Kerner Menyhért[1]

AUTONÓM, ELTÉRŐ BIZTONSÁGI POLITIKÁVAL RENDELKEZŐ INFORMATIKAI RENDSZEREK EGYÜTTES INFORMÁCIÓBIZTONSÁGÁNAK VIZSGÁLATA (1.)

Információvédelmi eltérések az informatikai rendszerek között

Absztrakt

Az informatikai rendszerek közötti információcsere mennyisége és jelentősége növekszik. A rendszerek közötti különbségek kockázatot jelentenek a rendszerek megosztott információira. A rendszerek közötti interoperabilitás szükségessé teszi az együttes információbiztonság vizsgálatát. Jelen publikáció összegzi a rendszerek közötti információvédelmi eltéréseket, az eltérések kockázatait, ellenük való védekezés lehetőségeit.

The amount and importance of information exchange among information systems is being increased. The differences of the systems cause risk to the shared information of the systems. The interoperability among the systems demands the examination of the common information security. This publication summarizes the differences of intersystem information security, their risks, and the possible protection options.

Kulcsszavak: *informatikai rendszerek interoperabilitása, információ-védelmi eltérések, együttes információbiztonság, eszközök és módszerek, információbiztonsági szabványok ~ interoperability of the information systems, information security differences, common information security, devices and solutions, information security standards*

BEVEZETÉS

Az informatikai rendszert létrehozó és üzemeltető szervezet céljai megvalósítása érdekében számára megfelelő információbiztonsági szintet kell létrehoznia. Ezt az információbiztonsági szintet a szervezet informatikai biztonsági filozófiájából és politikájából kiindulva az informatikai biztonsági stratégia megvalósítása során lehet elérni. Mivel az eltérő rendeltetésű szervezetek viszonya az általuk birtokolt, vagy kezelt információk biztonságával eltérő lehet, ezért a biztonsági filozófiák és politikák is ennek megfelelően eltérőek lehetnek. A kormányzati és a védelmi szférában általában kiemelt fontosságú a kezelt információk védelme. Az informatikai rendszer kialakítása során az eltérő biztonsági követelmények eltérő információvédelmi megoldásokat is jelentenek. Tovább bonyolítja a helyzetet, hogy azonos biztonsági szint eléréséhez számtalan módszer és eszköz áll rendelkezésre. Ezek közt a választás függ a szervezet anyagi lehetőségeitől és humán erőforrásainak minőségétől, mennyiségétől, a

[1] ZMNE BJKMK KMDI doktorandusz hallgató

kialakításához rendelkezésre álló időtől, tradícióktól, valamint a szervezettől és a hozzá kapcsolódó meglévő informatikai rendszerektől is.

Ma már csak elvétve található olyan informatikai rendszer, amely nem csatlakozik más rendszerhez is, tehát csak saját információkat használ. Többnyire az egyes informatikai rendszerek megosztanak másokkal információkat, információcserét végeznek velük. Ha a rendszer megoszt információt más rendszerekkel is, akkor már nem elegendő csak a rendszeren belül vizsgálni az általa birtokolt, illetve kezelt információk biztonságát. Ezt meg kell tenni az információcserében résztvevő összes informatikai rendszerrel kapcsolatban is. Ez az interoperabilitás napjainkban előtérbe került a katonai informatikai rendszerek fejlesztése során. A NATO stratégiai koncepciója is foglakozik az informatikai interoperabilitás témakörével. [1]

A megosztott információk miatt nem csak az egyes rendszerek információbiztonságáról lehet beszélni, hanem bevezethető az e felett álló, az összes információcserében résztvevő rendszerre vonatkoztatott együttes (eredő) információbiztonság fogalom. Az együttes információbiztonság a megosztott információ biztonsági szintje az információcsere által létrejött komplex rendszerben. Ugyanígy bevezethető az együttes bizalmasság, hitelesség, rendelkezésre állás és működőképesség fogalma is.

Mivel az egymással kapcsolatban lévő rendszerek eltérő informatikai eszközöket és módszereket használnak, ezért az információcseréhez ezeket illeszteni kell egymáshoz. Ez az illesztés a megosztott információ szempontjából biztonsági kockázatot jelenthet. Ennek oka, hogy minden az információcserében résztvevő rendszer számára páronként az információcsere érdekében plusz információkat kell kiadni (pl. közös eljárások és kulcsok). Az információcsere lehetősége érdekében a közös eljárások és módszerek alkalmazása nagyobb kockázatot jelent az információkra, mint az egyes rendszereken belül használatosak. További kockázatot jelenthet az egyes rendszerek közötti kevéssé védett csatornákon és csomópontokon való átvitel is.

A fentiekből látható, a nagyfokú autonómiával rendelkező informatikai rendszerek információcseréje során előfordulhat, hogy míg az egyes rendszereken belül az információk védelme megfelelő, addig az információcsere során létrejövő összetett rendszerben ugyanezen információk biztonsága nem megfelelő. Csak akkor szabad a védett információkat megosztani más rendszerekkel, ha azokon belül is megoldott az információk megfelelő védelme. Ehhez az információcserében résztvevő rendszereknek és az információcsere útvonalnak is ki kell elégítenie az információbiztonsági igényeket.

Mivel a legtöbb esetben kevés ismerettel rendelkezünk az információcserében résztvevő informatikai rendszerekről, az útvonal elemeiről (egyre inkább Interneten keresztül áramlanak az információk), ezért leginkább csak a szabványokra és ajánlásokra tudunk hagyatkozni. Az információvédelmi ajánlások, szabványok pontos megvalósítása esetén már lehetőség nyílik az összetett rendszer együttes információbiztonsági szintjének értékelésére, a kockázatok felmérhetővé válnak.

A szabványok, ajánlások pontos megvalósítása sem mindig jelenthet megoldást. Az egyes rendszerekben megvalósított eltérő információvédelmi ajánlások, szabványok esetén nehézséget jelenthet az együttes információvédelmi képesség értékelése. Ennek oka, hogy az egyes információvédelmi ajánlásokat más-más igények hívtak életre, más-más információvédelmi filozófiát követnek, nem azonosak bennük az információvédelmi kulcskérdések, egyes részterületeket más-más részletességgel tárgyalnak, esetleg némelyekkel abszolút nem foglalkoznak.

Megoldásként kínálkozik, azonos szabványok és ajánlások használata, mely megoldást jelenthetne. Ez több okból is problematikus, mert a meglévő rendszerek átalakítását igényelné (költség, idő, stb.), és adott szabvány vagy ajánlás nem feltétlenül felel meg minden szervezet számára.

A fent vázolt nehézségek ellenére szükséges az összetett, együttes biztonság értékelése, az információvédelmi veszélyforrások felmérése. E publikáció és az ezt követő második rész célja az informatikai rendszerek közötti információcsere információvédelmi kockázatainak felmérése, e kockázatok csökkentési lehetőségeinek bemutatása. Az első részben a lehetséges eszközök és módszerek, valamint az alkalmazott szabványok és ajánlások közötti különbségeket mutatom be. Majd a második részben e különbségek lehetséges kockázatait vázolom. Végül megmutatom, milyen módon lehet ezeket a kockázatokat csökkenteni.

Az informatikai rendszerek védelmére használt információvédelmi eljárások és módszerek jelentősen eltérhetnek egymástól, a hasonló elérendő információbiztonsági célok ellenére, ennek oka, hogy a rendszerek kialakítására, más-más tényezők hatnak. Adott rendszert birtokló egy-egy szervezet informatikai biztonsági filozófiája és politikája nagyban eltérhet egymástól, ezért az informatikai biztonsági stratégiák megvalósítása során jelentős eltérések mutatkozhatnak. A különbözőség annak ellenére létrejöhet, hogy a védendő információ akár meg is egyezhet, vagy hasonló fontosságú lehet több rendszerben is. Az eltérések alapja az informatikai rendszereket birtokló szervezetek alaprendeltetésében keresendőek. Ezek az eltérések kihatnak a kezelt információk biztonságára is. Vagyis előfordulhat, hogy az egyik rendszerben ugyanaz az információ fokozottan, míg egy másikban kevésbé védett lehet. A szervezetek sajátosságai miatt létrejövő eltérő biztonsági követelmények miatt eltérő információvédelmi megoldásokat alkalmazhatnak egy-egy informatikai rendszerekben. Azonos biztonsági szint elérését különbözőképpen lehet elérni, sok megoldás lehetséges. Az informatikai rendszer védelme érdekében használt módszerek és eszközök kiválasztását befolyásolja a szervezet anyagi, humán erőforrásainak mennyisége, a felépítésre szánt idő, tradíciók, a szervezet által birtokolt, vagy ahhoz kapcsolódó egyéb informatikai rendszer sajátosságai.

1. ALKALMAZOTT INFORMATIKAI ESZKÖZÖK ÉS MÓDSZEREK ELTÉRÉSEI

Számtalan szabványos eszköz és módszer áll rendelkezésre az informatikai rendszerek megfelelő biztonságának megteremtéséhez. Egy szervezeten belül hasonló feladatokra hasonló, vagy egyforma eszközöket célszerű alkalmazni. Ez a törekvés általában jellemző is az informatikai rendszereket birtokló szervezetekre. Ezt diktálja a célszerűség, mivel így a rendszer átláthatósága javul, karbantarthatóbb és általában költséghatékonyabb az így felépített rendszer működtetése. Az egységesség azonban sérülhet, ennek oka lehet az, hogy a rendszer folyamatos növekedése, változása során a régi eszközök sokáig megmaradhatnak az újak mellett a rendszerben. De hasonló feladatokra is indokolt lehet eltérő technológiák használata egy-egy részterületen, pl. speciális igények kielégítése érdekében. Az egységesebb felépítés a kevesebb fajta eszköz és módszer használata jelenthet olyan előnyöket, hogy érdemes akár a részfeladat igényeihez mérten redundanciával rendelkező, de több feladat elvégzésére alkalmas eszközökből felépíteni a rendszert.

Mivel egy-egy szervezet általában önállóan végzi (végezteti) informatikai rendszerének fejlesztését, más-más szempontok alapján dönt az informatikai beszerzéseiről, ezért szervezetenként nagyfokú eltérés lehetséges a rendszereket felépítő eszközökben.

Természetesen a szervezet (vezetőinek) viszonya a birtokolt informatikai rendszerhez végső soron kihat a rendszert felépítő elemekre is. Például két pénzügyi szolgáltatásokat végző szervezet esetén az egyik filozófiájához a széleskörű, gyors, és megbízható szolgáltatások tartoznak, akkor ehhez szükséges infrastruktúrán belül alapvető a gyors, megbízható és az új szolgáltatásokat (pl. e-banking) támogató informatikai rendszer kiépítése. A szintén pénzügyi szolgáltatásokat nyújtó másik szervezet esetében - mely filozófiájának alapja a versenyképesség alacsony költségekkel és erős marketing munkával való megteremtése - a szervezet nem érdekelt költséges informatikai fejlesztésekre beruházni, csak az alap informatikai háttér megteremtésére koncentrál. Az alacsonyabb szintű informatikai háttér okozta hátrányokat marketinggel és alacsonyabb színvonalú, de kisebb költséggel járó szolgáltatások nyújtásával kompenzálja. Természetesen az egyik esetben nagy sebességű, nagy megbízhatóságú informatikai rendszert kell felépíteni, gyors megbízható elemekből, ráadásul a felépítő elemeknek támogatni kell az új bevezetett szolgáltatásokat is. A második esetben nem alapvető kérdés a minőségi informatikai háttér, hanem költséghatékony megoldást kell találni, melyben a rendszer rendeltetésszerű működésén kívüli állapot még korlátozott költséggel járjon.

A szervezet informatikai biztonsági filozófiája kihat az alkalmazott eszközökre és módszerekre. A szervezet biztonsági filozófiájából következik végső soron a szervezet biztonsági stratégiája, így az informatikai biztonsági stratégia is. Az eltérő informatikai biztonsági stratégiák mentén az informatikai rendszereket felépítő eszközökkel és módszerekkel szemben is más-más követelmények fogalmazódnak meg. Ha egy szervezetben kiemelt fontosságú a benne kezelt információk biztonsága, akkor az informatikai rendszert felépítő eszközöknek és módszereknek is tükrözniük kell ezt.

Jó példa az eszközök eltérésére a Wi-Fi eszközök. Az IEEE802.11b WLAN szabvány megjelenése után kiderült, hogy a használt WEP-KEY titkosító eljárás nem nyújt kielégítő védelmet, magasabb biztonsági szintekhez. Ezt a problémát az eszközöket gyártó cégek úgy kezelték, hogy saját a szabványon kívüli eljárásokat fejlesztettek ki, mellyel megfelelő védelmet lehet adni a vezeték nélküli kapcsolatoknak. Ezek a megoldások gyártó specifikusak, ezért ezeket csak azonos gyártmányú eszközök összekapcsolásakor lehetett használni. Különböző eljárásokat használó eszközök esetén vissza kellett térni a szabvány által biztosított alacsonyabb védelmi eljárások használatához. A példánál maradva, hiába használnak a vezeték nélküli összekapcsoláskor az egyik hálózatban IEEE802.11i szabványú, már magasabb védelmi képességű eszközöket (támogatja az AES titkosítást), ha a másikban a „b” szabványú, vagyis kevésbé védett kapcsolatot lehetővé tevő eszközt használják.

2. INFORMÁCIÓVÉDELMI SZABVÁNYOK ÉS AJÁNLÁSOK KÖZÖTTI KÜLÖNBSÉGEK

Mivel egy szervezet informatikai rendszere igen bonyolult lehet, nem feltétlenül elegendő a használt eszközök és módszerek kiválasztása, szükséges egy magasabb szintű követelményrendszer megfogalmazása az informatikai rendszer kialakításához. Az információbiztonsági szabványok és ajánlások tartalmazzák a szükséges információvédelmi követelményeket. A nemzetközi információvédelmi szabványok és ajánlások tükrözik a

létrehozó személyek (szervezetek) gyakorlati tapasztalatait. Az információvédelmi szabványok, ajánlások használatával az informatikai rendszer védelme gyorsabban megoldhatóvá válik, az így létrehozott rendszerben kisebb valószínűséggel maradnak információvédelmi lyukak. A kialakított rendszer információbiztonsági vizsgálata elvégezhető, a fennmaradó információvédelmi kockázatok utólag értékelhetővé válnak. Az egyes információvédelmi szabványok és ajánlások tükrözik az alkotók preferenciáit, a megcélzott szervezetek elvárásait. Így fordulhat elő, hogy az adott ajánlás, vagy szabvány az információvédelem egy-egy területét részletesen tárgyalja, míg másikkal kevésbé, vagy egyáltalán nem foglalkozik.

Abban az esetben, ha egy információvédelmi szabvány sem ad teljes körű megoldást, lehetőség van több különböző együttes használatára. Így megvalósíthatóvá válnak a kitűzött információvédelmi célkitűzések. Pl. az EU agrártámogatásainak kifizetését végző ügynökségét támogató rendszerhez a COBIT (Control Objectives for Information and related Technology) könyvvizsgáló rendszert, az ISO 17799 és a német Bundesamt für Sicherheit in der Informationstechnik: IT-Grundschutzhandbuch információvédelmi eljárásokat használják. [2]

Az 1996-ban kiadott COBIT jelenlegi negyedik kiadásában férhető hozzá, 34 magas szintű osztállyal és 318 részletezett osztállyal rendelkezik, melyeket úgy hoztak létre, hogy segítsék a szervezetek IT eszközeinek felügyeletét. [3] A szabvány jól ismert, jól dokumentált, sok segítséget ad az IT szakembereknek. Felismerve az igényt, a COBIT-et kiadó szervezet az ISACA (Information Systems Audit and Control Association) kiadott egy speciálisan kis és közepes szervezetek számára kidolgozott egyszerűsített COBIT változatot („QuickStart”), ez az informatikai rendszereket üzemeltető szervezetek számára legkritikusabb elemekkel foglalkozik, így ehhez nem szükséges az egész szabvány ismerete. A COBIT alapvetően a szervezet vezetőit segíti a szervezet informatikai eszközeinek felügyeletében, vizsgálatában, úgy, hogy foglalkozik a felhasználókkal, az informatikai rendszerek vizsgálatával, ellenőrzésével, lehetőséget ad a rendszer teljesítményének mérésére is. Leginkább a pénzügyi és üzleti szférában terjedt el, ennek tudható be, hogy a szabvány szemlélete is ezt tükrözi. Alapvetően a hatékonyabb üzletmenetelt és az azt veszélyeztető kockázatok csökkentését hivatott támogatni. Előnyeként az idő és pénzkímélést lehet megemlíteni, melynek oka a jól dokumentáltsága, szakemberek sokasága, valamint könnyű alkalmazhatósága. [4] A COBIT 4.0 verzió újdonsága többek között harmonizáció és leképezhetőség más szabványokra (ITIL, CMM, COSO, PMBOK, ISF és ISO17799). [5]

Az ISO17799 (Information Technology – Code of Practice for Information Security Management) alapja az 1995-1999 között kiadott brit BS7799 információvédelmi szabvány. A szabvány központi eleme a biztonság, segítséget nyújt a szervezet számára információvédelmi terveik elkészítéséhez. A szabvány a következő magas szintű csoportokat tartalmazza: védelmi eljárások, szervezeti biztonság, értékek osztályozása és felügyelete, személyi biztonság, fizikai és környezeti biztonság, kommunikáció és működés felügyelet, elérés felügyelet, rendszerfejlesztés és karbantartás, üzlet folytonosság szervezés és illeszkedés. A jól ismert szabvány az informatikai biztonság széles területét fedi le. A szabvány a kockázatmenedzselést hangsúlyozza ki, kiindulva az információvédelmi politikából, felbecsülve a kockázatokat, majd azokat kezelhetővé teszi. Rugalmasságát mutatja, hogy lefedi az információ minden formáját, beleértve a hanganyagokat, képeket, és olyan médiákat, mint a például a mobiltelefon, vagy a FAX. Támogatja többek között olyan új területeket, mint az elektronikus kereskedelem, az Internet, az erőforrás kihelyezés (out-surcing), a távmunka és a mobil informatika. [6] A BS7799 második kiadása az 1999-ben publikált BS7799-2:2002, ami az ISO/IEC27001:2002 (2005) kiadásával vált nemzetközi szabvánnyá. [7] A BS7799-2 középpontjában az információ biztonsági

menedzsment rendszer alkalmazása áll, hivatkozva az információs biztonság menedzsment struktúrára és felügyeletére, melyek az ISO17799-ben találhatóak meg.

Az ITIL (Information Technology Infrastructure Library) kevésbé ismert, mint a fenti két auditáló szabvány. A nyolcvanas évek közepén hívta életre a brit Kereskedelmi Minisztérium, az üzleti élet IT eszközeinek jobb felügyelete érdekében. A szabvány leginkább az üzletmenetre és az információs technológiára fókuszál. [8] Az ITIL IT támogató szolgáltatások segítik elő a szervezet számára hatékonyabb szoftver, hardver és humán erőforrás menedzselést az üzem folytonosság fenntartása érdekében. Az ITIL-nek nem feladta minden informatikai terület lefedése, pl. a környezeti és fizikai biztonsággal nem foglalkozik.

A COBIT erőssége a felügyelet, ellenőrzés és mérőszámok, az ITIL kiváló gyakorlati példák és eljárások sokaságát tartalmazza, az ISO17799 pedig kiemelkedik a védelemben. [9]

Ide tartozik még a TCSEC, FC, CTCPEC és ITSEC létrehozói által 1996-ban létrehozott CC (Common Criteria) kritériumrendszer, mely általánosan elfogadott követelményrendszert tartalmaz az informatikai rendszerekkel szemben. [10] A CC hatóköre kiterjed az informatikai eszközökre, rendszerekre és termékekre. Az információbiztonságot fenyegető tényezőket megnevezi, ezek közül azokkal foglalkozik, melyeket az IT eszközöknek kell kivédeniük. Részletesen foglakozik a környezeti biztonsággal, szervezetbiztonsággal, IT hozzáférés biztonsággal, szoftverfejlesztés minőségellenőrzésével, speciális biztonsági mechanizmusok értékelésével. A CC hatókörén kívül esik, pl. az adminisztratív biztonsági intézkedések, környezeti biztonság értékelése, a kriptográfiai algoritmusok és azok belső jellemzőinek értékelésére vonatkozó kritériumok. Ennek ellenére például a CC előírja, hogy az értékeléshez a kriptográfiai algoritmusokkal is kell foglalkozni.

A fentiekből látható, hogy mindegyik információvédelmi szabványnak vannak erősségei, kiemelten kezelt, de kevésbé tárgyalt részterületei is. A szervezet által megfogalmazott követelményektől függ, mely információvédelmi szabványt érdemes a leginkább felhasználni.

ÖSSZEFOGLALÁS

Az informatikai rendszerekkel szemben támasztott információvédelmi követelményekben tükröződnek a rendszereket birtokló szervezetek elvárásai. Eme eltérések mellett tovább növeli a különbségeket az egyes szervezetre jellemző, a saját informatikai rendszeréhez való viszony. Az informatikai rendszerek fejlődésében megfigyelhető tendencia, hogy egyre több a rendszerek között megosztott információ, egyre fontosabbá válik a rendszer interoperabilitása. Az információcserében résztvevő egyes rendszerek felépítése, használt eszközeik és módszereik eltérhetnek egymástól, amit figyelembe kell venni az összekapcsolásuk során. Az eltéréseket a rendszerek biztonsági követelményeinek eltérése, rendelkezésre álló anyagi és humán erőforrások mennyisége, rendelkezésre álló idő, tradíciók okozzák. Az interoperabilitáshoz illeszteni egymáshoz kell az egyes rendszereken belül használt információvédelmi eszközöket és módszereket. Hogy az egyes módszerek és eszközök különbözőségével minél kevésbé keljen foglakozni, törekedni kell közös információvédelmi szabványokat és ajánlásokat teljesítő eszközök és módszerek használatára. A rendszert birtokló szervezet igényei szabják meg a használt információvédelmi szabványt is. Az egyes szabványok eltérhetnek az általuk tárgyalt információvédelmi terület feldolgozási mélységében, a használt módszerekben. Ezeket a különbségeket figyelembe kell venni a más-más szabványt, ajánlást kielégítő rendszerek

interoperabilitása során. Az eltérő információbiztonsági szabványok által használt eljárások különbségei miatt az információbiztonságot az egyes rendszerekben másképp vizsgálják, így azok összehasonlítása, egységes értékelhetősége nehézkessé válik. Nehéz összehasonlítani két az információ cserében résztvevő informatikai rendszert, ez információvédelmi kockázatot jelent a megosztott információkra.

(Folytatása következik)

FELHASZNÁLT IRODALOM

[1] *Dr. Munk Sándor: Az informatikai interoperabilitást támogató megoldások a NATO-ban*, Új honvédségi szemle, 2006/09
[2] *EU Selects COBIT as an Auditing Standard,* Certification magazine, [http://www.certmag.com/articles/templates/cmag_nl_extra_content.asp?articleid=1196&zoneid=37, 2006. 04. 20.]
[3] *Will O'Brien: IT Governance: Recovering from the Buzz Part 1*, The Manta Group, [http://www.mantagroup.ca/html/documents/wp-buzz1.pdf, 2007. 01. 08.]
[4] *Rod Amis: Introduction COBIT*, [http://management.itmanagersjournal.com/management/06/03/13/1845239.shtml?tid=88, 2006. 04. 22.]
[5] *COBIT 4.0: Major Update to International Standard Helps Businesses Increase IT Value, Decrease Risk*, ArriveNet, [http://press.arrivenet.com/industry/article.php/731636.html, 2006. 04. 23.]
[6] *COBIT*, Wikipedia, [http://en.wikipedia.org/wiki/COBIT, 2006. 04. 23.]
[7] *BS7799 How it Works*, IWS-The Information Warfare Site, [http://www.iwar.org.uk/comsec/resources/bs7799/works.htm, 2006. 04. 23.]
[8] *How ITIL-based IT Help Desk can help Small and Medium Businesses*, [http://manageengine.adventnet.com/products/service-desk/me-itil-sdp-helpdesk-smb.pdf, 2006. 04. 23.]
[9] *BS 7799*, Wikipedia, [http://en.wikipedia.org/wiki/BS_7799, 2006. 04. 23.]
[10] *Common Criteria* – Hunguard Kft., Budapest, 1997