Kerner Menyhért[1]

AUTONÓM, ELTÉRŐ BIZTONSÁGI POLITIKÁVAL RENDELKEZŐ INFORMATIKAI RENDSZEREK EGYÜTTES INFORMÁCIÓBIZTONSÁGÁNAK VIZSGÁLATA (2.)

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 egyes informatikai rendszerek információvédelmét a létrehozó szervezet informatikai biztonsági filozófiái és politikái alapján alakítják ki. [1] Az egyes szervezeteken belüli eltérő feltételrendszerek és biztonsági stratégiák miatt a kialakított informatikai rendszerek eltérnek egymástól. Ezek az eltérő rendszerek más-más információvédelmi eszközöket, módszereket, szabványokat és ajánlásokat használnak az általuk kezelt információk védelmére. A rendszerek közötti interoperabilitás érdekében megosztanak egymással információkat. Ez az információ megosztásból következik, hogy a megosztott információk biztonságát nem csak az egyes rendszerekben, hanem a rendszerek összekapcsolásával létrejövő összetett rendszerre is kell vizsgálni. A használt információvédelmi módszerek, eszközök, szabványok és ajánlások eltérhetnek az egyes rendszerek esetén, ezért a rendszerek közötti interoperabilitáshoz ezeket illeszteni kell egymáshoz. A módszerek és eszközök különbségeit és a különbségek okait az előző rész tárgyalja részletesen. Ezek a különbségek a használt kommunikációs csatornákkal együtt kockázatot jelentenek az együttes információbiztonságra. Vagyis, abban az esetben is

[1] ZMNE doktorandusz

foglalkozni kell az együttes információbiztonsággal, ha önmagában az egyes informatikai rendszerek megfelelően védik a saját rendszerükben lévő információkat.

Az informatikai szabványok, ajánlások pontos megvalósítása az egyes rendszerekben segíti a rendszerek egymáshoz való illesztését, csökkenti az összekapcsolás kockázatait. De az egyes rendszerekben más-más információvédelmi szabványt használhatnak. E szabványok összehasonlítását, az eltérések okainak bemutatását az előző rész tartalmazza. Ha az egyes rendszerekben más-más igényeket kielégítő eltérő információvédelmi ajánlásokat, szabványokat valósítottak meg, akkor nehézséget jelenthet az együttes információvédelmi képesség értékelése. Ezt küszöbölhetné ki azonos szabványok és ajánlások használata. A meglévő rendszerek átalakítását igényelné, és adott szabvány nem biztos, hogy megfelel minden egyes szervezet számára.

E publikáció és az ezt megelőző első rész célja az informatikai rendszerek közötti információcsere információvédelmi kockázatainak felmérése, e kockázatok csökkentésének lehetőségeinek bemutatása. Az első részben az alkalmazott eszközök, módszerek és szabványok, ajánlások közötti különbségeket mutattam be. Ebben a részben e különbségek lehetséges kockázatait vázolom, majd kitérek e kockázatok csökkentésének lehetőségeire.

1. AZ EGYMÁSSAL KAPCSOLATBAN LÉVŐ INFORMATIKAI RENDSZEREK EGYEDI ÉS EGYÜTTES INFORMÁCIÓBIZTONSÁGÁNAK KAPCSOLATA, AZ ELTÉRÉSEK KÖVETKEZMÉNYEI

Az autonómiával rendelkező rendszerek információcseréjével létrejövő összetett informatikai rendszer együttes hitelessége, bizalmassága, rendelkezésre állása sérülhet, az információcsere következtében az eredő rendszer információbiztonsági szintje alacsonyabbá válhat, az egyes őt felépítő rendszerekénél.

Alapvetően érvényes a leggyengébb láncszem elve, vagyis az összetett rendszerben lévő bármelyik felépítő elem védelmi hiányosságai kihathatnak az információcserében részt vevő összes rendszerre. Például, ha a közösen használt információkkal szemben sérül az egyik autonóm rendszerben a bizalmasság, úgy az együttes rendszerben is sérülhet az. Végső soron az összetett rendszert felépítő összes rendszerre kihat ez, mindenhol sérülhet ezen információkkal szembeni bizalmasság.

De lehetséges olyan eset is, amikor az információcsere következtében a rendszerek egyes információvédelmi képességei javulhatnak, jobb lehet, mint az információcsere nélküli autonóm rendszereké. Például a működőképesség javulhat azáltal, hogy a rendszerek erőforrásaikat megosztják egymással, egymás lehetséges tartalékai lesznek. Vagy a hitelesség szintje emelhető egyazon információ hitelességének több helyről való ellenőrzésével.

Továbbiakban avval foglalkozom, hogy mely esetekben sérülhet az amúgy az egyes rendszerekben megfelelő szintű hitelesség, bizalmasság, rendelkezésre állás és működőképesség az információcsere következtében.

1.1 ELTÉRŐ INFORMATIKAI ESZKÖZÖK ÉS MÓDSZEREK HASZNÁLATÁNAK KÖVETKEZMÉNYEI

Az egymással információcserét végző autonómiával rendelkező rendszerek együttes hitelességét, bizalmasságát, rendelkezésre állását és működőképességét befolyásolhatják az egyes rendszerekben használt eszközök és módszerek eltérése.

Az információcseréhez szükséges az egyes rendszereket egymáshoz illeszteni. Ez azért szükséges, mert eltérhetnek egymástól az ez egyes rendszerek által használt az információcserét szolgáló eszközök és módszerek. Illesztés nélkül nem jöhetne létre megfelelő információcsere. Az információcseréhez szükséges azonos kommunikációs, vagy egymással kompatibilis protokollok használata.

Fontos említést tenni a kommunikációs útvonal szerepére. Teljesíteni kell a kommunikációs útvonal igényeit, e nélkül nem hozható létre megfelelő információcsere. Információvédelmi szempontból igen fontos az útvonal vizsgálata, mert ez a kommunikációs csatorna egyre inkább a nyílt hozzáférésű globális Internet. Az Internet olcsó, mindenki által hozzáférhető, nagy sebességű, valamint nagyszámú eszköz és módszer támogatja. E nyílt hozzáférés és rugalmasság teszi sebezhetővé a rajta keresztül folyó információáramlást, és veszélyezteti az információcserében résztvevő informatikai rendszereket. [2] További gond az, hogy csak olyan információvédelmi eljárások használhatóak, amit maga az Internet és a csomagokat továbbító hálózati elemek támogatnak. Mivel az egyes rendszereken kívülálló dolog, ezért nem rendelkezhetnek pontos ismeretekkel az információcserében résztvevő többi rendszerről, azok információvédelmi szintjéről, ez további kockázatot jelent számukra.

1.1.1 Bizalmasság

A bizalmasság sérül, amikor adott információhoz illetéktelen személy hozzáfér. A bizalmasság megőrzése sokrétű feladat, számtalan módszert lehet használni. Rezsim intézkedések, környezeti biztonság, fizikai biztonság és informatikai biztonság együttese hozza létre a rendszerben tárolt információk védelmét. A bizalmasság fenntartása érdekében az információkhoz való hozzáférés korlátozása és szabályozása a rendszeren belül és kívül egyaránt fontos. [3] Amíg külső információcsere nincs, csak a hozzáférés védelemmel kell foglalkozni. De a gyakorlatban már alig van olyan informatikai rendszer, mely ne állna más rendszerekkel kapcsolatban. E kapcsolathoz az információcsere védelme érdekében közös információvédelmi eljárásokat kell használni. A nem megfelelő eljárások használata kockázatot jelent, a bizalmasság sérülhet. A nem megfelelő kommunikációs védelem a védendő információhoz való idegen hozzáférést nem megfelelően korlátozza a továbbítás során.

A bizalmasság megőrzésére tett intézkedések hangsúlyai eltérhetnek egymástól, az egyik rendszerben a megfelelő bizalmasságot IT eszközök és módszerek alkalmazásával, másikban, pedig erős rezsim és fizikai biztonságot érintő intézkedésekkel érik el. E két teljesen eltérő biztonsági megoldásokat felvonultató rendszer közötti információcsere során a következő kockázatok lehetnek. Az alacsonyabb IT színvonalú rendszer miatt korlátozottabb információvédelmi eszközöket és módszereket kénytelenek használni, ami nem csak a kommunikációs útvonalon fenyegeti az információcserében résztvevő rendszereket. Az alacsonyabb informatikai színvonalú rendszer olyan információit is

fenyegetés érheti kívülről, melyek nem is vesznek részt az információcserében. A kapcsolódási ponton keresztül a magasabb IT színvonalú rendszerből, vagy a kommunikációs csatorna felhasználásával hozzáférhetővé válhatnak a rendszerben tárolt információk. Ezt a fajta hozzáférést leginkább csak IT eszközökkel lehet korlátozni. Ilyen alacsony színvonalú információvédelemmel rendelkező rendszer védelme érdekében némelykor leválasztják a rendszert a külső kapcsolódásról. Ilyenkor a rendszer közvetlenül nem folytat információ cserét más rendszerekkel, hanem az értékes belső hálózattól elkülönített másik hálózat, vagy egy az információcserében résztvevő különálló számítógép végzi a feladatot. Ez hozzáférés korlátozásra megfelelő módszer, de igen rugalmatlan megoldás, meg kell oldani, hogy a két elkülönülő hálózat között mi módon áramoljon az információ. A legegyszerűbb esetben, az egyes információcserében résztvevő információkat egyenként kezelve, ellenőrizve erre kijelölt személyek töltik át az egy szervezethez tartozó két egymástól elkülönülő hálózat között. Ez a megoldás kevéssé járható, mert nagy mennyiségű információ feldolgozása gondot jelent, az emberi tévedés lehetősége felesleges kockázattal jár, jelentős humán erőforrást igényel, valamint a folyamat sebessége nagyon alacsony. Az információcsere során alkalmazott magasabb szintű védelmet nyújtó megoldások használata nehézségeket okozhatnak a kevéssé felkészült rendszer számára. Ez korlátot szabhat a használható megoldások kiválasztásakor.

Az eltérő védelmi eszközöket és eljárásokat használó rendszerek információcseréje során gond lehet a kompatibilitással. A kompatibilitási hiányosságok információvédelmi kockázattal járhatnak, kockázatot jelentenek a kezelt információk bizalmasságával szemben is.

Az információcseréhez az információk védelmére szolgáló eljárásokat, kulcsokat az információk megosztásában résztvevő összes rendszernek ismernie kell. Ez a védelmi eljárásokról több helyen meglévő ismeret növeli az összetett rendszer információinak bizalmasságával szembeni kockázatot. A közösen használt eljárások, kriptográfiai kulcsok megosztása, leváltása önmagában is biztonsági kockázatokat rejt magában.

A bizalmasság megőrzéséhez elengedhetetlen az információ hozzáférés védelem. [4] Ha eltérő eljárásokat és eszközöket használnak két rendszerben, akkor az okozhatja a jogosulatlan hozzáférés kockázatának növekedését, vagy jogosult személy hozzáférésének korlátozását. Például az információcserében résztvevő rendszerek közül az egyik rendszerben a hozzáférés védelem alapja valamely biometriás eljárás (pl. újlenyomat azonosítás), a másikban egyéni csip kártya. Akkor a második rendszerből információt lekérni szándékozó személy jogosultsága a biometriás interfész hiányában nem azonosítható az első rendszerben. Erre csak akkor nyílhat esély, ha a második rendszer csip kártya információkat ad át az elsőnek. Vagyis csak úgy oldható meg az összetett rendszeren belül a hozzáférés engedélyezéssel kapcsolatos illesztés, ha a hozzáférési információk is megosztásra kerülnek. De ez sem lehet teljes körű megoldás, mivel a hozzáférés védelem több lépcsős lehet (pl. kapu szolgálat). Így a használt hozzáférés védelmi megoldások egymás közötti megosztása, nem jeleni feltétlenül a másik rendszerből lekért információkkal szembeni bizalmasság követelményének teljesülését. A nem megfelelő, vagy aktualitását vesztett hozzáférési információk további kockázatot jelentenek. Pl., ha az egyik felhasználó adott információhoz való hozzáférését korlátozása az egyik rendszerben, csak akkor vonja maga után a másik rendszerben is a hozzáférés korlátozását, ha ezt a hozzáférési korlátozó információt a két rendszer megosztja egymással. Ennek hiányában másik rendszerben elérhet olyan információt, melyhez hozzáférését nem engedélyezték.

1.1.2 Hitelesség

A hitelesség megőrzése alapvető fontosságú több rendszer információcseréjének során, mert egy másik rendszerből nyert információ hitelessége nem mindig ellenőrizhető közvetlenül. A hitelesség megállapítására módot adhat, ha egy információ, vagy avval kapcsolatos más információk több helyen is elérhetőek. Így a hitelesség mértéke javítható. Az információcsere során a hitelesség megőrzésére a felhasznált információvédelmi eljárások használatával van mód. Például az elektronikus aláírás, a nyilvános kulcsú titkosítás használata lehetőséget ad az információk hitelességének megőrzésére.

Az eltérő hitelesítő eljárásokat használó rendszerek információcseréje során gondot jelenthet ezek különbözősége. Az egymás közötti információcsere során a hitelesség megőrzését célzó eljárások elhagyása csökkenti az együttes rendszer információ hitelességi szintjét. A közösen használt, a mindkét rendszerben használt eljárások információ átadásával járnak az adott rendszerben használatos eljárásokról, kulcsokról. És mivel a védelmi módszerekről információ több helyen is hozzáférhető ezért az összetett rendszer által birtokolt információk hitelességével kapcsolatos kockázatok is növekednek. Plusz kihívást jelent a hitelességgel kapcsolatos eljárások és kulcsok megfelelő, védett továbbítása az információcsere során, majd a működés során azok frissítése, cseréje.

Gondot okozhat, hogy a hitelesség megállapításához az egyes rendszerekben, más-más jellemzőket tárolnak.

1.1.3 Rendelkezésre állás

Az információ rendelkezésre állása az informatikai rendszerek számára lényeges jellemző. Az információ megsemmisülése, nem a megfelelő időben való hozzáférhetősége az informatikai rendszerekben történő információfeldolgozást nehezíti, vagy lehetetlenné teszi. Ha az információcserében résztvevő egyes rendszerekben az információk rendelkezésre állása megfelelő, akkor csak egy másik rendszer által biztosított információ okozhatja a rendelkezésre állás sérülését.

A legegyszerűbb eset, amikor az egymással információcserét végző rendszerek között kommunikáció akadozik, vagy leáll. Ekkor a két autonóm rendszer közötti kommunikációs gondok miatt a szükséges információk áramlása lelassul, vagy meg is szűnik. Ez az információcserében résztvevő rendszerek rendelkezésre állását veszélyezteti.

Akkor, amikor az egyik rendszer által tárolt és a többivel megosztott, fontos információ semmisül meg, az kihat a többi rendszerre is. Ebben az estben is több rendszer rendelkezésre állása hathat ez.

Az információ az egyes rendszerben más-más formában (adatstruktúra) áll rendelkezésre. Ugyanolyan, vagy hasonló információk tárolása jelentősen eltérhet az egyes rendszerekben. Ahhoz, hogy ezt az információt felhasználni, feldolgozni lehessen egy másik rendszerben, ahhoz megfelelő formára kell hozni, ennek hiányában nem értékelhető az információ. Vagyis az összetett rendszerben a megfelelő információ rendelkezésre állása csak a megfelelő információ konverziós eljárások használatával érhető el. Gond csak az, hogy az egyes rendszerekben más-más adatstruktúrák létezhetnek, ezen adatstruktúrák közötti konverziók során elveszhetnek, módosulhatnak részinformációk. Ezáltal az elvileg egyforma információ másképp jelenhet meg az információcserében résztvevő egy-egy rendszerben. Pl., ha az egyik rendszer nem kezeli a tárolt adatstruktúrákban az ékezetes

karaktereket, akkor a belső használathoz a kívülről jövő szöveges adatokat ékezet nélkülivé kell, hogy alakítsa. Evvel természetesen részinformáció veszik el, nem állítható vissza teljes egészében az eredeti szöveges információ. Összességében az információk rendelkezésre állását korlátozza ez a jelenség.

1.1.4 Működőképesség

A működőképesség az informatikai rendszer azon jellemzője, hogy hogyan képes végrehajtani a szervezet által megkövetelt feladatait. Ez általában az információ feldolgozó képességet jeleni. Az információ feldolgozó képesség szoros összefüggésben van a rendszert felépítő eszközökkel, módszerekkel, valamint a rendszer felépítésével. Az, hogy a rendszer fel tudja-e dolgozni az információkat, az a feldolgozni kívánt információk mennyiségével és minőségével is összefügg.

Az információcsere történik erőforrások megosztása során. Az erőforrás megosztás lehet, pl. tároló-, vagy számítási kapacitás megosztása. A megosztással nő a rendszerek együttes hatékonysága [5], növelhető a rendszerek biztonsága (pl. biztonsági mentés a másik rendszerben), vagy költség takarítható meg. De az előnyök mellett az erőforrás megosztás kockázatokat is rejthet az együttes működőképességre nézve. Ennek oka, hogy, ha a másik rendszerben lévő erőforrás szükséges egy vagy több rendszer számára, akkor annak működésében történő zavarok kihatnak azon rendszerekre is, amelyek azt használni kívánják

1.2 ELTÉRŐ INFORMÁCIÓVÉDELMI SZABVÁNYOK ÉS AJÁNLÁSOK HASZNÁLATÁNAK KÖVETKEZMÉNYEI

Az eltérő információvédelmi szabványok és ajánlások más-más célkitűzéssel jöttek létre, ezért eltérő a preferenciájuk, egyes információvédelmi területeket jobban, másokat kevésbé támogatnak. [6] E különböző ajánlások és szabványok felhasználásával fejlesztett, vagy auditált informatikai rendszerek információvédelme eltérhet egymástól, mert az eltérő szabványok és ajánlások teljesítése érdekében nem azonos információvédelmi eljárásokat és ajánlásokat kell alkalmazni. Továbbá egyes szabványok és ajánlások kimondva, vagy sem, nem, vagy csak részben foglalkoznak egyes információvédelmi területekkel. Így vagy másik szabványt kell alkalmazni az információvédelmi szakembereknek, vagy saját elképzeléseikre kell hagyatkozniuk.

A szabványok egyik része csak az IT eszközökkel, magával az informatikai rendszerrel szorosan összefüggő kérdésekkel foglakozik, másik része az információvédelmet komplex feladatnak tekinti, amihez hozzátartoznak az IT eszközökön és módszereken kívüli információvédelmi területek is, mint pl. a fizikai vagy az adminisztratív biztonság.

Az autonóm rendszerek információcseréjére akkor jelenthet kockázatot az eltérő szabványok és ajánlások használata, ha azok jelentősen eltérnek egymástól, kevéssé hasonlíthatóak össze. Könnyű belátni, hogy azonos szempontok alapján tervezett és azonos kívánalmaknak megfelelő rendszerek információcseréje során létrejövő kockázatok az azonos kritériumok miatt könnyen felmérhetőek. Pl., ha egy rendszer információt oszt meg egy másik azonos információvédelmi kritériumokat teljesítő rendszerrel, akkor biztos lehet

abban, hogy ezek az információk hasonlóan védettek lesznek ott is. Így csak a kommunikáció kérdéskörével kell foglalkozni. De abban az esetben, ha más szabványokat és ajánlásokat teljesítő és egymás között információcserét végző rendszert vizsgálunk, ezt azonnal nem lehet kijelenteni.

Például a COBIT egyáltalán nem foglalkozik a fizikai biztonság témakörével, de az ISO17799 már igen. Ebből következik, hogy, ha az IT eszközökre elfogadjuk mindkét szabványt az összetett rendszeren belül (egyik rendszer COBIT-ot, egy másik ISO17799-et használ), akkor még foglalkozni kell az összetett rendszer információbiztonságára ható fizikai biztonság kérdésével. Ennek az-az oka, hogy az összekapcsolás révén már nem érvényes az egyedi információbiztonsági szint, hanem az együttes információbiztonságot kell vizsgálni.

Az egyes információvédelemmel foglalkozó szabványok és ajánlások hatókörének korlátosságát komplex rendszerek esetén úgy tudják feloldani, hogy több különbözőt használnak. Csak azok a jellemzők hasonlíthatóak össze egyszerűen a különböző rendszerekben, melyeket mindkét rendszerben használt információvédelmi szabvány használata során lehet kinyerni.

2. AZ EGYÜTTES INFORMÁCIÓBIZTONSÁG MEGŐRZÉSE AZ AUTONÓM INFORMATIKAI RENDSZEREK INTEROPERÁBILITÁSA MELLETT

Az alkalmazott eltérő információvédelmi szabványok és ajánlások, valamint az egyes informatikai rendszerekben alkalmazott eltérő eszközök és módszerek kockázatot jelenthetnek az egyes rendszerek közötti információcsere során, sérülhet az így létrejövő összetett rendszerben az információk bizalmassága, rendelkezésre állása, hitelessége és a rendszerek működőképessége. Mivel a rendszerekben az információcsere során is mind a négy követelménynek teljesülnie kell, nem elég csak külön-külön vizsgálni a rendszereket. Az interoperábilitás következtében nem sérülhet a rendszerekben az információk biztonsága.

Az összetett, együttes információbiztonság könnyebben vizsgálható, abban az estben, ha az egyes autonóm rendszereket azonos vagy hasonló kritériumok, szabványok és ajánlásoknak megfelelően fejlesztetik és üzemeltetik, bennük használt módszerek és eszközök hasonlóak.

Ez az egységes felépítés nem várható el az eltérő informatikai biztonsági filozófiának és politikáknak megfelelően felépített különböző informatikai rendszerektől. Mivel más-más cél érdekében, más-más feltételek között hozták létre az egyes autonóm rendszereket, ezért elkerülhetetlen az egymástól eltérő felépítés. A rendszerek más-más informatikai szabványt és ajánlás elégítenek ki, más-más informatikai eszközt és módszert használnak.

Az összetett rendszert felépítő autonóm informatikai rendszereknek egymásról csak meglehetősen kevés információjuk lehet. Az információcserét megelőzően már létrejött rendszereket már csak kevésbé lehet módosítani az interoperábilitás kockázatainak mérsékléséhez. Ennek oka, hogy nem csak egy, hanem sok különböző rendszerhez való kapcsolódás lehetséges, mely lehetetlenné teszi az illeszkedést mindegyikhez. Továbbá a módosítások, változtatások nagy idő és költség igényt jelentenek. Ez a munka igen komplex feladat, aminek végrehajtása önmagában is biztonsági kockázatokat hordoz.

Jobb megoldás, ha a megosztott információkhoz rendelünk biztonsági követelményeket, melyek teljesítését az autonóm rendszerre bízzuk. Az interoperábilitásban közreműködő autonómiával rendelkező rendszerek érdekeltek az általuk használt információk biztonságának fenntartásában, ezért érdekükben áll a velük szemben támasztott információvédelmi követelmények kielégítése. A megosztott információk biztonsága érdekében minden rendszerre szükséges egységes követelményrendszer kidolgozása, így az egyes rendszereken belül kell megoldani a megosztott információk védelme. Ez még nem elégséges az együttes információbiztonsághoz, ezért speciális a rendszerek közötti interoperábilitás kockázatának kiküszöbölésére szolgáló követelményeket is meg kell fogalmazni az együttműködésben résztvevő összes informatikai rendszerrel szemben.

Az információvédelem komplex feladat, hozzá tartozik, pl. a fizikai, környezeti és dokumentum biztonság is. A közös információbiztonság megvalósításához ezeknek a követelményeknek a kielégítése is szükséges minden egyes rendszerben.

Az információk bizalmasságának, hitelességének, rendelkezésre állásának megőrzése érdekében megfogalmazandó követelményekhez ismerni kell az információ értékét, sérülése milyen kockázatokkal jár. E nélkül nem fogalmazható meg információvédelmi követelmény, amit, az információt felhasználó rendszereknek teljesíteniük kell. Az információcsere során átadható a megosztott információkon kívül az információ biztonságával kapcsolatos plusz információk is. Vagyis az információn kívül, avval együtt eljuttatható, a védelmével kapcsolatos további követelmények is.

Ezt a fajta kiegészítő információt régóta használják a dokumentum kezelés során és az információ (dokumentum) minősítésének hívják. Például a NATO és az EU minősítési kategóriái nagyon hasonlóak. Ezek a minősítési kategóriák országonként, vagy szervezetenként jelentősen el is térhetnek. Abban az esetben, ha két eltérő minősítést használó szervezet információt oszt meg egymással, akkor mindkét helyen ezt az információt be kell sorolni a megfelelő minősítési kategóriába. Ez bevett gyakorlat a papír alapú dokumentumok esetén, de igen munkaigényes feladat. Az informatikai rendszerek elterjedése és azok mindinkább egyre szorosabb kapcsolata és az egyre nagyobb mennyiségű információcsere miatt már nem célszerű, vagy nem is lehetséges az információk manuális kategorizálása. Mivel minden minősítési kategória részletesen körülhatárolt, ezért a besorolás közel egyértelmű. Ha különböző minősítési rendszerek közötti konverzióra van szükség, akkor nagy valószínűséggel megtalálható az adott minősítés másik minősítési rendszeren belüli párja. Egy kategóriához, akár több is megfeleltethető egy másik minősítési rendszerben, vagy fordítva. Ekkor már nem feleltethetőek meg közvetlenül egymással a minősítési rendszerek kategóriái.

2.1 ELTÉRŐ INFORMATIKAI ESZKÖZÖK ÉS MÓDSZEREK HASZNÁLATÁNAK KÖVETKEZMÉNYEI ELLENI VÉDEKEZÉS

Az informatikai rendszert üzemeltető szervezet célkitűzéseitől függnek végső soron az alkalmazott eszközök és módszerek. Az elérendő információbiztonsági szint, a rendelkezésre álló anyagi és humán erőforrások, idő és tradíciók határozzák meg a rendszer felépítését, a felépítő eszközök és módszerek kiválasztását. Mivel igen sok tényező befolyásolja az eszközök és módszerek kiválasztását, ezek jelentősen eltérhetnek különböző rendszerek esetén. A megosztott információk hitelességét, bizalmasságát, rendelkezésre állását és működőképességét meg kell őrizni a rendszerek közötti

interoperabilitás során, annak ellenére, hogy a kapcsolódó rendszerek esetleg jelentősen eltérnek egymástól.

Lehetőség szerint azonos szabványokat kielégítő eszközöket és módszereket kell alkalmazni az egymással kommunikációt folytató rendszerek között. Ha ez nem lehetséges illeszteni kell őket egymáshoz, illesztés nélkül nem lehetséges a rendszerek közötti kommunikáció. Eltérő rendszerek esetén megoldható, hogy a kommunikáció létrejötte érdekében azonos speciális eszközöket telepítsenek minden egyes rendszerhez, de ez jelentős idő és költség ráfordítással járna. Ezen kívül maga az eszközök telepítése is kockázattal jár (alapvetően a rendszertől idegen berendezés csatlakoztatása, az eszközök szállítása, karbantartása). Az eltérő eszközök és módszerek egymáshoz való illesztése is kockázatot jelenthet, mivel minél speciálisabb, kevésbé elterjedt az eszköz, annál kisebb az esélye az illesztéssel elkövetett információvédelmi hibák felszínre kerülésének. Ezért a legjobb megoldás az általánosan elfogadott, megfelelő biztonságot nyújtó szabványokat pontosan megvalósító, jó minőségű eszközök és módszereket használni az informatikai rendszerekben. Ha az információcserében résztvevő összes rendszer ennek a kívánalomnak megfelel, akkor gyorsan, kis ráfordítással lehet csatlakoztatni őket egymással. A szabványos eszközök azonos protokollokat használva teszik lehetővé a rendszerek interoperabilitását.

A rendszerek összekapcsolása a közöttük lévő útvonalon keresztül történik, mely egyre gyakrabban maga az Internet. Hogy az útvonalon az információk át tudjanak haladni, teljesíteni kell az eszközöknek és módszereknek a kommunikációs útvonal igényeit is. A kommunikációhoz csak olyan információvédelmi eljárások használhatóak, amiket, a csomagokat továbbító hálózati elemek támogatnak. Olyan információvédelmi eljárásokat kell alkalmazni az informatikai rendszerek között áramló információk védelmére, melyek megfelelő védelmet nyújtanak a rendszerek közötti kommunikációs csatornákra is.

Továbbiakban bemutatom, hogy milyen lehetőségek a megosztott információk bizalmasságát, hitelességét, rendelkezésre állását és a rendszerek működőképességét fenyegető kockázatok kivédésére.

2.1.1 Bizalmasság

A bizalmasság védelme a rendszereken belül alapvetően fontos, de ha információt kell megosztani más rendszerekkel, akkor még inkább előtérbe kerül védelmének szükségessége. Az információcsere során megosztott információ bizalmassága a kommunikációs útvonalon és az információt kérő rendszerben sérülhet az információ forrásán kívül.

Olyan esetekben, amikor a bizalmasság megőrzése érdekében használt módszerek jelentősen eltérnek egymástól, akkor azokat értékelni kell. Az értékelés eredményeként, abban a rendszerben, ahol nem megfelelő az információk bizalmassága, ott szükséges annak megerősítése a rendszerek együttes védelme érdekében. Ahol a rendszer nem tudja a kritériumokat teljesíteni, ott a külső védelmi kapuk létesítése célszerű. A kapuk feladata a rajta átmenő információkhoz kapcsolódó védelmi feladatok ellátása. Ez a megoldás megvédi a belső informatikai rendszerben lévő információk bizalmasságát.

A kockázatok csökkentésére, azonos, vagy hasonló információvédelmi eszközöket és módszereket használhatna az információcserében résztvevő rendszerek. Így az egymással való inkompatibilitás kockázatai mérsékelhetőek.

Mivel az információcsere nem jöhet létre némely az információvédelemhez szükséges információ nélkül, ezért gondoskodni kell ezen eljárások és módszerek bizalmasságának megtartásáról, mert csak így védhető a rendszerek között áramló információ, valamint a rendszerek saját információ is. E közösen használt eljárások és módszerek telepítésének és frissítésének (pl. új rejtjel kulcsok) védelmét és menetét nagy körültekintéssel kell elvégezni, mert ez a folyamat nagy kockázatot jelenthet a rendszerek számára.

Az információhoz való hozzáférés érdekében szükséges az információ kérőjének azonosítása. Az azonosítás érdekében szükséges a jogosultakkal kapcsolatos információk átadása. Mivel eltérhetnek az azonosítási eljárások az egyes rendszerekben, az azonosításhoz szükséges eljárásokat és adatbázisokat egymáshoz kell illeszteni. Az illesztés nélkül jogosulatlan információlekérés kockázata megnő, de előfordulhat jogosult hozzáférésének korlátozása is. Ezen kívül gondoskodni kell az információkhoz való hozzáféréssel kapcsolatos információk aktualitásáról is.

2.1.2 Hitelesség

Több rendszer információcseréje során feltétlenül szükséges a hitelesség megőrzése. A hitelesség szintjének növelésére megoldást nyújt több az információval rendelkező helyről beszerzett hitelességi információ. A hitelesség igazolására megfelelő eszközök, módszerek alkalmazása nyújthat garanciát. Pl. az elektronikus aláírás széles körben elterjedt, módszer az információk hitelességének megállapításához. Kiegészíthető speciális hardver elemekkel (pl. chip kártyaolvasó), melyek a használt algoritmusokkal együtt garantálják az információk megfelelő hitelességét. [7]

Az eltérő hitelesítő eljárások használata esetén gondoskodni kell ezek illesztéséről, a hitelesítési eljárások és szükséges adatok biztonságos cseréjéről.

2.1.3 Rendelkezésre állás

Az informatikai rendszereknek feladataik elvégzéséhez információkra van szükségük, ha nem férnek hozzá, akkor azt nem tudják elvégezni. Az információk rendelkezésre állása sérülhet, ha azok nem a megfelelő időben, vagy formában férhetők hozzá, vagy megsemmisülnek. Ha egy rendszer sok külső információt igényel más rendszerektől, akkor a belső információinak rendelkezésre állása mellett figyelembe kell venni a külső információk rendelkezésre állását is. A külső információ rendelkezésre állásával kapcsolatos kockázatok úgy csökkenthetők, hogy ha a rendszer csak a minimálisan szükséges információt szerzi be más rendszerből. Ha ugyanaz az információ több rendszerből is lekérhető, akkor ennek kihasználása növeli a rendszer által igényelt külső információk rendelkezésre állását. Az információcserében résztvevők közötti kommunikációs csatorna megbízhatóságának, sebességének javításával is lehet javítani a megosztott információk rendelkezésre állást.

A rendszereken belül az információk különböző adatformában vannak tárolva, az információcsere során lényeges hogy a különböző rendszerek azonosan értelmezzék ezeket. A különböző adatstruktúrák között konverzióra van szükség, a konverzió kockázatot jelent az információ rendelkezésre állására nézve. Ezért olyan konvertáló módszerekre van

szükség, melynek használata során az információ sérülésének, megváltozásának kockázata kicsi. Ennek a kockázatnak a kiiktatására, a konverzió elhagyására mód nyílik azonos, esetleg szabványos adatstruktúrák használatával.

2.1.4 Működőképesség

Egymás között információkat megosztó rendszerek működőképességére hatással lehet az interoperabilitásuk. A hatás annál kisebb minél kevésbé szorul a rendszer külső erőforrásokra, minél kevésbé hatnak a rendszer feladatvégzési folyamataira a megosztott információk. Így a működőképességre való hatás csökkenthető külső erőforrásoknak a feladatvégzéshez való szükségletének korlátozásával, azok kiesésének hatásait csökkentő eljárásokkal, pl. más erőforrások bevonásával. A működőképességre való hatás korlátozásának további módja az információcsere által szoláltatott információk kiesésének kezelése (pl. más forrásokból való helyettesítéssel). Törekedni kell arra, hogy a rendszeren kívüli információk nélkül is lehetőség szerint rendeltetésszerűen működjön az informatikai rendszer. A több helyről hozzáférhető információk, valamint a megbízhatóbb kommunikációs csatornák javítják a rendszer működőképességét, mert kisebb a valószínűsége, hogy információhiány lépjen fel a feldolgozás során, valamint gyorsabban áll elő a szükséges információ.

2.2 ELTÉRŐ INFORMÁCIÓVÉDELMI SZABVÁNYOK ÉS AJÁNLÁSOK HASZNÁLATÁNAK KÖVETKEZMÉNYEI ELLENI VÉDEKEZÉS

Az információcserében résztvevő informatikai rendszerek esetén előny az, ha azonos információvédelmi szabványokat és ajánlásokat használnak. Ilyenkor a megosztott információkra nézve azonos követelmények betartását könnyű ellenőrizni. Az egyes rendszereket azonos módon vizsgálják, azonos követelményeket lehet megfogalmazni velük szemben, könnyen összehasonlíthatóak egymással. A Nehezebb a követelmények ellenőrzése és betartatása abban az esetben, ha ezek a szabványok és ajánlások eltérnek egymástól. Tovább nehezíti az információvédelmi szakemberek munkáját, hogy egy informatikai rendszeren belül több félét is használhatnak. Ennek oka, hogy az eltérő információvédelmi szabványok és ajánlások nem egyformán támogatják az információvédelem egy-egy részterületét. Így a gyakorlatban elterjedt módszer, több különböző információvédelmi szabvány és ajánlás együttes használata. Ennek előnye inkább nagy komplex rendszerek esetén jelentkezik. Több eltérő követelményrendszernek is meg tud felelni az ilyen informatikai rendszer.

A különböző információvédelmi szabványt és ajánlást használó rendszerre is azonos információvédelmi kritériumokat kell meghatározni. A kritériumoknak való megfelelést a szabványokban rögzített módszerekkel kell elvégezni. Ez megnyugtató eredménnyel járhat, abban az esetben, ha ezek támogatják a megfogalmazott célokat.

ÖSSZEFOGLALÁS

Az informatikai rendszereknek feladataik ellátása érdekében külső, más informatikai rendszerek által birtokolt információkra van szükségük. Ennek az információcserének a kielégítéséhez információcserét végeznek más informatikai rendszerekkel. Az információcsere információbiztonsági plusz kockázatokat jelenthet az egyes rendszerek számára. Sérülhet a megosztott információk bizalmassága, hitelessége, rendelkezésre állása és a rendszerek működőképessége.

A kockázatok forrása alapvetően a rendszerek különbözőségéből adódnak. A különböző használt információvédelmi eszközök, módszerek, szabványok és ajánlások a rendszereket fenntartó szervezetek eltérő céljaiból és körülményeiből adódnak. Az információcserében résztvevő rendszerekben használt eszközök és módszerek, valamint szabványok és ajánlások különbségeinek feltérképezése után megbecsülhető ezeknek a különbségeknek az információvédelmi kockázatai.

A kockázatok mérséklésére lehetőség nyílik a hasonló szabványos széles körben elfogadott információvédelmi eszközök és módszerek, információvédelmi kapuk használatával. Azonos információvédelmi szabvány és ajánlás használatával olyan kritériumrendszer fogalmazható meg az információ megosztásban résztvevő rendszerekre, melyek garantálják az azonos információvédelmi szintet minden az interoperabilitásban résztvevő rendszer esetén. Eltérő használt szabványok és ajánlások esetén is törekedni kell minden rendszer esetén a megosztott információk védelmére szolgáló kritériumok teljesítésére.

FELHASZNÁLT IRODALOM

[1] Dr. Váncsa Julianna: Az informatikai biztonság alapjai – Budapest: ZMNE, 2000

[2] *Kaufman, Charlie: Network Security* – Private Communication in a Public World, New Jersey, 2002., ISBN: 0-13-046019-2

[3] Ködmön József: Kriptográfia, Az informatikai biztonság alapjai, a PGP kriptorendszer használata – Budapest: ComputerBooks Kiadó, 1999, ISBN: 9636182248

[4] Marvin V. Zelkowitz: Information security - New York: Academic Press, 2004., ISBN: 0-12-012160-3

[5] *Matt Bishop: Computer security*; Addison- Wesley, Boston Mass, 2003., ISBN: 0-201-44099-7

[6] *Muha Lajos-Bodlaki Ákos: Az informatikai biztonság* - Budapest: PRO-SEC Kft., 2005, ISBN: 963-86022-6-0

[7] *F. Ható Katalin: Adatbiztonság, adatvédelem* – Budapest: SZÁMALK Kiadó, 2005