AZ INFORMATIKAI BIZTONSÁG OKTATÁSA

Muha Lajos
főiskolai docens
Gábor Dénes Főiskola Informatikai Rendszerek Intézete

Absztrakt

Felértékelődik az informatikai biztonság szerepe és jelentősége, egyre nagyobb szüksége van olyan szakemberekre, akik képesek az informatikai rendszerekben előforduló biztonsági és megbízhatósági problémák kezelésére, valamint a kapcsolódó tervezési és fejlesztési feladatok elvégzésére, továbbá rendelkeznek a mélyebb elméleti alapokra épülő módszerek megértéséhez szükséges alapismeretekkel. Az informatikai biztonság oktatása ma még sok helyen „kísérleti jelleggel" folyik. A képzés lehetséges témájára, tartalmára és hangsúlyaira szeretnénk rámutatni.

1. BEVEZETÉS

Alapvető elvárássá vált, hogy az informatikai rendszerek biztonságosak legyenek, és az általuk kezelt adatok védve legyenek. A téma iránti érdeklődést mutatja az, hogy a 2006. szeptember 26-án megrendezett Informatikai Biztonság Napja rendezvényt 29 vállalat, köztük kiemelt hazai és multinacionális informatikai cégek támogatták. Az eseményen több mint nyolcszáz érdeklődő jelent meg. A piaci lehetőséget legjobban a *The American Institute of Certified Public Accountants (AICPA)* évente közzétett, a tíz vezető technológiát elemző jelentései (the Top Ten Technology Concerns of business managers) mutatják be – az informatikai biztonság 2001 óta folyamatosan az első helyen áll [1]. Ezek a tények is bizonyítják, hogy az informatikai biztonság az informatika egyik legfontosabb részterületévé válik, az informatikusok egyre komolyabban veszik az informatikai biztonság kérdését, és a végfelhasználók körében is mélyül az ezzel kapcsolatos tudatosság, és ezzel együtt az igény a hozzáértő szakemberekre.

2. AZ INFORMATIKAI BIZTONSÁG

Ahhoz, hogy az informatikai biztonság oktatásáról tárgyaljunk magának az informatikai biztonságnak kell a fogalmát, tartalmát és terjedelmét tisztáznunk. A védelem és a biztonság, az informatikai biztonság a fogalmaival, értelmezésével és pontos meghatározásával sokan nem szeretnek, nem is akarnak törődni.

A legszélesebb osztály a mi esetünkben a védelem és a biztonság fogalma. A védelem – a magyar nyelvben – tevékenység, illetve tevékenységek sorozata, amely arra irányul, hogy megteremtse, szinten tartsa, fejlessze azt az állapot, amit biztonságnak nevezünk. Tehát a védelem tevékenység, amíg a biztonság állapot. Az (amerikai) angol nem tesz különbséget a biztonság és a védelem között, mindkettőre a security szót használja.

---

[1] http://infotech.aicpa.org/Resources/Top+Technology+Initiatives/2007+Top+10+Technology+Initiatives/

A biztonság értelmét, tartalmát sokan sokféleképpen magyarázzák. Például a Magyar Értelmező Szótár szerint „a biztonság veszélytől, vagy bántódástól mentes, zavartalan állapot”. Ezt, és a hasonló megfogalmazásokat tudományos és műszaki szemlélettel elég nehéz elfogadni, mert egyrészt zavartalan állapot – mint tudjuk – nem létezik, másrészt nem a zavar teljes hiánya, hanem valamilyen „még elviselhető” mértéke és gyakorisága az, ami már valamilyen szinten biztonságnak tekinthető. Azonban ahhoz, hogy teljes legyen ez a biztonság az szükséges, hogy minden valós fenyegetésre védelmet nyújtson, ugyanakkor „körkörös” legyen, vagyis minden támadható ponton biztosítson valamilyen akadályt a támadó számára. Mindezek mellett elvárható, hogy ne csak „kettőtől hatig”, hanem folyamatosan létezzen. [2]
Így született az a definíció, hogy „az informatikai biztonság a védelmi rendszer olyan, a védő számára kielégítő mértékű állapota, amely az informatikai rendszerben kezelt adatok bizalmassága, sértetlensége és rendelkezésre állása szempontjából zárt, teljes körű, folytonos és a kockázatokkal arányos.” [3]
Az informatikai biztonságot gyakran keverik két másik fogalommal. Az egyik az adatvédelem, a másik az információbiztonság. Az adatvédelem – érdekes módon az angol nyelvben (data protection) is – a személyes adatok védelmére vonatkozik. Az információbiztonság az informatikai biztonságnál szélesebb, a szóban, írásban, az informatikai rendszerekben, vagy bármilyen más módon információk védelmére vonatkozik. Igaz, hogy angolul többnyire information security-ként jelenik meg mindkettő, de a szövegkörnyezet többnyire egyértelművé teszi, hogy miről van szó. Például az ISO/IEC 27001:2005 szabvány címe angolul *Information technology - Security techniques - Code of practice for information security management*, ahol az előtag elég egyértelműen meghatározza, hogy itt az informatikai rendszerek biztonságáról és nem általában információk biztonságáról van szó.

2.1. Az informatikai biztonság területei

Az oktatás szempontjából alapvető kérdés, hogy egy tantárgy mit oktasson, mire terjedjen ki. Ehhez magát az informatikai biztonságot, annak részterületeit kell elemeznünk. Az egyik lehetséges kiinduló pont az, mire kell tekintettel lenni az informatikai biztonság megteremtése során. A Miniszterelnöki Hivatal Informatikai Tárcaközi Bizottság 8. számú ajánlása (Informatikai Biztonsági Módszertani Kézikönyv) szerint a következő rendszerelemeket kell figyelembe venni:

- az informatikai rendszer fizikai környezete és infrastruktúrája,
- hardver rendszer,
- szoftver rendszer,
- kommunikációs, hálózati rendszerek
- adathordozók,
- dokumentumok és dokumentáció,
- személyi környezet (külső és belső).

E rendszerelemekre különböző fenyegetések[4] hatnak, amelyek a rendszerelemek meghatározott láncán keresztül az adatokat veszélyeztetik:

---

[2] MUHA Lajos (szerk.): **Az informatikai biztonság kézikönyve** (lektor: PAPP György) – Budapest: Verlag Dashöfer, 2000-2005

[3] DÉRI Zoltán, LOBOGÓS Katalin, MUHA Lajos, SNEÉ Péter, VÁNCSA Julianna: **Az informatikai biztonság irányításának követelményrendszere** – Információs Társadalom Koordinációs Tárcaközi Bizottság ajánlástervezet, Budapest, 2004.

[4] MUHA Lajos: A terrorizmus és az informatikai biztonság, előadás a HISEC 2004 Nemzeti adatvédelmi és adatbiztonsági konferencián, 2004. október 26.

- kiberterrorizmus (cyberterrorizm);
- információs hadviselés;
- gazdasági hírszerzés;
- ipari kémkedés;
- hackerek, crackerek;
- számítógépes bűncselekmények;
- gazdasági bűncselekmények;
- hanyagság, felelőtlenség.

Az ISO/IEC 17799:2005 szabvány is segítséget nyújt, hiszen az informatikai biztonság egészére kiterjednek az intézkedései:

1. Biztonságpolitika (Az informatikai biztonság dokumentumai)
2. Az informatikai biztonság szervezete
3. Az eszközök biztonsági besorolása és ellenőrzése
4. Személyzeti biztonság
5. Fizikai és környezeti biztonság
6. A hálózat és az üzemeltetés menedzsment
7. Hozzáférés menedzsment
8. IT rendszerek fejlesztése és karbantartása
9. Az informatikai biztonsági események kezelése
10. Üzletmenet-folytonosság menedzsment
11. Megfelelés az előírásoknak

Ezek alapján, a gyakorlati igényeket és elvárásokat is figyelembe véve megtervezhető az oktatás témája is.

3. Mérnök informatikus képzés

3.1. Az informatikai biztonság alapjai tantárgy

A BSc képzésben a tantárgy célja, hogy a hallgatók megismerjék az informatikai rendszerek biztonságának alapjait, valamint a kapcsolódó eszközök és eljárások kérdéseit. Az informatikai rendszerek teljes életciklusát felölelve az informatikai biztonsággal kapcsolatos jogi előírások, nemzetközi és hazai szabványok, ajánlások alapelvei, követelményei és a teljesítésükhöz szükséges alapvető teendőek elsajátítását követően a az informatikai rendszerek biztonságához tartozó technológiai kérdések (pl.: megbízható rendszerek, határvédelem, vírusvédelem, digitális aláírás, biztonsági ellenőrzés stb.) elméleti alapjait, a felhasználási alapelveit és megoldásait érdemes oktatni

Az informatikai biztonság tantárgy egy lehetséges tematikája:

1. A biztonság összetevői, az információvédelem és az informatikai biztonság
2. Az informatikai biztonság elméleti alapjai, rendszerszemléletű megközelítése
3. Szabványok és ajánlások
4. Információbiztonsági jogi ismeretek
5. A titokvédelem alapjai, a dokumentumkezelés elvei, rendszere és folyamata, ügyvitel-szervezési alapismeretek.
6. Az informatikai biztonságpolitika, az informatikai biztonsági szabályzat
7. Az informatikai biztonság irányítási rendszere (ISO/IEC 2700)
8. A hibatűrő rendszerek alapismeretei (a probléma és gyakorlati megoldások)
9. Logikai védelem
10. A hálózati alkalmazások biztonsága:
11. Az elektronikus szolgáltatások védelmének alapjai

12. Az informatikai biztonság vizsgálata
13. Üzletmenet-folytonosság és katasztrófa-elhárítás tervezése

A mesterképzésben ezekre az ismeretekre alapozva, a szakiránytól – is – függő témák elméleti kérdéseinek és gyakorlati megoldásainak mélyebb megismertetése lehet az oktatás célja

3.2. Informatikai biztonsági szakirány

Akár az alap-, de különösen a mesterképzésben egy az informatikai biztonsággal foglakozó szakirány lehetséges célja, hogy felkészítse a hallgatókat az informatikai biztonsági eszközök és eljárások tervezésének, alkalmazásának kérdéseibe, és az üzemeltetés (működtetés) részleteiben a napi gyakorlatban használható ismereteket nyújtson. A képzés során az informatikai rendszerek biztonsági és megbízhatósági kérdéseit, megoldásukra alkalmazott módszereket és technológiákat kell megismertetni. Meg kell teremteni a szakmai alapokat az informatikai biztonsággal kapcsolatos tervezési és fejlesztési feladatok ellátásához, betekintést kell kapniuk a vezetői feladatok kérdéseibe is.

A szakirány „kötelező” tantárgyai:

1. Megbízható informatikai rendszerek;
2. A kriptográfia alapjai;
3. Operációs rendszerek és alkalmazások biztonsága;
4. Hálózatbiztonság;
5. Eseménykezelés;
6. Biztonsági vizsgálatok.

A szakirány további ajánlott tantárgyai:

7. Az informatikai infrastruktúra védelme;
8. A humánmenedzsment feladatai a biztonságban;
9. Informatikai bűnözés;
10. Informatikai hadviselés.

4. Egyéb szakok

A MAB által a műszaki, mérnök, matematikus szakok egyik lehetséges (javasolt?) informatikai szakiránya az informatika biztonság. Ez esetben a mérnök informatikus képzés „kötelező” tárgyait érdemes oktatni a szaknak megfelelő kiegészítésekkel.

A közgazdász, pénzügyi-számviteli szakokon fontos lenne már a biztonság kezelésének nem megtérülő, de a kárelhárítás érdekében szükséges voltát oktatni. Itt nagy szerepe lenne a kockázatelemzés, a kockázatkezelés kérdésein túl az üzletmenet-folytonosság és katasztrófa-elhárítás tervezésével is foglalkozni.

5. A jövő

Húsz évvel ezelőtt hazánkban még nem képeztek informatikus mérnököket, ma ez az – az informatika általánossá válása miatt – az egyik legnépszerűbb szak a felsőoktatásban. Az informatikai biztonságot tíz évvel ezelőtt hazánkban még nagyon kevesek vették komolyan. Ma már megszámlálhatatlan cég kínálja szolgáltatásait ezen a területen. Ezek a cégek már most is igény tartanak a szervezetszerű képzésből kikerülő informatikai biztonsági szakemberekre. A téma ismeretét is egyre több helyen követelik meg informatikával foglalkozó szakembereiktől. Ez arra kell sarkalja a felsőoktatás műhelyei, hogy minél előbb a piaci igényeknek megfelelő képzést folytassanak ezen a téren is