POČÍTAČOVÁ BEZPEČNOSŤ
COMPUTER SECURITY

OLÁHOVÁ Eva, (SR)

ABSTRACT
Information society is a society with a wide-spread information infrastructure and is characterized by a movement of values from the material form to the information form. The aim of the information society is an equal and balanced utilization of individual abilities of its population and an improvement in the quality of life. The increasing interconnection of information systems and computer networks requires a formation of an effective complex of security barriers against the increasing number of threats. Information security is not only about making the computer hardware at system level secure, it is also about a physical security, about a personal security and education, about an organization and management. However, the weakest element of information security is always a human being.

KEY WORDS
computer security, user, threats from internet and LAN, social engineering

ÚVOD
Implementácia a používanie technologicky špičkových počítačových a telekomunikačných systémov rozšírili priestor bezpečnostného manažmentu a informačnej bezpečnosti (IB) o pojem bezpečnosť IKT. Otázka IB v praxi si vyžaduje systémový prístup a uvedomenie si hodnoty a dôležitosti spracovávaných informácií pre organizáciu ako i stabilitu jej počítačových systémov.
Dôležitým faktorom bezpečnosti IKT je dôraz na samotného používateľa IKT, a to na jeho znalosti a zručnosti ale i počítačovú etiku a zodpovednosť. Vo väčšine organizácií nie je koncový používateľ odborníkom v oblasti IT. Počítač, dostupnosť služieb Internetu považuje za svoj pracovný prostriedok alebo zdroj informácií na dosiahnutie určitých cieľov. Vo väčšine prípadov ho teda ani nezaujíma, že ním spracovávané údaje, resp využívané internetové služby sú možným zdrojom ohrozenia alebo zneužitia spracovávaných údajov organizácie, resp. jeho osobných údajov.

MATERIÁL A METÓDY
Zabezpečenie počítačov v období implementácie internetu je a musí byť v popredí záujmu organizácie a jej strategických cieľov. Ide o problematiku, o ktorú na jednej strane existujú rozdielne záujmy jej použitia (resp. zneužitia) a na strane druhej existuje o nej rôzna úroveň vedomostí.
Pojem *perimeter bezpečnosti* je známy ako ochrana *„hraníc“* počítačovej siete – t.j. *rizikového bodu*, kde sa vnútorná sieť spája s verejným Internetom. Ochranu IKT organizácie pred bezpečnostnými hrozbami zabezpečujú poverení IT pracovníci. Posilnenie tejto hranice v rámci vnútornej siete organizácie môžu dosiahnuť napríklad rozdelením siete do segmentov, ktoré sú odolné voči útokom a hrozbám z Internetu Ochrana IKT sa však týka i manažéra IB, resp. príslušného útvaru, ktorí definujú jednotlivé štandardy a postupy IB a bezpečnostnú politiku. A nemožno zabúdať ani na riadiaci manažment organizácie – jeho podpora je kľúčovou otázkou celého procesu riešenia informačnej bezpečnosti organizácie. Zamerať sa treba i na koncové body – veľa vecí sa na sieťovej úrovni robiť – je potrebné chrániť jednotlivé stanice a servery.

Z uvedených skutočností je zrejmé, že je pomerne ťažké definovať jednotlivé úrovne ochrany ohrozenia informácií. Ich zraniteľnosť je ako na úrovni fyzickej, organizačnej, procedurálnej, personálnej, riadiacej, administratívnej tak i na úrovni hardvéru a softvéru. Slabým miestom môže byť napríklad prerušenie dodávky elektrickej energie, „nepoučený" používateľ aplikačného softvéru, ale i nechránené komunikačné linky.
Základná definícia cieľov IB môže byť nasledovná: *„Základným cieľom je eliminovať prípadné priame a nepriame straty spôsobené zneužitím, poškodením, zničením alebo nedostupnosťou informácií, vytvorením uceleného, nákladovo optimalizovaného a efektívne fungujúceho systému riadenia bezpečnosti informácii.*"
Ak chceme budovať uvedomelú a efektívnu vedomosť o IB, musíme v praxi začať od základného piliera – koncového používateľa PC. Používateľ často ani nezistí, že je cieľom útoku, resp. v prípade útoku nevie okamžite zareagovať adekvátnymi protizásahmi. Je preto potrebné vytvoriť vhodný systém *bezpečnostného vzdelávania všetkých používateľov IKT prostriedkov* v organizácii.
Pri práci s počítačom pripojeným do lokálnej počítačovej siete a používaní štandardných sieťových aplikácií za zdroje, z ktorých sú útoky vedené, považujeme nasledovné aplikácie:

- Klientov (prehliadač) webových stránok,
- Klientov elektronickej pošty a prílohy elektronickej pošty.
- Ostatné sieťové aplikácie,

Treba však spomenúť, že zdrojom ohrozenia sú i samotné hardvérové zdroje počítača – nové typy útokov sa zameriavajú na periférne zariadenie PC, serverov.

VÝSLEDKY

Bezpečnosť IKT bola na úrovni Centra informačných technológií riešená vo viacerých projektoch a interných úlohách od roku 1998. Častý výskyt bezpečnostných incidentov na osobných počítačoch používateľov (v poslednom období), ich analýza ako i snaha o elimináciu potenciálnych bezpečnostných incidentov nás viedli k vypracovaniu metodických podkladov vzdelávacích kurzov k IB. Výsledkom je implementácia do formy on-line vzdelávacieho kurzu *Podpora používateľov* v prostredí LMS Moodle, ktorý je v rámci FEM používaný už 2 roky. Na adrese URL *http://www.fem.uniag.sk/moodle/* sú voľne dostupné spracované materiály, ktoré sú priebežne aktualizované a dopĺňané. Cieľom kurzu nie je „zavaliť" používateľa množstvom informácií a nových pojmov, ale postupne formou krokových návodov ho oboznámiť s „ošetrením" nastavení operačného systému jeho počítača do požadovanej úrovne softvérovej bezpečnosti.
Z pohľadu tvorcov kurzu dôležitý je kontakt s používateľom prostredníctvom elektronickej pošty. Používateľ zaslaním elektronickej pošty s uvedením problému a odpoveďou získa návod na jeho vyriešenie..
Obsahová štruktúra kurzu bola tvorcami členená do troch okruhov:

- Počítačová bezpečnosť ako celok
  Základné nastavenia operačného systému pre zabezpečenie jeho integrity.
- Internet a jeho hrozby
  Odporúčané pre nastavenie programov pre prezeranie webových stránok, blokovanie reklamných okien, resp. odporučenia pre bezpečné používanie Internetu. Pomerne rozšírenými hrozbami Internetu sú postupy založené na sociálnom inžinierstve, ktorých cieľom je „oklamať" používateľa určitej internetovej služby a následné zneužitie takto získaných údajov.
- Škodlivý softvér
  Typy tzv. malware softvéru: vírusy, trójske kone, key-loggery, root-kity, červy, spyware a adware a spôsoby jeho infiltrácie do PC.

DISKUSIA

S nástupom nových, škodlivých prejavov a hrozieb pri používaní sieťových služieb internetu je potrebné zamerať sa na jednoduchý, používateľsky dostupný systém oboznámenia používateľov s problematikou bezpečnosti. Je možné „odkázať" používateľa na široké zdroje internetu, ktoré sa problematike bezpečnosti venujú na profesionálnej úrovni a ponúkajú návody na jej riešenie. Tieto webové stránky však neriešia špecifické zameranie organizácií v používaní rôzneho aplikačného, antivírového softvéru a nezohľadňujú ani používané interné dokumenty definovanej IB organizácie. Riešením sú v rámci organizácií vzdelávacie programy a to vo forme pravidelných školení alebo on-line vzdelávacích dokumentov. Hlavné zameranie podpory zo strany centier IKT vo forme e-vzdelávania musí riešiť:

- Zvýšenie praktických zručností používateľov IKT s dôrazom na bezpečnosť operačného systému a inštalovaného softvéru.
- Zabezpečenie správy a prevádzky osobného počítača samostatne, resp. s použitím postupov uvedených na webovej stránke.
- Počítačová uvedomelosť a zodpovednosť.

Postupy definované v týchto dokumentoch musia odrážať hlavné zásady bezpečnostnej politiky organizácie a v konečnom dôsledku eliminovať výskyt bezpečnostných incidentov na PC používateľov, ktoré sú zapríčinené neznalosťou, ale často i určitým skúšaním s vedomím, že daný postup môže v sebe skrývať riziko. Výsledkom je vypestovanie určitých návykov zodpovedného prístupu k PC, aplikačnému softvéru, intranetu, internetu.

Je ťažké vyjadriť prínos IB ako celku pre organizáciu. Pokiaľ nie sú globálne ohrozené informačné zdroje, interné databázy a ich integrita, narušená webová stránka organizácie, zavírená pracovná stanica, je otázka informačnej bezpečnosti zľahčovaná, resp. považovaná za nutné zlo. V skutočnosti, pri uplatňovaní a hlavne dodržiavaní IB, je jej efekt viditeľný najmä v kvalitatívnych parametroch IKT. Preto túto problematiku nemožno podceňovať, ale zaujať k nej aktívny postoj a vyžadovať jej dodržiavanie v každodennom používaní prostriedkov IKT.

ANOTÁCIA

Informačná spoločnosť je spoločnosťou so široko dostupnou informačnou štruktúrou a je charakteristická presunom hodnôt z podoby materiálnej do podoby informácií. Cieľom informačnej spoločnosti je rovnoprávne a vyvážené využívanie individuálnych schopností jej obyvateľov a zlepšenie kvality života. Rastúca prepojenosť informačných systémov a počítačových sietí vyžaduje vytvorenie účinného komplexu bezpečnostných bariér pred zvyšujúcim sa počtom ohrození. Informačná bezpečnosť totiž nie je len o zabezpečení počítačovej techniky na systémovej úrovni, je to i o fyzickej bezpečnosti, o personálnej bezpečnosti a vzdelávaní, o organizácii a riadení. Najslabším článkom IB je ale vždy človek.

KĽÚČOVÉ SLOVÁ

počítačová bezpečnosť, používateľ, hrozby z internetu a LAN, sociálne inžinierstvo

LITERATÚRA

1. BUDIŠ, P. 2004. Jak vypracovať bezpečnostní politiku v podniku. In *PC World Security*, 2004, č. 4, s. 44-46.
2. BUIGL, P. 2003. Proč prodávat antispam? In *Reseller Magazine*, roč. 1, 2003, č. 3, s. 40-41.
3. DOSEDĚL, T. 2005. *21 základních pravidel počítačové bezpečnosti*. Brno: CP Books, 2005. ISBN 80-251-0574-1.
4. Halouzka, J. a kol. 2001. *Informační bezpečnost – příručka manažera*. Praha: Tate International, 2001. ISSN 1211-8737.
5. KLANDER, L. 1998. *HACKER PROOF*. Brno : UNIS Publishing, 1998. ISBN 80-86097-15-3.

6. PERRY, D. 2005. Bezpečnosť je sociologický problém v technologickom „háve“. In *INFOWARE*, roč. 24, 2005, č. 9, s. 8-10.
7. WOLFE, P. 2004. *Antipsam metody, nástroje a utility pro ochranu před spamem.* Brno: Computer Press, 2004. ISBN 80-251-0479-6.

KONTAKTNÁ ADRESA

Ing. Eva Oláhová, Centrum informačných technológií, FEM SPU v Nitre, Tr. A. Hlinku 2, 949 76 Nitra, E-mail: Eva.Olahova@fem.uniag.sk

Recenzent: Ing. Zuzana Korcová