpečnosti lokálnej podnikovej siete i siete Internet, riešenie a predchádzanie bezpečnostným incidentom. Ich súčasťou by mal byť popísaný účel smernice, definované povinnosti zamestnancov a zodpovednosti za vzniknuté škody.

F. Definovanie aktív v podniku:

V každom podniku sú aktíva, ktoré je potrebné chrániť. Aktívami z hľadiska informačnej bezpečnosti nazývame všetko, čo má pre podnik nejakú hodnotu (hardvér, softvér, materiálne vybavenie, financie, personál a informácie). V dnešnej dobe sú informácie cennými aktívami, preto ich ochrana z hľadiska dôvernosti a autentickosti má veľký význam.

G. Vzdelávanie v oblasti bezpečného využívania IT a IS v podniku:

Permanentné vzdelávanie v oblasti informačnej bezpečnosti je veľmi dôležité, pretože hrozieb a rizík je stále viac. Používateľov IT je preto potrebné systematicky informovať a zvyšovať ich povedomie v oblasti informačnej bezpečnosti. Ide najmä o informovanie zamestnancov o typoch možných bezpečnostných incidentov, existencii bezpečnostných smerníc v podniku, postupoch pri nahlasovaní vzniknutých bezpečnostných incidentov a pod. Modernou formou vzdelávania sú kurzy vypracované formou e-learningu, ktoré môže každý zamestnanec absolvovať sám, vlastným tempom a pri svojom počítači.

ZÁVER

Pre dosiahnutie a udržanie požadovaného stavu informačnej bezpečnosti je potrebné na podnikovej úrovni koordinovať ochranu aktív podniku a zároveň vytvoriť efektívny systém jej riadenia. Na zvýšenie úrovne riadenia je potrebné poskytovať inštitúciám nielen metodickú pomoc pri riešení koncepčných otázok, ale pomáhať im aj pri riešení konkrétnych aktuálnych problémov (vrátane prípravy nariadení, odbornej pomoci, metodických materiálov, školení a poradenstva).

Významným faktorom, ktorý priamo ovplyvňuje informačnú bezpečnosť a schopnosť implementovať riešenia bezpečnostných problémov je aj vzdelávanie ľudí v oblasti informačnej bezpečnosti. V tejto oblasti je potrebné špecifikovať potreby znalostí jednotlivých kategórií používateľov IKT (laickí používatelia, informatici a odborníci v informačnej bezpečnosti) a obsahové možnosti vzdelávania (celoživotné vzdelávanie, firemné kurzy, e-learning a pod.) Na základe analýzy potrieb vzdelávania je možné navrhnúť rozšírenie obsahu informatických predmetov študijných programov stredných a vysokých škôl o problematiku informačnej bezpečnosti, systém celoživotného vzdelávania pre správcov systémov a podporovať vydávanie literatúry a metodických dokumentov zameraných na problematiku informačnej bezpečnosti.

ABSTRAKT

Informačné a komunikačné technológie a informačné systémy v podniku musia byť schopné poskytovať manažérom aktuálne a hodnoverné informácie v reálnom čase a preto musia byť adekvátne bezpečné. Informačná bezpečnosť je veľmi dôležitá úloha pre všetkých užívateľov IKT a IS. Informačná bezpečnosť je definovaná ako schopnosť siete alebo informačného systému ako celku odolať s určitou úrovňou spoľahlivosti náhodným udalostiam, alebo nezákonnému, či zákernému konaniu, ktoré ohrozuje dostupnosť, pravosť, integritu a dôvernosť uchovávaných alebo prenášaných údajov a súvisiacich služieb poskytovaných alebo prístupných prostredníctvom týchto sietí a systémov.

KĽÚČOVÉ SLOVÁ

informačné a komunikačné technológie (IKT), informatizácia spoločnosti, informačná bezpečnosť, informačný systém

LITERATÚRA

[1] HAMÁŠOVÁ, Katarína. 2012. *Aspekty informačnej bezpečnosti v oblasti implementácie IT a IS v podnikoch agrosektora* : dizertačná práca. Nitra : SPU, 2012, 199 s.

[2] HENNYEYOVÁ, Klára – HAMÁŠOVÁ, Katarína. 2012. *Aspekty informačnej bezpečnosti v podnikoch agrosektora* : vedecká monografia. Nitra : SPU, 2012. 123 s. ISBN 978-80-552-0879-4.

[3] HENNYEYOVÁ, Klára – KORCOVÁ, Zuzana – POPELKA, Vladimír. 2010. *Selected aspects of the information security in Slovakia*. In Global Economy 2010. (CD). Nitra : SPU, 2010 s. 2559-2565. ISBN 978-80-552-0386-7.

[4] LIPIANSKA, Júlia – HLAVATÝ, Ivan. 2011. *Informačná bezpečnosť podniku v kontexte krízového vývoja hospodárstva.* [online], 2011. [cit. 2012-11-03]. Dostupné na: <http://of.euba.sk/zbornik2011/Zbornik_vedeckych_stati_2011>.

[5] *Národná stratégia pre informačnú bezpečnosť SR*. 2011 [online]. Ministerstvo financií Slovenskej republiky, aktualizované 2011. [cit. 2012-11-10]. Dostupné na: <http://www.informatizacia.sk/narodna-strategia-pre-ib/6783c>.

KONTAKT

doc. Ing. Klára Hennyeyová, CSc.
Slovenská poľnohospodárska univerzita v Nitre,
Fakulta ekonomiky a manažmentu,
Katedra informatiky,
Tr. A. Hlinku 2,
949 76 Nitra
e-mail: Klara.Hennyeyova@uniag.sk

Recenzoval(a): doc. Ing. Vladimír Popelka, CSc.