Információbiztonság az ellátási láncokban

Michelberger Pál

Budapesti Műszaki Főiskola, Keleti Károly Gazdasági Kar, Szervezési és Vezetési Intézet, 1081 Budapest, Népszínház utca 8., michelberger.pal@kgk.bmf.hu

Lábodi Csaba

Pannon Egyetem, Gazdaságtudományi Kar, Alkalmazott Gazdaságtan Tanszék, 8200 Veszprém, Egyetem utca 10., labodi.csaba@almos.uni-pannon.hu

Absztrakt: Az információbiztonság alapvető fontosságú a strtégiai szövetségként is működő ellátási láncokban. Az alapvető fogalmak tisztázása után a szerzők a logisztikai információs rendszerek sajátosságaiból kiindulva vezetik le az ellátási láncban szereplő, ill. oda igyekvő vállalatokkal szemben megfogalmazható követelményeket. A cikk témájához kapcsolható, néhány fontosabb szabvány számbavétele segítséget nyújthat egy – nem feltétlenül drágán, harmadik tanácsadó fél által kidolgozott és auditált – információbiztonsági irányítási rendszer kialakításához és integrált logisztikai rendszerbe történő beilleszkedéshez.

1. Bevezetés

A vállalatok közötti beszállítói kapcsolatok sok esetben ellátási láncként jelennek meg. Ezek egyre több és bonyolultabb információs- és kommunikációs technológiát alkalmaznak.

A vállalatok közötti üzleti tranzakció-, ill. információkezelés létfontosságú a hosszú távú együttműködés, a stratégiai partnerkapcsolat szempontjából. A résztvevők kommunikációs viselkedésének meghatározó jellemzői a minőség, az információ-megosztás és a részvétel. Az ellátási láncban közreműködő, önállóan gazdálkodó szervezetek hálózatot alkotnak, amelynek jellemzői az együttélés, az együttműködés, a kooperáció, a hosszú távú elkötelezettség, a közös értékrend, a kölcsönös egymásra hatás és a közreműködő gazdálkodó szervezetek folyamatos interakciója [5]. A cégek információs rendszerei ezért átlépik a vállalati határokat, biztosítva az ellátási láncban stratégiai szövetséget kötő vállalatok együttműködését. A sajátos vállalati kultúrák, az ellátási láncban betöltött eltérő szerepek, a változó üzleti érdekek és a különböző információtechnológiák nehézzé tehetik a hatékony integrációt, ugyanakkor az információbiztonság alapvető

fontosságú az ellátási lánc elemei között létrejövő kapcsolat létrehozásában és működésében.

2. Információbiztonság

Az információ a gazdálkodó vállalat számára érték. Döntések, ill. az üzleti sikeresség alapja. Vonatkozhat többek között termékre, szolgáltatásra, technológiai ismeretekre és a rendelkezésre álló erőforrásokra, valamint az üzleti partnerekre, tehát az ellátási lánc működésének eredményességét befolyásoló minden elemre. Ha hiányoznak, pontatlanok, vagy nem időszerűek, esetleg illetéktelenek kezébe kerülnek, akkor ez a vállalat számára károkat okozhat. Az információt tehát védeni kell... Ez ma az információk [16];

- **bizalmasságát** (az információ csak az arra felhatalmazottak számára legyen elérhető),

- **sértetlenségét** (az információk teljességének és pontosságának megőrzése),

- és **rendelkezésre állását** jelenti (a felhatalmazott felhasználók akkor férjenek hozzá az információhoz, amikor az szükséges).

Az információbiztonság lényegesen összetettebb problémakör, mint az informatikai biztonság. John Ward 1995-ben még csak a bizalmasság mellett a helyreállíthatóságot és biztonsági mentést tekintette az információ biztonság alapjának [12]. Ma már nem elég vírusirtókban, tűzfalakban, megbízhatóan működő hardverben és egyértelmű azonosító rendszerekben gondolkodni. A technológiai háttér tudatos kialakítása nem elégséges. Egy információbiztonsági irányítási rendszer elsősorban az információhordozók kezelését szabályozza. Ez független attól, hogy milyen az információ megjelenési formája. A védelem akkor működik helyesen, ha meghatározzuk a védendő információkat, a külső és belső fenyegetéseket, ill. azok kockázatát valamint, a védelemhez szükséges szabályozást és eszközrendszert [17]. A vállalati „információ vagyont” fenyegető veszélyforrások a teljesség igénye nélkül is sokrétűek lehetnek:

- hibás szoftver alkalmazások,

- üzemzavar,

- szakszerűtlen információtechnológiai tervezés és üzemeltetés,

- illetéktelen használat, ill. hozzáférés,

- katasztrófa helyzet (tűzeset, árvíz, földrengés),

- vírusok, kémprogramok,

- hálózat szándékos túlterhelése (sniffing) és eltérítése (spoofing),

- meg nem engedett szoftverhasználat,

- szakképzetlen munkaerő,

- szándékos csalás, ill. visszaélés,

- rongálás.

Azoknál a vállalatoknál különösen fontos az információvédelem, amelyek [11];

- működésük alapjául információk szolgálnak, vagy azt alapvetően az adatok és információk határozzák meg,
- informatikai úton kapcsolódnak partnereikhez, az elektronikus kapcsolat meghatározó a külső kapcsolatokban (pl. logisztikai szervezetek),
- más (partner, ügyfél, stb.) szervezetek, személyek adatainak fogadásával, feldolgozásával, tárolásával, továbbításával foglalkoznak (pl. pénzintézetek, biztosítók, adatkezelő és feldolgozó szervezetek),
- informatikai rendszerek kidolgozását, fejlesztését, üzembe helyezését, telepítését végzik (pl. informatikai cégek),
- olyan kutatási-fejlesztési tevékenységet végeznek, ahol a keletkező eredmény és érték alapvetően információ formájában testesül meg (pl. kutatóintézetek),
- bizalmas, személyes információt birtokló, keletkeztető, ezekkel tevékenykedő szervezetek (pl. egészségügyi intézmények).

Az információvédelem célja tehát, hogy biztosítsuk az üzletmenet folytonosságát és szabályozott működéssel mérsékeljük a biztonsági eseményekből adódó károkat. Információbiztonságot a kockázatokat figyelembevevő óvintézkedésekkel lehet elérni. Ezek a vállalati folyamatokat leíró szabályzatokból, folyamatokat tükröző szervezeti felépítésből és az ezeknek megfelelő információtechnológiai eszközök (hardver, szoftver, telekommunikációs elemek) szabályozott működtetéséből állnak.

3. Az ellátási láncok menedzsmentje

Az ellátási lánc értékteremtő folyamatok és erőforrások összehangolt rendszerét jelenti, amely több vállalatot érintve az alapanyagok beszerzésével kezdődik és a végtermék fogyasztóhoz történő eljuttatásával fejeződik be. Részét képezik a beszállítók, a gyártók, logisztikai szolgáltatók, raktárak és a disztribúciós folyamatok egyéb szereplői is. Működését elsősorban a végső fogyasztók igényei határozzák meg, közös érdekeltséget teremtve a lánc résztvevői számára [2].

Az amerikai Supply Chain Council (**SCOR modell**) által megfogalmazott definíció alapján az ellátási lánc minden olyan tevékenységet magában foglal, amely a termék előállításával és kiszállításával kapcsolatos, a beszállító

beszállítójától kezdve a végső fogyasztóig bezárólag [24]. Az 5 fő folyamat, amely meghatározza az ellátási láncot;

1. tervezés (a kereslet-kínálat elemzése és a termékek, ill. szolgáltatások előállításának minőségi, mennyiségi és időrendi meghatározása),
2. beszerzés (alapanyag, alkatrész és kooperációs szolgáltatások),
3. gyártás (alkatrészgyártás és szerelés),
4. kiszállítás (készletezés, rendelés-feldolgozás, elosztás, valamint a végső fogyasztó kiszolgálása),
5. visszaszállítás (hibás, felesleges és karbantartandó termékek kezelése, ill. vevőszolgálati tevékenység).

A vevői igények kielégítésére hatással lehet, ha az ellátási láncot alkotók kellő hatékonyságú információkezelő rendszert alkalmaznak. Ennek eredményeként nem az egyedi szervezetek diszkrét eredményei összegződnek, hanem az erőforrás-allokációból adódóan a gazdálkodás különböző területein szinergikus hatások alakulnak ki. Az ellátási lánc menedzsmentje a vállalatok tudatos együttműködését jelenti. Elfogadják, hogy annak léte versenypozíciójuk javulását eredményezi. A lánc tagjai hajlandók lemondani saját, rövidtávú előnyeik érvényesítéséről a teljes lánc optimális működésének érdekében. A vállalatok belső logisztikai és információs rendszerei nélkülözhetetlenek a vállalatok közötti folyamatok koordinálásához [9].

A vevői igények- és azok kielégítésében játszott szerepek ismerete, valamint a nem teljesítésből az ellátási lánc működésére vonatkoztathatóan származó hátrányok tudatosítása ugyanakkor hozzájárul az ellátási láncot alkotó gazdálkodó szervezetek elkötelezettségének kialakulásához. A folyamatosan változó gazdasági környezetben ma a gazdálkodó szervezetek számára rendkívüli jelentőséggel bír az, hogy egy értékalkotó hálózat részeként lehetőségük nyílik környezetük irányítási struktúráinak befolyásolására.

Az ellátási láncok kialakítása és működtetése két lehetséges úton valósulhat meg [2]. Az első esetben egy domináns vállalat képes irányítani az egész lánc tevékenységét. Itt a beszállítók kénytelenek elfogadni az erő pozíciójából diktált feltételeket. Igaz ez az információs rendszerek esetében is. A beszállítók előzetes minősítéséhez hozzátartozik a megfelelő IT infrastruktúra meglétének és alkalmazhatóságának ellenőrzése. A másik esetben egy tényleges stratégiai szövetség jön létre az „egyenlő" partnerek között. A résztvevők viszonylag hosszabb távon kívánnak együttműködni a kölcsönös előnyök érvényesítése érdekében, de nehezebben tudják az ellátási lánc működését optimalizálni a mégis megjelenő egyéni érdekek alapján.

4. Az információ megosztása az ellátási láncokban

Az ellátási láncok minimális szinten történő működéséhez néhány alapvető vállalati adatot mindenképpen szükséges a többi résztvevő számára biztosítani (készletszintek, értékesítési adatok és előrejelzések, vevői rendelések állapota, termelési és szállítási ütemezések, kapacitásadatok). Itt a vállalat által előírt belső információbiztonsági követelményekről világos, dokumentált tájékoztatást kell adni az ellátási lánc többi tagjának.

Az integráció egy magasabb szintjén már közös, integrált információs rendszereket is használnak. Az ellátási lánc tagjai „szabadon" hozzáférhetnek a termékek, vevők, beszállítók és piaci helyzetre vonatkozó információkhoz is. Sok esetben megismerhetik a társak belső vállalati folyamatait és korábban titkosnak tartott adatait is [8]. Empirikus felmérések alapján megállapítható, hogy az ellátási láncban szereplő vállalatok számának növekedésével és információtechnológiai integráció fokozódásával, valamint az információ megosztásával emelkedik az informatikai incidensek száma [10]. Ilyenkor közös információbiztonság irányítási rendszerek kialakítása sem elképzelhetetlen.

Az ellátási láncok ma már nem működnek információtechnológia nélkül. A résztvevő vállalatok számára fontos, hogy a bemenő erőforrások milyen csatornákon (beszállítókon) keresztül milyen feltételekkel és költségekkel érkeznek, ill. mi történik a kimenő „termékekkel", milyen közvetítőkön keresztül jut el a végső fogyasztóig. Az az ellátási lánc lesz sikeres, amely gyorsabb, megbízhatóbb, karcsúbb és kisebb költségű, mint a versenytársai.

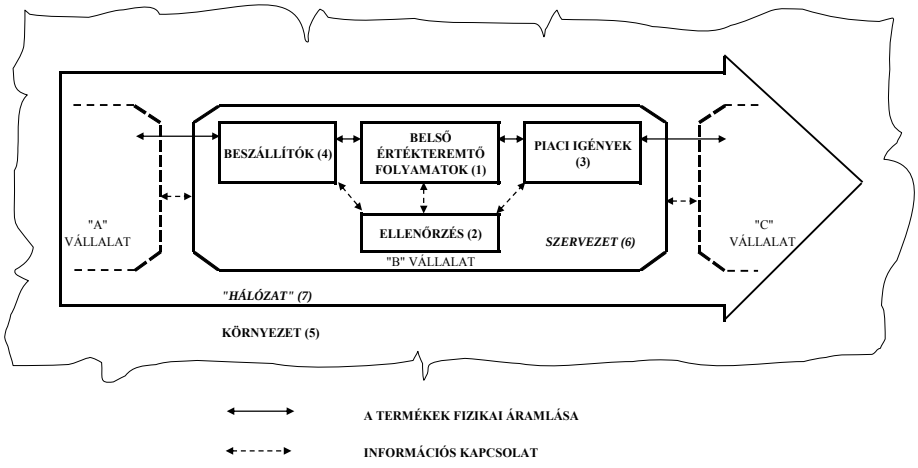
5. Az ellátási láncok kockázata

Az ellátási láncok kockázatát tekintve a szakirodalom egységes álláspontot képvisel. Az ellátási lánc kockázata olyan potenciális események, zavarok bekövetkezése az ellátási láncon belül és annak környezetében (akár piacán is…), amelynél veszélybe kerül a vevői igény kielégítése, vagy a vevő biztonsága is. A hagyományos kockázati megfontolás (a bekövetkező kockázati tényezőből származó kár nagysága és a kockázati esemény valószínűsége) helyett, ill. mellett bevezették a „sebezhetőség" fogalmát. A kockázatokat, ill. az ellátási láncok sebezhetőségét eredetük alapján 5 csoportba lehet sorolni [3]:

1. értékteremtő folyamatok zavarai (gyártás, beszerzés, raktározás, szállítás, ütemezés),
2. ellenőrzés (annak hiánya, ill. hibája),
3. piaci igények (információhiány, kiszámíthatatlanság, váratlan események),

4. beszállítók (megbízhatatlanság, kapacitáshiány, vis maior),
5. környezet (gazdasági-, politikai események, balesetek, természeti katasztrófák).

Ezt további két kockázat „forrás" egészíti ki [10]. A belső vállalati szervezet **(6)** szintén sebezhető, ha az nem felel meg a kialakított értékteremtő folyamatoknak és nem jól használja az információs rendszereket. Az ellátási lánc tagjai között is előfordulhatnak együttműködési zavarok mind az információ-, mind az anyagáramlásban. A több önálló vállalatból álló hálózat **(7)** is kockázati tényezőt jelent (1. ábra).



1. ábra
Az ellátási láncok kockázat-forrásai [10]

Az ellátási láncok integrált információs rendszereinek kockázatkezelését információtechnológiai oldalról is megközelíthetjük. A fizikai védelem a megfelelő környezet és információtechnológiai infrastruktúra kialakítását jelenti a környezeti ártalmak és a szándékos, vagy véletlen károkozás ellen.

A logikai vagy „üzemeltetési" védelem kiterjed az összekötött hálózatokra, az alkalmazott alapszoftverekre (operációs rendszerek és adatbázis-kezelők), az alkalmazásokra (pl. ERP és EAM rendszerek) valamint a tárolt adatokra. Meghatározzák a munkavégzés módját (pl. naplózási szabályok, vírusfertőzés elleni tevékenység), megadják a felhasználók jogosultságát és illetékességét.

A szabályozási munka eredménye általában Üzletmenet Folytonossági Terv (Business Continuity Plan) és Katasztrófa-elhárítási Terv (Disaster Recovery Plan) lesz. Az előbbi az üzleti folyamatokat támogató informatikai erőforrások meghatározott időben és funkcionális szinten történő rendelkezésre állásának biztosítása, valamint váratlan esemény által okozott károk minimalizálásáról szól.

Az utóbbi helyettesítő megoldásokat ad meg súlyos károkat és az informatikai szolgáltatás meghiúsulását okozó események bekövetkezésére. A cél, hogy a negatív hatások minimalizálhatók legyenek és az eredeti állapot visszaállítása elfogadható költségek mellett, gyorsan megtörténhessen.

6. Logisztikai információs rendszerek

Az üzleti életben használt vállalati információs rendszerek csoportosítása a szakirodalomban már kikristályosodott [7]. Ez a csoportosítás kisebb kiegészítéssel az ellátási láncok területén is alkalmazható [4].

A tranzakció kezelő rendszerek a vállalati és vállalat-közötti értékteremtő folyamatok során keletkező adatok rögzítésére, feldolgozására és tárolására szolgálnak (rendelés felvétel, raktárgazdálkodás, külső és belső szállítás, készletkövetés, termelésirányítás, beszerzés). A vezetői munkát a döntéstámogató és vezetői információs rendszerek támogatják, amelyek többek között a tranzakció kezelő rendszerekben tárolt adatokból nyújtanak operatív döntésekhez összesített információkat. Az anyagszükséglet- és gyártási erőforrás-tervező rendszereken túl megjelennek a különböző szállítási útvonal és rakomány optimalizációval foglalkozó alkalmazások és a strukturális döntésekhez segítséget nyújtó szimulációs megoldások is. Az ellátási láncokban fontosabb a teljes hálózat hatékony működése, mint a tagvállalatok egyéni erőforrás felhasználási optimuma. Ez esetenként közös információs rendszerek üzemeltetését is jelentheti… Erre készteti a vállalatokat a Voluntary Interindustry Commerce Standards Association által kifejlesztett ellátási láncok tagjai közötti együttműködést támogató „Collaborative Planning, Forecasting and Replenishment" (CPFR) folyamatmodell is [23]. A szükséglettervezés alapja a végső fogyasztói igény. A modellt alkalmazása egy konszenzuson alapuló előrejelzést eredményez, amely azután meghatározza a disztribúció, a termelés és a beszerzés tagokra is lebontott terveit. Az ellátási lánc tagjai törekednek arra, hogy az előrejelzés alapját szolgáló adatok minél pontosabbak legyenek.

A taktikai és stratégiai döntésekhez szükséges múltbéli adatok sokszor olyan adatpiacokból vagy adattárházakból származnak, amelyek tisztított és redundancia-mentes adatbázisok. Ezek alapjai lehetnek a különböző üzleti intelligencia alkalmazások felhasználásának is.

Az ellátási láncok szempontjából kiemelt fontosságú a kommunikáció kérdésköre. A kommunikációs rendszer alapját az automatikus azonosító rendszerek képezik (vonalkód, szabványos áruazonosítás, rádiófrekvenciás azonosítás), de ide tartozik a tagok közötti kapcsolattartást megvalósító kommunikációs technikák is (elektronikus adatcsere, értéknövelő hálózatok, Internet, globális helymeghatározó rendszerek) Ezek többnyire szabványokhoz és ajánlásokhoz kötött megoldások.

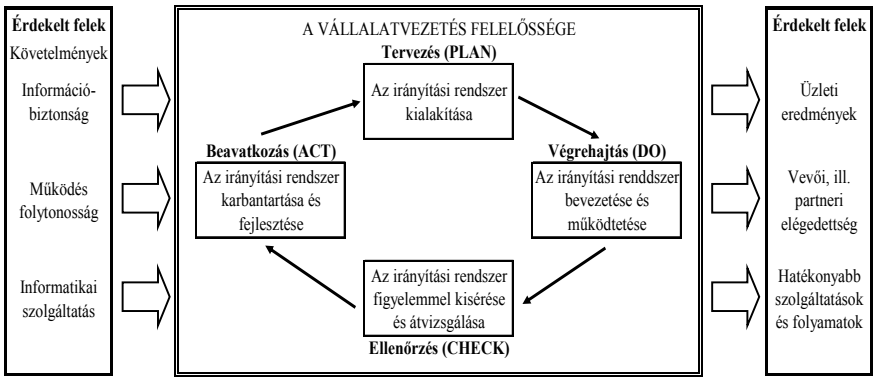
Részletes ismertetésükre terjedelmi okokból nincs lehetőség. Egyedül az értéknövelő hálózatokról osztunk meg néhány gondolatot. A különböző kommunikációs szabványok közös alkalmazása teljesítményjavulást hozhat az ellátási láncban. A tagok eltérő szerepe, funkciója miatt sokszor a szabványosítás indokolatlan kötöttségeket is okozhat. Az értéknövelő hálózatok különböző szabványú, egymással nem kompatibilis tranzakciós üzeneteket „fordítanak le, ill. át" és továbbítják azokat az ellátási lánc többi tagja felé. (Gyakorlatilag értéknövelő hálózatnak tekinthető a külső, harmadik fél által üzemeltetett EDI rendszer is…)

Az ellátási lánc tagjai számára fejlesztett „egyéni" vállalati információs rendszerekben, ill. a teljes hálózat számára készülő integrált alkalmazásokban ilyen éles határt húzni a részrendszerek között nem lehet. A tranzakció kezelés, a döntéstámogatás és a kommunikáció egymástól elválaszthatatlan.

7. A javasolt szabványok

Az itt röviden bemutatott dokumentumok mellett számos más, hasznos, nemzetközileg elfogadott szabvány, ill. ajánlás létezik még, amelyet érdemes lehet ellátási láncok információbiztonságával kapcsolatban megemlíteni (pl. MSZ ISO/IEC 9126 – Szoftvertermékek értékelése; MSZ ISO/IEC 15408 – Szabványcsomag az informatikai biztonságértékelés közös szempontjairól…, más néven „Common Criteria"; ISO/IEC 24762 – Útmutató az információs és kommunikációs technológiák katasztrófa elhárítási szolgáltatásairól; ISO 28000-es széria – ellátási láncok biztonság irányítási rendszerére vonatkozó követelmények [13, 14, 15]; vagy a Control Objectives for Information and related Technology – CobIT).

A szerzők itt megpróbálták azt a dokumentumkört összeállítani, amely elégséges egy ellátási láncba törekvő vállalat információbiztonsági irányítási rendszerének kialakításához. Mindegyik szabványcsomag folyamatszemléletű és alkalmazza a PDCA (plan-do-check-act) modellt (2. ábra).



2. ábra
PDCA modell információbiztonsági folyamatokra

7.1. ISO/IEC 2700x

Brit eredetű információbiztonsági irányítási rendszer, ill. szabványcsomag, amely az információvédelmi tevékenységhez ad útmutatót [25]. A vállalatok a biztonsági követelményeket és az ezzel kapcsolatos intézkedéseket az üzleti célok és a szervezeti stratégia alapján határozzák meg. Kiemelt szerepet kap az információbiztonság (sértetlenség, bizalmasság és rendelkezésre állás). Nem kötődik egyetlen információtechnológiához sem. A szabvány [16] a vállalati működését és az ezzel kapcsolatos követelményeket 11 védelmi területre és ezen belül 39 célkitűzésre [6] és 133 óvintézkedésre osztja. A kialakított és dokumentált információbiztonsági irányítási rendszer tanúsítása független tanúsító szervezet által elvégezhető [17]. A szabványcsomagban található még néhány – önálló szabványként megjelenő – kiegészítő rész is (pl. információbiztonsági kockázat kezeléssel kapcsolatos előírások – ISO/IEC 27005 [18]). A fejlesztés nem áll meg. Tervezik további szabványok megjelentetését is (pl. bevezetési útmutató – ISO/IEC 27003; szektorok közötti kommunikáció szabályozása információbiztonsági szempontból – ISO/IEC 27010; a telekommunikáció információbiztonsága – ISO/IEC 27011).

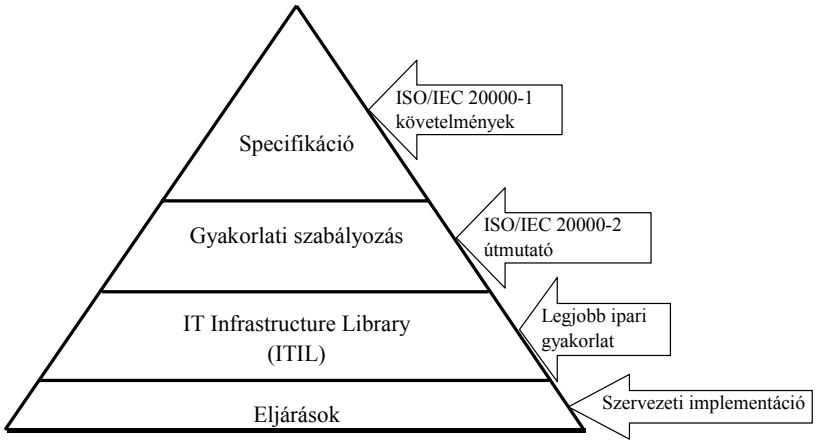
7.2. ISO/IEC 20000-1, -2

A szabvány az információs rendszerek üzemeltetési kérdéseivel foglalkozó, brit eredetű ITIL (Information Technology Infrastructure Library) ajánlás alapján, ill. azzal összhangban készült [26] (3. ábra). A dokumentum első része egy formális követelményrendszer az elfogadható informatikai szolgáltatásokkal kapcsolatban [19], míg a második rész [20] útmutató a szolgáltatásirányításhoz és az első rész

szerinti audithoz. A szolgáltatás menedzsment tevékenységek a ma népszerű, a többi szabványban is alkalmazott PDCA modellhez kapcsolódnak.

A menedzsment rendszer, az informatikai szolgáltatások tervezésének és megvalósításának kérdésköre, valamint az új szolgáltatások tervezése mellett öt alapvető területe van a teljes szolgáltatás menedzsmentnek;

- Szolgáltatásbiztosítás (szolgáltatási szint, szolgáltatási jelentések, kapacitás, szolgáltatás folytonosság és rendelkezésre állás, információ biztonság, informatikai szolgáltatás költségtervezése és pénzügyi kezelése)
- Szabályozási folyamatok (konfiguráció- és változás menedzsment)
- Kiadási folyamatok (dokumentumok, működési leírások kiadás kezelése, a jóváhagyott változások dokumentálása)
- Megoldási folyamatok (incidens- és problémakezelés)
- Kapcsolattartás (ügyfélszolgálat, üzleti- és szállítói kapcsolatok kezelése)



3. ábra
Kapcsolat az ISO/IEC 20000-es szabványcsomag és az ITIL között [1]

7.3. BS 25999-1, -2

A brit üzletmenet folytonossággal foglalkozó szabványcsomag [21, 22] szintén egy vállalati működést szabályozó irányítási rendszer kialakítását teszi lehetővé. Minden szervezetre alkalmazható. A potenciális veszélyek és kockázati tényezők feltárása egy összetett hatáselemző munka eredménye (Business Impact Analysis, BIA). Megvizsgálják a vállalat kulcstermékeit, ill. annak előállítási lépéseit, a szolgáltatásokat támogató folyamatokat, az üzleti tevékenység megszakadásának

maximálisan elfogadható időtartamát és a külső üzleti partnerektől való függőséget.

Az üzleti hatáselemzés alapján a vállalat olyan üzletmenet folytonossági tervet alakít ki (Business Continuity Plan), amely segítségével a váratlan események sem okozhatnak gondot (katasztrófa helyzet, alapanyaghiány, közműzavarok, munkaerőhiány, technológiai berendezések meghibásodása, informatikai problémák, vevői reklamációk stb.). Megmarad a cég jó híre és képes folytatni az értékteremtő tevékenységeket, kiszolgálni az üzleti partnereket.

A vállalat minden kritikus anyagi és információs folyamata rendelkezik olyan helyettesítő megoldással, amely lehetővé teszi a rendkívüli helyzetben történő működést és az eredeti állapotba történő visszatérést. A PDCA ciklus alapján fontos az irányítási rendszer dokumentálása és rendszeres vezetői átvizsgálása, valamint tesztelése és folyamatos fejlesztése is.

8. Az információbiztonság irányítása az ellátási lánc szereplőinél

A stratégiai üzleti partnerek kiválasztásánál ma legalább olyan fontos a stabil, megbízható IT alapokon nyugvó kapcsolattartási lehetőség, mint a megvásárolt termék v. szolgáltatás ára és minősége, valamint a leellenőrizhető referenciák megléte. Az ISO/IEC 27001-es szabvány célkitűzéseit, valamint az auditáláshoz szükséges gyakorlati útmutatót végig elemezve számos területen kell a kockázatokat kezelni.

Egy információs rendszerek kölcsönös, de természetesen korlátozott használatát is megengedő üzleti kapcsolatban alapvető, a partnerekkel egyetértésben megfogalmazott elvárások lehetnek a következők:

- a titoktartási nyilatkozat elkészítése és mindkét fél által történő elfogadása,

- a fizikai beléptetés szabályozása (egyszeri vagy rendszeres lehetőség…, engedélyezés és visszavonás rendje),

- a megfelelő jogosultsági rendszer kialakítása (jelszavak kiadása és érvénytelenítése, a hozzáférés körének tisztázása),

- az információ továbbítás és hordozás szabályainak megállapítása (pl. másolatok készítése, a megsemmisítés kérdése…),

- az alárendelt szerződő partner felelősségvállalása a saját alkalmazottaiért (pl. hozzáférésre feljogosított személyek névsorának átadása…),

- csak a szükséges és elégséges adatok/információk biztosítása a partnerek számára,

- informatikai outsourcing szabályozása (a szervezet egyes információfeldolgozási feladatait egy másik szervezet látja el, és emiatt hozzáfér hálózati elemekhez, adatbázisokhoz és szoftver-alkalmazásokhoz…),

- az együttműködés során bekövetkezett káros események (incidensek) tapasztalatainak leszűrése, a hibaelhárítás ráfordításainak számszerűsítése és a felelősség egyértelmű megállapítása,

- formális eljárások lefolytatása, ha valamelyik fél alkalmazottai megsértik a megállapodásokat,

- információs rendszer közös kialakítása esetén a fejlesztés során és a napi működésben használt IT eszközök egyértelmű elkülönítése,

- az üzleti kapcsolat fenntartásában nélkülözhetetlen szoftverek szabályozott, írott megállapodások alapján történő átadása (pl. banki rendszerekkel történő kapcsolattartás),

- az elektronikus kereskedelem (EDI is…) és levelezés biztonságának szabályozása különös tekintettel az üzleti tranzakciós adatok, ill. az üzenetek hitelességére, titkosságára és sértetlenségére,

- az elfogadott feltételek és követelmények írásba foglalása a későbbi jogviták elkerülése miatt…

Az információbiztonsági irányítási rendszer kiépítésének célja a partnerek elvárásainak, a vonatkozó hazai és nemzetközi előírásoknak megfelelő működés és az információbiztonság megteremtése, az adatok és információk sértetlenségének, bizalmasságának megőrzése, ezek rendelkezésre állásának biztosítása. Minimalizálható legyen az esetlegesen bekövetkező üzleti kár és biztosítani tudjuk az üzletmenet-folytonosságot.

8.1. Információvédelmi átvilágítás

A rendszer kiépítésének első lépése a vezetői döntés és a munkát elvégző ideiglenes szervezet kialakítása után az információvédelmi átvilágítás és helyzetfelmérés.

Általánosságban elmondható, hogy az irányítási rendszerek kiépítésének előkészítő fázisában alapvetően a védelmi igény feltárása, a fenyegetettség-elemzése, a kockázatelemzés és a kockázat kezelés témakörei kerülnek terítékre különböző formában, melynek során a következő alapvető kérdésekre keresünk választ:

- Milyen jellegzetességekkel bír az alkalmazott információ-, ill. adatkezelési gyakorlat?
- Képes-e a szervezet információtechnológia rendszere zavartalanul, megfelelő szinten ellátni az összes külső és belső információszolgáltatási

igényt, amely a szervezet működésével kapcsolatban felmerül, vagy megfogalmazható?

- Adatbiztonsági szempontból megfelelő színvonalú-e a rendszer?
- Megfelelően szabályozott-e az adatokhoz való hozzáférés joga és annak módja?

Az információvédelmi átvilágítás „információtechnológiai csoportosításban" érinti a környezeti infrastruktúra, az adathordozók, a hardver, a szoftver, a dokumentumok, az adatok, a kommunikáció, és az emberi tényezők területét is.

Az átvilágítás információvédelmi fejezetének fontos része a részletes és minden egyes informatikai elemre és kapcsolatra kiterjedő hardver-, szoftver-, és kapcsolatrendszer „leltár" felvétele, amely alapján érdemben lehet a „fenyegetettség-veszély" meghatározást és elemzést elvégezni, valamint a szükséges szabályozó rendszert kialakítani.

8.2. Kockázatértékelés és elemzés

A feltárás során elemzésre kerülnek a vizsgálati területeken értelmezhető gyenge pontok és fenyegető tényezők, megtörténik ezek értékelése, elemezése, rangsorolása. Csoportosítják az egyes fenyegetettségekhez kapcsolódó esetleges károkat és kockázatokat. Hozzárendelik a kivédésükhöz, elfogadható mértékre történő csökkentésükhöz és kezelésükhöz szükséges és/vagy lehetséges intézkedéseket.

Ennek megfelelően a kockázatértékelés és elemzés lépései az alábbiak:

- a védelmi igény feltárása, az információvagyon meghatározása, a szervezet számára kiemelten fontos adatok feltárása és ütemezése,
- fenyegetettség elemzés; a fenyegető tényezők összegyűjtése,
- kockázatelemzés; a fenyegetettség hatásainak vizsgálata,
- kockázatok kezelése és a védelmi intézkedések meghatározása; a kockázatok kivédése, ill. minimalizálása a kockázatelemzés alapján a lehetséges módozatok meghatározásával.

8.3. A dokumentálás

Az információvédelmi irányítási rendszer kiépítésének következő lépése a dokumentáció elkészítése. Ennek során szükséges figyelembe venni a szervezet nagyságát és struktúráját, a folyamatok összetettségét és azok kölcsönhatásait, a szervezet működésére vonatkozó külső- és belső előírásokat, a szakmai sajátosságokat és hagyományokat.

Dokumentációs és szabályozórendszer kialakítása az általános célok elérése mellet a szervezet működésének és védelmi céljainak függvényében konkrét feladatok megvalósítását igényli, melybe bele tartozik:

- a védelmi igények és követelmények, valamint a védendő értékek (pl. alkalmazás, adatok hardver, szoftver, adathordozó, dokumentumok, személyi és szervezeti környezet, építészeti környezet, kommunikációs rendszerek, eszközök, szervezeten belüli személyi kockázatok) felmérése alapján történő kockázatelemzés,
- az információvédelemi célok és politika meghatározása,
- a rendszer érvényességi területének, valamint egységes vezetői elvek és szabályok rögzítése egy vezetői kézikönyvben, amely összefoglalja az irányítási rendszer folyamatait és rögzíti a rendszer elemeinek kapcsolatát, meghatározva a kapcsolódó feladatokat és azok felelőseit,
- kockázati- és védelmi területek és szintek meghatározása,
- a célok és a működés ismeretében a kapcsolódó folyamatok, módszerek és szabályozások (pl. géptermi belépés rendje, archiválási utasítás, jelszókezelés rendje, informatikai szabályzat) kidolgozása,
- az információvédelemhez rendelt feladatok és a kapcsolódó felelősségek meghatározása,
- a rendszer tervezett és automatikus felügyeletének, valamint eseti ellenőrzésének kialakítása, az elfogadási kritériumok rögzítése,
- a hibák felismerése és a szükséges válasz-intézkedésekhez kapcsolódó prioritások meghatározása,
- a feljegyzések kezelési rendjének kialakítása, mellyel a szervezet biztosítja a kívánt információvédelmi célok elérésének megfelelő dokumentálását, igazolja az előírt követelményeknek való megfelelést és bizonyítja az információvédelmi rendszer hatásos működését,
- alkalmazhatósági nyilatkozat kidolgozása, melyben kifejtésre kerül, hogy a rendszer hogyan tesz eleget a funkcionális követelményeknek, ill. a megvalósítás és az üzemeltetés hogyan felel meg a kitűzött biztonsági céloknak.

8.4. Bevezetés

A szabályozások elkészítésével együtt és azt követően számos gyakorlati feladatot szükséges elvégezni, többek között:

- a szabályozás hatályba léptetése, az alkalmazásukkal és a menedzsment rendszer működésével kapcsolatos ismeretek oktatása és az elsajátítás mértékének meghatározása,

- a kialakított szabályozási rendben rögzítettek rutinszerű alkalmazásának bevezetése, és felügyelete,
- fizikai védelem rendszerének kialakítása, üzletmenet folytonosság biztosítása háttérszerződésekkel, fejlesztések-, eszközcserék-, eszköz elidegenítés és megsemmisítés-, külső terminálok-, mobil eszközhasználat- stb. biztonsági követelményeinek biztosítása, alkalmazottakkal kapcsolatos védelmi módozatok kimunkálása és bevezetése,
- a belső auditok lebonyolításához szükséges team és ellenőrzési rend kialakítása, az ehhez szükséges jogosultságok és erőforrások biztosítása a vezetés részéről, a kapcsolódó oktatások megtartása,
- vezetői átvizsgálás lebonyolítása, majd a vizsgálat eredményei alapján a következő periódus fejlesztési céljainak meghatározása.

Az általános szempontok alapján az alábbi területek szabályozása indokolt az irányítási rendszer kialakítása során:

- dokumentumkezelés,
- humánpolitikai tevékenység,
- az információ kezelő eszközök védelmi osztályozása, fizikai és környezeti védelem,
- a tevékenységek tervezése, fejlesztése, az információkezelés rendszerének fejlesztése,
- beszállítói szerződéskötések rendje és a beszállítók minősítése,
- a „szabványos” munkafolyamatok,
- az integrált irányítási rendszer felülvizsgálata,
- a munkafolyamatok ellenőrzése és vizsgálata,
- biztonsági zavarok, működési hibák kezelése,
- a helyesbítő és a megelőző tevékenység.

8.5. Auditálás mint lehetőség

Az információvédelmi irányítási rendszer független szervezet által történő auditálása lehetséges. Ez nagyobb mértékű garanciát képes nyújtani a kialakított rendszer megfelelőségére és kedvezően befolyásolhatja a vállalatról kialakult képet. Az irányítási rendszer auditálása is kiterjed az ügyfelek szempontjainak, követelményeinek teljesíthetőségére, a rendszer által nyújtott garanciák vizsgálatára. A most felsorolt területek átfogják az irányítási rendszer kiépítésekor

figyelembe vett követelményrendszer előírásait, ill. ezek megfelelő szabályozását és dokumentálását;

- a biztonságpolitika,
- kockázat elemzés és kezelés,
- üzletmenet folytonossági terv,
- katasztrófa elhárítási terv,
- alkalmazhatósági nyilatkozat,
- adatvédelem, vírusvédelem,
- incidensek, események rögzítése, kivizsgálása,
- munkakörökhöz, személyekhez kötődő biztonsági előírások, vonatkozó jogszabályok, egyéb (külső) előírások, szakmai ajánlások megléte, ismerete és ezeknek való megfelelés,
- adminisztratív (ügyviteli) – környezeti (őrzés-védés) – információs technológiai szabályozások, ismeretek és gyakorlat megléte, ezek egyidejű működése.

Következtetések

A tárgyalt nemzetközi szabványok és szakmai ajánlások alapján kidolgozott információbiztonsági irányítási rendszer segítheti a vállalatok beilleszkedését az ellátási láncokba. A belépéshez és pozíció megtartásához szükséges információtechnológiai- és folyamatfejlesztések könnyebben elvégezhetők, hiszen van egy követelményrendszert kiegészítő, ill. teljesítő szabályozás.

Az egymáshoz látszólag alig kapcsolódó szabványok és ajánlások közös alkalmazása azért is indokolt, mert az ellátási láncok integrált információs rendszereinek optimális működése nemcsak információtechnológiai kérdés. A hálózatba szervezett vállalatok számára létfontosságú, hogy ki, mikor és hogyan férhet hozzá a számára szükséges információkhoz, ill. mikor indíthat el vagy nyúlhat bele egy vállalaton belüli vagy vállalatok közötti üzleti tranzakcióba. A kockázatok kezelése nem szétválasztható az anyagi- és információs folyamatokban valamint az információtechnológiában.

Irodalom

[1] Bon, J. V., Verheijen, T.: IT Service Management Forum: Frameworks for IT Management. Van Haren Publishing, 2006

[2] Chikán, A., Gelei A.: Az ellátási láncok és menedzsmentjük. Harvard Business Manager (magyar kiadás), 2005. január, pp. 35-44

[3] Christoper, M., Peck, H.: Building the Resilient Supply Chain. International Journal of Logistics Management, Vol. 15, No. 2, 2004, pp. 1-13

[4] Gelei, A., Kétszeri, D.: Logisztikai információs rendszerek felépítése és fejlődési tendenciái. Műhelytanulmány, Corvinus Egyetem, Budapest, Vállalatgazdaságtan Intézet, 2007. június

[5] Gerlach, M. L.: Alliance Capitalism. Berkeley University of California Press, 1992

[6] Ködmön, I. (szerk.): Hétpecsétes történetek (Információbiztonság az ISO 27001 tükrében). Hétpecsét Információbiztonsági Egyesület, Budapest, 2008

[7] Laudon, K. C., Laudon, J. P.: Management Information Systems: Managing the Digital Firm. Prentice Hall, 9th edition, 2006

[8] Lőrincz, P.: Az ellátási láncok sajátosságai menedzsment és informatikai szempontból. MEB 2008, 6th International Conference on Management Enterprise and Benchmarking. May 30-31, 2008, Budapest, pp. 239-249

[9] Mentzer, J. T., DeWitt, W., Keebler, J. S., Min, S., Nix, N. W., Smith, C. D., Zacharia, Z. G.: Defining Supply Chain Management. Journal of Business Logistics. Vol. 22, No. 2, January 2001, pp. 1-25

[10] Smith G. E., Watson K. J., Baker W. H., Pokorski J. A.: A Critical Balance: Collaboration and Security in the IT-enabled Supply Chain. International Journal of Production Research. Vol. 45, No. 11, June 2007, pp. 2595-2613

[11] Vadász, I., Lábodi, Cs., Ulrich, A.: Az első magyarországi integrált minőség- és információvédelmi irányítási rendszer kiépítése és tanúsíttatása. ISO 9000 Fórum, Dunaújváros, 2003, konferenciakiadvány

[12] Ward J.: Principles of Information Systems Management. Routledge, London, 1995

[13] ISO 28000:2007, Specification for Security Management Systems for the Supply Chain

[14] ISO 28001:2007, Security Management Systems for the Supply Chain – Best Practices for Implementing Supply Chain Security, Assesment and Plans – Requirements and Guidance

[15] ISO 28003:2007, Security Management Systems for the Supply Chain – Requirements for Bodies Providing Audit and Certification of Supply Chain Security Management Systems

[16] MSZ ISO/IEC 27001:2006, Informatika, Biztonságtechnika. Az információbiztonság irányítási rendszerei. Követelmény

[17] ISO/IEC 27002:2005, Information Technology – Security Tehniques – Code of Practice for Information Security Management

[18] ISO/IEC 27005:2008, Information Technology - Security Techniques - Information Security Risk Management

[19] MSZ ISO/IEC 20000-1:2007, Informatika. Szolgáltatásirányítás. 1. rész: Előírás

[20] MSZ ISO/IEC 20000-2:2007, Informatika. Szolgáltatásirányítás. 2. rész: Alkalmazási útmutató

[21] BS 25999-1:2006, Business Continuity Management – Code of Practice. (www.bs25999.com)

[22] BS 25999-2:2006, Business Continuity Management – Specification. (www.bs25999.com)

[23] Collaborative Planning, Forecasting and Replenishment (CPFR). Overview, 2004, Voluntary Interindustry Commerce Standards (VICS). (www.vics.org)

[24] Supply Chain Council: Supply-Chain Operations Reference-Model (SCOR). Overview. Version 9.0, 2008 (www.supply-chain.org)

[25] ISO27k Toolkit. Version 3.2, 2008 (Prepared by the international community of ISO27k implementers at www.ISO27001security.com)

[26] An Introductory Overview of ITIL V3. IT Service Management Forum, 2007 (www.itsmfi.org)