KONVERGOVANÁ BEZPEČNOSŤ
CONVERGENCE SECURITY

TOTHOVÁ Darina, (SR)

ABSTRACT

Information and communication technologies became necessary part of our life. Managers invest considerable finances for their obtaining and innovation. That is why it is more and more important to secure them. Also handling of users' access to the sources of ICT is important. Relation of physical access systems and secure systems of information technologies, for firms and organisations, presents basis of effective solution of accession, diverting of attacks and engaging better authentification for users.

KEY WORDS

information security, access systems, security systems, convergence security

ÚVOD

Bezpečnosť informačných systémov (IS) je potrebné chápať ako komplexné riešenie. Systém riadenia informačnej bezpečnosti a bezpečnosti informačných technológií je treba zároveň vidieť v súlade s legislatívou a platnými medzinárodnými normami. Popritom je potrebné zohľadniť možnosti súčasných technológií a vhodne navrhnúť integráciu a implementáciu bezpečnostných riešení do prostredia informačných systémov organizácie.

MATERIÁL A METÓDY

V oblasti bezpečnosti je potrebné mať v organizácii komplexné riešenia, ktoré je možno rozdeliť do troch základných kategórií:

1. Správa a riadenie informačnej bezpečnosti a bezpečnosti informačných systémov:
- vypracovanie analýzy rizík,
- vypracovanie bezpečnostnej politiky v súlade s ISO/IEC 17799,
- návrh bezpečnostných opatrení v súlade s ISO/IEC 17799,
- vypracovanie bezpečnostnej architektúry, návrh bezpečnostných procedúr pre správu a prevádzku IS špecialistami na správu bezpečnosti s certifikátmi CISSP a CISM,
- bezpečnostný audit certifikovaným auditorom,
- vypracovanie havarijných plánov IS, vypracovanie Bezpečnostného projektu na ochranu osobných údajov v zmysle Zákona č. 428/2002 Z.z.

2. Bezpečnosť sieťovej prevádzky sa týka realizácie nasledovných častí:
- firewall systémy,
- virtuálne privátne siete,
- systémy na detekciu sieťových prienikov,
- správa bezpečnostných incidentov,
- penetračné testovanie,
- systémy zberu, centralizácie a spracovania auditných záznamov,
- bezpečnosť a prevádzka serverov, komplexná antivírusová ochrana intranetu,
- audit bezpečnosti operačných systémov (Windows, Unix),

- audit sieťového prostredia a pripojenia do Internetu.

3. Bezpečnostná infraštruktúra na aplikačnej úrovni**:**
- PKI infraštruktúra a certifikačná autorita,
- autentifikačné systémy,
- Kontrola prístupu a overovanie totožnosti, správa používateľov.

Ďalšie dôležité súčasti informačnej bezpečnosti:
- Bezpečné pripojenie do Internetu.
- Bezpečnostné projekty na zabezpečenie ochrany osobných údajov.
- Havarijný plán informačného systému.
- Systémy na detekciu prienikov (IDS).
- Podpora používateľov v oblasti služieb informačnej bezpečnosti.
- Správa incidentov.
- Autentifikačné riešenia.
- PKI (z angl. Public Key Infrastructure).
- IAM (z angl. Identity and Access Management).
- Systém manažérstva informačnej bezpečnosti.
- Bezpečnostné nástroje a utility (antivirus, antispam, detekcia útokov, správa trafiku ...).

VÝSLEDKY A DISKUSIA

Ponuka kvalitných produktov a služieb, schopnosť presadiť sa na trhu a prudký rozvoj informačných technológií sú príčinou neustáleho rastu objemu dát a ich dôležitosti v modernej spoločnosti, čím narastá potreba zabezpečiť ich správu a ochranu pred poškodením a stratou spôsobenou odcudzením dát a informácií, technickou chybou, živelnou pohromou, chybou spôsobenou ľudským činiteľom (vymazanie, prepísanie a podobne).
Potreba trvalého poskytovania kvalitných služieb vyžaduje neustálu prístupnosť kritických systémov a aplikácií. Kritické dáta musia byť uchovávané pre prípad ich znehodnotenia a v čo najkratšom čase obnovené. Mnohé organizácie používajú pri svojich činnostiach veľké objemy dát, čím sa zvyšuje záťaž a tlak na pracovníkov centier IKT v organizácii.
Riešenie otázok zálohovania, archivácie a obnovovania dát súvisí s riešeniami pre správu, zálohovanie a archiváciu systémových dát i dát aplikácií a databázových prostredí za využitia sieťových prostredí LAN, SAN, integráciou softvérových systémov na manažovanie „storage“ prostredia.
S problematikou informačnej bezpečnosti priamo súvisia nasledovné časti IS: zabezpečovacie systémy, prístupové a monitorovacie systémy, zálohovanie a archivácia, správa dokumentov, programová podpora používateľov.
Zabezpečovacie systémy: Väčšina organizácií si chráni svoj majetok zabezpečením priestoru predovšetkým elektronickými zabezpečovacími systémami (EZS). Základom každého zabezpečovacieho systému je ústredňa, ktorá vyhodnocuje všetky signály zo snímačov a ovládacích zariadení a na základe ich analýzy rozhodne o vyhlásení poplachu. Prístupový kód sa zadáva pomocou klávesnice alebo diaľkového ovládača. Súčasťami sú väčšinou PIR snímač, magnetický dverový snímač, dymový detektor, ionizačné, optické nebo tepelné požiarne snímače, detektor úniku plynu, vonkajšia siréna, interiérové sirény a pod.
Prístupové a monitorovacie systémy: Hlavnou úlohou prístupových a monitorovacích systémov je zabezpečovať automatickú kontrolu oprávnenia vstupov do objektov, tzn. vstup do areálu, budovy, vyhradených priestorov v budove (napr. počítačových cvičební, laboratórií,

miestnosti serverovne a pod.), parkoviska, atď. Pomocou čipových identifikačných kariet (kontaktných, bezkontaktných) je možné riadiť prístup do týchto priestorov, otvárať všetky dvere, závory, turnikety na základe pridelených oprávnení osobám používajúcim zabezpečované priestory. Karta môže slúžiť ako preukaz zamestnanca, študenta, návštevníka, môže byť multifunkčná. Do skupiny zabezpečovacích systémov patria aj kamerové monitorovacie systémy (trvalý záznam obrazu) v kombinácii so systémami kontroly prístupov. Inštalujú sa vo vnútri priestorov alebo monitorujú vonkajšie priestory. Pre organizáciu je dôležité, aby zabezpečovacie a prístupové systémy neboli samoúčelné, ale aby spĺňali niekoľko na seba nadväzujúcich služieb. Napríklad aby zabezpečovací systém zároveň umožňoval robiť záznam udalostí pri vniknutí do objektu, aby prístupový systém pomocou prístupovej karty neriešil iba prístup do budovy, ale aby umožňoval aj ďalšie možnosti využitia, aby monitorovací systém riešil aj záznam udalostí s možnou identifikáciou incidentov. Integrácia viacerých služieb umožní šetriť prostriedky, ale vyžaduje dôkladnú analýzu potrieb.

Zálohovanie a archivácia: Význam zálohovania dát ide do popredia najmä v prípade, keď príde k poškodeniu operačného systému, niektorej z aplikácií, údajov z databáz alebo hardvéru počas prevádzky daného systémového zariadenia. V takých situáciách je dôležité uviesť počítačové systémy do požadovanej činnosti v čo najkratšom čase, k čomu výraznou mierou napomáhajú zálohovacie a archivačné systémy. Zálohovacie systémy by mali poskytovať sofistikovaný prístup k možným riešeniam vytvorením architektúry, ktorá odráža situáciu v daných operačných podmienkach. Je dôležité sa rozhodnúť, či pôjde o multiplatformové riešenie alebo členené riešenie napr. na servery, pracovné stanice, členenie podľa operačných systémov.

Správa dokumentov: Správa dokumentov úzko súvisí so systémom riadenia obsahu web stránok (CMS), ktorý je výhodný pre všetkých, ktorí s informáciami pracujú, od tvorcu informácie, vrcholového manažéra až po návštevníka stránky. Výhodou zavedenia pre mamažment organizácie je publikovanie aktuálnych informácií, možnosť publikovania informácií hneď po ich vzniku, vedenie k samostatnosti jednotlivých zložiek manažmentu. Nevyhnutnými aspektami pre použitie CMS sú: jednoznačná podpora vedenia organizácie, pochopenie dôležitosti používania CMS, centrálna databáza používateľov – dôležité pre autentifikáciu používateľa – tvorcu obsahu, centrálne číselníky – jednotné používanie dôležitých údajov, definícia behu procesov (tok práce, workflow), vytvorenie centrálneho adresára – LDAP, definícia úloh používateľov, určenie prístupových práv, hierarchické zabezpečenie prístupu.

Programová podpora používateľov (HelpDesk)**:** Základ riešenia spočíva v odpovedi na základné otázky: KTO, ČO, KEDY, KDE, KOMU, AKO. Tento základ je vyriešený programovou podporou poskytujúcou objasnenie problému, návod na riešenie a organizačné odporúčania pre zložitejšie problémy. Jej súvis s informačnou bezpečnosťou je zjavný, nakoľko požívateľ IKT si v HelpDesku musí nájsť odpovede aj na otázky súvisiace s touto problematikou.

ZÁVER

Problematika bezpečnosti IS je proces, ktorý nemôže byť nikdy ukončený a musí sa rozvíjať s rozvojom nových IKT. Je pravdou, že porovnávať rozsah škôd pri prieniku do počítačovej siete vo finančnej sfére a akademickej sfére sa nedá, ale podceňovať tento problém v žiadnej organizácii, teda ani v akademickej sfére, už dnes nie je možné.

V súčasnosti sa kladie veľký dôraz na informačnú bezpečnosť, najmä v jej komplexnom riešení. Vytváranie bezpečnostnej politiky je dlhodobá a zložitá úloha. Nemusí byť písaná právnickým štýlom, i keď nesmie byť s ním v rozpore. Skutočná politika v praxi je iná, ako tá napísaná. Žiadna politika nesmie vyžadovať bezpečnosť za každú cenu, je potrebné primerane hodnotiť i iné hľadiská, ktoré môžu zmierniť riziká bezpečnostných incidentov.

Ak nie je z rôznych dôvodov možné napísať bezpečnostnú politiku, je potrebné aspoň spísať, čo sa v tejto oblasti robí a prečo, čo by sa malo a prečo sa nerobí (napr. z nedostatku financií), podpísať tieto informácie a odovzdať ich vedeniu univerzity.

ANOTÁCIA
Informačné a komunikačné technológie sa stali nevyhnutnou súčasťou nášho života. Na ich získavanie a inováciu sa vkladajú nemalé finančné prostriedky. Preto sa stále viac kladie do popredia aj ich zabezpečenie vrátane ošetrenia prístupu používateľov k zdrojom IKT. Spojenie fyzických prístupových systémov s bezpečnostnými systémami informačných technológií predstavuje pre podniky a organizácie základ efektívneho riešenia kontroly prístupu, odvracanie útokov a zaistenie lepšej autentizácie používateľov.

KĽÚČOVÉ SLOVÁ
informačná bezpečnosť, prístupové systémy, zabezpečovacie systémy, konvergovaná bezpečnosť

LITERATÚRA
1. Bezpečnosť IT systémov. 2006. [online]. [cit. 2006 - 03 - 28]. In *Profesionálne IT služby a riešenia v oblasti informačných technológií*. Dostupné na internete: <http://www.tempest.sk>.
2. HENNYEYOVÁ, K. - TÓTHOVÁ, D. - KORCOVÁ, Z.: Informačné technológie v dištančnom vzdelávaní na FEM SPU v Nitre. In: *Zborník anotácií zo seminára Dištančné vzdelávanie - Aplikovaná informatika + príspevky na CD*. Nitra : Univerzita Konštantína Filozofa (UKF), 2003, s. 20-21. ISBN 80-8050-602-7
3. OLÁHOVÁ, E.: Technológie bezdrôtových sietí. In: *Zborník anotácií z medzinárodnej vedeckej konferencie Informačné technológie vo vzdelávaní + príspevky na CD*. Nitra:SPU, 2003, ISBN 80-8069-242-2
4. ŠEMELÁKOVÁ, Ľ. - PEŇÁK, P. - KOŠŤÁL, L.: Jednoznačná autentifikácia užívateľov. In: *Zborník z medzinárodnej konferencie UNINFOS 2003*. Nitra : SPU, 2003, s. 270-273. ISBN 80-8069-241-6
5. POLÁČIK, T.: Baracoda Pencil - čiarové kódy prostredníctvom Bluetooth. In: *Zborník príspevkov na CD z celoškolského seminára SIT 2004*. Nitra : CIT FEM SPU v Nitre, 2004, ISBN 80-8069-320-X
6. TÓTHOVÁ, D. 1999. Návrh bezpečnostnej politiky univerzity. In: *Zborník z medzinárodnej konferencie UNINFOS '99*. Bratislava: MFF UK, 1999, s. 166-171.
7. TÓTHOVÁ, D. – BELLEROVÁ, B.: Open Access to Information. In: *EUNIS 2002 - The 8th International Conference of European University Systems*. Porto: FEUP, 2002, s. 435-442. ISBN 972-752-051-0
8. TÓTHOVÁ, D.: Teoretické aspekty použitia CMS na univerzite (prispevok na CD.In: *Zborník z medzinárodnej konferencie UNINFOS 2004*. Bratislava : Slovenská technická univerzita (STU), 2004. ISBN 82-227-2096-8
9. Zabezpečovací systém. 2006. [online]. [cit. 2006 - 03 - 28]. In *Zabezpečovacie systémy*. Dostupné na internete: <http://www.macet.sk/zab_systemy/art126.html>.

KONTAKTNÁ ADRESA
RNDr. Darina Tothová, PhD., Centrum informačných technológií Fakulty ekonomiky a manažmentu Slovenskej poľnohospodárskej univerzity v Nitre, Tr. A. Hlinku 2, 949 11 Nitra, E_mail: Darina.Tothova@uniag.sk

Recenzent: doc. Ing. Klára Hennyeyová, CSc.