



M Ű E G Y E T E M 1 7 8 2

**Budapesti Műszaki és Gazdaságtudományi Egyetem
Gazdaság- és Társadalomtudományi Kar
Információ- és Tudásmenedzsment Tanszék**

BIZTONSÁG MENEDZSMENT KUTATÓ CSOPORT

VASVÁRI GYÖRGY CISM

Tiszteleti egyetemi docens

A kutató munkában részt vett még:

LENGYEL CSABA

Biztonsági menedzser, KELER Rt

VALÁDI ZOLTÁN

Biztonsági menedzser, GIRO Bankkártya Rt

VÁLLALATI BIZTONSÁG KERETRENDSZERE

Vagyonbiztonság, Üzembiztonság, Informatikai
Biztonság

AJÁNLÁS

6.0 változat

2006

A KUTATÓ CSOPORT tagjai, akik véleményükkel támogatták az ajánlás elkészítését.

Az ajánlás szabadon felhasználható a forrás megjelölése mellett.

Tartalomjegyzék

1. Bevezetés	4
1.1. A KUTATÁS CÉLJA	4
2. A kiindulás	5
2.1. Üzleti cél, üzleti követelmény	5
3. A vállalat rendszer	8
3.1. Makrogazdasági rendszer	8
3.2. Mikrogazdasági rendszer	8
4. A vállalatirányítás	10
4.1. Vállalatirányítás struktúrája	10
4.2. Vállalatirányítás (Enterprise Governance) funkcionális modellje (COBIT3 alapján)	12
4.3. Felelősségek elosztása	14
4.4. Üzleti, termelési, informatikai és biztonsági stratégia összefüggései	15
4.5. A menedzsment értelmezése	16
4.6. A vállalat irányítás szintjei	17
4.7. A vállalatirányítás ellenőrzésének céljai	18
5. A biztonság	21
5.1. A vállalati biztonság	21
5.2. A vállalati szintű biztonság mgm	22
5.3. A biztonság elemei a biztonsági alrendszerekben	24
5.3.1. A biztonsági rendszer alrendszerei	24
5.3.2. A biztonsági alrendszerek közötti összefüggések	26
5.4. Egyenszilárdság	29
5.4.1. Rendszer szemlélet	29
5.4.2. Egyenszilárdság elve	29
5.5. Biztonságirányítás	32
5.5.1. A biztonságirányítás fogalma	32
5.5.2. A biztonságirányítás módszerei	33
5.6. A vállalati biztonság megvalósítása	33
5.6.1. A vállalati biztonság szervezése	33
5.6.2. Néhány biztonságsszervezési feladatról	36
5.6.2.1. Adatok és titkok osztályozása	36
5.6.2.2. A kockázat menedzsment	37
5.6.2.3. A kockázatok csökkentése	40
5.6.2.4. Védelmi intézkedések köre I (a biztonsági alrendszerekben)	40
5.6.2.5. Védelmi intézkedések köre II (a biztonsági alrendszerekben)	41
5.6.2.6. Védelmi intézkedések köre III (a biztonsági alrendszerekben)	42
5.6.2.7. A védelmi intézkedések üzemeltetése	43
5.6.2.8. A biztonsági szervezet és működés	44
5.6.2.9. ÜFT, és a hátterek megválasztása	46
5.6.2.10. Outsourcing	48
6. Kis vállalatok biztonsága	51
7. A KUTATÓ MUNKA EREDMÉNYEI	53
7.1. A vállalatbiztonsági követelmények	53
7.2. Tipikus hibák a tapasztalatok szerint	53
7.3. További teendők	54
8. Felhasznált irodalom	55

1. BEVEZETÉS

1.1. A KUTATÁS CÉLJA

Az elmúlt évtizedben alapvető változásokon mentek keresztül a hazai vállalatok, követve a világ igen gyors változásait (pl. globalizáció). Ezek a változások a vállalatok számára kihívásokat hoztak létre. A vállalati menedzsmentnek meg kell értenie, illetve az a kérdés, hogy mennyire érti meg, hogy ezek a változások hogyan jelennek meg az egyes országok szabály rendszerében, vagy milyen változtatásokat igényelnek a ma vállalatának belső szabályozásával szemben.

Néhány jellegzetes kihívás:

- annak a felismerése, hogy a határokon átnyúló globalizáció új üzleti felfogást követel meg,
- annak a megértése, hogy egy tudásbázisú társadalomban a szellemi tőkének mi és mekkora a szerepe,
- annak a felismerése, hogy a vállalati informatikát és a nemzetközi hálózatokat is felhasználva, a vállalat papíralapú irodája átmegy az elektronikus irodába.

Természetesen a pozitív válaszok nemcsak a hatékonyság és az eredményesség növekedését hozzák magukkal, hanem új fenyegetések lépnek fel a vállalatok biztonságára nézve. A vállalatirányításnak tehát nemcsak a kihívásokra kell pozitív választ találnia, hanem az ezekkel járó új fenyegetések, képezte kockázatok csökkentésére is. A rohanó világ azonban az új válaszok keresését sohasem engedi lezárni, ez a folyamat állandóan újraindul (veszélyforrások feltárása, fenyegetések és kockázatok elemzése, védelmi intézkedések a kockázatok csökkentésére, azaz kockázatmenedzsment). A munka alapvetően támaszkodik a szerző 12 év alatt végzett biztonsági auditálási tapasztalataira, valamint a veszélyérzet hiányára visszavezethető problémákra a biztonság menedzsment területén.

A kutatáscélja, hogy

- tisztázza a vállalatirányítás (Enterprise Governance) és azon belül a vállalati biztonságirányítás (Enterprise Security Governance) egyaránt kiterjed-e a vállalat teljes tevékenységi körére, és
- a biztonság szervezése egy vállalatnál milyen megközelítést kíván.

2. A KIINDULÁS

2.1. ÜZLETI CÉL, ÜZLETI KÖVETELMÉNY

A vállalatokat, akár kereskedelmi, akár nem kereskedelmi vállalatok, valamilyen feladatra hozzák létre. Ez a feladat képezi a vállalat tevékenységének az alapját, célját, a vállalat létrehozásának értelmét.

- **Az üzleti cél** tehát a vállalat létrehozásának indokát képező feladat hatékony és eredményes megvalósítása.

Az *eredményesség* alatt (COBIT3) az erőforrások produktív és gazdaságos (profit orientált) felhasználását, *hatékonyság* alatt az üzleti folyamatok időben megfelelő, pontos, konzisztens és felhasználható megvalósítását értjük.

A vállalat küldetése pedig azt fejezi ki, hogy a vállalat milyen módon kívánja azt az üzleti célját megvalósítani, amely a működési körét, a belső működési elveket és a gazdasági környezettel kiépítendő kapcsolatait is magába foglalja.

Ezekből egyértelműen következik, hogy mindent, ami a vállalatnál történik, az üzleti cél teljesítésének kell alárendelni.

Az üzleti követelményeknek kell tehát alárendelni a vállalaton belül végbemenő minden olyan tevékenységet, amik az üzleti cél elérése érdekében szükségesek.

- **Az üzleti követelmények (COBIT 3 alapján)**
 - Minőség
 - ✓ magas színvonal (hibamentesség, vonzó kivitel)
 - ✓ költség (gazdaságosság)
 - ✓ szállítókészség (az elvárt és szerződött feladat megfelelő teljesítése)
 - Megbízhatóság
 - ✓ hatékonyság, eredményesség
 - ✓ kiszámíthatóság (az elvárt feladat teljesítése)
 - ✓ jogszabályi megfelelés
 - Biztonság
 - ✓ bizalmasság (valamit csak korlátozott számú kevesek ismerhetnek)
 - ✓ sértetlenség (valami az eredeti állapotának megfelel)

- ✓ rendelkezésre állás [az eredeti szolgáltatások meghatározott helyen (működőképesség) és időben (elérhetőség) rendelkezésre állnak].

Témánk szempontjából kiemelendő, hogy a biztonság üzleti követelmény, amiből az következik, hogy a biztonság nélkül az üzleti cél(-ok) nem teljesíthetők. Ennek belátása a vállalat irányítói részéről elemi követelmény. „A nálunk ilyen nem fordulhat elő” nézet igen káros, és vajon, aki ezt vallja, mit válaszol arra az USA-beli kérdésre, hogy „és ha mégis?”.

A vállalaton belül folyamatok mennek végbe, amelyek olyan módon realizálják a vállalat küldetését, hogy az üzleti követelményeket teljesítve, valamint az erőforrásokat felhasználva, előállítják az inputokból az outputokat,

A folyamatok meghatározott kapcsolatban álló és sorrendben végrehajtandó tevékenységek, amelyek az erőforrásokat felhasználják.

- Az üzleti folyamatok a vállalat alaptevékenységét realizálják (pl. bankokban többek között a betétgyűjtés, hitelnyújtás, folyószámla vezetés, vagy kereskedelmi vállalatoknál a beszerzés, értékesítés). Az üzleti folyamatokat a vállalat belső támogató folyamatai segítik, mint pl. a vállalt pénzügyi, munkaügyi, marketing, humán erőforrás gazdálkodás, biztonsági vagy ügyvitel-technikai folyamatai.
- A termelési (szolgáltatási) folyamatok, amelyek a vállalat által értékesíteni (szolgáltatni) kívánt termékek előállítását végzik, és amiket a termelést támogató folyamatok egészítenek ki, mint pl. a termeléshez szükséges anyagok, áruk, félkész áruk, vagy adatok, információk, dokumentumok, pénzeszközök biztosításának a folyamatai.
- Az informatikai folyamatok (alkalmazási rendszerek), amelyek azáltal szolgálják ki az üzleti és a termelési folyamatokat, hogy a tőlük kapott adatokat feldolgozzák, majd a feldolgozott adatokat számukra visszaadják. A támogató folyamatok itt is megjelennek.

Hangsúlyozni kell, hogy minden folyamatnak az üzleti cél megvalósulását kell szolgálnia, az üzleti követelmények érvényesítése mellett. Azaz már itt hangsúlyoznunk kell, hogy a biztonságnak is az

üzleti célt kell szolgálnia, tehát minden biztonsági követelménynek át kell mennie az üzleti cél és az üzleti követelmények szűrőjén.

AZ ERŐFORRÁSOK:

A vállalatirányítás az üzleti célok megvalósításához erőforrásokat biztosít, amelyek a következők lehetnek:

az üzleti rendszerben

- ⇒ adatok, értékek, áruk,
- ⇒ tőke (pénzügyi, szellemi),
- ⇒ technológia (ügyvitel-technikai eszközök, személy- és teherszállító eszközök, automatizált raktározási rendszerek, épület automatikai rendszer, biztonsági rendszer, távközlési rendszer, vagy bankoknál pl. a pénzfeldolgozó berendezések),
- ⇒ üzleti és azokat támogató folyamatok, eljárások,
- ⇒ infrastruktúra (mint pl. létesítmények, energiaellátás, légkondicionálás, papírfeldolgozás stb.),
- ⇒ ember (alkalmazottak, vevők, szállítók, beruházók stb.).

a termelési, szolgáltatási rendszerben

- ⇒ nyersanyagok, anyagok, félkész áruk, adatok, termékek,
- ⇒ szállítási és/vagy termelési technológia, termelő- és termelésirányító rendszerek,
- ⇒ szállítási és/vagy termelési folyamatok, eljárások,
- ⇒ támogatások (pl. létesítmények, légkondicionálás, energiaellátás, papírfeldolgozás stb.),
- ⇒ ember (alkalmazottak, megrendelők, szállítók stb.).

az információ rendszerben

- ⇒ adatok,
- ⇒ technológia (pl. hardver, rendszerszoftver, hálózati szoftver, stb.),
- ⇒ alkalmazások (alkalmazói szoftver),
- ⇒ támogatások (pl. létesítmények, energiaellátás, légkondicionálás, papírfeldolgozás stb.),
- ⇒ ember (alkalmazottak, külső felhasználók, szállítók stb.).

3. A VÁLLALAT RENDSZER

3.1. MAKROGAZDASÁGI RENDSZER

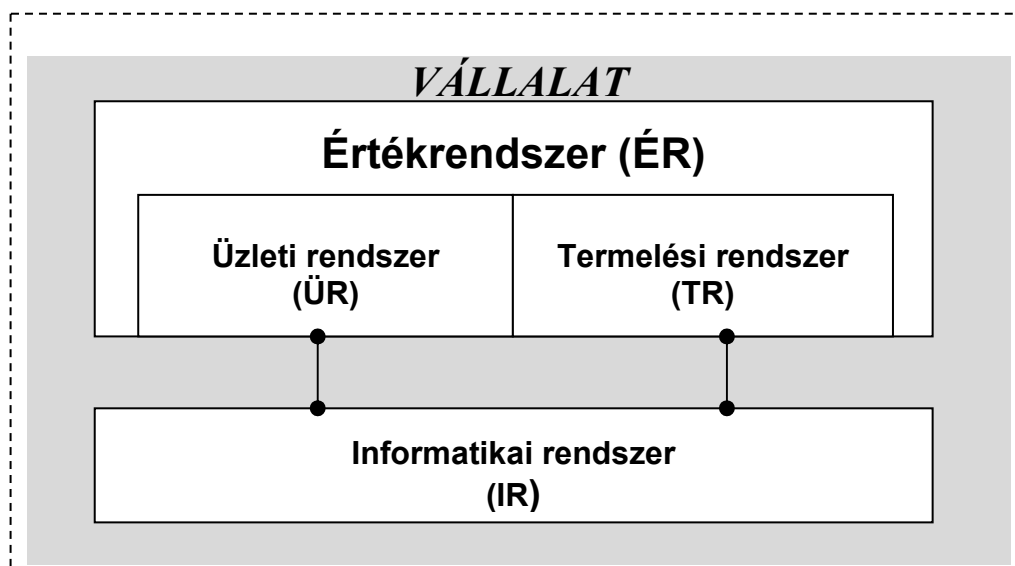
A *rendszer fogalma*: a rendszer egymással meghatározott összefüggésben álló elemek összessége.

A makrogazdasági rendszer valójában a nemzetgazdasági rendszer, azaz ezen az egész nemzetgazdaságot értjük. A nemzetgazdaságon belül kisebb rendszerek - vállalatok, gazdasági szervezetek - működnek, amelyeket mikrogazdasági rendszernek tekintünk.

3.2. MIKROGAZDASÁGI RENDSZER

A vállalatot a rendszerelmélet általában nagy rendszernek tekinti, amelyet az jellemez, hogy az alkotóelemei inhomogének, és közöttük a kölcsönhatások végtelen sok relációt eredményeznek. Ebből az következik, hogy a vállalat működésének optimalizálása az elemek és az ezekből képződő alrendszerek folyamatos elemzéséből, valamint az elemzések alapján megtett azon intézkedésekből áll, amelyek lehetőséget adhatnak az optimális működés megközelítéséhez.

A mikrogazdasági rendszer - vállalat vagy gazdasági szervezet – a feladatát, küldetését a tevékenységei útján látja el. Ezeket a tevékenységeket a vállalat vagy a gazdasági szervezet az erőforrások felhasználásával az értékrendszerben és az információ rendszerben látja el. Az értékrendszerben (ÉR) definiálhatjuk az üzleti rendszert (ÜR) és ha van, a termelési (szolgáltatási) rendszert (TR):



Az értékrendszerben zajlanak az üzleti (és támogató) folyamatok, és ha az alaptevékenység a termelés vagy a szolgáltatás, a termelési és/vagy a szolgáltatási folyamatok, amelyeket kiszolgál az információ rendszer (IR). Így a vállalat vagy a gazdasági szervezet tevékenysége felbontható

- ⇒ az **értékrendszerre** (ÉR), amely áll
 - az üzleti rendszerből (ÜR) és
 - a termelési (szolgáltatási) rendszerből (TR) (ha a vállalat vagy a gazdasági szervezet ilyen jellegű), valamint
- ⇒ az **információ rendszerre** (IR).

Az értékrendszeren belül

- az *üzleti rendszerben* valósul meg a papír alapú iroda, az üzleti (a küldetés határozza meg) és a támogató folyamatok (pl. értékesítés, marketing, számlázás, pénzügy, bérszámfejtés, HR, jogi tevékenység, fejlesztés, szervezés, minőségbiztosítás, kontrolling, ingatlan gazdálkodás és üzemeltetés). E folyamatok lehetnek
 - manuális,
 - manuális és technikával támogatott manuális.
- a *termelési rendszerben* (ha van) a termelés, a szolgáltatás, a termelési és szolgáltatási folyamatok, valamint a támogató folyamatok mennek végbe. E folyamatok lehetnek
 - technikai,
 - manuális,
 - manuális és technikával támogatott manuális.

Az információ rendszeren belül

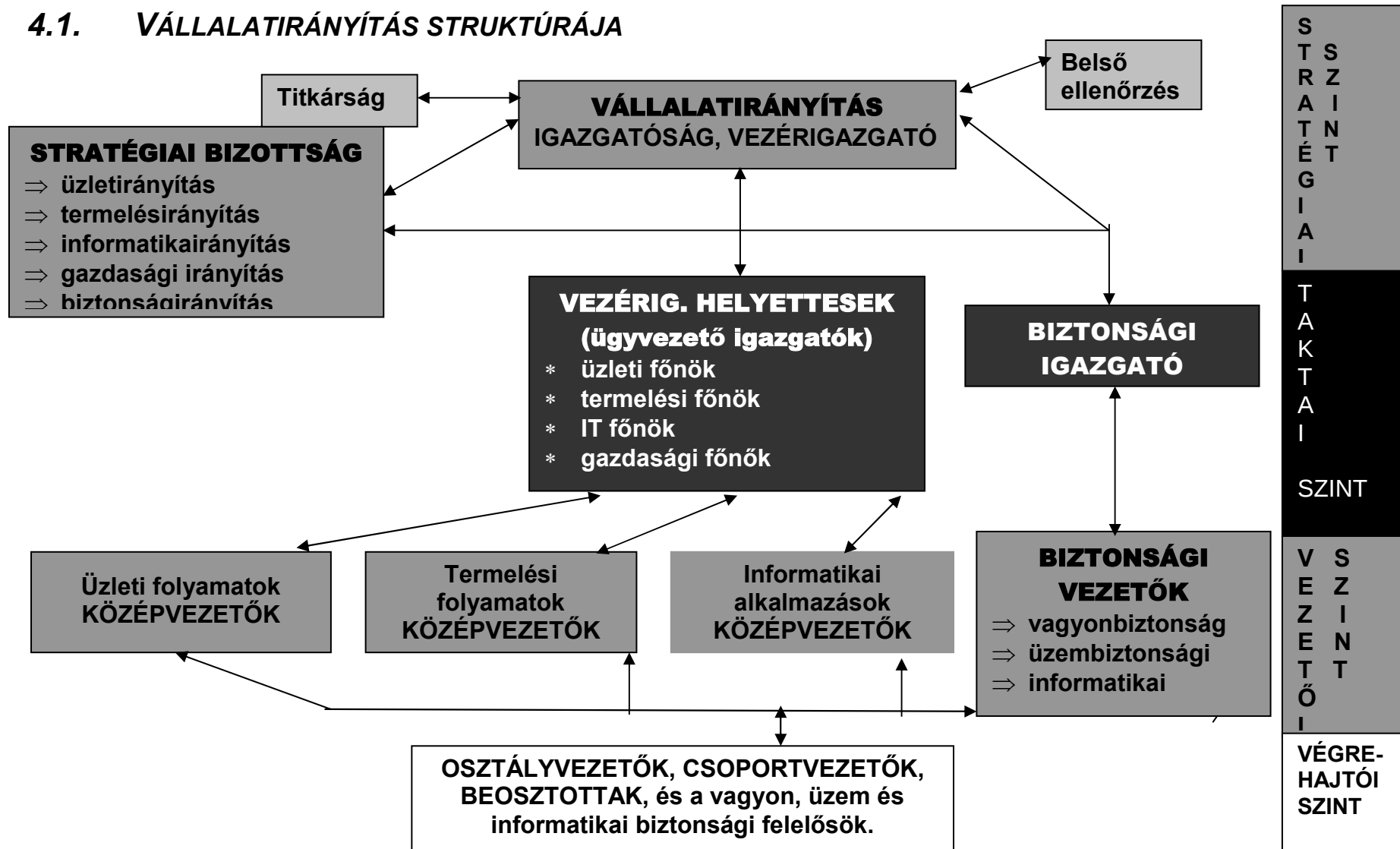
- az elektronikus iroda valósul meg, az elektronikus adatok feldolgozása, tárolása, illetve továbbítása megy végbe. Az információ rendszer folyamatai lehetnek
 - alkalmazások (informatikai folyamatok),
 - manuális támogató folyamatok,
 - manuális és technikával támogatott manuális.

A teljes vállalatot átfogja a **biztonsági rendszer**, amely három biztonsági alrendszerből áll:

- vagyonbiztonsági,
- üzembiztonsági (ha van termelés) és
- informatikai biztonsági alrendszerekből.

4. A VÁLLALATIRÁNYÍTÁS

4.1. VÁLLALATIRÁNYÍTÁS STRUKTÚRÁJA



Vállalatirányítás definíciója (COBIT 3 alapján):

A vállalatot irányító és ellenőrző összefüggések és folyamatok struktúrája annak érdekében, hogy a vállalat értékhozzáadással elérhesse céljait, mérlegelve a kockázatokat az ÉR és IR, illetve folyamataik hasznával szemben.

{Ez és a következő fejezet ISACA anyagok alapján készült (lásd [1],[2],[3], [4], [5])}.

A vállalatirányításnak biztosítania kell a vállalat stratégiai irányítását, ellenőrzését (auditálását), az irányításhoz a szerepek és felelőségek elosztását, valamint ez utóbbiak számonkérését.

A vállalatirányítás ciklikusan valósul meg, egy ciklus állandóan újraindul, hiszen a körülmények (pl. a piac, a jogszabályok, stb.) folyamatosan változnak.

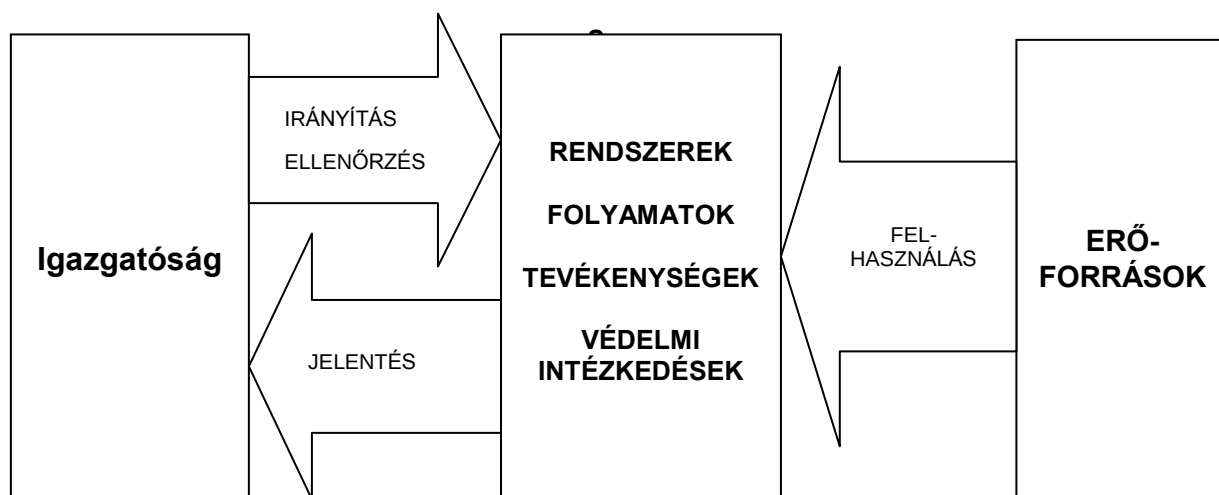
- A vállalati stratégia a célok és a célok megvalósításához szükséges eszközök, tevékenységek (követelmények) viszonylag hosszú távú meghatározása.

A vállalati stratégia részstratégiákra bontható fel, ilyenek az üzleti, a termelési, az informatikai és a biztonsági stratégiák.

A viszonylag hosszú táv magában hordoz bizonyos bizonytalanságot, amelyet a tervezéskor figyelembe kell venni.

A stratégia kidolgozását és megvalósítását a vállalatirányítás irányítja.

4.2. VÁLLALATIRÁNYÍTÁS (ENTERPRISE GOVERNANCE) FUNKCIONÁLIS MODELLJE (COBIT3 ALAPJÁN)



A vállalat funkcionális struktúrája:

VÁLLALAT

RENSZEREK (üzleti, termelési, informatikai)

SZAKTERÜLETEK*

TERVEZÉS ÉS SZERVEZET
BESZERZÉS ÉS MEGVALÓSÍTÁS
SZOLGÁLTATÁS ÉS TÁMOGATÁS
MONITOROZÁS

FOLYAMATOK (és támogató folyamatok)

TEVÉKENYSÉGEK (feladatok)

*A négy általános jellegű szakterület értelmezése az üzleti, a termelési és az informatikai rendszereknél:

TERVEZÉS ÉS SZERVEZET

A stratégia, a taktika és az üzleti cél megvalósításának tervezése az üzleti, *termelési* és informatikai rendszerek vonatkozásában, valamint a megfelelő szervezet és infrastruktúra biztosítása.

BESZERZÉS ÉS MEGVALÓSÍTÁS

Az üzleti, *termelési* és informatikai rendszer stratégiák megvalósításához az erőforrások biztosítása, aktualizálása, karbantartása.

SZOLGÁLTATÁS ÉS TÁMOGATÁS

Az üzleti szolgáltatás biztosítása (termelés, üzemeltetés), beleértve a biztonsági rendszert, valamint a képzést.

MONITOROZÁS:

A folyamatok, tevékenységek és védelmi intézkedések folyamatos ellenőrzése (belső, ill. külső audit).

Az üzleti, *termelési* és informatikai rendszereken belül részterületeket határozhatunk meg, amelyeken belül a részfolyamatok és a résztvétekenységek megvalósulnak:

- * a vállalatirányítás az igazgatóság és a vezérigazgató feladata (stratégiai szint), a gyakorlati bonyolítást a vezérigazgató helyettesek végzik,
- * az egyes szakterületek irányítása (amely a taktikai szint, lehet üzlet, termelés, informatikairányítás, biztonságirányítás) a vezérigazgató helyettesek, ügyvezető igazgatók feladata,
- * a biztonságirányítás a biztonsági igazgató feladata, aki részt vesz a vállalati-stratégia irányításában, míg a szakterületek biztonságirányításáért (vagyon, üzem, informatikai biztonságirányítás) a biztonsági vezetők (vagyon-, üzem- és informatikai biztonsági vezetők) a felelősek.

A biztonságirányítás kockázatmenedzsment alkalmazásával valósul meg, feladat a veszélyforrások felmérése és a kockázatok elemzése, majd ez alapján a kontrollok és védelmi intézkedések kidolgozása. A védelmi rendszer megvalósítása, valamennyi kontrollt beleértve, a biztonságirányítás önálló feladata.

A kontrollok az üzleti cél realizálása érdekében tett biztonsági intézkedések, ami a biztonságpolitika megvalósulását biztosítja az üzleti, *termelési* és informatikai rendszerek, a szervezeti struktúra, a garanciák

biztosítása terén egyaránt a nem várt események megelőzésére, jelzésére (ellenőrzésére) és javítására (védelmi intézkedések).

4.3. FELELŐSSÉGEK ELOSZTÁSA

A felső vezetés (igazgatóság, vezérigazgató) feladata a vállalatirányítással kapcsolatban:

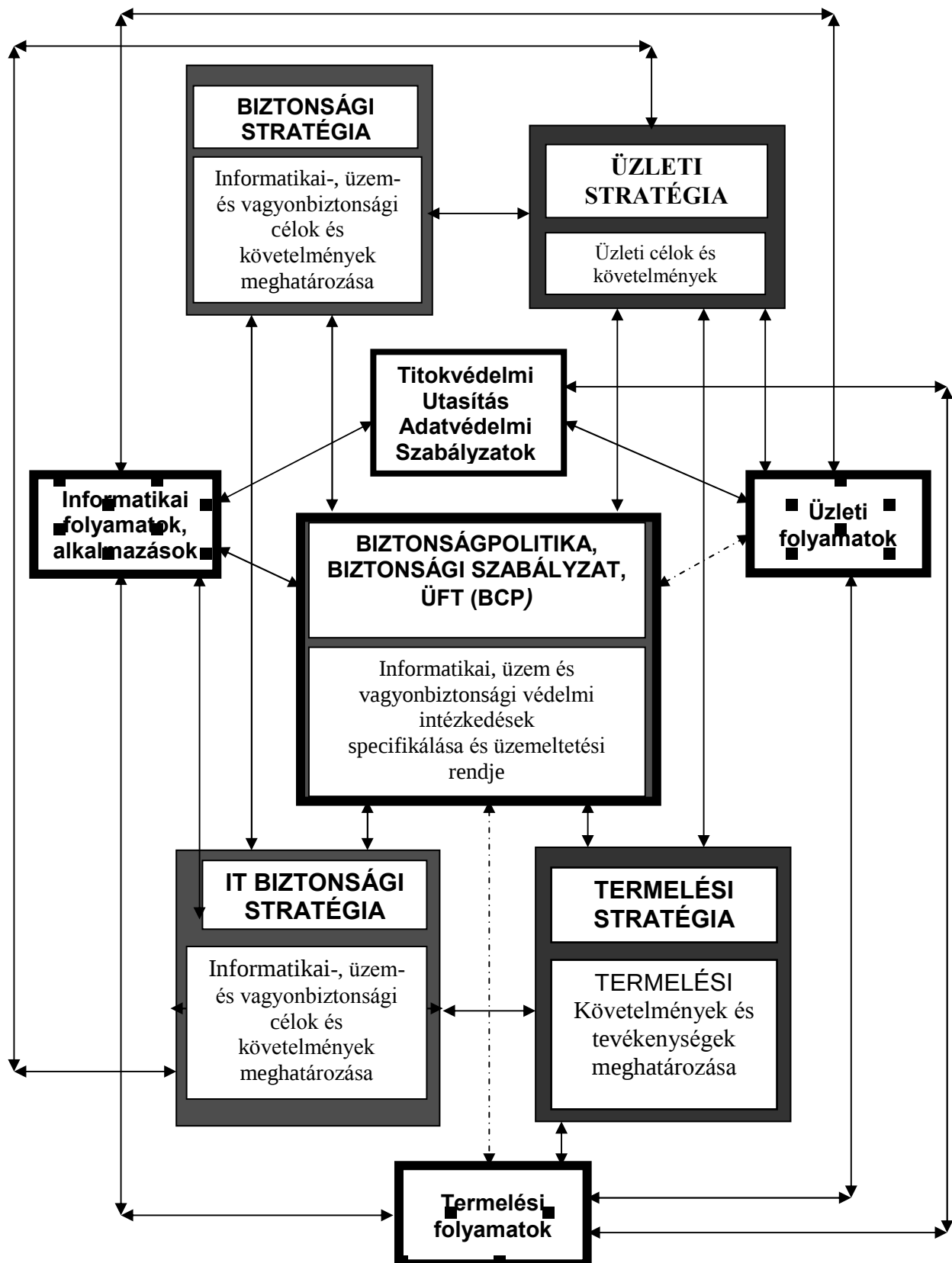
- ⇒ meghatározza a vállalati stratégiát, valamint a biztonsági irányelveket,
- ⇒ értékeli a költségeket, lehetőségeket, kockázatokat (beleértve a biztonsági kockázatokat),
- ⇒ értékeli a célok teljesülését, a megvalósítási folyamatok eredményeit (ellenőrzés, számonkérés),
- ⇒ stratégiai bizottságokat hoz létre az üzleti, *termelési* és informatikai stratégiák kialakítása végett.

A vezérigazgató helyettesek, ügyvezető igazgatók, biztonsági igazgató tevékenységei:

- ⇒ közreműködnek az üzleti célok, a stratégia érvényesítésében,
- ⇒ gondoskodnak a stratégiai céloknak megfelelő erőforrások rendelkezésre állásáról,
- ⇒ elvégzik a költségek optimalizálását,
- ⇒ meghatározzák a külső erőforrások szerepét, és azt ellenőrzik,
- ⇒ közreműködnek a kockázatok feltárásában és csökkentésében, a biztonság megteremtésében és folyamatos biztosításában.

A vállalati biztonságirányítás része a vállalatirányításnak, de a biztonság kialakításában az igazgatóságnak, a vezérigazgatónak elsődleges a felelőssége, szerepe.

4.4. ÜZLETI, TERMELÉSI, INFORMATIKAI ÉS BIZTONSÁGI STRATÉGIA ÖSSZEFÜGGÉSEI



*Az MSZ ISO/IEC 17799-es szabvány a biztonságpolitikát biztonsági szabályzatként fordítja le, így nem ismer biztonságpolitikát, a kettőt egyként kezeli.

Az összefüggéseket úgy kell értelmezni, hogy a folyamatos nyíl a közvetlen összefüggést, míg a szaggatott a ráhatást jelenti. Pl. az üzleti folyamatok függenek, pontosabban meg kell felelniük az üzleti stratégiának, azt kiszolgálják, az informatikai alkalmazásoknak meg kell felelniük az üzleti folyamatoknak, ezért ezek kapcsolatait folyamatos nyilak jelölik. A Biztonsági Politika (Szabályzat), az Üzletmenet Folytonossági Terv (ÜFT) az üzleti folyamatokat kiszolgálni képes védelmi intézkedések meghatározásával hat az üzleti folyamatokra, ezért ezek kapcsolatát szaggatott nyíl jelöli.

4.5. A MENEDZSMENT ÉRTELMEZÉSE

A menedzsment fogalmát egy szóval nem szokták lefordítani (egyes fordítók szerint kezelés, szervezés), értelmezése

- * irányítás,
- * szervezés,
- * ellenőrzés, felügyelet és
- * döntés.

Ugyanakkor rá kell mutatnunk arra, hogy angolul a menedzsment egyaránt jelent tevékenységet vagy vezetést, a vezetőket magukat. Pl. elterjedt használata a top menedzsment, amely a vállalat felső vezetését jelenti. Esetünkben a biztonság menedzsmenten a biztonság irányítását, szervezését, ellenőrzését és az ezzel kapcsolatos döntések meghozatalát értjük. A menedzsereket másképpen funkcionális vezetőknek is nevezik.

A biztonság menedzsment felelőssége, hogy gondoskodjon a biztonsági program végrehajtásáról, azaz, hogy

- a védelmi követelmények kikényszerítsék a védelmi intézkedéseket,
- a vállalat minden munkatársa napra készen tartott biztonsági tudatossággal rendelkezzen.

A felső menedzsmentnek ehhez látnia kell, hogy a biztonság üzleti követelmény, amely nélkül a cég küldetése nem teljesíthető.

4.6. A VÁLLALATIRÁNYÍTÁS SZINTJEI

A vállalatirányítás különböző szinteken valósul meg. Ezeken a szinteken természetesen a feladatok változnak. Éspedig

- ⇒ stratégiai szint, ahol a hosszú távú üzletpolitika kidolgozása történik, a fentiek értelmében a megvalósításhoz szükséges erőforrások biztosításának politikája és a vállalati szintű szabályozások, szabályzatok politikájának kidolgozásával (igazgatóság, vezérigazgató),
- ⇒ taktikai szint, ahol a rövid távú üzletpolitika kidolgozása és irányítása történik az egyes területekre, a szükséges erőforrások allokációja mellett (vezérigazgató helyettesek, ügyvezető igazgatók, biztonsági igazgató),
- ⇒ vezetői szint, ahol az egyes területeken az erőforrások hasznosítását irányítják az üzletpolitika és a stratégiák alapján (középvezetők),
- ⇒ végrehajtási szint, ahol az erőforrások felhasználásával az üzleti kötelezettségek teljesítése, végrehajtása történik a hatékonyság biztosítása mellett (alsó szintű vezetők, beosztottak).

Az irányítás egyik eszköze a szabályozás (a végrehajtás közvetlen irányítása és ellenőrzése mellett). Általában az alábbiak szerint alakul a vállalatban belül a szabályozás az egyes szinteken:

- STRATÉGIAI SZINT: célok, küldetés és a főbb elvek hosszú távú meghatározása az üzleti, informatikai, termelési és biztonsági területekre vonatkozóan. (lásd a 4.4. pontot);
- TAKTIKAI SZINT, rövid távú: a stratégiát megvalósító módszerek követelmények, erőforrások, védelmi intézkedések meghatározása, mint Üzletpolitika, Informatikai Fejlesztési Terv, Termelési Fejlesztési Terv, **valamint a mind három rendszerrel foglalkozó** Biztonsági Politika (Szabályzat), BCP (és az utóbbi kettő Akció tervei), Adatvédelmi Szabályzatok, Titokvédelmi Utasítás, Iratkezelési Szabályzat, Selejtezési Szabályzat és Üzletmenet Folytonossági Terv;
- VEZETŐI SZINT napi szintű végrehajtási rendelkezések: informatikai, üzleti, biztonsági (folyamatok, tevékenységek szabályozása), termelési szabályozások (biztonsági, üzleti, termelési, informatikai menedzserek, középvezetők);

- **VÉGREHAJTÁSI SZINT** a folyamatos feladat végrehajtás az eljárás rendek, de gyakorlatilag minden szabályozás alapján (alsó szintű vezetők, munkatársak).

Természetesen ezeket a szabályozásokat napra készen kell tartani.

A szabályozások lehetnek: szabályzatok, utasítások vagy eljárásrendek, amelyek értelmezése a következő:

- a szabályzat magatartást, cselekvést meghatározó szabályok összessége. A szabályzat MIT és HOGYAN orientált.
- az utasítás valaminek a végrehajtására kiadott rendelkezés. Az utasítás TEVÉKENYSÉG orientált.
- az eljárásrend valamilyen üzleti folyamat vagy informatikai alkalmazás vagy részfolyamat során végrehajtandó tevékenységek és végrehajtásuk időbeli sorrendjének szabályozása. Az eljárásrend SORREND orientált.

4.7. A VÁLLALATIRÁNYÍTÁSI ELLENŐRZÉS CÉLJAI

Az üzleti ellenőrzési célok:

- * minőség: a termékek és szolgáltatások minőségbiztosítása.
- * költségek: a termékek és szolgáltatások költségeinek optimalizálása az erőforrások optimális használatával.
- * szállítókészség: a rendelkezésre állás és pontosság a termékek és szolgáltatások a fogyasztó számára történő biztosításánál.

A vállalatirányítás által végzett ellenőrzések azt a célt szolgálják, hogy a vezetés felelősségét az üzleti célok elérésében folyamatosan ébren tartsák. Ez egyet jelent azzal, hogy az üzleti, illetve informatikai követelmények megvalósulását rendszeresen ellenőrizni kell (belső és/vagy külső ellenőrzés).

Az ellenőrzést nagymértékben segíti, ha a számonkérhetőség a vállalatot átfogóan biztosított (pl. naplózás). A vezetés nem rendelkezhet sem felmentéssel, sem elnézéssel a feladatainak teljesítése kérdésében a vállalat tulajdonosa(i) felé.

A vállalatirányítás alapvető része tehát az ellenőrzés (lásd a modellt is), amely nélkül nem lehet pl. értékelni a védelmi intézkedések

megfelelőségét és azt, hogy azok kikényszerítik-e a gyakorlatban a védelmi követelményeknek való megfelelést.

A rendszerek ellenőrzése

Az információ rendszer, illetve informatikai biztonság ellenőrzésére irányadó a COBIT 3, valamint az MSZ ISO/IEC 17799. A másik két rendszerre is **(üzleti és termelési)** el kell készíteni a Biztonsági Stratégiában, Biztonságpolitikában (Szabályzatban) és az Üzletmenet-folytonossági Tervben (ÜFT) foglaltak megfelelésségének és megvalósulásának ellenőrzésére szolgáló biztonságellenőrzési módszereket a belső ellenőrzési jogszabályok, szabályok és gyakorlat alapján.

A vállalatirányítás lényeges eleme a szervezetiileg független, közvetlenül a vezérigazgatóhoz rendelt belső ellenőrzési szervezet. A belső ellenőrzési szervezet ellenőrzési hatásköre a vállalat teljes területére kiterjed, és a jelentéseit a vezérigazgató számára készíti. A belső ellenőrzés az üzleti, termelési, informatikai és a biztonsági események szabályozottságát, a rendeltetésszerű működést és a belső szabályzatoknak, utasításoknak és eljárás rendeknek való megfelelést ellenőrzi. Ebből következik, hogy a belső ellenőrzés területén szükség van egy olyan szakemberre, aki egyaránt kompetens az üzleti, termelési, informatikai és biztonsági kérdésekben.

Az egyik fontos biztonság ellenőrzési feladat, a vállalati szintű egyenszilárdságú biztonság ellenőrzése.

A biztonsági ellenőrzés kiterjed arra, hogy

- a jogszabályoknak, az előírt belső szabványoknak a belső szabályozások és utasítások megfelelnek-e (megfelelőség),
- a belső szabályozások és utasítások megvalósítása teljesül-e (megvalósulás).

Az USA-ban az ENRON botrány után, 2002-ben, igen szigorú és részletes szabályokat vezettek be az ellenőrzésre, amelyet a Sarbanes-Oxley törvény tartalmaz (elsősorban az éves pénzügyi jelentés ellenőrzésére). Ezt figyelembe véve az EU Bizottság 2003-ban kiadta a 8. direktívát. Várhatóan ezek a szabályok valamilyen formában meg fognak jelenni a hazai szabványokban, módszertanokban is, és hatással lesznek a belső ellenőrzés teljes

rendszerére. Ez természetesen kihat az információ rendszerre, amely nyilván követelményeket jelent a biztonsági rendszerrel szemben is.

Utalunk arra, hogy a 8. direktiva szerint audit bizottságokat kell létrehozni, az auditorokat regisztráltatni kell, és az auditor számára biztosítani kell a vállalaton belüli függetlenséget. Az auditor munkája egyaránt kiterjed az előírt üzletvitel, biztonság és minőség megvalósulásának ellenőrzésére. Továbbá a COBIT 3 kiegészítéseképpen megjelent 2003-ban az „IT Control Objectives for Sarbanes Oxley” (lehívható: www.itgi.org). Ebben megtalálhatók, pl. a törvényalkalmazás feltételei, a törvénynek való megfelelés biztosítása, az ellenőrzési listák alapján történő ellenőrzések meghatározása (terjedelmes lista a biztonság ellenőrzés szempontjairól).

5. A BIZTONSÁG

5.1. A VÁLLALATI BIZTONSÁG

A vállalatoknak új kockázatokkal kell szembenézniük, mint ahogy a bevezetőben erről már szó volt. Ezek között a biztonsági kockázatok komoly fenyegetést jelentenek számukra, tehát bekövetkezésük ellen intézkedéseket kell tenni.

Induljunk ki e kérdéskör vizsgálatánál a biztonság fogalmából.

- A biztonság olyan kedvező állapot, amelynek megváltozása nem valószínű, de nem is kizárt.

A kedvező biztonsági állapot azt jelenti, hogy a kockázatok az elviselhető, pontosabban vállalható mértékűek, azaz a fenyegetések bekövetkezési valószínűsége elfogadhatóan kicsi. Ugyanakkor ez azt is jelenti, hogy a veszélyforrások bekövetkezése nem is zárható ki. Azaz 100%-os biztonság nem érhető el, csak folyamatos követéssel megközelíthető. A kockázatnak egy része, a maradék kockázat, nem küszöbölhető teljesen ki (lásd 5.5 pontban a kockázatmenedzsment részletesen).

Már említettük, hogy a biztonság egy vállalat esetében üzleti követelmény, amely azt jelenti, hogy az üzleti cél elérése biztonság nélkül nem lehetséges.

A vállalati biztonság elfogadható, ha a vállalat (a vállalatot alkotó rendszerek) erőforrásainak bizalmosságának, sértetlenségének és rendelkezésre állásának fenyegetettsége, azaz a kockázatok (belső és külső), megfelelnek a stratégiában meghatározott biztonsági szintnek.

A vállalati biztonság elemi feltétele, hogy a menedzsment felismerje ennek szükségességét, és gondoskodjon a megfelelő védelmi intézkedésekről. Ez azonban nem tartozik a könnyen megoldható kérdések közé, mivel egy évben a szükséges költségek elérhetik a vállalati költségek akár 5%-át is.

Fel kell hívjuk a figyelmet arra, hogy egy 50 fős vagy annál kisebb vállalat esetében a „megfelelő” biztonság biztosítása csak komoly kompromisszumok árán lehetséges. A felső vezetőnek vállalnia kell bizonyos kockázatokat, és csak a nem vállalhatóakra kell a védelmi intézkedéseket megtenni. A biztonságtechnika rendelkezik azokkal a

módszerekkel, amelyek alkalmazásával elérhető, hogy egy kisvállalat nem lesz szabadon kitéve a nem vállalt kockázatok, fenyegetések esetleges következményeinek. Az adatok és egyes erőforrások biztonság érzékenységen alapuló osztályozás adhatja ehhez a vezetői döntéshez az alapot.

5.2. A VÁLLATI SZINTŰ BIZTONSÁG MGM

Egyre jobban elterjed az a meggyőződés a biztonságtechnikában, hogy az üzleti célnak meg kell határoznia minden vállalati tevékenységet, azaz az üzleti (termelési) és az informatikai folyamatok ennek a célnak az elérését szolgálják, és közöttük keresztösszefüggések vannak. Nyilvánvaló, hogy e folyamatok biztonságát szolgáló rendszerek között hasonló Keresztösszefüggések állnak fenn. A biztonsági alrendszerek közötti együttműködés hiánya, az egyébként nem szükségszerű kockázatok sorát eredményezi.

A nemzetközi irodalomban (pl. ISACA kiadványokban) megjelentek az olyan kifejezések, követelmények, mint vállalatot átfogó, vállalatszintű biztonságirányítás, kockázatmenedzsment, illetve biztonsági rendszer. Az elmúlt évben az ISACA kiadta az „IT biztonsági program kritikus siker tényezői” című tanulmányt. Ebben két csoportot állapít meg: 1. kritikus és 2. kiegészítő sikertényezők. A kritikus sikertényezők között a következő szerepel: integrált fizikai és IT biztonság.

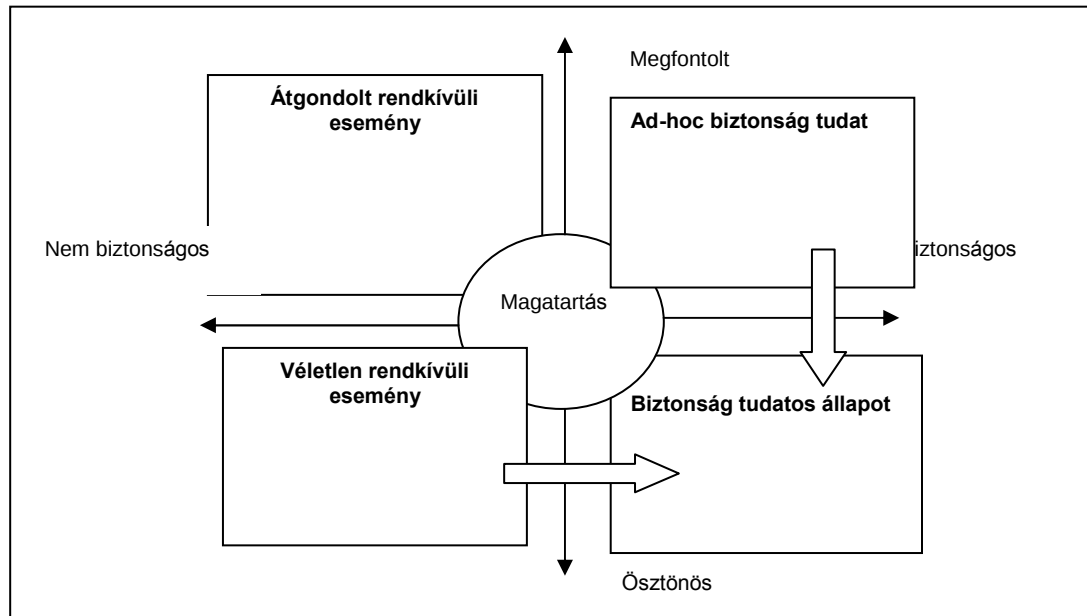
5.3. BIZTONSÁG TUDATOSSÁG

A tudatosság egy olyan állapot, mely az egyének napi rutinját, valamint az ehhez kapcsolódó ismeretanyagát fejezi ki.

A biztonságtudatosság, ebből levezetve, egy a biztonság számára kedvező állapotot jelent, ahol minden egyén ismeri és rutinszerűen alkalmazza a számára szükséges és elégséges információkat, erőforrásokat, szem előtt tartva a biztonság legfőbb alapelveivel kapcsolatos egyéni teendőit (*bizalmasság, sértetlenség, rendelkezésre állás*).

A biztonságtudatosság kialakítása egy szervezeten belül az a magatartásforma, amely adott vállalat biztonsági stratégiájával egybehangzóan, minden személyzeti (egyéni) szinthez differenciáltan olyan napi rendszeres magatartást határoz meg, hogy a szervezet alkalmazottjai tisztába legyenek azzal, hogy:

- biztonság és az ehhez tartozó adott biztonsági szintek megfelelőek és szükségesek a szervezet számára,
- a biztonság fontos és a biztonság hiánya következményekkel jár,
- az ő felelősségük és tevékenységük kihatással van a biztonság egyes területeire.



5.4. BIZTONSÁGI KULTÚRA

A kultúra fogalma megjelent a szakirodalomban, ezért szükséges ennek a fogalomnak a pontos definiálása:

a COBIT4, például egy sor magas szintű auditálási szempontban, szerepelteti a kultúrát, mint ellenőrzési követelményt. Ugyanakkor ez a fogalom az említett anyagban nincs definiálva. Összehasonlítva a követelményeket, szempontokat a COBIT 3 megfelelő pontjaival (a COBIT3. megfelelőségeket a COBIT4 táblázatban adja meg), következtetni lehet arra, hogy a COBIT4

- *a kultúrán általában az erkölcsi tartást, az etikai értékeket, és a magatartást érti.*

Először szükséges tisztázni a kultúra fogalmát, majd a kisebb közösségekre vonatkozó szervezeti kultúra fogalmát. Továbbá felmerül a kérdés, hogy mit értünk, beszélhetünk-e a szervezeti kultúrán belül biztonsági kultúráról, és amennyiben igen, milyen viszonyban van, az eddig használt biztonsági tudatossággal. A szervezeti kultúra nem tárgya

ennek az ajánlásnak, ezért a továbbiakban a jelen anyag csak a biztonsági kultúra alapjait érinti:

a biztonsági kultúra az, amikor az emberek tudják jogaikat, és ami a legfontosabb, érvényesítik azokat, és akik egy biztonsági kultúrához tartoznak, tudják, mi kompromittálja a biztonságot, és oktatják, elmarasztalják azokat az embereket, akik tudatlanságból, feledékenységéből vagy személyes gyengeségből nem biztonságos magatartást tanúsítanak

Biztonsági kultúra megléte esetén tehát az emberek napi szinten gyakorolják a biztonsági feladataikat, ismerik és együtt élnek a felelőségeikkel, rendszeres időközönként frissítik a biztonsági ismereteiket.

5.5. A BIZTONSÁG ELEMEL A BIZTONSÁGI ALRENDSZEREKBEN

5.5.1. A biztonsági rendszer alrendszerei

A vállalat, mint mikró gazdasági rendszer (lásd fentiekben), három rendszerből épül fel, amennyiben termelőmunka is folyik a cégnél. E három rendszerben kell a biztonságról gondoskodni a biztonsági rendszer keretében, amely átfogja mind a hármat, és a következő alrendszerekből áll:

- **a vagyonbiztonsági alrendszer**, amelyben a vagyonbiztonsági védelmi intézkedéseken kívül vannak informatikai biztonsági védelmi intézkedések is,
- **az üzembiztonsági alrendszer**, amelyben vannak az üzembiztonsági védelmi intézkedéseken kívül vagyon és informatikai biztonsági védelmi intézkedések is,
- **az informatikai biztonsági alrendszer**, amelyben vannak vagyonbiztonsági védelmi intézkedések is.

(Lásd részletesen az 5.2.2. pontban.)

A biztonság a vállalaton belül tehát egy egységes rendszert képez, amely alrendszerekből áll, úgymint a vagyon-, üzem- és informatikai biztonsági alrendszer, így átfogja a teljes vállalatot.

A vállalati biztonsági rendszer, tehát a vagyonbiztonság, üzembiztonság és az informatikai biztonságból képzett alrendszerekből áll, amelyek hivatottak az erőforrások (üzleti,

termelési és informatikai) fenyegetettségeknek való kitettségét, a kockázatokat az üzleti célkitűzések megvalósításához szükséges mértékűre csökkenteni.

A gyakorlatban ezeken az alrendszeren belül adminisztratív, humán, fizikai és logikai biztonságról beszélhetünk. Az elmúlt évek technikai fejlődése azonban magával hozta, hogy

- az üzleti rendszerben a vagyonbiztonsági alrendszer területén megjelennek olyan eszközök, technikák, amelyekben a biztonság a logikai biztonság körébe tartozik. Ilyen eszköz pl. az épület automatikát, biztonsági rendszert, távfelügyeletet irányító információ rendszer, amiben természetesen logikai biztonságról kell többek között gondoskodnunk;
- az informatikai rendszerben az informatikai biztonság területén új fizikai és logikai védelmi intézkedési lehetőségek jelennek meg, amelyek valójában a vagyonbiztonsági intézkedések;
- a termelési rendszerben az üzembiztonság és a termelésirányítást ellátó informatikai rendszerben fizikai és logikai biztonságról is gondoskodnunk kell. Ezenkívül egyre gyakoribb a termelő rendszerekben magukban a számítástechnika alkalmazása, ahol szintén fizikai és logikai védelmet kell alkalmazni;
- a három alrendszerben az erőforrások között jelen van a humán erőforrás is, ami a humán biztonságot helyezi előtérbe;
- a vállalatoknál egységes Iratkezelési Utasítás, Adatvédelmi és Adatbiztonsági Szabályzat, valamint Titokvédelmi Utasítás van.

A biztonsági alrendszerekben valójában a következő biztonsági struktúráról beszélhetünk:

a. szervezési (adminisztratív és humán) biztonság

- biztonsági szervezet és működése (integrált biztonsági infrastruktúra),
- papír és elektronikus alapú iratok biztonsága (Iratkezelési Utasítás),
- az adat és az egyéb erőforrások biztonság érzékenységük szerinti kezelésének szabályai (Adatvédelmi Szabályzatok, Titokvédelmi Utasítás),

- humán biztonság (humán biztonsági politika),
- biztonság a harmadik felekkel kötött szerződésekben (biztosítás, outsourcing, szerviz szerződések, SLA-k);

b. technikai biztonság

- fizikai biztonság
 - fizikai hozzáférés védelem (belépés, mozgás ellenőrzés, behatolás védelem),
 - fizikai rendelkezésre állás védelme (tűzvédelem, fizikai háttérbiztosítás, akusztikai, elektromos és elektronikus kisugárzás védelem, selejtezés),
- logikai biztonság
 - logikai hozzáférés védelem (informatikai rendszerekben belépés és jogosultság menedzsment, behatolás védelem /pl. tűzfal/, lehallgatás elleni védelem),
 - logikai rendelkezésre állás védelme (újraindíthatóság biztosítása, vírus védelem, logikai rombolás elleni védelem /pl. tűzfal, behatolás detektálás-IDS, illetve védelem IPS/, logikai háttér biztosítás),
 - életciklus védelem (rendszerek, folyamatok, alkalmazások életciklusának [fejlesztés, beszerzés, átadás/átvétel, üzemeltetés, selejtezés] védelme,
 - hálózatok (beszéd és adat hálózatok) védelme (pl. titkosítás, elektronikus aláírás).

5.5.2.A biztonsági alrendszerek közötti összefüggések.

Az előbbiek szerint tehát a szervezési és a technikai védelmi intézkedések egyaránt előfordulhatnak bármelyik biztonsági alrendszerben, és egy vállalatnál nem lehet pl. több egymástól független biztonsági politika (Szabályzat).

Továbbá pl. az Iratkezelési Utasítás ma már egyaránt vonatkozik a papíralapú és az elektronikus iratokra. A Titokvédelmi Utasítás pedig foglalkozik nemcsak a személyes adatok és egyéb adatok, hanem minden további biztonság érzékeny erőforrás titokvédelmi osztályozásával. Pl. titkos papíralapú iratok tárolásával (helyiségek osztályozása) vagy titkos osztályozású papíralapú iratok elektronikus továbbításával, vagy a kinyomtatott titkos minősítésű informatikai outputok védelmével. A termelési rendszerben vagyonvédelmi (pl. a

technológiát védő), a termelésirányító rendszerben informatikai védelmi intézkedések, a vagyonvédelmi alrendszerben az informatikai védelmi intézkedések is szükségesek.

Mind ebből következik, hogy a három alrendszerben a fentiekben megadott biztonsági összetevők egyaránt előfordulhatnak, így ma már indokolt és az egyik biztonsági alapkövetelmény a rendszer szemléleten alapuló integrált, vállalati szintű védelmi rendszer kialakítása.

A védelmi intézkedések a három biztonsági alrendszerben, és példák az átfedésre:

Alrendszerek⇒ Védelmi intézkedések ↓	1. Vagyon-biztonsági alrendszer	2. Üzembiztonsági alrendszer		3. Informatikai biztonsági alrendszer
		Termelési rendszer	Termelés irányító r.	
SZERVEZÉSI Humán Véd. int.	Humán politikai védelmi intézkedések			
Biztonsági szervezet és működés	Integrált biztonsági szervezet, és működés			
Adat és titok Kezelés	Adatvédelmi, Adatbiztonsági Szabályzatok Titokvédelmi Utasítás			
Iratkezelés	Iratkezelési Utasítás (papír és elektronikus)			
Biztonság a Szerződésekben	Szolgáltatási, karbantartási, szállítási, biztosítási szerződésekben a biztonsági követelmények			
TECHNIKAI Fizikai hozzáférés védelem	Fizikai hozzáférés védelem (belépés és mozgás ellenőrzés, behatolás védelem)			
Fizikai rendelkezésre állás biztosítása, biztonsága	Erőforrás és rendszer fizikai háttérbiztosítás, tűzvédelem, kisugárzás védelem, energiaellátás folyamatossága	← Az előző + a termelési rendszer specifikus rendelkezésre állás biztosítása	Erőforrás és rendszer háttérbiztosítás, tűzvédelem, kisugárzás védelem, energiaellátás biztosítása	
Logikai hozzáférés védelem	Logikai belépés és behatolás védelem	← Az előző + a termelési rendszer specifikus hfv.	Logikai belépés, és behatolás védelem	
Logikai rendelkezésre állás biztosítása	Erőforrás és rendszer logikai háttérbiztosítás, ki- és besugárzás védelem	← Az előző + termelési rendszer specifikus, logikai rendelkezésre állás biztosítása	Erőforrás és rendszer logikai háttérbiztosítás, ki- és besugárzás védelem	
Életciklus védelem	A teljes életciklus alatt a biztonsági követelmények biztosítása			
Hálózatok védelme	A hálózat és a továbbított adatok védelme	A termelési rendszeren továbbított félkész és kész termékek védelme	A hálózat és a továbbított adatok védelme	

5.6. EGYENSZILÁRDSÁG

5.6.1. Rendszer szemlélet

A védelmi rendszer integrált kiépítése a vállalat, mint rendszer megközelítését, azaz rendszerszemléletet kíván meg. Ez nem kevesebbet jelent, mint azt, hogy a védelmi rendszert az egész vállalatra tekintve egységesen kell kiépíteni. Nem lehetséges a biztonsági kockázatokat megfelelően csökkenteni, ha egyes kiragadott problémákat oldunk meg, pl. a belépés ellenőrzés önmagában nem nyújt megfelelő védelmet, csak további védelmi intézkedésekkel együtt. Hasonlóképpen informatikai védelem vagyonvédelem nélkül nem hozhatja a kívánt eredményt.

5.6.2. Egyenszilárdság elve

A rendszerszemlélettel kialakított védelem azonban még mindig kevés. A támadó a támadás előkészítésére általában sok idővel rendelkezik, ezért kikeresheti a védelmi rendszer gyenge pontját, és ott támad majd. Vigyázat! Gyenge pont a megkerülhetőség kockázatát képezi, és olyan hatással, hogy az egyik alrendszeren belüli gyengeség a másik alrendszer(-ek) megkerülhetőségét eredményezi. Az Internetről letölthetők szabadon olyan scanner programok, amelyek egy tűzfalnál akár 200 gyengeséget tudnak találni, amelyek erős behatolási lehetőséget jelentenek a támadó számára, azaz a megkerülhetőséget. Ez ellen csak erős behatolás, illetve hozzáférés védelmi rendszer plusz biztosításával lehet védekezni.

- Az egyenszilárdság elve kimondja, hogy a hatékony védelem előfeltétele a vállalat minden pontján legalább azonos erősségű és ellenálló képességű védelmi intézkedések alkalmazása.

Egy rendszer, elsősorban az információ rendszer, illetve informatikai termékek erősségét, biztonsági szempontból authorizált szervezetek minősítik (lásd pl. MSZ ISO/IEC 15408-as szabvány).

Felvetjük, hogy például az azonos erősséget az ellenálló képesség értékelésével is megadhatjuk.

- Az ellenálló képesség (E) azt fejezi ki, hogy az alrendszer milyen szakértelemmel és erőforrásokkal rendelkező lehetséges támadásokat tud visszaverni, azok sikerét megakadályozni.

Az ellenálló képességet a kockázat elemzés eredményeképpen kapott kockázatok határozzák meg. Azaz a kapott kockázatok közül a legnagyobbhoz (XL) (ha ilyen van), a leggyengébb minősítés tartozik, *tehát növekvő kockázat esetén csökken az ellenálló képesség, és fordítva*. Egy rendszer

- ⇒ **NEM ELLENÁLLÓ**, ha a rendszerben gyakorlatilag nincsenek védelmi intézkedések,
- ⇒ **NYILVÁNVALÓAN ELLENÁLLÓ**, ha a védelmi intézkedések egyszerű szakértelemmel és erőforrásokkal rendelkező nyilvánvaló, illetve véletlen támadás ellen védenek,
- ⇒ **MÉRSÉKELTEN ELLENÁLLÓ**, ha a védelmi intézkedések korlátozott alkalmakkal és szakértelemmel, illetve erőforrásokkal rendelkező közepes támadás ellen védenek,
- ⇒ **MAGASAN ELLENÁLLÓ**, ha a védelmi intézkedések magas, kifinomult szakértelemmel és erőforrásokkal rendelkező támadás ellen védenek.

Az alábbi táblázaton bemutatjuk a támadási potenciál (T_p), a bekövetkezési valószínűség (P), a kockázat (K) és az ellenálló képesség összefüggését (E).

↓ T_p	↑ P	↑ K	↓ E
VS	XL	XL	NYILVÁNVALÓ
S	L	L	NYILVÁNVALÓ
M	M	M	MÉRSÉKELT
L	S	S	MAGAS
XL	VS	VS	MAGAS

A nyilak a növekedés irányát mutatják, azaz **annál nagyobb T_p** szükséges a sikeres támadáshoz

- ⇒ **mennél nagyobb** a támadás visszaverésének ellenálló képessége (**E**).

Az eljárás során feltételezzük, hogy minden veszélyforrás feltárássra került.

K.D. Mitnick [lásd 8.] most megjelent könyvében azt írja:

A social engineering a befolyásolás és rábeszélés eszközeivel megtéveszti az embereket, manipulálja, vagy meggyőzi őket a támadó, hogy tényleg az, akinek mondja magát. Ennek eredményeként képes az embereket információ szerzés érdekében kihasználni.

Pl. egy erős logikai hozzáférés védelmi rendszerbe a behatolást el lehet úgy is érni, hogy e módszerrel szerzi meg a behatoláshoz szükséges információkat (pl. jelszó). Ez a megtévesztésen alapuló eljárás úgy válik lehetségessé, hogy a védelem nem egyenszilárdságú, a humán erőforrás nincs felkészítve az ilyen jellegű támadásra, és a biztonsági tudatossága nem megfelelő színvonalú. Ezt a műveletet hívják megkerülésnek.

Megkerülésnek számtalan módja van. Pl. egy erős tűzfallal és behatolás védelemmel, valamint erős hozzáférés védelemmel rendelkező rendszernél a támadó nem fog az Internet felől behatolni. Megkeresi a fizikai védelem gyenge pontját, és ott behatolva az egyéni munkahelyre (PC-re) felragasztott jelszóval lép be. Az információ rendszerek és a beléptető rendszerek többsége nem véd pl. az ellen, ha egy jelszóval két ember lép be.

A biztonságértékelő rendszerek a rendszerek minősítésénél a meg nem kerülhetőséget követelménynek tekintik. Az informatikai minősítéshez használt biztonságértékelő rendszerek:

- A CC 2.1 nemzetközi informatikai termék biztonságértékelési szabvány, ilyenek még az ISO/IEC 15408, TCSEC amerikai szabvány és ITSEC európai szabványok. Megjegyezzük, hogy egzakt azonosságot nem lehet kimutatni közöttük. Időközben megjelent a CC 2.1 magyar szabványként is, MSZ ISO/IEC 15408 1-3 kötet. Az értékelést akkreditált szervezetek végezhetik el. Az alábbi összehasonlítások e szabványok funkcionális és garanciális osztályait hasonlítják össze. A funkcionális osztályok összehasonlítása (amelyek a védelmi intézkedéseket adják meg):

CC	TCSEC, ITSEC
Átvilágítás (FAU)	Átvilágítás
Távközlés (FCO)	Adat csere
Felhasználói adatvédelem (FCS)	Hozzáférés védelem Pontosság Objektum újra felhasználás

<i>Személyes adatok védelme (FPR)</i>	
<i>Azonosítás, hitelesítés (FIA)</i>	<i>Azonosítás, hitelesítés</i>
<i>Bizalmas biztonsági funkciók védelme (FPT)</i>	
<i>Erőforrás felhasználás (FRU)</i>	<i>Szolgáltatás megvalósíthatósága</i>
<i>TOE Hozzáférés (FTA)</i>	<i>Hozzáférés védelem</i>
<i>Rejtjelezési támogatás (FCS)</i>	
<i>Biztonság Menedzsment (FMT)</i>	
<i>Bizalmas útvonal/Csatornák (FTP)</i>	<i>Hozzáférés védelem</i> <i>Adatcsere</i>

A garanciális szintek (amelyek azokat az intézkedéseket adják meg, amelyek gondoskodnak arról, hogy a védelmi intézkedések kikényszerítsék a biztonsági követelményeket) összehasonlítása:

CC	TCSEC	ITSEC
EAL0	D	E0
EAL1		
EAL2	C1	E1
EAL3	C2	E2
EAL4	B1	E3
EAL5	B2	E4
EAL6	B3	E5
EAL7	A1	E6

A vagyonbiztonsági és a termelési alrendszerek biztonsági értékelésére sem szabványok, sem egyéb ajánlások nem ismertek.

5.7. BIZTONSÁGIRÁNYÍTÁS

5.7.1.A biztonságirányítás fogalma

A biztonságirányítási rendszer készítése és karbantartása gondoskodás a garanciákról, hogy a biztonsági tevékenységeket meghatározó Biztonsági Stratégia megfeleljen az üzleti céloknak, és legyen konzisztens a törvényekkel és szabályokkal, valamint rendeltetésszerűen legyen végrehajtva.

A biztonságirányítás céljai

- az üzlet lehetővé tétele és maximalizálása,

- az erőforrások felelősséggel való használata,
- a kockázatok megfelelő menedzselése.

5.7.2.A biztonságirányítás módszerei

A biztonságirányításra különböző módszertanok vannak, ezek mindegyike az üzleti cél érdekében az üzleti követelmények között szereplő biztonsági követelmények teljesítésének a módszereit határozza meg. Ilyen módszertanként használhatjuk az ISACA által kidolgozott vállalatirányítási modellt (Enterprise Governance), a BS 7799:2000 brit információ menedzsment szabványt (melyet időközben váltott a nemzetközi ISO/IEC 27001:2005), illetve a szabvány első fejezetének magyar változatát az MSZ ISO/IEC 17799-t. A szerző által kidolgozott Biztonság Menedzsment Módszertan (Security Management Methodology, SMM 5.6).

A biztonságirányítás módszerei között szerepel:

- a biztonsági auditálás, kockázatok elemzése,
- a kockázatok csökkentésére teendő védelmi intézkedések,
- a biztonsági stratégia és politika, az Üzletmenet Folytonossági Terv (ÜFT), a biztonsági események kezelése,
- biztonság tudatosság kialakítás, valamint a biztonsági kultúra elterjesztése.

5.8. A VÁLLALATI BIZTONSÁG MEGVALÓSÍTÁSA

5.8.1.A vállalati biztonság szervezése

A vállalati biztonság szervezése az a tevékenység, amellyel egy a menedzsment által elhatározott szintű biztonság megteremtésére teszünk intézkedéseket, a folyamatos és rendeltetésszerű működés érdekében. Ez a következő lépések végrehajtásának rendjét, illetve sorrendjét határozza meg, amelyeket mind a három rendszerre el kell készíteni (habár a termelési rendszerrel, az üzembiztonsággal, annak vállalatonkénti eltérése miatt nem foglalkozunk).

A biztonság szervezés szintjei (lépései) a Common Criteria alapján:

AZ ALAP		A feladat		AZ EREDMÉNY
		❶ SZINT		
JOGSZABÁLYOK, ÜZLETI STRATÉGIA BELSŐ SZABÁLYOK ERŐFORRÁSOK MŰKÖDŐ VÉDELEM	⇒	Mit kíván az üzleti érdek?	⇒	BIZTONSÁGI KÖRNYEZET AZONOSÍTÁSA
		❷ SZINT		
BIZT.-I KÖRNYEZET FENYEGETÉSEK	⇒	Mi a gyakorlat?	⇒	KOCKÁZATOK
		❸ SZINT		
KOCKÁZATOK	⇒	Mit kell elérni ?	⇒	BIZTONSÁGI KÖVETELMÉNYEK
		❹ SZINT		
BIZTONSÁGI KÖVETELMÉNYEK	⇒	Mit, hogyan kell védeni?	⇒	VÉDELMI INTÉZKE- DÉSEK SPECIFIKÁCIÓJA
		❺ SZINT		
VÉDELMI INTÉZKEDÉSEK IMPLEMENTÁLÁSA	⇒	Hogyan kell megvalósítani?	⇒	BIZT. ALRENDSZER

A biztonságszervezés lépései (a végrehajtás sorrendjében):

1. Adat és Titokvédelmi utasítások készítése
2. Iratkezelési Utasítás készítése
3. Biztonsági Átvilágítás, amely áll
 - 3.1. a helyzetfeltárásból (a rendszer és a működő védelmi intézkedések gyengeségeinek a feltárása, a környezeti veszélyforrások azonosítása),
 - 3.2. a veszélyforrás elemzésből (a feltárt gyengeségek következményeinek elemzése) és
 - 3.3. a kockázatelemzésből (a feltárt gyengeségek bekövetkezési valószínűségének és a lehetséges kárkövetkezmények elemzése). Szükséges a veszélyforrás- és kockázatelemzés rendszeres (min. 2 évenkénti vagy ISO 27001 szerint évenkénti és kockázat arányos) karbantartása.
 - 3.4. A csökkentendő kockázatok, és a csökkentésükre védelmi intézkedések meghatározása

4. A Biztonsági Stratégia készítése, amely a felső vezetés elkötelezettségét határozza meg, egy konkrét erősségű védelem kialakítása mellett, valamint meghatározza az Üzleti Stratégia szerinti üzleti cél és követelmények megvalósításához szükséges biztonsági elvárásokat, így

4.1. a biztonsági célt (bizalmasság, sértetlenség, rendelkezésre állás, valamint egyes szabványok szerint számon kérhetőség és garanciák),

4.2. a biztonsági követelményeket, amelyek azokat biztonsággal összefüggő funkcionális és garanciális követelményeket jelentik, amelyek hivatottak a biztonsági cél megvalósulását, sőt kikényszerítést biztosítani. Szükséges a Biztonsági Stratégia rendszeres (min. 3 évenkénti) karbantartása.

5. A Biztonsági Szabályzat (ISO/IEC 27001 szerint) meghatározza a megvalósítani kívánt biztonsági intézkedéseket, esetleg szabványokat. Szükséges rendszeres (min. 2 évenkénti vagy ISO 27001 szerint évenkénti) karbantartása a bizalmasságot, sértetlenséget és az elvárt rendelkezésre állást biztosító védelmi intézkedések, valamint a fennálló kockázatok csökkentéséhez szükséges további biztonsági intézkedések feltárása céljából. Az intézkedések széles körűek, és magukba foglalják pl. az erőforrások biztonsági beállításainak előírását, a biztonságos üzemeltetés feltételeinek a meghatározását, külső és belső támadások megelőzésére fogantatandó biztonsági megoldásokat, intézkedéseket biztonsági szervezet hatékony működtetésére, a biztonsági események kezelésére, naplózására stb. Szükséges a biztonsági szabályzat rendszeres (min. 2 évenkénti vagy ISO 27001 szerint évenkénti) karbantartása és oktatása.

6. Az Üzletmenet Folytonossági Terv (ÜFT) meghatározza a katasztrófa bekövetkezése esetén az üzletmenet folytonosságának biztosításához szükséges helyettesítő, valamint az eredeti, katasztrófa előtti működés helyreállításához szükséges visszaállító eljárásokat. Szükséges az ÜFT rendszeres (évente többszöri) karbantartása, tesztelése és oktatása.

7. A Biztonság Ellenőrzése folytonos monitorozással és rendszeres belső és külső auditok útján biztosítható. Külső audit akkor indokolt, ha jogszabály vagy felettes szerv az auditálást végző szervezet/személyek vállalattól való függetlenségét írja elő.

8. A Biztonsági Program, illetve akciótervek a fentiek végrehajtására teendő intézkedéseket tartalmazzák.

Felhívjuk a figyelmet arra, hogy külföldön a Biztonsági Szabályzat szakkifejezés ismeretlen, helyette a Biztonsági Politikát (Security Policy) használják. Hazánkban elterjedt a Biztonsági Szabályzat használata. Az MSZ ISO/IEC 17799-es magyar szabvány készítői (az eredeti angol nyelvű szabvány fordítói) az angol Security Policy-t Biztonsági Szabályzatként fordították le. Az angol policy szónak a jelentése tágabb mint a magyar politika, a Security Policy kifejezés inkább a Biztonsági Szabályrendszerhez hasonlatos.

5.8.2. Biztonság tudatosság alapjai

Ahogy a fenti definícióból látható, a biztonság tudatosság egy viselkedésbeli, hozzáállásbeli változást, változtatás kíván meg. Ezek a változások soha nem egyszerűek. Ezekhez a változásokhoz az alábbi öt feltétel szükséges egy szervezetnél:

- menedzsment elkötelezettség
- felelősségre vonhatóság
- dedikált erőforrások
- formális és folyamatos biztonság tudatosság program, (továbbá hogy a programot mindenki magáénak érezze)
- szükség esetén más osztályok / szervezetek bevonása

5.8.3. Néhány biztonságszervezési feladatról

5.8.3.1. Adatok és titkok osztályozása

A vállalatok olyan adatokkal is dolgoznak (személyes és egyéb üzleti titkot képező adatok), amelyek biztonság érzékenyek. Az erőforrások (pl. eszközök) és helyiségek is lehetnek biztonság érzékenyek, ha azok üzleti titkot dolgoznak fel vagy őriznek. A biztonság érzékenységek függvényében az adatokat, eszközöket és helyiségeket, osztályozni kell, amely azt a célt szolgálja, hogy azokhoz különböző erősségű védelmi szintek legyenek rendelhetők. A minősítés az államtitkokra és szolgálati titkokra vonatkozó eljárások, hasonló az osztályozáshoz. A különböző szakkifejezések használatának oka, hogy minősítésre jogosultságot jogszabályok állapítanak meg, míg az osztályozás a védelem kialakításának egyik szabványokban meghatározott előfeltétele. Mindezt a Titokvédelmi Utasításban kell meghatározni.

2004 január 1-én hatályba lépett az 1992. évi LXIII. tv. módosítása, amely a személyes adatok védelmével foglalkozik. A törvény alapján személyes adatok kezelését végző vállalatoknak Adatvédelmi Szabályzatot és Adatbiztonsági Szabályzatot kell készíteni, adatvédelmi felelőst kell kinevezni. A Titokvédelmi Utasítás az üzleti titkot képező adatok, az Adatvédelmi Szabályzat a személyes adatok védelmére fogalmazza meg az eljárásokat. Ha az adatbiztonságról beszélünk, lényeges tehát megkülönböztetni, hogy a személyes és/vagy az üzleti titkot (egyéb titkot) képező adatok biztonságáról van szó.

5.8.3.2. A kockázat menedzsment

- A kockázat az erőforrások bizalmassága és/vagy sértetlensége és/vagy rendelkezésre állása sérülésének valószínűsége.

A kockázatmenedzsment célja, hogy a vállalaton belül átfogóan, veszélyforrásonként meghatározza, hogy a veszélyforrás bekövetkezése milyen káros következményekkel járhat, és ennek alapján eldöntsük a szükséges védelmi intézkedéseket, azaz a kockázat csökkentésére teendő védelmi intézkedéseket. A kockázatot meghatározó tényezők a fenyegetettség, a bekövetkezési valószínűség és a kárkövetkezmény, részletesen:

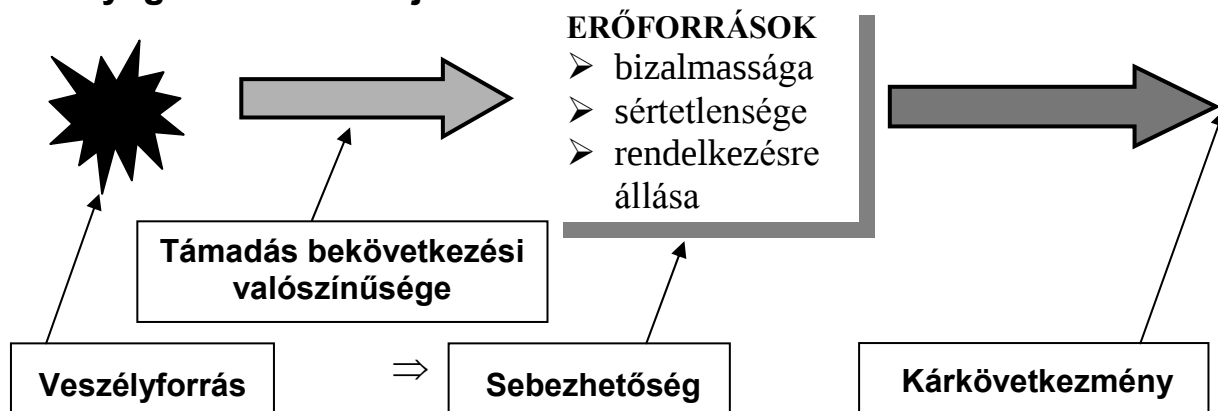
⇒ *a fenyegetettség (T)*

- *a támadás lehetőségét jelenti egy vagy több erőforrásra,*
- *egy olyan állapot, amelyben az erőforrások által kezelt adatok felfedésre (bizalmasság), módosításra (sértetlenség) vagy elpusztításra kerülhetnek (rendelkezésre állás).*
- *támadást eredményezhet egy külső vagy belső veszélyforrásból kiindulva az erőforrások bizalmassága és/vagy sértetlensége és/vagy rendelkezésre állása ellen.*

A támadás, amennyiben sikeres, az erőforrások biztonsága sérül. A támadás módszere lehet aktív vagy passzív. Az *aktív támadási módszer* behatol a rendszerbe, és ott fejti ki tevékenységét. A *passzív támadási módszer* a rendszer környezetére gyakorolt akusztikus, illetve elektromágneses hatás, a támadás nem hatol be a rendszerbe, hanem a környezetében fejti ki a hatását.

Az alábbiakban az informatikai kockázatmenedzsmenttel foglalkozunk, a másik két területre javasoljuk az alábbiakat mintának tekinteni.

A fenyegetés struktúrája:



⇒ A bekövetkezési valószínűség (P).

Bekövetkezési valószínűség annak az esélye, hogy a veszélyforrás támadás formájában megvalósuljon, azaz a fenyegetettség bekövetkezzék. A bekövetkezési valószínűség lehet: kicsi (**S**), közepes (**M**), nagy (**L**), vagy igen nagy (**XL**).

⇒ A kárkövetkezmény, V)

Támadás esetén annak esélye, hogy az erőforrás megsérül és kárkövetkezmény keletkezik. A támadás bekövetkezésekor a teljes rendszer vagy egy eleme sérülhet (a lehetséges kárkövetkezmény), eszerint a sebezhetőség lehet

- globális (**G**), azaz valamennyi erőforrás folyamatos működése megszakad rövid (S), közepes (M) vagy hosszú (L) időre, vagy
- részleges (**R**), azaz csak egyes erőforrások sérülnek rövid (S), közepes (M), és hosszú (L),

⇒ A kockázat (K)

A kockázatot (**K**) a **KOCKÁZATI MÁTRIX** segítségével, azaz a bekövetkezési valószínűség (P) és a sebezhetőség (V) becsült értékeinek egybevetésével kaphatjuk meg (az alábbi táblázat). A kockázat lehet kicsi (**S**), közepes (**M**), nagy (**L**) vagy igen nagy (**XL**).

A kockázatok nagysága az egyes biztonsági alrendszerekben eltérhet egymástól, így azonos fenyegetettség képezte kockázat az egyes biztonsági

alrendszerekben más-más védelmi intézkedéseket kíván meg.

A kockázat nem csökkenthető nullára, így mindig van maradék kockázat, amely hasonlóan a kockázathoz, lehet: **S, M, L, XL**.

Néhány nagy kockázat az egyes biztonsági alrendszerekben, a téma kutatását végzők tapasztalatai alapján becsülve:

- üzleti alrendszerben nagy kockázatot képeznek a humán veszélyforrások és a jogosulatlan fizikai hozzáférések,
- termelési alrendszerben nagy kockázatot képeznek a humán veszélyforrások és a technika rendelkezésre állásának zavarai,
- informatikai biztonsági alrendszerben nagy fenyegetést képeznek a humán veszélyforrások és jogosulatlan a logikai hozzáférések.

A kockázati mátrix egy adott veszélyforrásra vonatkoztatva bekövetkezési valószínűség (probability, P) és az általa okozott kárkövetkezmény függvényében ábrázolja a kockázatot (Részleges kárkövetkezmény: R, a Globális kárkövetkezmény: G). A kockázati mátrix ismerete lehetőséget teremt a kockázatok kezelés módjának eldöntésére, a védelmi intézkedés szükségességének és erősségének a meghatározására.

Veszélyforrás neve	Fenyegetettség	Bekövetkezési valószínűség	Kárkövetkezmény	Kockázat	Maradék kockázat	Védelmi intézkedés
Tűz	Rendelkezésre állás	M	G L	L	S	Tűzvédelem

A fenyegetettség megsértheti a bizalmasságot, a sértetlenséget ill. a rendelkezésre állást, vagy ezek kombinációját.

A bekövetkezési valószínűség és a kárkövetkezmény függvényében a kockázat lehet: VS= igen kicsi, S= kicsi, M= közepes, L= nagy, XL= igen nagy.

5.8.3.3. A kockázatok csökkentése

A kockázatok csökkentésére a védelmi intézkedések (kontrollok) szolgálnak, amely a COBIT 3 szerint:

- azok a politikák, folyamatok, gyakorlatok és szervezeti struktúrák, amelyeket arra terveztek, hogy ésszerű garanciát adjanak az üzleti célok elérése érdekében, a nem kívánt események megelőzésére, jelzésére, kivédésére.

A védelmi intézkedések az 5.5.2.4, 5, és 6-ban megadott struktúrába sorolhatók be, és ezt a következő két oldalon a táblázatok mutatják.

A táblázatok a fentiekben leírtaknak megfelelően nem tartalmazzák az üzembiztonsági védelmi intézkedéseket, mivel azok a termelés adottságaitól függenek. Könnyű belátni ezt, ha arra gondolunk, hogy egy vegyi üzem vagy egy élelmiszeripari termelő vállalatnál mennyire különböznek az üzembiztonság védelmi követelményei.

5.8.3.4. Védelmi intézkedések köre I (a biztonsági alrendszerekben)

A. RÉSZLEGES

I. SZERVEZÉSI

1. szabályozás

1.1. titokvédelmi szabályzat, osztályozás

1.2. integrált biztonsági szervezet

1.3. iratkezelés

2. humánpolitikai

védelmi intézkedések

2.1. munkaviszony létesítés és megszüntetés

2.2. teljesítménykövetés

2.3. feladatszétválasztás

2.4. oktatás, biztonsági tudatosítás

3. szerződések

3.1. biztosítás

3.2. biztonsági

követelmények a harmadik fél felé

5.8.3.5. Védelmi intézkedések köre II (a biztonsági alrendszerekben)

A. RÉSZLEGES (Biztonsági Szabályzat - Politika)

II. TECHNIKAI

2. fizikai (vagyon)védelmi intézkedések

2.1.aktív támadás elleni

hfv*

2.1.1.objektum védelem

2.1.2.belépés és mozgás ellenőrzés

2.1.3.behatolás védelem

2.1.4.értéktárolás védelem

2.1.5.értékszállítás védelem

2.1.6.üres íróasztal és képernyő politika

2.2.passzív támadás elleni

hfv

2.2.1.sugárzás elleni védelem

2.3.rendelkezésre állás

2.3.1.megbízhatóság

2.3.2.redundancia

2.3.3.energiaellátás

2.3.4.villámvédelem

2.3.5.tűzvédelem

2.3.6.dokumentáció

*Hfv= hozzáférésvédelem

1. logikai

(informatikai)védelmi int.-ek

1.1.aktív támadás elleni

hfv

1.1.1.jelszó mgm

1.1.2.jogosultság mgm

1.1.3.hitelesítés

1.1.4.tanúsítás

1.1.5.időbélyegzés

1.1.6.behatolás védelem

1.1.7.tűzfal

1.2. passzív tám. elleni

hfv

1.2.1.rejtjelezés

1.2.2.titokmegosztás

1.3. rendelkezésre állás

1.3.1.mentés,
újraindítás

1.3.2.vírusvédelem

1.3.3. logikai rombolás

1.4.Számon kérhetőség biztosítása

3. Hálózati véd int.-ek

3.1. Fizikai védelem

3.2. **Bizalmas útvonal**

3.3. Tartalom hitelesítés

3.4. Partner hitelesítés

3.5. Letagadhatatlanság

3.6. Eszköz hitelesítés

3.7. Tanúsítás (PKI)

3.8. Tűzfal

3.9. Behatolás védelem

4. Életciklus védelme

4.1. Fejlesztés véd.

4.2. Átadás/átvétel véd.

4.3. Üzemeltetés véd.

4.4. Selejtezés véd.

5.8.3.6. Védelmi intézkedések köre III (a biztonsági alrendszerekben)

ÁTFOGÓ (ÜFT)

I. SZERVEZÉSI

II. TECHNIKAI

1. szabályozás

- 1.1.katasztrófaminősítés
- 1.2.katasztrófa teamek szervezése
- 1.3.katasztrófa-terv karbantartása
- 1.4.oktatás

2. szerződés

- 2.1.biztosítás a folyamatos működésre
- 2.2.üzemi háttérszerződés
- 2.3.szállítói háttérszerződés

1.rendelkezésre állás védelme

- 1.1.visszaállítás
- 1.2.hátterek, háttér eljárások
- 1.3.katasztrófakezelő központ
- 1.4.helyreállítás

A BETŰTÍPUSOK JELENTÉSE

(a védelmi intézkedés mit véd?):

Ariel black = címsor

Ariel = bizalmasság

Ariel = sértetlenség

ARIEL = bizalmasság és sértetlenség

Courier new = rendelkezésre állás

Courier new = mind a három

5.8.3.7. A védelmi intézkedések üzemeltetése

A védelmi intézkedések üzemeltetése (amely a Biztonsági Szabályzat valójában) alatt a védelmi intézkedés

⇒ működtetését, illetve végrehajtását (szervezési védelmi intézkedéseknél), valamint

⇒ karbantartását értjük.

Értelemszerűen az egyes védelmi intézkedések üzemeltetésének szabályozásánál mind a hárommal foglalkozni kell. A szervezési védelmi intézkedéseknél (pl. humánpolitika), mivel azok utasítás formájában valósulnak meg, végrehajtásról, míg a technikai védelmi intézkedéseknél működtetésről lehet szó. A technikai védelmi intézkedések egy része azonban nem igényel működtetést, de karbantartást viszont igen (pl. Faraday kalitka, vagy egy helyiség speciális falazata).

A védelmi intézkedések tulajdonosai:

- A tulajdonos egy adatgazda, vagy rendszergazda, vagy menedzser, aki egy meghatározott adatállományért, vagy egy folyamatért (alkalmazói rendszerért), vagy a védelmi intézkedésekért felelős (ez nem vonható össze az előbbiekkal).

Azaz a tulajdonos folyamatosan felelős azért, hogy a hatáskörében a védelmi intézkedések megfeleljenek a jogszabályoknak, belső szabályzatoknak, és a gyakorlatban megfelelő szintű védelmet nyújtsanak (kikényszerítsék a biztonsági követelményeket).

- * A szervezési védelmi intézkedések üzemeltetésén végrehajtásukat és napra készen tartásukat, a technikai védelmi intézkedések üzemeltetésén működtetésüket, és karbantartásukat értjük.

TULAJDONOSOK

VAGYON ÉS INFORMATIKAI BIZTONSÁG:

➤ SZERVEZÉSI védelmi intézkedések

- | | |
|-------------------------------------|-------------------|
| • Szervezet és működés szabályozása | Titkárság |
| • Biztonságszervezési dokumentumok | Biztonsági vezető |
| • Titok (adat) védelem szabályozása | Titkárság |

- Iratkezelés szabályozása Titkárság
- Adatvédelem szabályozása Titkárság
- Humán politika Humán erőforrások vezető
- Szerződések (kockázat áthárítás) Gazdasági vezető

➤ TECHNIKAI védelmi intézkedések

⇒ Fizikai védelmi intézkedések A vagyon biztonsági vezető

- Hozzáférés védelem
- Rendelkezésre állás

⇒ Logikai védelmi intézkedések Az informatikai biztonsági vezető

- Hozzáférés védelem (hfv)
- Rendelkezésre állás biztosítása
- Hálózati védelem
- Védelem az életciklus során

ÜZEMBIZTONSÁG:

➤ SZERVEZÉSI véd. int.-ek A fentiek szerint

➤ TECHNIKAI véd. int.-ek

- Termelő rendszerek védelme A termelési biztonsági vezető
- Termelés irányító rendszerek védelme A fentiek szerint
- Informatikai alkalmazások védelme
- Üzleti folyamatok védelme

Ebből következik, hogy a három biztonsági vezető (üzleti, termelési, informatikai) a védelmi intézkedések rendeltetésszerű üzemeltetéséért felelős (ők a védelmi intézkedések tulajdonosai).

5.8.3.8. A biztonsági szervezet és működés

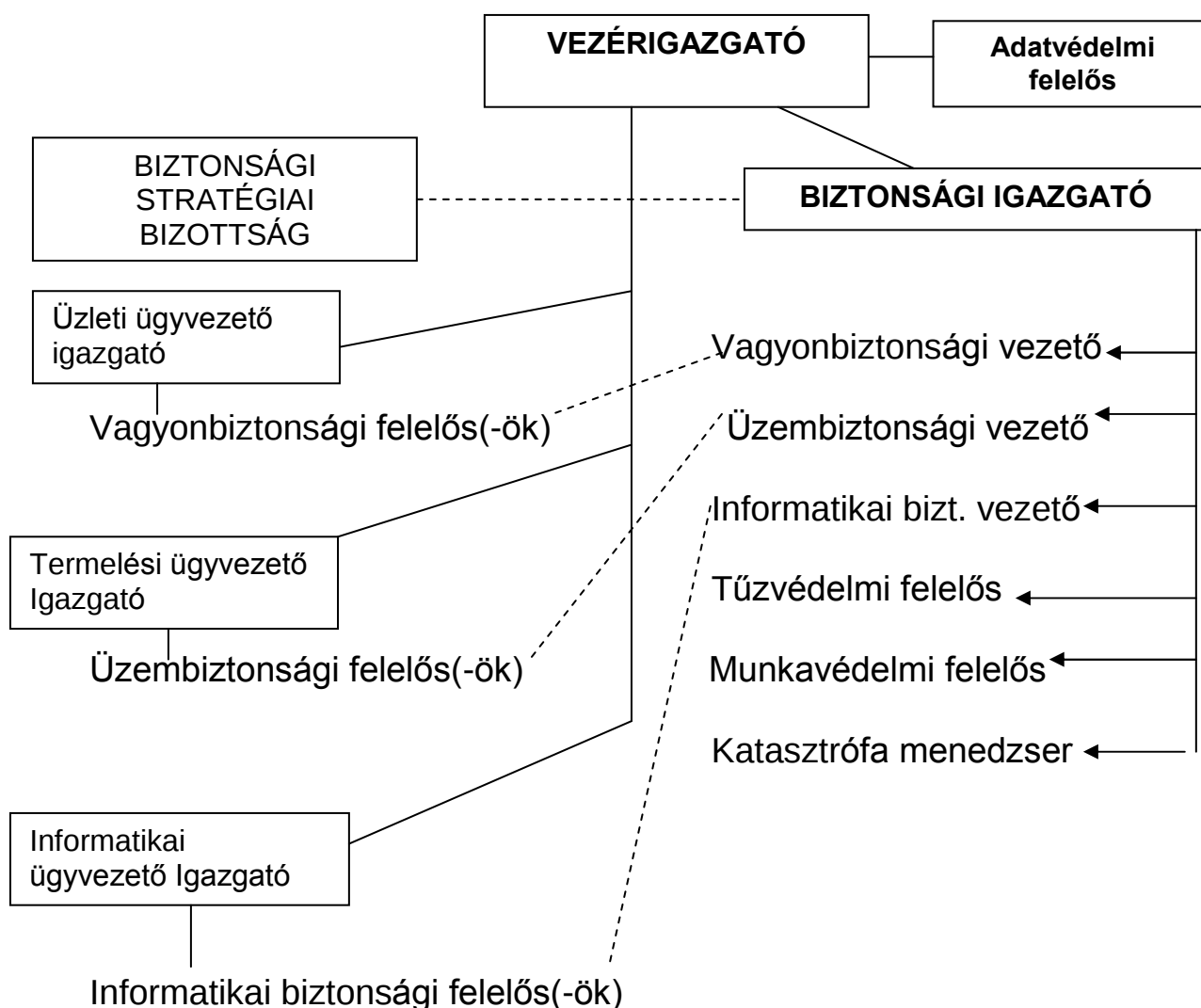
A biztonsági szervezetnek a függetlenségen kell alapulnia, azaz nem lehet alárendelve csak a vezérigazgatónak. Ugyanakkor a három biztonsági alrendszer biztonsági irányítását olyan biztonsági felelősöknek kell végezniük, akiknek a szakmai irányítása nem tartozik a szolgálati főnökük hatáskörébe, hanem a vállalati biztonsági vezető alatt dolgozó három alrendszer biztonsági főnökéhez (lásd ábra). Ez

gondoskodik arról, hogy a biztonsági intézkedések szakmai függetlensége biztosítva legyen.

Itt természetesen nem foglalkozunk csak a technikai biztonsággal, míg a vállalatok gazdasági biztonsága (pl. pénzügyi szervezeteknél: likviditási, átutalási, hírnév, kamat, hitel, jogi, működési biztonság stb.) egy külön téma és külön szervezet. Az együttműködést a két terület között biztosítani kell. A vállalati informatika, vagyon és ha van, üzembiztonság, a működési biztonság része, de külön foglalkozunk vele, mivel az előbbieket gazdasági, gazdálkodási, míg az utóbbi biztonságtechnikai kérdés (BIS állásfoglalás).

A biztonsági szervezeti séma a következő oldalon található.

BIZTONSÁGI SZERVEZETI SÉMA



Jelmagyarázat:

Szolgálati alárendeltség

Szakmai alárendeltség

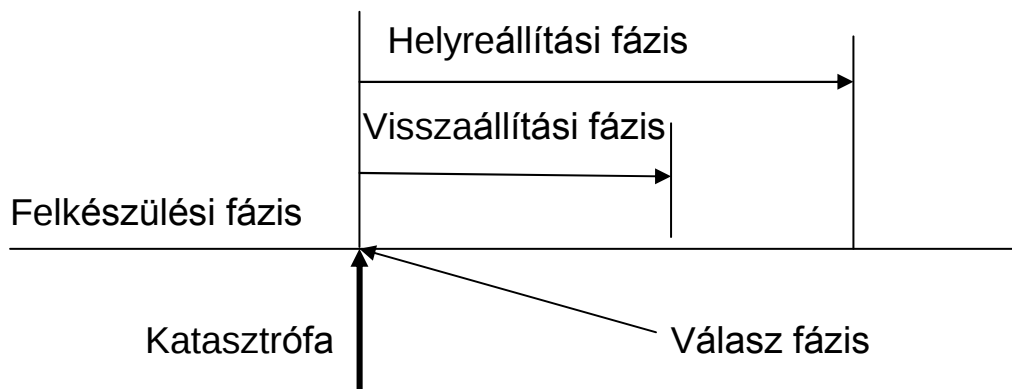
5.8.3.9. ÜFT, és a hátterek megválasztása

Az üzletmenet folytonosság megszakadása a vállalat számára azt jelenti, hogy a küldetését nem tudja teljesíteni. Ezért ezt másképpen katasztrófának is nevezhetjük.

Az ÜFT-nek elsősorban a küldetés kritikus folyamatok lehető legrövidebb ideig tartó kiesésének a feltételeit kell megteremteni.

A katasztrófa elhárításának tervét a katasztrófa elhárítás időbeli lefolyásának meghatározásából kiindulva készíthetjük el, ugyanis az ÜFT nem a katasztrófa megelőzésére, hanem a katasztrófa kárkövetkezményeinek elhárítására szolgál. A katasztrófa megelőzését a Biztonsági Politikában meg határozott védelmi intézkedések szolgálják.

A katasztrófa elhárítás folyamata:



A katasztrófa elhárítás fázisai:

- felkészülési fázis: amelyben a rendszerek és a munkatársak felkészítése (az elhárítás kiépítése, oktatás és az ÜFT karbantartása) történik meg;
- válasz fázis: amelyben bármely időpontban egy meghatározott személy azonosítja a bekövetkezett katasztrófát, és megteszi az elhárítás megkezdéséhez szükséges lépések;
- visszaállítási fázis, amelyben háttér eljárásokkal, rendszerekkel biztosítják az üzletmenet újraindítását, illetve fenntartását (esetleg kompromisszumok árán);
- helyreállítási fázis, amelyben az eredeti erőforrásokkal, általában az eredeti helyen újraindítják az üzletmenetet, és a visszaállításhoz használt erőforrásokat leállítják.

Az előbbiekből is egyértelműen következik, hogy a háttérreljárás a vagyonbiztonsági alrendszerben az üzleti és támogató folyamatok újraindítására, illetve a háttérrendszer az informatikai biztonsági alrendszerben az informatikai alkalmazások újraindítására kell szolgáljon, a lehető legrövidebb idő alatt, és a lehető legkevesebb adatvesztéssel. A szakszerű kiválasztás tehát alapvetően meghatározza az üzletmenet folytonosság biztosíthatóságát.

Az üzleti rendszerben a küldetés kritikus folyamatok megszakadása esetén a háttér eljárások szolgálnak a minimálisan elfogadható szolgáltatások biztosítására, amely lehet

- manuális eljárás,
- fél automatikus eljárás, mint manuális megoldás + számítástechnikai, ügyvitel technikai eszköz (pl. kézi számológép) alkalmazása,
- automatikus eljárás, azaz számítástechnikai eszköz (off-line), és/vagy ügyvitel technikai eszköz alkalmazása.

Az információ rendszerben az alkalmazások kompromisszumos, vagy teljes futtatásához a háttérrendszerek lehetnek:

- *nagy megbízhatóságú (nagy MTBF, Mean Time Between Failures értékű) hw eszközök alkalmazása, és hideg tartalék berendezések biztosítása (ezzel a fizikai rendelkezésre állásnál kell foglalkozni),*
- *magas rendelkezésre állást biztosító rendszerek alkalmazása, mint:*
 - *lokális, vagy távoli passzív redundans háttérrendszer alkalmazása, rövid vagy hosszabb kiesés és adatvesztés kockázatával,*
 - *lokális aktív, hibatűrő redundans háttérrendszer alkalmazása, folyamatos rendelkezésre állás (jelentéktelen adatvesztés és kiesés kockázatával) biztosítására,*
 - *túlélő katasztrófatűrő aktív redundans háttérrendszer, folyamatos rendelkezésre állás (néhány tized másodperc kiesés és adatvesztés kockázatával) biztosítására,*
 - *katasztrófatűrő távoli aktív redundans háttérrendszer alkalmazása, folyamatos rendelkezésre állás (jelentéktelen, és adatvesztést nem okozó kiesés mellett) biztosítására.*

Természetesen mind az üzleti, mind az információ rendszerben, az objektum esetleges kiesése esetére biztosítani kell a vállalat küldetésének, az üzletmenet megszakadás érzékenysége függvényében kialakított, háttér objektumot.

5.8.3.10. Outsourcing

Az elmúlt években igen elterjedt a feladatok, erőforrások harmadikfélllel történő végrehajtása, az outsourcing (az erőforrás kihelyezés).

Ez a megoldás biztonsági szempontból több kockázatot hoz létre. A COBIT 3 megadja, hogy az outsourcing szerződésnek minimum milyen biztonsági garanciákat kell tartalmaznia. Ugyanis ki kell mondani, hogy ebben az esetben nincs közvetlen „hatalmunk” az outsourcing-ba vevő cég felett, azaz például a biztonsági követelményeket a saját elképzelései szerint alakíthatja ki. Ugyanakkor az outsourcing-ba adó cég érdekelt abban, hogy a biztonsági szabályai, a biztonság irányítási rendszere ebben az esetben is egyenszilárdságú maradjon. Az egyetlen lehetőség a szerződésben erre biztonsági garanciákat beépíteni, amely nem tartozik az egyszerű feladatok közé. A fontos az, hogy az ilyen esetekben nem megakadályozni kell a vállalat költségcsökkentési igényeinek realizálását, hanem az informatikai szabványokban - ISO/IEC27799, illetve a COBIT 3-ban - erről megadott követelményeket kell mind a három alrendszerben alkalmazni.

A biztonsági követelmények a szerződésekben:

a cél: fenntartani az egyenszilárdságú vállalati biztonságot akkor is, ha a szervezet tevékenységét, és ezzel a felelősséget (részben vagy egészében) más szervezetnek alvállalkozásba adták ki. Az MSZ ISO/IEC 17799 szerint biztosítani kell:

- a jogi követelményeket kielégítését, pl. az adatvédelmi szabályozást,
- garantált kell legyen, hogy az erőforrás kihelyezésben /alvállalkozásba adásban/ résztvevő valamennyi fél, a további alvállalkozókat is beleértve, tudatában van saját felelősségének,
- biztosított legyen a szervezet üzleti vagyonának sértetlensége és bizalmassága/titkossága,
- a vagyonbiztonsági és informatikai biztonsági *védelmi intézkedések* korlátozzák és behatárolják az outsourcingba

vevő jogosult használóinak a hozzáférését az outsourcing-ba adó szervezet biztonság érzékeny üzleti információihoz /adataihoz,

- a szolgáltatások rendelkezésre álljanak katasztrófa esetében,
- megfelelő vagyonbiztonsági szintek legyenek kialakítva az erőforráshelyezésben/alvállalkozásba adásban érintett berendezések esetében,
- legyen biztosítva az átvilágítás/auditálás joga az outsourcingba adó részére, az outsourcingba vevőnél.

Az outsourcing szerződésen belül célszerű meghatározni a nyújtandó szolgáltatások színvonalát. Erre szolgál a szolgáltatási szint megállapodás (SLA, Service Level Agreement), amelynek a következők szerint kell alakulni:

- a megállapodásnak fel kell vázolnia azokat a feltételeket, amelyek szerint a szolgáltató a speciális szolgáltatásokat nyújt a megbízónak vagy az ő szervezeteinek. A célkitűzés magas színvonalú szolgáltatás nyújtása, amely megfelel az outsourcingba adó szükségleteinek;
- a szolgáltatási szint megállapodást (SLA) a reagálási készség, a teljesítmény, a feldolgozási idő, a biztonság és a rendelkezésre állás határozzák meg.

A COBIT 3 szerint a megállapodásnak legalább a következőket kell tartalmaznia:

- a szolgáltatás meghatározása,
- a szolgáltatás költsége,
- a számszerűsíthető (mérhető) minimális szolgáltatási szint,
- az informatika által nyújtott támogatás szintje,
- rendelkezésre állás, megbízhatóság, bővítési kapacitás,
- az üzletmenet folytonosság tervezése,
- biztonsági követelmények,
- a megállapodás bármely pontjának módosítása esetén a követendő eljárás,
- az érvényességi idő és annak felülvizsgálata/megújítása kizárása,

- a teljesítési jelentések gyakorisága és tartalma, valamint a szolgáltatási díjfizetések, azok reális volta,
- a díjtételek számításának módja,
- a szolgáltatás javítására tett kötelezettségvállalás.

5.8.4. Feladatok a biztonság tudatosság kialakításához

Menedzsment elkötelezettség megszerzése a legfontosabb és talán a legnagyobb kihívás. Egy szervezet vezetése alapvetően profit- és üzletorientált. A profit oldaláról nem érdemes közelíteni, mert a biztonság közvetve nem termel nyereséget, tehát az egyetlen lehetséges megközelítési út az üzleti lehetőségek területén rejlik. A teljes elkötelezettségéhez szükséges a menedzsment számára megvilágítani a biztonság tudatosság pszichológiai hátterét.

Felelősségre vonhatóság

Dedikált erőforrások

Formálisan jóváhagyott és a legfelsőbb menedzsment által támogatott **biztonság tudatossági program** végrehajtásához a legjobb egy letisztult és jól körül határolható tervet készíteni. Ezen tervnek mindenképpen tartalmaznia kell a javasolt intézkedés halmazát, a megközelítést (milyen módon szeretne hozzáfogni a tudatosság kialakításához), valamint az elérni kívánt célokat.

Ebből levezethető, hogy a 21. században ez nem egy egyszeri feladat, hanem egy folyamatos tevékenység. (Az ISO/IEC 27001 alapelve az úgynevezett PDCA ciklus Plan-Do-Check-Act). Ugyanis az elérni kívánt célok évről-évre változnak, az ezekhez kapcsolódó intézkedéseket pedig tudatosan felül kell vizsgálni. Javasolt ezért egy biztonság tudatossági koordinátort megbízni, hogy az elkészült terv megvalósítását folyamatosan figyelje és tartsa karban a biztonsági irányelvek alapján.

6. KISVÁLLALATOK BIZTONSÁGA

A kisvállalatoknál a biztonság alaptevékenységük, küldetésük biztonság érzékenységének függvényében, hasonlóan a nagy vállalatokhoz, meghatározó szerepet játszik. Ugyanakkor a kisvállalatot az jellemzi, hogy

- korlátozottak a létszám lehetőségei (általában 50 főnél kevesebbet foglalkoztat állományában),
- korlátozottak a biztonságra fordítható anyagi eszközei,
- feladatainak jelentős részét erőforrás kihelyezéssel oldja meg.

Felmerül a kérdés, hogy ilyen feltételek mellett, hogyan lehet a küldetés orientált biztonsági igényeket kielégíteni?

A biztonsági szabványok, ajánlások számtalan biztonsági követelményt határoznak meg, és a biztonságértékelési eljárások (akkreditált szervezetek végezhetik) meghatározzák az adott vállalat biztonsági szintjét. A kisvállalat vezetőinek nem kisebb a felelőssége a vállalat biztonságáért, mint a nagyvállalatok vezetőié.

Ezek után egy út kínálkozik számukra:

- a biztonsági kockázatok felmérése mind a két (három) biztonsági alrendszerben,
- a kockázatok egyenkénti vizsgálata, és döntés arról, hogy tesznek-e védelmi intézkedést az adott kockázat csökkentésére, és ha igen, milyen erős védelmi intézkedést. Ez annyit jelent, hogy
 - a felső vezetésnek fel kell vállalnia azokat a kockázatokat, amelyek csökkentésére nem tesznek védelmi intézkedést,
 - a biztonság esetleg nem egyenszilárdságú lesz,
 - a védelem erőssége az értékelő eljárások alsó osztályaiban fog elhelyezkedni.

A felső vezetésnek igen komolyan kell venni a biztonsági események kezelését, és az értékelésnél le kell vonni azt a következtetést, hogy a kockázatok csökkentésével kapcsolatos döntéseik helyesek voltak-e.

Végül az átlagosnál nagyobb gondot kell fordítani az állomány biztonsági tudatosságának folyamatos megőrzésére és a kihelyezett erőforrásokkal szembeni biztonsági követelmények folyamatos ellenőrzésére.

Mindebből az is következik, hogy nagy gondot kell fordítani a vállalat biztonságának, a biztonsági intézkedéseknek a napra készen tartására.

A COBITQUICKSTART [13], és a COBIT SECURITY BASELINE [14] jelentős segítséget nyújthat egy ilyen vállalat informatikai biztonsági alrendszerének kialakításához.

7. A KUTATÓ MUNKA EREDMÉNYEI

7.1. A VÁLLALATBIZTONSÁGI KÖVETELMÉNYEK

A kutató munka során az alábbi következtetésekre jutottunk, amelyek sem a hazai gyakorlatban, sem a nemzetközi irodalomban nem találhatók, illetve amelyeket nem alkalmazták.

- A vállalat egy mikrogazdasági rendszer, amin belül a vállalatot alkotó három rendszert (üzleti, termelési és informatikai) átfogja a biztonsági rendszer (a három biztonsági alrendszer). Tehát **biztonsági rendszer egy cégen belül csak egy integrált rendszer lehet.** Az eredményes biztonsági rendszer készítésének előfeltétele a rendszer szemléletű megközelítés.
- A vállalat biztonsági rendszere - vagyon, üzem (ha van) és informatikai - biztonsági alrendszerekből áll, amelyek átfedik egymást.
- A védelmi intézkedések így az egyes biztonsági alrendszerekben azonosak is lehetnek. Ez indokolja, hogy az a biztonsági alrendszer foglalkozzon vele, amelyhez valójában tartozik. (A fentiekben megadott védelmi intézkedések, mint látható, bármelyik alrendszerben előfordulhatnak, de az alkalmazásuk az adott biztonsági alrendszer specifikumait természetesen vegye figyelembe).
- A biztonságirányítási dokumentumoknak (stratégia, politika, folyamatos működés terve) biztosítani kell a három biztonsági alrendszer összehangolt irányítását, amelyet a Biztonsági Stratégiában kell megfogalmazni.
- A biztonsági infrastruktúra vezetőjének a vezérigazgató közvetlen alárendeltségébe integráltan kell tevékenységét végeznie.

7.2. TÍPIKUS HIBÁK A TAPASZTALATOK SZERINT

- A biztonságirányításban igen sok vállalatnál a vállalati biztonság rendszerszemléletű megközelítése hiányzik.
- Nincs egységes biztonságirányítási rendszer, a biztonsági alrendszerek külön kerülnek kiépítésre, üzemeltetésre.

- Nincs integrált biztonsági szervezet, tehát nem egy vezetőhöz tartoznak az alrendszerekért felelős vezetők, akik szakmailag irányítják az üzleti, termelési és információ rendszerben dolgozó biztonsági felelősöket.
- Nem mindenhol tartozik a biztonsági vezető közvetlenül a vezérigazgatóhoz. Ez pedig együtt jár azzal, hogy nincs megoldva a biztonsági szervezet függetlensége.
- Az egyes biztonsági események nem mindig ismertek vállalati szinten, így a válasz védelmi intézkedések is csak korlátozott területen, nem az egész vállalatnál következnek be.
- A biztonsági rendszerben nincs megnyugtatóan rendezve a meg nem kerülhetőség elve, azaz a profi támadó megtalálja a megkerülhetőség lehetőségét.
- A biztonsági megoldások megvalósítását nem előzi meg kiterjedt, vállalati szintű veszélyforrás felmérés és kockázatelemzés.
- A biztonság szerepe a felső vezetésben nem a megfelelő módon tudatosodik.
- Hamarabb költenek a termelés bővítésére, mint 1-1 biztonsági megoldásra.

7.3. TOVÁBBI TEENDŐK

- Folytatni kell, elsősorban a vagyonbiztonság és az üzembiztonság területén, a fentiekben megadottak kutatását.
- Ki kell dolgozni mind a három biztonsági alrendszerben az egymással kapcsolatban lévő ÜFT-eket.
- El kell érni, hogy mind a hazai, mind a külföldi elméletben és gyakorlatban egyaránt elfogadják a vállalati biztonság rendszerszemléletű megközelítését.

8. FELHASZNÁLT IRODALOM

- [1] Control Objectives for Enterprise Governance. IT Governance Institute. 2003.
- [2] IT Governance Executive Summary. IT Governance Institute 2003.
- [3] Information Security Governance: Guidance for Boards of Directors and Executive Management. IT Governance Institute. 2003.
- [4] IT Strategy Committee. IT Governance Institute. 2003.
- [5] Horváth, Lukács, Tuzson, Vasvári: Informatikai Biztonsági Rendszerek. Ernst&Young, BMF Kandó Kar. 2002.
- [6] CISM Review Manual. ISACA. 2003.
- [7] J. Ward: Principles of Information System Management, az Információ Rendszerek Szervezésének Elvei. Ernst & Young. 1998. (kétnyelvű kiadvány).
- [8] K. Mitnick: A megtévesztés művészete. Perfect- Pro Kft.2002.
- [9]OECD: Principles of corporate governance
- [10] Európai Bizottság 8. sz Direktíva
- [11] COBIT 3. IT GOVERNANCE INSTITUTE. 2000.
- [12] SLA TOOLKIT. Easytech Solution. 2002.
- [13] COBITQUICKSTART. IT Gouvernance Institut. 2004.
- [14] Vasvári György: Security Management Methodology, Biztonságszervezési módszertan. (Jelenleg az SMM 5.6 változat). A szerző saját kiadása.
- [15] COBIT SECURITY BASELINE: IT Gouvernance Institut. 2004.
- [16] COBIT 4. IT Governance Institut. 2005.
- [17] Convergence of Enterprise Security Organization. ISACA. 2005.
- [18] Critical Elements of Information Security Program Success. ISCA. 2005.