XXII. Fiatal Műszakiak Tudományos Ülésszaka, 2017. Kolozsvár, 37–42. *DOI: 10.33895/mtk-2017.07.02*
http://hdl.handle.net/10598/29758

INFORMÁCIÓBIZTONSÁG TUDATOSSÁG

IT-SECURITY CONSCIOUSNESS

Rajnai Zoltán

Óbudai Egyetem, Bánki Donát Gépész és Biztonságtechnikai Mérnöki Kar,
Cím: 1081 Budapest, Népszínház u. 8., Tel: +36-1-666-5401
rajnai.zoltan@bgk.uni-obuda.hu

Abstract

Information security is one of today's most important issues. How it is reflected back in higher education? What are the training and education of the most important criteria? What solutions and rules must be followed in order to meet the standards? In Hungary, the government and administrative systems need close to two thousand information security specialists. How can be replaced this problem with professionals? The publication gives the answer and present a solution.

***Keywords**: Information security, Cybersecurity, education*

Összefoglalás

Az információbiztonság napjaink egyik legfontosabb kérdése. Az oktatásban ez hogyan tükröződik vissza? Melyek a képzés, az oktatáslegfontosabb kritériumai? Milyen megoldásokat és szabályokat kell betartani ahhoz, hogy az előírásoknak megfeleljünk? Magyarországon a kormányzati és közigazgatási rendszerekben közel kettőezer információbiztonsági szakember hiányzik. Hogyan pótolható ez a szám szakemberekkel? A publikáció erre ad választ és mutat be megoldási javaslatot.

***Kulcsszavak:** Információbiztonság, kibervédelem, felsőoktatás*

Az információ megszerzése és védelme, vagyis az információbiztonság évezredek óta foglalkoztatja az emberiséget. A történelem vizsgálata során megfigyelhetjük, hogy a XX. század közepéig a társadalmak politikai, gazdasági és egyéb mozgásait két fontos tényező motiválta: egyrészt a terület megszerzése és megtartása, másrészt a nyersanyagokhoz való hozzáférés, ezek birtoklása és elzárása.

A kezdetleges számítógépek megjelenésekor, majd később a fejlett, adatkezelő rendszerek kifejlesztésével az információ megszerzésének és védelmének jelentősége, módja is megváltozott.

A 19. század végétől kezdve olyan dinamikus változások kezdődtek az egész világon, melyek az élet minden területén gyors fejlődést, átalakulást eredményeztek. Gondoljunk csak a közlekedés, híradás, energetika területére, melyek rendkívüli változást hoztak az emberiség életében, ugyanakkor sérült az egyén, a közösségek, nemzetek, országok, vagyis az egész világ biztonságérzete.

A követelményeknek megfelelő információbiztonság csak akkor érhető el, ha minden szereplő tisztában van azokkal a szabályokkal, eljárásrendekkel, amelyek a biztonságot befolyásolják. Ezek a szabályok adják meg a biztonság kiinduló alapjait és garantálhatják a vállalatok információbiztonságát. A hazai és nemzetközi területen is egyre többet találkozunk a kibertér fogal-

mával. De tudjuk-e, mit jelent a kibertér? Ha egyszerűen akarunk fogalmazni, akkor a számítógépes hálózatok, a mobil infokommunikációs eszközök által felhasznált vezetékes, vagy vezeték nélküli csatlakozásokkal szolgáltatást nyújtó hálózatok összességét érthetjük. Ezek mérete, nagysága bár elvi síkon meghatározhatók, azonban valós dimenziói határtalanok.[1]

Hogyan, miért következhetnek be adatvesztések?

Az információbiztonság gyökerei tulajdonképpen egészen az ókorig nyúlnak visszsza, de általánosságban elmondható, hogy a kriptográfia egészen a XX. századig inkább művészet volt, ami olyan fejlődésen ment keresztül, amely nem volt tudatos.

„Magyarországon az ezredfordulóra megszületett a jövő **globális** tudománya, a biztonságtudomány. Ma a biztonságnak a társadalom által elvárt magas szintje a gyakorlatban csak korszerű védelmi, biztonságtechnikai rendszerekkel valósítható meg. Az elvárt biztonsági szint egyre növekszik, s az ennek eléréséhez szükséges műszaki megoldások, rendszerek egyre bonyolultabbakká válnak.” [2]

Adatvesztés, hekkertámadások, zsaroló vírusokkal és egyéb módszerekkel való támadások és általában az incidensek saját hibáinkból, a humán-erőforrás figyelmetlenségéből, a szabályok figyelmen kívül hagyásából, a biztonságtudatosság mellőzéséből következnek be. A biztonsági rendszer kockázatainak elemzése során egyértelműen kijelenthető, hogy még mindig a humán faktor (emberi tényező) a legtöbb biztonsági rendszer leggyengébb láncszem.

Biztonságtudatosság, biztonságtudatos szervezet jellemzői

A szervezet biztonságáért vállalt felelősség, a szervezet vezetése által meghatározott biztonsági szintnek, mint követelménynek elfogadása és a hiánya következményeinek elismerése, valamint a biztonsági szempontból erkölcsös, etikus magatartási kultúra együttesen jellemzi a biztonság tudatos szervezetet.

Fejlett biztonsági kultúráról akkor beszélhetünk, amikor az ismeretek elsajátítása és a megvalósítás együttesen érvényre jutnak. Ha felkészítjük a szervezet alkalmazottait arra, hogy felelősen, a biztonságot veszélyeztető tényezők ismeretében végezzék munkájukat, valamint a munkavégzéshez szükséges munkaeszközöket és információs rendszereket biztonságtudatosan használják, akkor bizonyosak lehetünk abban, hogy kisebb anyagi ráfordítással érjük el az információbiztonsági kockázatok csökkenését. Itt elsősorban arra gondolok, hogy a szervezet dolgozói megfelelő oktatásban, képzésben részesülnek, és az ott elsajátított ismereteket alkalmazni tudják és alkalmazni akarják.

Az információbiztonság szempontjából különlegesen fontos a szervezeti kultúra, annak okán, hogy a szervezet általános információbiztonsága valójában annak tagjain, az egyéneken, továbbá azok aktuális viselkedésén múlik. A szervezet dolgozóinak tudatos információbiztonsági magatartását – a megfelelő képzés mellett – leginkább a felsővezetői elkötelezettség és tudatosság befolyásolja pozitív irányban, melyet a dolgozóknak meg is kell tapasztalniuk (a valóságban hallaniuk kell). Vezetői elfogadás, akarat, támogatás nélkül nem lehetséges rendszert kiépíteni, működtetni.

Az ISACA által 2015 tavaszán elvégzett felmérés célcsoportja a releváns magyar vállalatok és intézmények voltak. A vizsgálat szerint a vezetők az információbiztonságot nagyon fontosnak tartják, de a biztonság megszilárdítására tett lépések nagyon gyakran elmaradnak, vagy csak részben valósulnak meg. [3]

Az oktatás, képzés, mint a belső szervezeti kultúra kialakításának és fejlesztésének pillére

Sik Zoltán Nándor: Elektronikus információbiztonság és közigazgatás előadásában kihangsúlyozza, hogy a biztonsági kultúra kialakítása és fejlesztése nem szervezeti szintű feladat, hanem társadalmi ügy, vagyis fontos az egész társadalom biztonságtudatosságának megalapozása, és folyamatos fejlesztése. A megalapozáshoz a családok, szülők és az oktatási intézmények is hozzájárulhatnak azáltal, hogy már a gyermekkor korai szakaszában biztonságtudatosságra szocializálják a gyermekeket. Ez az iskolákban a Nemzeti Alaptantervbe való beépítéssel még könnyebben kivitelezhető lenne. Az e–learning-ek és egyéb képzések pedig a felnőttek esetében lehetőséget adnak arra, hogy akár autodidakta módon azok is tájékozódni, fejlődni tudjanak, akik munkájuk révén nem kapnak megfelelő képzést.

Az információbiztonsági kultúra kialakításának és fejlesztésének fontosságát elméletben felismerték a szervezetek vezetői, de kevés gyakorlati lépést tettek a megvalósítás érdekében. A megvalósítást gátolja a területre fordítható pénzügyi forrás. Korábban már esett szó arról, hogy a humán faktornak igen erős szerepe van a biztonság megteremtésében, ugyanakkor az ember hatalmas veszélyforrása is lehet az információk kiszivárgásának. Az emberek felkészületlensége, vagy hiányos felkészültsége veszélybe sodorhatja az információ biztonságát, ezt azonban kellő színvonalú felkészítéssel orvosolni lehet, jobb esetben pedig meg lehet előzni.

A végzett hallgató mire legyen képes?

A közigazgatás részére képzett szakemberek elsősorban a biztonság területeire, azon belül az információbiztonságra specializálódhatnak a Biztonságtechnikai mérnöki alapszakon.

Képzési rendszerüket úgy alakítjuk ki, hogy felkészültek legyenek:

- az adatkezelő rendszereket érintő kérdésekben az információbiztonság teljes körű képviseletére;
- kezelni az állandó telepítésű adatkezelő nemzeti és külföldi nyílt, nem nyilvános, minősített elektronikus adatokat feldolgozó rendszerek tervezésével, létrehozásával, üzemeltetésével, fenntartásával, megszüntetésével kapcsolatos szakmai kérdéseket;
- a konferenciák, rendezvények rendszereinek tervezésére, fejlesztésére, beszerzésére, tesztelésére, üzembe helyezésére, üzemeltetésére, illetve megszüntetésére;
- az elektronikus adatkezelő rendszer személyi, fizikai, adminisztratív biztonsági követelményeinek megvalósítására;
- az adatkezelő rendszerek biztonsági követelményeinek és az ezek megvalósítására irányuló rendszabályok meghatározására;
- a szervezet, illetve rendszer specifikus biztonsági szabályzatok kidolgozására, kidolgoztatására;
- a rendszerek hatósági akkreditálásával, auditálásával és egyéb hivatalos ügyintézéssel kapcsolatos feladatok végzésére;
- szervezetek közötti együttműködés szervezésére, szabályozására, a külső ügyfelekkel, harmadik fél hozzáférésével kapcsolatos biztonsági kérdések megoldására, valamint információvédelmi feladatok összehangolására;
- a nemzeti és a külföldi nyílt, nem nyilvános, minősített elektronikus adatkezelő rendszerek biztonságát javító intézkedésekre, azok végrehajtására, kockázatarányos biztonsági eljárások kidolgozására javaslatot tenni;
- elektronikus adatokat feldolgozó rendszerek kockázatelemzésének végzésére, dokumentálására;

– a minősített elektronikus adatkezelő rendszer felelős feladatainak végzésére; rendszer biztonsági ellenőrzésére, a tapasztalatok kiértékelésére; a biztonsági incidensek kezelésére; szervezetek szakmai tevékenységének irányítására, támogatására;
– az elektronikus biztonsági feladatokat ellátó személyek részére a szakmai képzés tervezésére, szervezésére, valamint szakmai továbbképzések, felkészítések megtartására;
– javaslatot tenni a NATO, az EU, a nemzeti nem nyilvános, minősített rendszerek védelmét biztosító rejtjelző eszközök biztonságát javító intézkedésekre és jóváhagyás után azok végrehajtására;
– megfelelő szakmai gyakorlat megszerzését követően a nemzetközi szervezetekben feladatok végrehajtására.

Érdemes megvizsgálni azt is, milyen személyiség jegyekkel rendelkezzen egy információbiztonsági szakember, egyáltalán meghatározhatók-e specilis jegyek azok részére, akik e területen kívánnak dolgozni?

Napjainkban a menedzseri munka egyik alapvető feltétele mások helyes megítélésének és megértésének képessége. Ez a képesség az emberi erőforrás menedzsment számos tevékenységében kulcsfontosságú, ezek közül kiemelkedik a kiválasztási, felvételi folyamat, de további fontos területei között szerepel a beosztottak munkájának értékelése is. A megítélés alapja az érzékelés és észlelés.

Az érzékelés és az észlelés egymásra épülő történések, ahol az előbbi az alacsonyabb rendű, szenzoros folyamatokat jelenti, az utóbbi az észlelő személy további gondolkodási tevékenységét igényli (szelektív figyelmi szűrés, korábbi tapasztalatok nyomán kialakuló elvárások, kategorizálás) a megfigyelt jelenség jelentésének meghatározásában.

A munkára való alkalmasság egzakt, tudományos eredmények alapján történő megállapításának professzionális módja a munka alkalmassági vizsgálat. Célja, hogy egy adott munkakörre, szakterületre a legalkalmasabb dolgozók kerülhessenek. Az alkalmassági vizsgálat arra törekszik, hogy a dolgozók későbbi munkahelyi magatartását (teljesítményüket, munkájuk minőségét) a belépéskor elvégzett vizsgálatokkal előre jelezze. Az alkalmassági vizsgálat legfőbb értéke egyrészt az, hogy segítségével kiszűrhetők azok az egyének, akik az adott munkavégzéshez alapvetően szükséges kompetenciákkal, emberi tulajdonságokkal nem rendelkeznek, másrészt növelhető azok aránya, akik – a kiválasztást követően – kiválóan megfelelnek, beválnak az új munkahelyükön. Bár a vizsgálatokkal sem tudjuk teljes bizonyossággal meghatározni egy-egy jelölt jövőbeni magatartását, beválását, de mindenképpen csökkenteni tudják a hibás kiválasztás és a be nem vált munkaerő arányát. A hatékony munka, a megfelelő teljesítmény előfeltétele a megfelelő ismeretek, készségek, képességek, tulajdonságok birtoklása. A kiválasztás lehetőséget ad az alkalmatlanok, a szükséges sajátosságokkal, képességekkel, ismeretekkel nem rendelkezők kiszűrésére.

Az információbiztonság szintjének növelése a kiválasztási rendszer alkalmazásával

A közszolgálati kiválasztásnál fő funkciója, hogy minden szakterületen a legalkalmasabbak kerüljenek be a közigazgatási szervezetekbe. Ehhez professzionális kiválasztási politika szükséges. Ezért a közszolgálat számára nagy megtérülést jelent, ha folyamatosan fejleszti személyzet-kiválasztási stratégiáját.

A fenti megállapítással teljes mértékben egyetértek, a professzionális kiválasztás során a magam részéről is kulcsszónak tartom a megtérülést, beválást. A hatékonyság érdekében a honvédelmi szervezeteknek is a munkakör tartalmához leginkább illeszkedő kiválasztási módszereket és eszközöket

kell alkalmazniuk. Ennek természetes előfeltétele, hogy a kiválasztási eszközök és módszerek beválási indexén túl figyelmet fordítsanak a módszerek esetleges kombinációjának lehetőségére is.

Felvetődik bennem az a kérdés, vajon azok a munkakörök, amelyek az információbiztonság számára kockázatot jelenthetnek, miért nem igényelnek speciális szűrést?

Meggyőződésünk, hogy óriási veszélyt hordoz egy munkatárs, aki nem rendelkezik olyan személyiségjegyekkel, mint a megbízhatóság, magabiztosság, elkötelezettség, pontosság, tudatosság, szabálytudat, önállóság, felelősségtudat, befolyásolhatatlanság vagy önkontroll. Meglehetősen nagy a kockázata, hogy ez az ember felületesen fog kezelni olyan minősített adatokat, adatkezelő rendszereket, amelyek talán Magyarország katonai védelmét veszélybe sodorják. Gondoljunk Magyarország katonai reptereire, légiirányító központjaira, radar helyszíneire. Ezen túl fontos kiemelni hazánk Ország Védelmi Tervét, a minősített informatikai rendszereket, rejtjelző berendezéseket, minősített adathordozókat, és nem utolsósorban a minősített dokumentumokat.

Az információvédelmi beosztásokra a fentiek miatt csak olyan munkatársakat célszerű tervezni, akik a legnagyobb valószínűség szerint beválnak. Egy alaposan átgondolt kiválasztási rendszer mind a szervezet, mind a munkavállaló számára hasznos, hiszen egy olyan munkatárs, aki alapvetően pontos és megbízható, semmi áron nem kompromittálható, egy információbiztonsági munkakört nagy valószínűséggel színvonalasabban tud ellátni, a szervezet pedig nagyobb biztonságban, kevesebb kockázattal tud működni. Egy kompetencia alapú szakmai kiválasztás nem csupán a munkakörben való beválás miatt fontos, hanem szükséges hangsúlyozni, hogy információvédelmi beosztásokban dolgozó katonák ritka esetben kerülnek át más szakmai területre, tehát egy közigazgatásban dolgozó esetében egy biztonsági munkakör a legtöbb esetben hosszú távra, akár egy pályafutásra is szólhat. Ez alátámasztja azt a feltételezésünket, hogy érdemes időt és energiát fektetni a MINŐSÉGI KIVÁLASZTÁSRA.

Az információbiztonság erősítése, fokozása az informális ellenőrzés lehetőségeinek kihasználásával

Hisszük, hogy egy vállalat akkor tud eredményesen működni, ha a szervezet vezetője nem csupán a szervezet vezetője, hanem egyben menedzsere is. Egy szervezet irányítása során a vezetést olyan tevékenységként kell felfogni, amely célokat tűz ki, a célok elérése érdekében erőforrásokat biztosít. Kialakítja és működteti az általa irányított szervezetet a hatékonyság érdekében, mozgósítja a szervezet tagjait. A vezetés nem más, mint egy tudomány, szakma, egy olyan folyamat, amely során a vezető befolyásolja a beosztottakat a kívánt célok elérése érdekében. A menedzsment feladata pedig a tervezés, szervezés, utasítás, koordinálás, valamint az ellenőrzés is.

Kétféle módszert tartunk hasznosnak, amik igen jelentős információkat adhatnak egy vezető részére a beosztottakról.

Az egyik az alkalmazottak személyes megfigyelése. Mivel a szervezet vezetője a jogszabályokban leírtakon túl bármikor ellenőrizheti a szervezetében munkát végző személyt, jogában áll munkaidőn belül, és munkaidőn túl is belépni az alkalmazott irodájába, és meggyőződni arról, hogy beosztottja az információbiztonsági előírásoknak megfelelően tárolja dokumentumokat, vagy a szabályokban meghatározottak szerint működteti a minősített adatkezelő rendszert. [4]

A másik informális ellenőrzési lehetőséget a kommunikációban látjuk. A szervezetben kialakított úgynevezett „kommunikációs csatornák” biztosítják a vezetői tájékozódást. A vezetők a kommunikáció révén

visszajelzést kapnak a szervezet keretében folyó tevékenységekről, személyekről, melyeket akár informális információáramlásnak is nevezhetünk. A kommunikáció két részre osztható: a formális kommunikáció egy hivatalos forma, mely általában a vezetőtől a beosztottak felé áramlik. Ilyen lehet például célok közlése, utasítások, elvárások közlése, nevelő szándékú üzenetek, visszajelzés a teljesítményről, stb… A beosztottak részéről gyakran fordul elő problémák közlése, javaslatok felterjesztése, viták közlése, stb…. Az informális kommunikáció többnyire nem tudatos, kötetlen, legtöbb esetben a szervezetet irányító személy kezdeményezi. Meggyőződésünk, hogy egy menedzser típusú vezető az informális kommunikáció és ellenőrzés révén sokkal inkább tud valós képet kapni beosztottjairól, mint a jogszabályokban meghatározott ellenőrzések során.

Összefoglalva az információbiztonság humán faktora az egyik legnagyobb kritikus pont. Személyükben párosul a szakmai követelményeknek való megfelelés, valamint a személyes felelősségvállalás az információk védelmének biztosításában és a beosztottak, munkatársak feladatainak biztonságos végzésében, és annak irányításában. Ezekre kell felkészítenünk azokat a szakmérnököket, akiktől elvárjuk, hogy a közigazgatás rendszerében lássanak el feladatokat az elkövetkezendő időben.

Szakirodalmi hivatkozások

[1] Farkas Tibor, Sándor Miklós: *A honvédség állandó hírhálózatának fejlesztési kérdései*, Kard és toll: válogatás a hadtudomány doktoranduszainak tanulmányaiból 1:(2) pp. 158-164. (2006).

[2] Farkas Tibor, Hronyecz Erika: *The infocommunication system requirements and analysis of the communication of the deployable rapid diagnostic laboratory support „sampling group" II.*, Academic and applied research in public management science XIV:(1) pp. 53-61. (2015) NKE

[3] Információbiztonsági helyzetkép 2015 ISACA www.mpgehirportal.hu/documents/informaciobiztonsagi-helyzetkep-2015-%20pdf_20151019133850_84.pdf (letöltés ideje. 2017. 02. 02.)

[4] Farkas Tibor: *Signal Officer Training at the National University of Public Service (Budapest, Hungary),* In: New Trends in Signal Processing 2014: Tatranské Zruby, Slovakia. Liptovski Mikulas: Armed Forces Academy of General Milan Rastislav Štefánik, 2014. pp. 37-43.