Nástrahy a riziká pri využívaní IKT

Dangerous situations and risks in using ICT

Mária WENZLOVÁ

Abstract
The article is dealing with the question, what kind of dangerous situations and risks are connected with using information and communication technologies for a single user, organization and the whole society. The article outlines some solutions of this problem.

Key words
Using ICT, data security

Úvod

Na každom kroku kde sa len pohnete, hocijaké noviny, či časopis otvoríte, zapnete televíziu, či počúvate rádio všade čítate, počúvate a stretávate sa s pojmami týkajúcimi IKT a ich vývoja, aplikácie, implementácie, jednoducho ich prieniku do bežného každodenného života. Tento prienik do všetkých oblastí života - súkromného, spoločenského, hospodárskeho a politického sa vstupom našej krajiny do EÚ a globalizáciou svetovej ekonomiky niekoľkokrát znásobil. Veľmi významným a čoraz častejšie používaným sa stal pojem „informačná spoločnosť".

V konečnom dôsledku konzumentom – koncovým užívateľom v tomto ponímaní je človek jednotlivec. Využívanie IKT zahrňuje veľmi širokú škálu činností a procesov, pri ktorých sa užívateľ stretáva s rôznymi nástrahami a podstupuje rizikám, ktoré s tým súvisia. Závažnosť tohto problému je rôzna. Nie je jedno o akého užívateľa sa jedná, myslíme tým či ide o jednotlivca, jednoduchý systém informácií alebo o zložitý niekoľkoúrovňový nadnárodný informačný a komunikačný systém. Vo všeobecnosti sa problém ale chápe ako bezpečnosť informácií v automatizovaných informačných a komunikačných systémoch. Tento proces sa vo väčšine spája s počítačovou technikou.

Pojem IKT je veľmi široký ale vždy ide o informáciu ako takú, ktorá má pre konzumenta v tom konkrétnom čase rozhodujúcu úlohu a význam. Hovoríme, že hodnoty spoločnosti sa výrazne presunuli z podoby materiálnej do podoby informačnej. V súčasnom svete sa stále častejšie ukazuje, že jedným z faktorov, ktoré rozhodujú o úspechu či neúspechu, sú informácie, čiže správne informácie v správny čas a na správnom mieste tvoria podstatu schopnosti konkurovať a uspieť.

Materiál a metódy.

Informačné zdroje pre napísanie príspevku tvorili poznatky z odbornej literatúry, články a publikácie z odborných časopisov zaoberajúcich sa danou tematikou, vlastné skúsenosti ako aj výučbové materiály. Pri spracovaní týchto zdrojov sa použili metódy zisťovanie a štúdium najnovších poznatkov, porovnávanie a dedukcia.

Výsledky a diskusia

Informácia je považovaná za jeden z najvýznamnejších faktorov rozvoja. Objektívne, správne a rýchle adresné informácie sú významným podkladom pre efektívne riadenie firiem

a organizácií. Je to dôvod, ktorý podmieňuje vytvárať bezpečnostnú politiku organizácie na zamedzenie neoprávnenej manipulácie – od zneužívania až po zničenie.

Informačný systém organizácie tvorí päť navzájom prepojených prvkov:

- hardvér – technické zariadenia na získavanie, spracovanie, vizualizáciu, uloženie a distribuovanie dát,
- softvér – množina inštrukcií slúžiacich na ovládanie hardvéru, za účelom zabezpečenia informačného procesu, ktoré tvorí:
  - systémový softvér,
  - aplikačný softvér,
- ľudia – zabezpečujúci plánovanie, budovanie, vývoj softvérového vybavenia a obsluhu /prevádzku/ IS,
- informačná báza údajov,
- procedúry – zamerané na vývoj a implementáciu programov, údržbu hardvéru a softvéru.

Požiadavky kladené na informačný systém sú:

- použiteľnosť – vhodnosť pre danú organizáciu, jednoduché ovládanie, spoločné užívateľské rozhranie subsystémov tvoriacich integrovaný balík, dodržaná vzájomná kompatibilita údajov,
- spoľahlivosť – odolný voči chybám užívateľa, voči možným poruchám, na dostatočnej úrovni bezpečnosti,
- udržateľnosť – možnosť vykonávať úpravy ako odozvy na organizačné a legislatívne zmeny a zmeny hardvérovej platformy,
- a efektívnosť – zjednodušenie a urýchlenie práce užívateľa, efektívne využívanie disponibilných technických prostriedkov, poskytnutie zázemia pre realizáciu strategických cieľov podniku.

Vychádzajúc z tejto skutočnosti, cieľom zaistenia bezpečnosti je zabezpečiť:

- dostupnosť,
- dôvernosť,
- integritu,
- a zodpovednosť informácií.

Na dosiahnutie tohto cieľa pri daných požiadavkách sa ochrana týkajúca sa už spomenutých prvkov pozostáva z aplikácie komplexných ochranných mechanizmov, čím sa myslí *fyzická, personálna, režimová, programová, dátová a komunikačná ochrana.*

Problém ochrany údajov proti vonkajším aj vnútorným narušiteľom nadobudol obrovských rozmerov rozšírením internetu, jeho využívaním ako platformy pre podnikanie /e-commerce/, zábavu, získavanie informácií, vzdelávanie a komunikáciu. Je nesporné, že aj väčšina bezpečnostných incidentov pochádza z tohto zdroja. Táto skutočnosť je podporená aj faktom neustáleho rastu investícií do obranných a ochranných mechanizmov IS. Podľa najnovších poznatkov obsah súčasných bezpečnostných projektov je zameraná na ochranu v troch hlavných smeroch: *technickej, fyzickej a organizačno-personálnej.* Ktorá z tých troch oblastí je najdôležitejšia ? Ani jedna. Všetky musia tvoriť harmonický a komplexný celok.

Záver

Od čias rozšírenia sieťovej technológie spracovania, ale predovšetkým od vzniku a využívania celosvetovej siete Internetu, ako informačného zdroja, problém ochrany informácií nadobudol takých rozmerov, že v súčasnosti sa s tým musí zaoberať každý jednotlivec, organizácia či celá spoločnosť.

Situácia je v podstate iná vo veľkých firmách a inštitúciách kde otázkou informačnej bezpečnosti sa zaoberá špecializované oddelenie, naproti tomu v malých firmách, ktoré len okrajovo podporuje zahraničný kapitál a kvôli šetreniu finančných prostriedkov dochádza ku kumulovaným funkciám je rozpočet na bezpečnosť výrazne obmedzený.

Každý jednotlivec spoločnosti sa nachádza na určitej úrovni informačnej gramotnosti. Zaradenie moderných informačných technológií do vzdelávacieho procesu a modernizácia vyučovacieho procesu na každom stupni škôl je základným prvkom ovplyvňujúcim túto skutočnosť. Pri výchove a vzdelávaní je potrebné budúcich užívateľov a konzumentov informácií upozorniť aj na aspekt ochrany. Vyplýva to z doterajších skúseností, že najslabším článkom pri zabezpečení a kontinuálnom riadení bezpečnosti IS je vždy človek.

Súhrn

Príspevok sa zaoberá otázkou, aké nástrahy a riziká súvisia s využívaním informačných a komunikačných technológií pre jednotlivca, organizáciu aj celú spoločnosť a načrtáva niektoré aspekty riešenia tohto problému.

Klúčové slová

využívanie IKT, informačná bezpečnosť

Literatúra:

[1] DOBDA, L.: Ochrana dát v informačných systémoch. Praha: Grada Publishing, s.r.o., 1998, 288 s. ISBN 80-7169-765-6

[2] POPELKA, V.: Informačné zabezpečenie subjektov agrosektora. SPVTS 2003. In.: Zb. vedeckých prác Aktuálne problémy riešené v agrokomplexe. CD ROM. ISBN 80-8069-295-5.

[3] PŘIBYL, T.: Bezpečnost v malých firmách. Business World , 2004, č.6, s. 14 ISSN 1213-1709

[4] TÓTHOVÁ, D.: Informačná politika organizácie. In: Zborník vedeckých prác z MVD 2001. III. zväzok. Nitra: SPU, 2001, s. 805-808 ISBN 80-7137-868-2

Kontaktná adresa:
Ing. Mária Wenzlová, Katedra informatiky FEM SPU, Tr. A. Hlinku 2, 94976 Nitra
e-mail: Maria.Wenzlova@fem.uniag.sk

Recenzent: doc. Ing. Vladimír Popelka,CSc.