VASVÁRI GYÖRGY CISM

VÁLLALATI BIZTONSÁGIRÁNYÍTÁS

INFORMATIKAI BIZTONSÁGMENEDZSMENT

2007

Lektorálta: Dr. Kiss Ferenc
Szerkesztette. Vasvári József

ISBN

Kiadó: Time-Clock Kft 2340.Kiskunlacháza Dózsa György u.39.

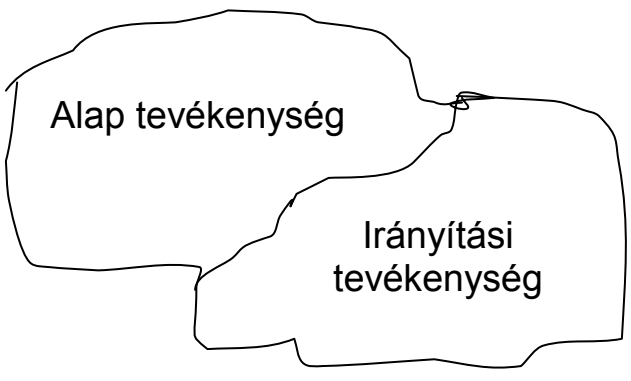
1. TARTALOMJEGYZÉK

2. BEVEZETÉS

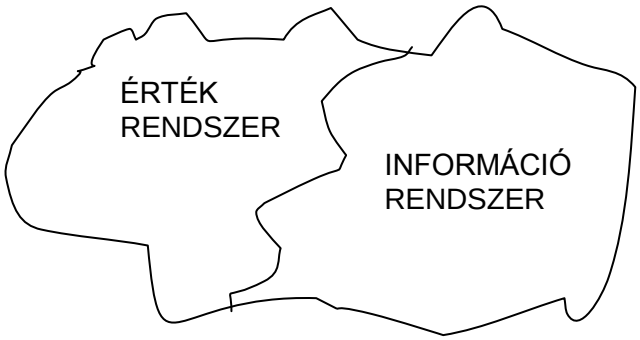
A vállalatvezetés alapvető érdekeltsége az üzleti cél, a vállalat küldetésének megvalósítása. Ebből következik, hogy elemi érdeke, a teljes vállalat eredményes, és hatékony működése, amely nem lehetséges vállalati szintű biztonság nélkül. Induljunk ki abból, hogy a gazdasági szervezet, a vállalat mikró gazdasági rendszer. Ebből, pedig azt a következtetést vonjuk le, hogy a biztonságszervezésnek a problémákat rendszerszemlélettel kell megközelíteni. Ennek kifejezője a vállalat minden pontján az egyenszilárdságú biztonság követelménye. Ma már a vállalatok is egyre inkább belátják, hogy nem lehet csak informatikai biztonsággal, és elkülönítve a vagyonbiztonság egyes elemeivel foglalkozni, hanem a vállalat biztonsága integrált biztonságirányítást, és rendszert, kíván meg a vállalatirányításon belül. A könyv célja annak bemutatása, hogy a gazdasági szervezetek, a vállalatok irányítása, valamint az informatikai biztonság irányítása, és menedzsmentje, miként értelmezhető, hogyan épül egymásra (vállalatirányítás➔IT irányítás➔IT biztonságirányítás), valamint a vagyonbiztonság, üzembiztonság, és az informatikai biztonság, hogyan függ össze. A CISM REVUEW MANUAL 2004 azt írja, hogy minden informatikai biztonsági döntésnek át kell esnie a szervezet üzleti modelljének a szűrőjén. Ebből következik, hogy *a gazdasági szervezetek komplex (rendszer szemléletű) biztonság menedzseléséből indulunk ki.*
Az informatikai biztonságmenedzsment az ISO/IEC 17799: 2002 (magyar: MSZ ISO/IEC 17799: 2002) „Az informatikai biztonság menedzselésének eljárás rendje”, és a MSZ ISO/IEC 27001:2006. „Információ Biztonsági Menedzsment Rendszer (ISMS). Követelmények.”, szabványokon, a COBIT 3, és 4-en, és egyéb ISACA anyagokon alapul.

2.1. A BIZTONSÁG HELYE A GAZDASÁGI SZERVEZETBEN

A gazdasági szervezet rendszer, mégpedig mikró gazdasági rendszer, amely feladatát, küldetését a gazdasági szervezet alaptevékenysége, és az irányítási tevékenység útján látja el.



Ezeket a tevékenységeket, 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):



2.2. MIT KELL VÉDENI

Az IT szervezet az üzleti célok teljesítése érdekében, egyértelműen meghatározott folyamatok útján szolgáltat. A folyamatok, pedig felhasználják az **emberi** tudást, ismeretet, és a technológiai **infrastruktúrát** az automatizált üzleti **alkalmazások** futtatására, mialatt befolyásolják, meghatározzák, az üzleti **információt** (a COBIT 4 szerint).

Az összefüggés a következő **a vastagon szedettek az erőforrások (**részletesen lásd a következő pontban):

Tehát az informatikai biztonság az informatikai erőforrások, és folyamatok maximális biztonságának megteremtésével valósítható meg.

A biztonsági cél, a védelem tárgya a vállalati erőforrások **bizalmassága, sértetlensége, és rendelkezésre állása** fenyegetettségének, a kockázatoknak a minimálisra csökkentése. Hozzá szokták ezekhez tenni a számon kérhetőség, és a garanciák biztosítását is. Fel kell hívni a figyelmet arra, hogy a biztonsági cél teljesítésével lehet **az információt, információkat megvédeni, hiszen az erőforrások sérülésével, végeredményben az információ sérül, sérülhet.**

Az informatikai biztonság elemei az MSZ ISO/IEC 17799: 2002 alapján:

*A **bizalmasság*** a biztonság érzékeny erőforrások jogosulatlan hozzáféréstől, feltárástól, megismerésétől való védelme.
*A **sértetlenség*** az informatikai erőforrások pontosságának, és teljességének védelme. (A hitelesség a sértetlenség kiterjesztése, azaz nemcsak a sértetlenség, hanem annak a biztosítása is, hogy az erőforrások forrása eredeti).
*A **rendelkezésre állás*** a gondoskodás arról, hogy az informatikai erőforrások akkor amikor, és ahol szükségesek (elérhetőség), működőképesek legyenek.

Továbbá:

A számon kérhetőség gondoskodás arról, hogy minden erőforrás rendeltetésszerűen felhasználható legyen, és a velük, valamint rajtuk végrehajtott tevékenységek naplózva legyenek.

A garanciák azt biztosítják, hogy a védelmi intézkedések kikényszerítsék a biztonsági követelményeket.

3. A VÁLLALAT

A vállalat közvetlen gazdasági tevékenységet végző jogilag önálló szervezet, amelyre épülve a küldetését, üzleti célját megvalósítja.

AZ ÜZLETI CÉL tehát a vállalat létrehozásának indokát képező feladat hatékony és eredményes megvalósítása.

Az *eredményesség* alatt (COBIT3, lásd [2]) az erőforrások produktív és gazdaságos (profit orientált) felhasználását, míg a *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, amelyek az üzleti cél elérése érdekében szükségesek.

AZ ÜZLETI KÖVETELMÉNYEK (COBIT 4 ALAPJÁN)

- Minőség
- Megbízhatóság
- Biztonság

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 vállalat pénzügyi, munkaügyi, marketing, humán erőforrás gazdálkodás, biztonsági, ügyvitel technikai folyamatai.

Az üzleti folyamatok az ISACA anyagai szerint (pl. lásd [15]) az alábbi négy csoportba sorolhatók:

- A termékek, szolgáltatások folyamatai, mint például értékesítés, termelés (szolgáltatás), és elosztás.
- A készpénzforgalom (cash flow), mint például a fizetés a szállítóknak, és a beszedés a vevőktől.
- Gondoskodás az üzleti folyamatok támogatásáról (emberi, pénzügyi és más erőforrások által).
- Az erőforrások tervezése, beszerzése, allokációja.

A termelési (szolgáltatási) folyamatok, amelyek a vállalat által értékesíteni (szolgáltatni) kívánt termékek előállítását végzik, és amelyeket, 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 kiszolgálják az üzleti és a termelési folyamatokat, a tőlük kapott adatokat feldolgozzák, majd a feldolgozott adatokat számukra visszaadják. A támogató folyamatok itt is megjelennek.

AZ ERŐFORRÁSOK:

Erőforrás valamely cél megvalósítása érdekében biztosított anyagi vagy szellemi tényező.

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

Az üzleti rendszerben

- adatok, értékek, áruk, nyersanyagok
- tőke (pénzügyi, szellemi)
- infrastruktúra
  - technológia (ügyvitel-technikai eszközök, személy- és teherszállító eszközök, automatizált raktározási rendszerek, épület automatikai rendszer, biztonsági rendszer, távközlési rendszer, vagy a bankoknál, pl. a pénzfeldolgozó berendezések),
  - támogatások [mint pl. létesítmények (helyiségek), energiaellátás, légkondicionálás, papírfeldolgozás, épületautomatika, és biztonság stb.].

- üzleti és azokat támogató folyamatok, eljárások,
- ember (alkalmazottak, vevők, szállítók, beruházók, stb.).

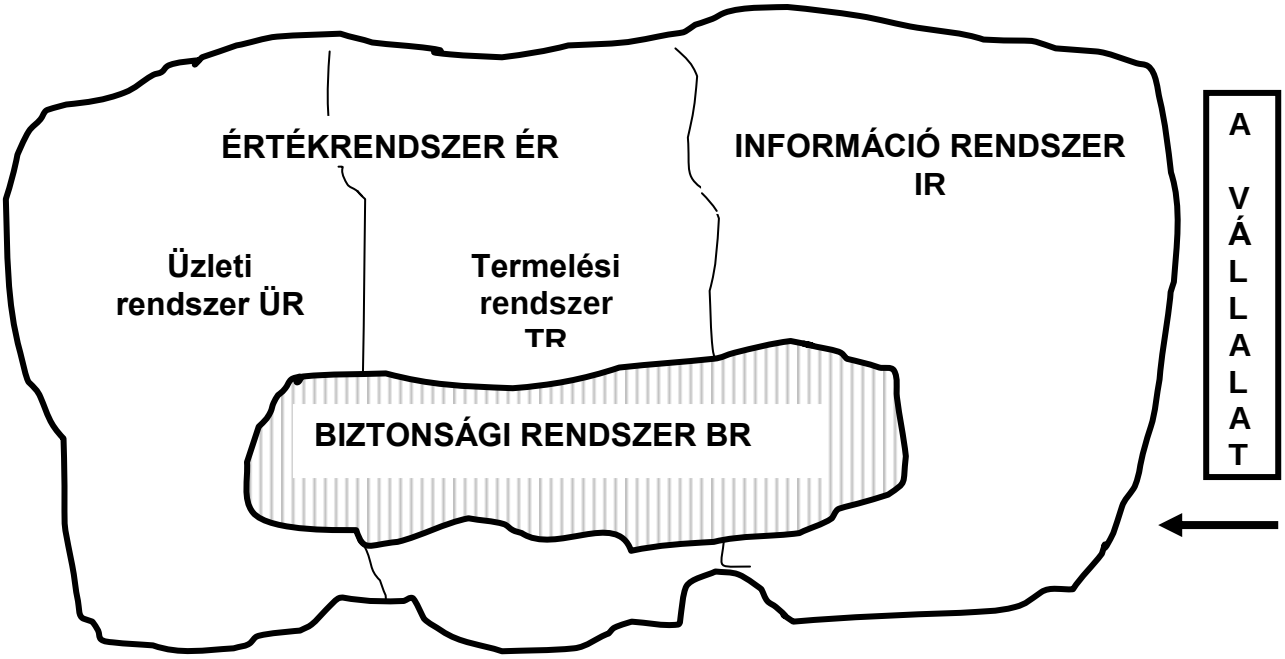
A termelési, szolgáltatási rendszerben

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

Az információ rendszerben

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

A nemzetgazdaságon (amely a makrogazdasági rendszer) belül kisebb rendszerek - vállalatok, gazdasági szervezetek - működnek, amelyeket mikro gazdasági rendszernek tekintünk. A mikró gazdasági rendszer - vállalat vagy gazdasági szervezet feladatát, küldetését a folyamatok, és azokon belül, tevékenységek útján látja el, amelyek erőforrásokat használ fel, és az értékrendszerben vagy az információ rendszerben működnek. Az értékrendszerben (ÉR) definiálhatjuk az üzleti rendszert (ÜR) és, ha van, a termelési (szolgáltatási) rendszert (TR):



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

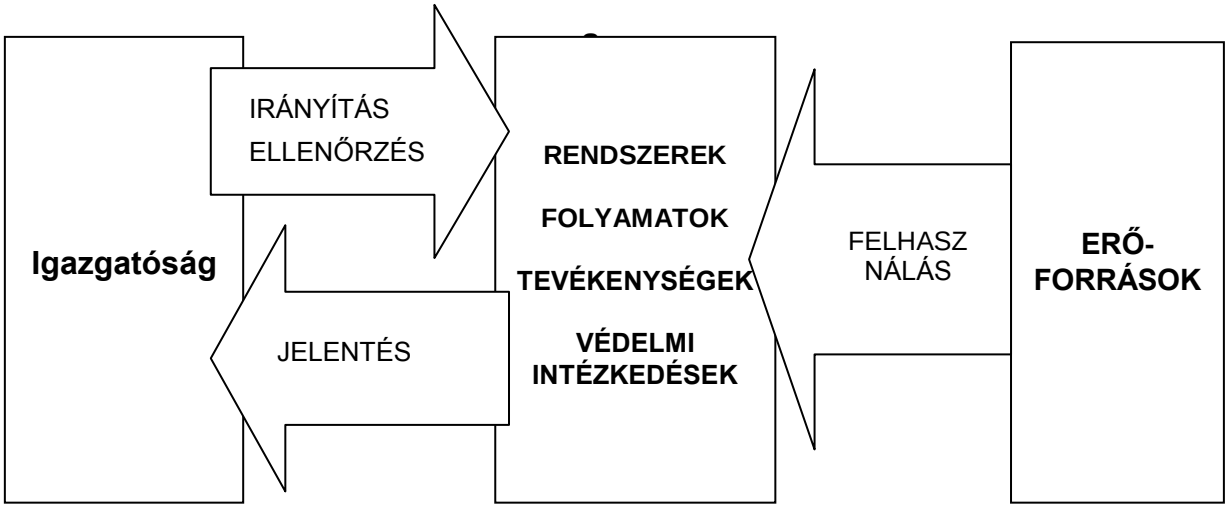
- vagyonbiztonsági,
- üzembiztonsági (ha van termelés) és
- informatikai biztonsági alrendszerekből.

Vállalatirányítás definíciója (COBIT 4 alapján):

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

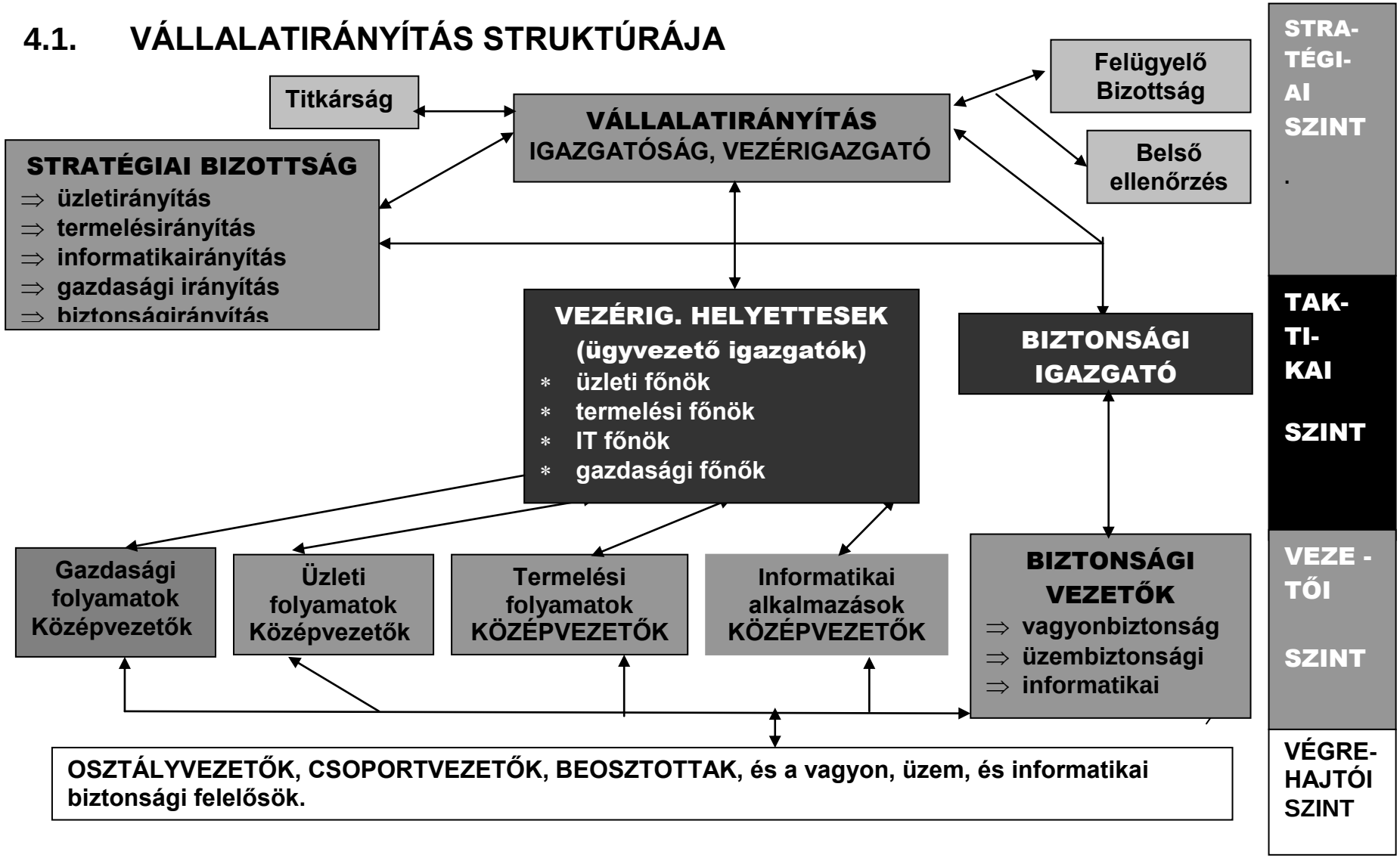
A vállalatirányítás az üzleti követelményekből kiindulva először a vállalati, üzleti, ha van termelési, majd informatikai, és biztonsági stratégiák, kidolgozását igényli. Ezek összefüggéseit lásd a következő oldalon.

Vállalatirányítás (Enterprise Governance) funkcionális modellje (COBIT3 alapján)

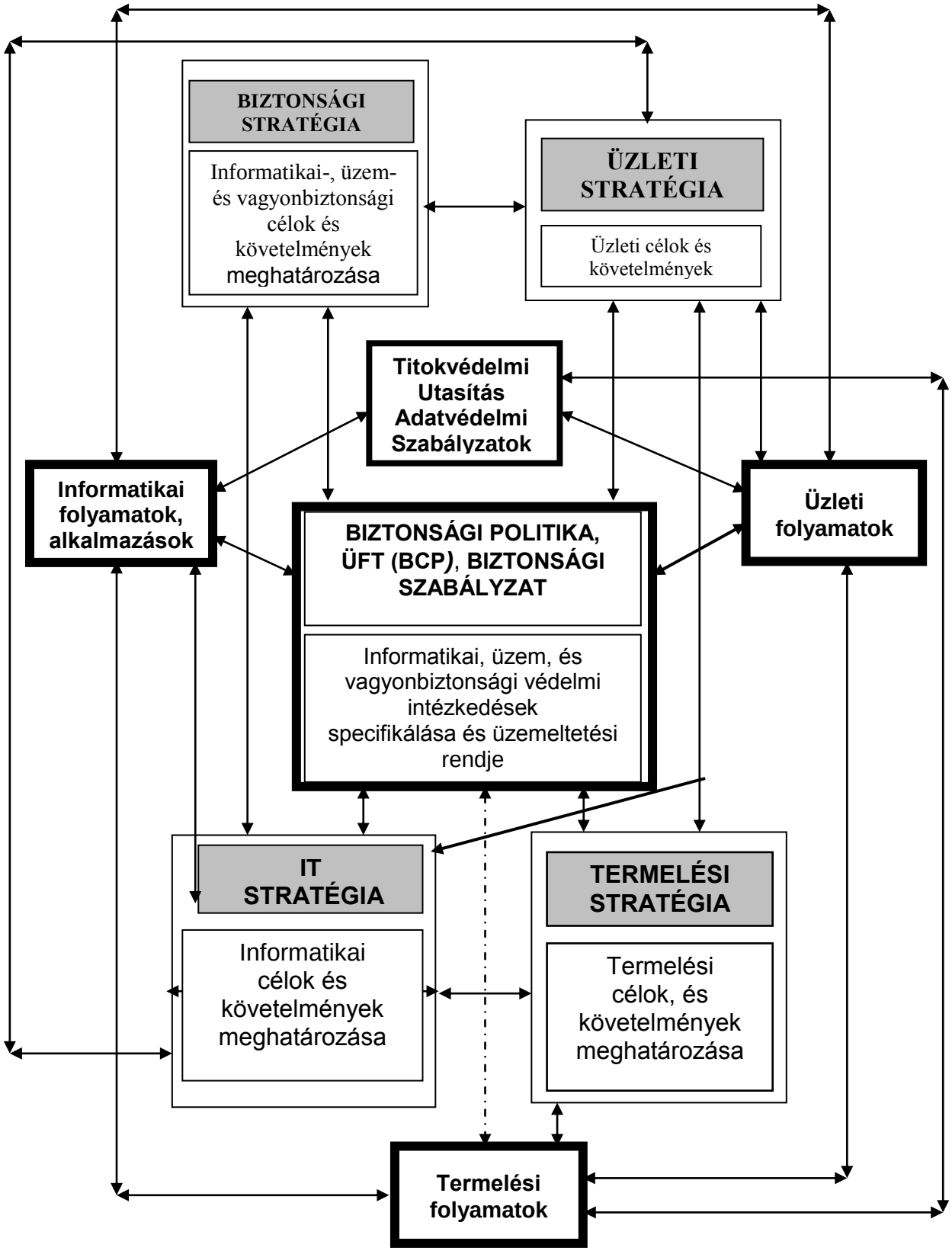


4. A VÁLLALATIRÁNYÍTÁS ÉS BIZTONSÁG

4.1. VÁLLALATIRÁNYÍTÁS STRUKTÚRÁJA



4.2. ÜZLETI, TERMELÉSI, INFORMATIKAI ÉS BIZTONSÁGI STRATÉGIA ÖSSZEFÜGGÉSEI



4.3. 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.

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 bizalmasságának, 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.

A kisvállalatoknál csekély anyagi és létszám lehetőségek mellett kell a biztonság megvalósítást biztosítani. Ez a feladat csak úgy oldható meg, ha a felső vezetés hajlandó kompromisszumokat kötni, azaz meghatározza azokat a kockázatokat, amelyeket nem kíván, csökkenti, és felvállalja ennek biztonsági következményeit.

Érdemes ilyen biztonság szervezési feladat esetén a COBIT QUICKSTART, illetve COBIT SECURITY BASELINE ISACA anyagokat [lásd 10, 9] figyelembe venni.

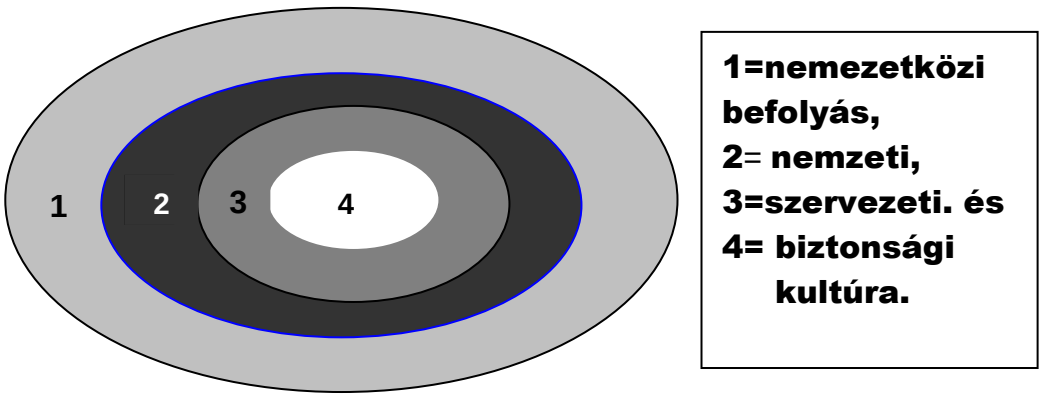
4.4. A VÁLLALATI, ÉS A BIZTONSÁGI KULTÚRA

A vállalati, illetve szervezeti kultúra fontos jellemzője, és meghatározója a vállalat hatékony, és eredményes irányításának, és a biztonság megteremtésének, valamint fenntartásának. Björck írja [21]-ben, hogy „az informatikai biztonságmenedzsment egy szervezetben főleg a szociális világ ellenőrzésének, bizonyos szempontokból a megkísérlése, az informatikai biztonsággal kapcsolatos emberi magatartás befolyásolásával". Ezért tisztáznunk kell, hogy mit értünk ezen a fogalmak alatt, és miként kell biztosítani azok elvárt szintű megvalósítását, és fenntartását.

4.4.1. A VÁLLALATI (SZERVEZETI) KULTÚRA

A szervezetről írja W.E. Schneider, hogy „Minden szervezet, élő társadalmi szervezet, a saját kultúrájával, jellemzőivel, természetével, és azonosságaival." Továbbá: „a szervezetek/vállalaltok egy küldetéssel rendelkező emberek közösségei". A szervezeti kultúra tágabb fogalom, mint a vállalat, (vannak szervezetek, amelyek nem vállalatok) magába foglalja a szervezet tagjainak a felelősség vállalásait, az etikai értékeket, a normatívákat, ezeknek a megjelenési formáit, a szervezet magatartását, a vezetési filozófiát. A szervezeti kultúra alapvetően a szervezet személyisége, az alkalmazottak véleményének, szokásainak, értékítéletének, magatartásának, gondolkodási és cselekvési módjainak összessége. A szervezeti kultúra a szervezet közös gondolkodása, amelyet a szervezet közös problémáinak megoldása során tanul meg. A szervezeti/vállalati kultúra integrálja a szervezetet, és elősegíti a környezethez történő alkalmazkodást, amelyen elsősorban az üzleti célok követelmények változását követő *változás menedzsmentet értjük.*

A kultúrák egymásba ágyazódása Bakacsi [23] alapján:



4.4.2. A BIZTONSÁGI KULTÚRA

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

Minden alkalmazottnak van meghatározott szintű felelőssége, szerepe, a szervezeten belül. Ezen kívül a szervezetbe érkezésekor mindenki hoz magával, gondolkodásmódot, viselkedés, magatartás jegyeket, többek között a biztonsággal kapcsolatban, amelyeknek azonosulniuk kell a szervezet kultúrájával, biztonsági kultúrájával.

A biztonsági kultúrát ki kell alakítani nem csak az alkalmazottak, és időszakos alkalmazottak, szerződéssel munkát vállalók körében, hanem a szervezettel foglalkozó, tevékenységében résztvevő harmadik felek munkatársaiban is.

A biztonság tudatosan egy kultúrává válik, ha a szervezet, mint egész, a biztonság megsértését szociálisan, és erkölcsileg a szervezetben elfogadhatatlannak tartja, és a biztonság, pedig átfogja, a szervezetet, és mindenhol, és mindenkinek része van a biztonságért való felelősségben (egyenszilárdság elve, humán vonatkozásban), amelyet a szervezet számon is kér tőle.

A biztonsági kultúra elemei a szervezeti kultúra elemeinek részét képezik, kiegészítik azokat. A biztonsági kultúra elemei a Mc. Kinsey 7S modellje alapján:

⇒ **kemény elemek:** a biztonságirányítás struktúrája**,** és módszerei, a biztonsági stratégia, a biztonsági alrendszerek (vagyon, üzem és informatikai biztonsági alrendszer),

⇒ **lágy elemek:** a biztonsági tudatosság színvonala a szervezet, és az egyének szintjén, az alkalmazottak elkötelezettsége, a képzettsége, a biztonsági szakképzettsége, és a biztonsági ismeretei, a biztonsági értékrend, a környezet.

A Szerző szükségesnek tartja a lágy elemek közé **a környezetet (**pl. társadalmi, jogi, piaci, természeti**)** is felvenni. Ezt alátámasztja Bakacsi is [23].

A kemény, és a lágy elemek egyaránt arra utalnak, hogy a biztonsági kultúráról, a szervezet, a vállalat, és az egyének szintjén beszélhetünk. A szervezeti kultúrával kapcsolatban, a fentiekben azt állapítottuk meg, hogy „A szervezeti kultúra a szervezet közös gondolkodása, amelyet a szervezet közös problémáinak megoldása során tanul meg. A biztonsági problémák megoldása a szervezet, ilyen közös problémája. Ebből

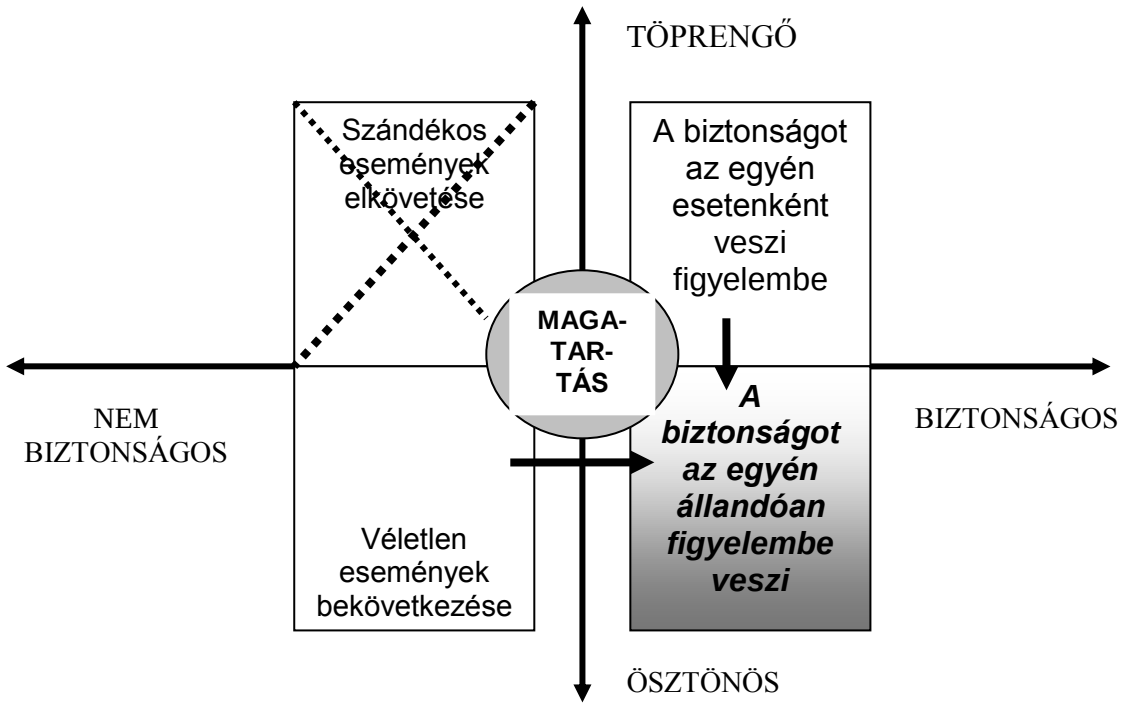
következik, hogy a biztonsági kultúráról is a szervezet, és az egyének szintjén beszélhetünk.

4.4.3. A BIZTONSÁGI TUDATOSSÁG

A biztonsági tudatosság, a szervezet biztonsági szintjének, mint követelménynek elfogadása, és esetleges hiánya következményeinek elismerése, valamint a felelősség vállalása a szervezet biztonságáért, a biztonsági szempontból erkölcsös, etikus magatartás kultúra. Azaz annak felismerése, hogy

- a biztonsági követelmények elfogadása, a veszélyérzeten alapul, és egyaránt vonatkozik az elvárásoknak megfelelő biztonsági intézkedésekre, és a biztonsági események kezelésére.
- a veszélyérzet hiányának hatása, a következmények biztonsági kockázatának fel nem ismerését eredményezi, amely az üzleti cél, és a rendeltetésszerű üzletmenet sérüléséhez vezethet.

A biztonsági tudatosság a biztonsági kultúra előfeltétele, valamint alakítója. A biztonsági kultúra a vezetés, és a munkatársak viszonya biztonsághoz, míg a biztonsági tudatosság az egyik elem, amely lényegesen hozzá járulhat, a biztonsági kultúra kialakításához, fenntartáshoz. A biztonsági kultúra a bővebb tartalmú. A biztonsági tudatosság a biztonsági kultúra egyik eleme. A biztonsági kultúra csak tudatos magatartás eredménye lehet, amikor a szervezetben az egyéneknek a biztonságos magatartás ösztönös magatartás jegye. Az ISACA [7] ezt az alábbi ábrán mutatja be:



4.4.4. A VÁLLALATI BIZTONSÁGI KULTÚRA PROGRAM

A szervezet tagjainak, az egyéneknek az azonosulása a szervezeti kultúrával, és a szervezet biztonsági kultúrájával, egy véget nem érő folyamat. Ezt a folyamatot célirányos tevékenységgel, a vállalati, és a biztonsági kultúra vonatkozásában a Vállalati, és a Biztonsági Kultúra programja útján lehet, és kell napra készen tartani. A vállalati, és a biztonsági kultúra program megvalósulása, pedig egyik feltétele a biztonsági követelmények teljesülésének. A Program főbb elemei a következők:

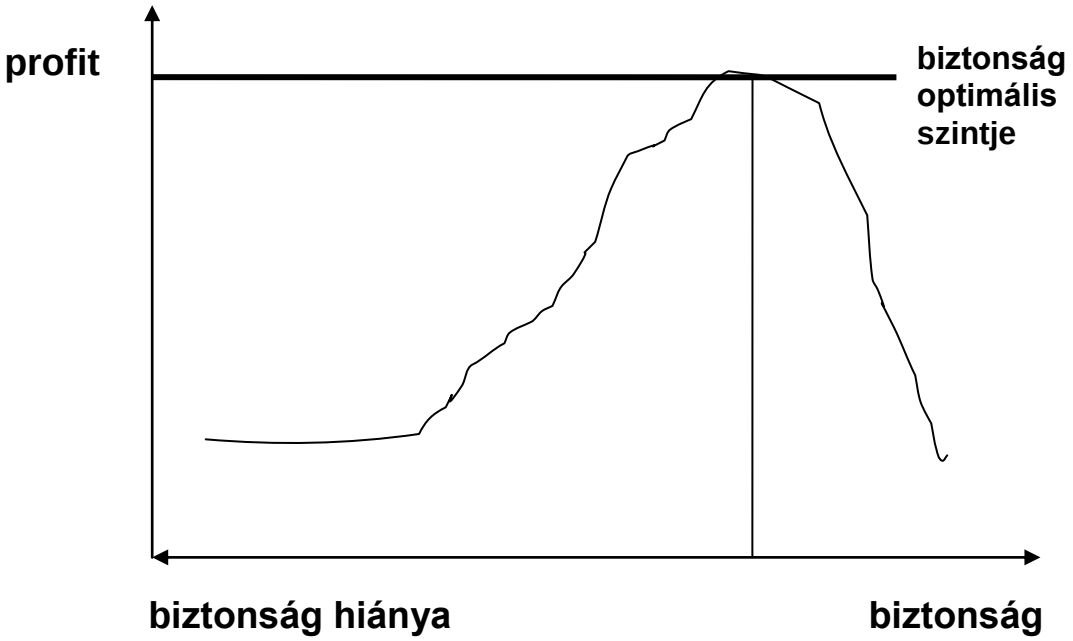
A BIZTONSÁGI KULTÚRA PROGRAMJA FŐBB ELEMEI		
1.	A program céljai (a biztonsági tudatosság is benne szerepel)	MIT?
2.	A program célterületei	HOL?
3.	Tevékenységek, módszerek	HOGYAN?
4.	A program értékelése	EREDMÉNY?
5.	Programjavító intézkedések	TEENDŐ!

4.5. KÖLTSÉG HATÉKONY BIZTONSÁG

A vállalatok üzleti érdeke a biztonság, de ez egyúttal annyit is jelent, hogy a biztonság nem lehet mindig, a védelem költségeinek, és a sikeres támadások, okozta költségek, üzleti szempontból elviselhető aránya. Az üzleti érdek tehát módosíthatja ezt az arányt. Björck a [21]-ben írja Martinra (1992) hivatkozva, hogy a biztonság optimális szintje egy szervezetben, pénzügyi szempontból ott van, ahol a védelmi költségek a támadások által okozható költségek csökkentésével azonosak. Egyúttal a következő görbével ábrázolja a biztonságmenedzsment balanszírozási lehetőségének alakulását, a biztonság optimális szintjének (azaz itt csak a pénzügyi szempontok szerepelnek).

Az ábrából következik, hogy a kis biztonsági szint, a sikeres támadási arány nagyobb valószínűsége miatt, a profit csökkenését eredményezheti, míg a túl sok biztonság esetén a védelem nagyobb költségei csökkentik a profitot. A biztonsági beruházások megtérülési szintjét, egyébként a Return on Security Investment (ROSI) mutató fejezi ki. A biztonsági költségek megtérülnek, ha a hatásukra a kockázatok elfogadható szintre (a ROSI elfogadható) csökkennek.

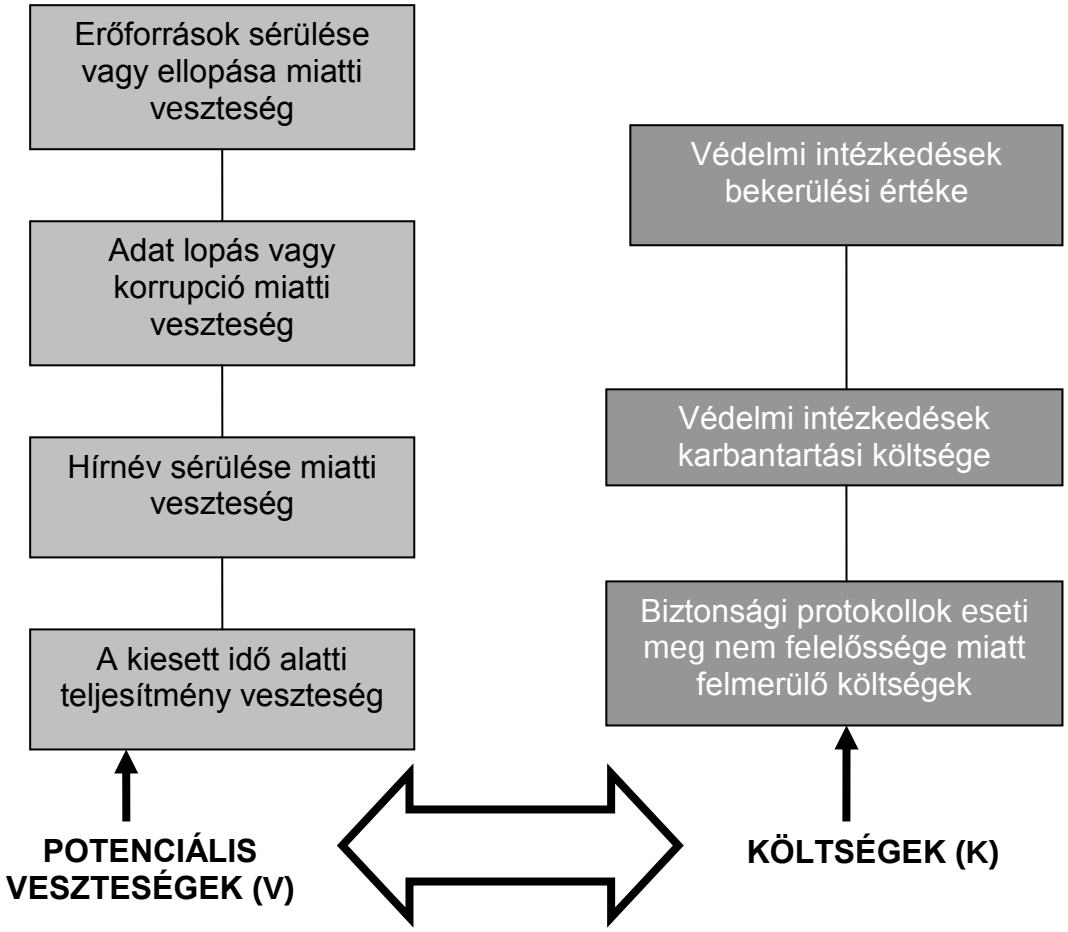
Erre mutat rá az ISACA most készülő szabványának tervezete is [27].



A számszerű meghatározás nehézsége ott van, hogy egy támadás esetében a kár elsősorban a vagyontárgyakban (tárgyi, és szellemi) keletkezik, és a tárgyiakban határozható meg csak számszerű módszerekkel, nem beszélve a vagyontárgyakon kívül az erőforrásokhoz tartozó humán erőforrásokról. Így a kárnak lesz egy becsült összetevője is. Általában azt tartják, hogy a biztonságra nem szabad többet költeni, mint amit egy biztonsági eseménynél veszíthetünk (a tárgyi, és szellemi vagyontárgyak, egyéb erőforrások sérülésével).

Az informatikai biztonságra vonatkozóan A. Mizzi [25]-ben, az előző bekezdésben írtakat felvetve, bemutat egy eljárást, összefüggéseket ad meg, az informatikai biztonsági beruházás megtérülési mutatójának (ROISI, Return on Information Security Investment) számítására. A károknál azonban csak a hw, és sw károkat, és az ezekkel kapcsolatban fellépő tárgyi, és szellemi (nem tárgyiasult) károkat veszi figyelembe. Ismert, hogy az informatikai erőforrások a hw, és sw-en kívül, humán, valamint egyéb (pl. létesítmények) elemeket is tartalmaznak, amelyek szintén sérülhetnek.

S. Niels [26]-ban egy jó megközelítést add meg a védelmi intézkedések költségei, és a potenciális, lehetséges, becsült veszteségek közötti egyensúlyozásra. E módszert, alkalmazva a könyvben meghatározott fogalmakat, az alábbiakban mutatjuk be:



A potenciális veszteségek, mint az előbbiekben erről szó volt, összességében, tehát csak becsülhetők, míg a költségek számíthatóak. Ezekből következtetve, *a biztonsági beruházás megvalósítható, ha*

$$K<V$$

tehát a költségek kisebbek, a becsült veszteségeknél.

A számításos módszert tehát az jár el helyesen, aki tájékoztatásnak tekinti, nem teljesen pontos adatnak.

Ugyanakkor rá kell mutatni arra, hogy mennél biztonság érzékenyebb egy szervezet tevékenysége, annál inkább a döntő, a költséghatékonysággal szemben a biztonsághoz fűződő érdek.

E témához érdemes átgondolni Albert Einstein mondását:
„Nem minden, amit tudunk számítani, számít, és nem minden, ami számít, tudjuk számítani.”

4.6. A BIZTONSÁGI RENDSZER

4.6.1. 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 védelmi intézkedések is, mivel az üzleti rendszerben működik épület automatikát irányító informatika, biztonsági informatika, távközlés irányító informatika. Az intelligens épületben ezeket egy információ rendszer fogja össze.
- **az üzembiztonsági alrendszer**, amelyben vannak az üzembiztonsági védelmi intézkedéseken kívül vagyon, és informatikai védelmi intézkedések, mivel a termelő berendezéseket fizikailag is védeni kell, valamint a termelésirányítást információ rendszer szolgálja ki.
- **az informatikai biztonsági alrendszer,** amelyben vannak vagyonbiztonsági védelmi intézkedések is, mivel az informatikai erőforrásokat fizikailag is védeni kell.

A vállalati biztonsági rendszer, tehát a vagyonbiztonság, üzembiztonság és az informatikai biztonsági alrendszerekből áll, amelyek hivatottak az erőforrások (üzleti, termelési és informatikai) fenyegetettségét, a kockázatokat az üzleti célkitűzések megvalósításához szükséges mértékűre csökkenteni.

4.6.2. A BIZTONSÁG STRUKTÚRÁJA

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, Szervezeti, Biztonsági kultúra]
- Biztonság a harmadik felekkel kötött szerződésekben (biztosítás, outsourcing, szerviz szerződések, SLA-k, Service Level Agreement)

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, logikai háttérbiztosítás)
  - Életciklus védelem (a rendszerek, folyamatok, alkalmazások életciklusának [fejlesztés, beszerzés, átadás/átvétel, üzemeltetés, selejtezés] védelme
  - Hálózatok (beszéd és adat hálózatok) védelme (pl. titkosítás, elektronikus aláírás)

4.6.3. A BIZTONSÁGI ALRENDSZEREK KÖZÖTTI ÖSSZEFÜGGÉSEK

A védelmi intézkedések a három biztonsági alrendszerben, mint azt már említettük, átfedik egymást, kölcsönhatásban vannak. Ezt mutatja be a következő ábra.

Alrendszerek⇒ Védelmi intézkedések ⇓	1Vagyon biztonsági alrendszer (Üzleti rendszer)	2. Üzembiztonsági alrendszer (Termelési rendszer)		3. Informatikai biztonsági alrendszer (Információ rendszer)
		Termelési rendszer	Termelésirányító 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 hozzá-Férés 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 termelő rendszer specifikus rendelkezésre állásának biztosítása		Erőforrás és rendszer háttérbiztosítás, tűzvédelem, kisugárzás védelem, energiaellátás biztosítása
Logikai hozzá-Férés védelem	Logikai belépés és behatolás védelem	← Az előző + a termelő rendszer specifikus hfv.		Logikai belépés, és behatolás védelem
Logikai Rend. állás biztosítása	Erőforrás és rendszer logikai háttérbiztosítás, ki- és besugárzás védelem	← Az előző + a termelő rendszer specifikus logikai rendelkezésre állásának biztosítása		Erőforrás és rendszer logikai háttérbiztosítás, ki- és besugárzás védelem
Az életciklus Védelem	A teljes életciklus alatt a biztonsági követelmények biztosítása			
Hálózatok védelme	A hálózat és a továbbított adatok védelme	A továbbított félkész és kész termékek védelme		A hálózat és a továbbított adatok védelme

4.7. A BIZTONSÁGIRÁNYÍTÁS

A biztonságirányítási rendszer (Security Gouvernance System) 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.

4.7.1. A VÉDELMI INTÉZKEDÉSEK ÜZEMELTETÉSE

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

- *Végrehajtását (szervezési védelmi intézkedéseknél), valamint*
- *Működtetését, és karbantartását (technikai védelmi intézkedéseknél) 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 (például Faraday kalitka vagy egy helyiség speciális falazata).

A védelmi intézkedések tulajdonosai:

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

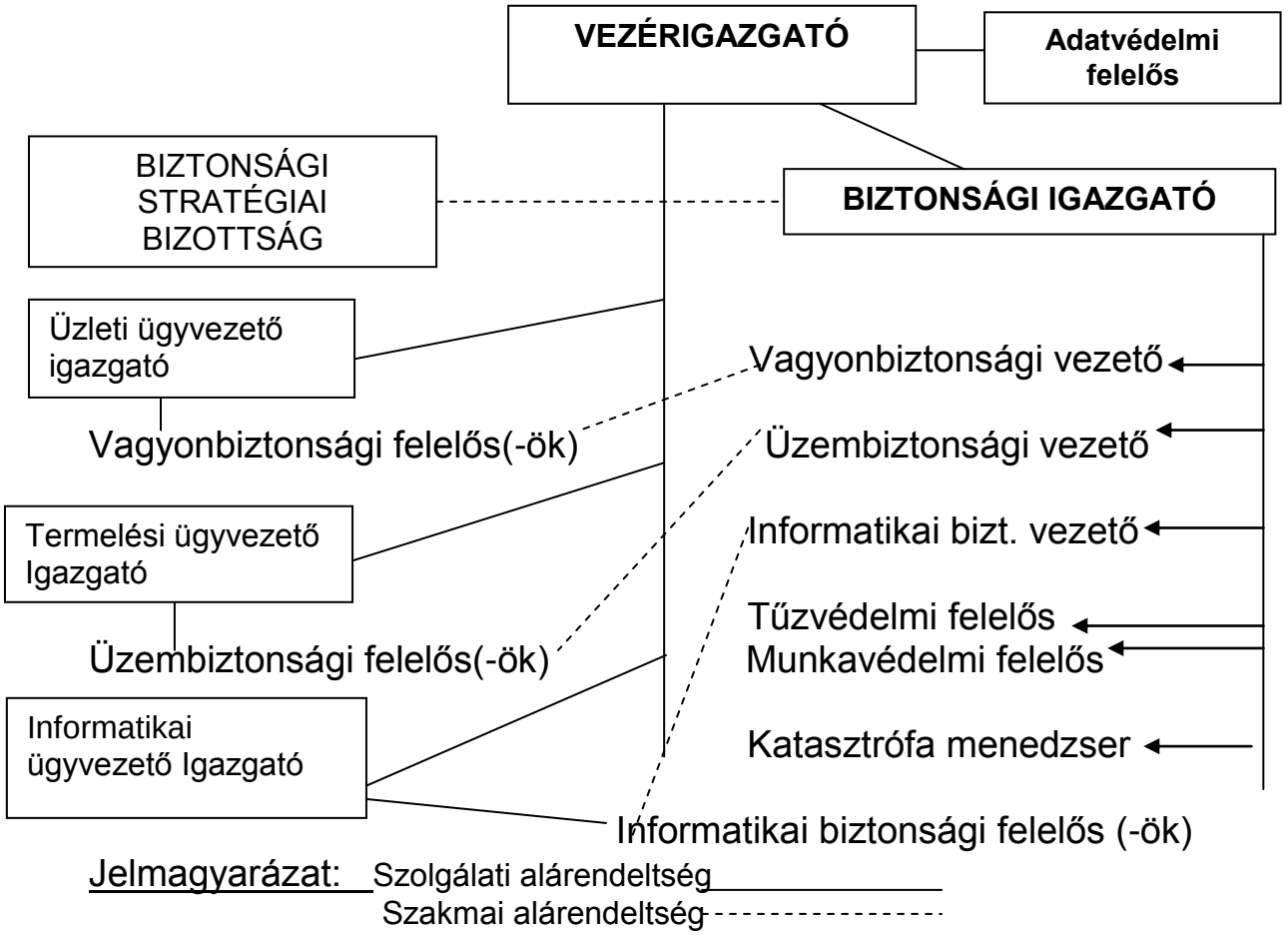
Azaz a tulajdonos folyamatosan felelős azért, hogy a hatáskörében a védelmi intézkedések megfeleljenek a jogszabályoknak, belső szabályzatoknak, és a gyakorlatban megfelelő szintű védelmet nyújtsanak (kikényszerítsék a biztonsági követelményeket).

4.7.2. 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. Így oldható meg, hogy a biztonsági intézkedések szakmai függetlensége biztosítva legyen.

BIZTONSÁGI SZERVEZETI SÉMA



4.8. EGYENSZILÁRDSÁG

4.8.1. RENDSZER SZEMLÉLET

A. Targowski, és T.RIENZO írja [17]-ben, hogy

> „a rendszer elemek cél orientált készlete, valamint azok tudatosan orientált, strukturált kapcsolatai, amelyek mérhető eredményeket állítanak elő…”, továbbá „….a rendszer több mint a részeinek összessége”.

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

Természetesen, 100%-os biztonság nem érhető el, a rendszerszemléletű biztonságszervezés nem vezethet a kockázatok teljes megszüntetéséhez, így egy rendszer biztonság szempontjából mindig fog meghatározott, minimálisra csökkenthető bizonytalanságot hordozni.

4.8.2. EGYENSZILÁRDSÁG ELVE

A rendszerszemlélettel kialakított védelem azonban még mindig kevés. A támadó a támadás előkészítésére általában sok idővel rendelkezik, ezért ki keresheti 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 is eredményezheti. 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. Vagy például 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 arról, hogy a támadó, tényleg az, akinek mondja magát.

Ennek eredményeként, az ezzel élő támadó képes az alkalmazottakat információ szerzés érdekében kihasználni, amely ellen csak magas színvonalú biztonsági kultúrával, biztonsági tudatossággal, valamint erős behatolás, illetve hozzáférés védelmi rendszer 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.

Az információ rendszer, illetve informatikai termékek erősségét biztonsági szempontból authorizált szervezetek minősítik, tanúsítják (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.*

- ***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 visszaverésére a rendszer ellenálló képessége ***(E).***
Az eljárás során feltételezzük, hogy minden veszélyforrás feltárásra került.

5. AZ IT BIZTONSÁGI VEZETŐ ÉS A SZAKÉRTŐ

5.1. AZ INFORMATIKAI BIZTONSÁG SZAKMA

Mielőtt az IT biztonsági vezetővel foglalkoznánk, meg kell állapítanunk, hogy az informatikai biztonság szakma, még akkor is, ha napjainkban ezt az informatikusok, hw, sw, és nw szakemberek, vállalati vezetők általában igen nehezen ismerik el. Ennek oka gyakran a szakmai féltékenységen (én is tudom azt, amit Ő), illetve hatalmi érdekeken alapul.

A szakma fogalma egységesen nem meghatározott, sok különböző meghatározás létezik, illetve létezett. Az Encyclopaedia Britannica szerint a szakma egy hivatás, amely a törvények szerint meghatározott szakismereteken alapul. Furner azt mondja, hogy a szakértőket megkülönbözteti, hogy miként határozzák meg a különböző foglalkozások, és a szakemberek, valamint az ügyfeleik között a határokat. B. Davies [22]-ben a következőket írja: a szakma három dolgot igényel, megfelelő természetet, tudást, gyakorlatot. Továbbá a szakma személyek foglalkozási csoportja, amely rendelkezik, a következő jellemzőkkel:

- Speciális tudás anyaggal, és jártassággal.
- Hivatalos testület (-ek) vesz részt a szakma szervezésében, amely karbantartja a tevékenységét, és gyakorlatát, és ellenőrzi a jogszabályi megfelelősségét, gondoskodva arról, hogy csak minősített személyek kerüljenek a szakmába.
- A szakemberek szakmai státuszának vannak elismerési módjai.

Az informatikai biztonság rendelkezik megfelelő tudás anyaggal, lásd informatikai biztonsági szakemberek egyetemi képzéseinek anyagait, a CISM (ISACA) minősítő vizsga anyagát, vagy a COBIT 3, és 4 biztonsági vonatkozásait, valamint az MSZ-ISO/IEC 17799.2002, MSZ-ISO/IEC 27001, és MSZ-ISO/IEC15408 szabványokat.

Vannak akkreditált testületek, amelyek a fenti szervezési ellenőrzési, minősítési feladatot ellátják, mint például az NJSZT, vagy az ISACA. Az informatikai biztonság a fentiekben megadott három követelményt teljesíti, tehát szakma.

Végül rögzíteni kell, hogy a szakma társadalmi státuszt is jelent, ami a professzionalizálódó világunkban nem lényegtelen.

5.2. IT BIZTONSÁGI VEZETŐ és FELELŐSSÉGI KÖRE

Az IT Biztonsági Vezető (manager) az IT irányítási (a szervezeti) struktúrában, a taktikai szinten (lásd a 4. 1 pontban az ábrát) elhelyezkedő Biztonsági Igazgató alárendeltségében, a vezetői szinten helyezkedik el.

Az IT biztonsági vezető (menedzser) az alábbiakért felelős:

- A vállalati biztonsági vezető alárendeltségében az informatikai biztonsági felelősök szolgálati és/vagy szakmai irányításáért.
- Gondoskodásért arról, hogy a Biztonsági Stratégiát megvalósító folyamatok tervezhetők, implementálhatók, üzemeltethetők, karbantarthatók legyenek.
- A biztonsági kockázat menedzsmentért.
- Az IT biztonságirányítási programtervezés, fejlesztés, implementálás menedzselésért.
- Az IT biztonság irányítási program menedzseléséért.
- A biztonsági események válasz menedzsmentjéért.
- Az IT biztonsági alrendszer üzemeltetésének menedzseléséért.

A felsorolásból kitűnik, hogy a felelősségi kör megegyezik a 6. fejezetben foglaltakkal (CISM VIZSGA ANYAG VÁZLATA), amely ezeket a tevékenységeket tartalmazza.

5.2.1. A MENEDZSMENT ÉRTELMEZÉSE

A menedzsment fogalmát egy szóval nem egyszerű lefordítani (egyes fordítók szerint kezelés, szervezés). Úgy értelmezhetjük, hogy

- Irányítás,
- Szervezés,
- Ellenőrizés, felügyelés,
- Döntés, és
- Valaminek a kezelése.

Ugyanakkor rá kell mutatnunk arra, hogy angolul a menedzsment egyaránt jelent tevékenységet, vagy a vezetést, a vezetőket, magukat. Például elterjedt használata a top menedzsment, amely a vállalat felső vezetését jelenti. Esetünkben a biztonságmenedzsmenten, a biztonság

irányítását, szervezését, ellenőrzését, és az ezzel kapcsolatos döntések meghozatalát értjük. A menedzsereket másképpen funkcionális vezetőknek is nevezik.

Szervezésen olyan alkotó szellemi tevékenységet értünk, amely – esetünkben - az üzleti cél (és üzleti követelmények) érdekében, az erőforrások felhasználásával, az üzleti (és támogató) folyamatok, illetve az informatikai folyamatok (alkalmazások) és az általuk felhasznált erőforrások

- *létrehozására,*
- *fejlesztésére,*
- *működési (szervezeti és működési) rendjének, szabályozásának meghatározására, és*
- mindezek rendeltetésszerű működtetésének megvalósítására irányul.

Az üzleti (és ha van) termelési rendszerben ezt a tevékenységet a **munka, és üzemszervezés,** míg az információ rendszerben **az informatikai szervezés** látja el.

A szabályozás lehet szabályzat, utasítás, eljárás rend, amelyek fogalma a következőket jelenti:

- ***A Szabályzat*** *magatartást, cselekvést meghatározó szabályok összessége.*
  - A szabályzat HOGYAN KELL VÉGEZNI orientált.
- ***Az Utasítás*** *valaminek a végrehajtására kiadott rendelkezés.*
  - Az Utasítás TEVÉKENYSÉG orientált.
- ***Az Eljárás rend*** *valamilyen üzleti folyamat vagy informatikai alkalmazás vagy rész folyamat során végrehajtandó tevékenységek, és végrehajtásuk időbeli sorrendjének szabályozása.*
  - Az Eljárási rend SORREND orientált.

A biztonsági szempontból fontosabb szabályozásokkal a 3, és 4. sz. Mellékletek foglalkoznak.

5.3. AZ INFORMATIKAI BIZTONSÁGI SZAKÉRTŐ

Az informatikai biztonsági szakértő az a szakember, aki széleskörű szakmai elméleti ismertekkel, és széleskörű szakmai tapasztalatokkal rendelkezik az informatika, és az informatikai biztonság területén, és szakértői vélemény nyilvánítására jogosult, amelyet egy erre jogszabályban felhatalmazott szervezet ítélt meg számára. Pl. NJSZT, vagy az ISACA.

Az informatikai biztonsági szakértőnek felkészültnek kell lennie

1. Az informatikai biztonságirányítás struktúrájának, feladatainak meghatározására. az informatikai biztonsági alrendszer biztonság szervezésének menedzselésére.
2. Az információ rendszert fenyegető veszélyforrások kockázatainak felmérésére, és az üzleti cél elérése érdekében javaslatok tételére, csökkentésük érdekében.
3. Biztonsági események értékelésére, kezelésére.
4. Az üzletment folytonosság biztosítására.
5. Az informatikai biztonsági alrendszer ellenálló képességének, a legjobb gyakorlat szerinti felmérésére.
6. Az informatikai biztonsági menedzsment etikai kódexének betartására.

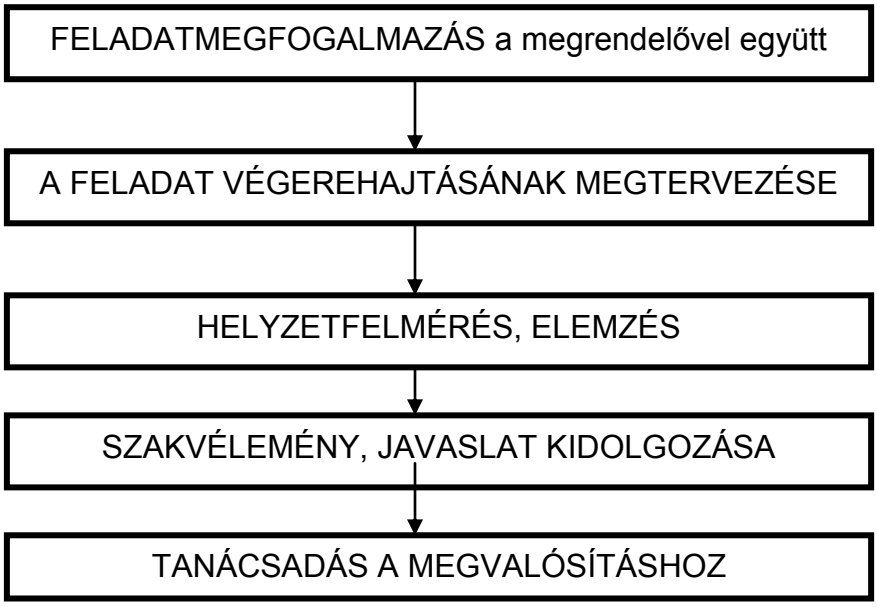
A feladatokat lásd részletesen a 6. Fejezetben, amelyek egyaránt érvényesek az IT biztonsági menedzser, és a szakértő számára, csak a szakértő feladatai, mint a fentiekből kitűnik mindezt, magában foglalják, de végül is a megvalósításuk az IBV –től eltérő. A szakértői munka, a gyakorlatban tanácsadói tevékenység is. M. KUBR a Nemzetközi Munkaügyi Hivatal munkatársa írja [lásd 11-ben], hogy

„Tanácsadást végzünk mindenkor, amikor valamilyen helyzetet meg akarunk változtatni, vagy jobbá kívánunk tenni, de nincs közvetlen hatalmunk a tanácsok megvalósításra”. Illetve

„… a tanácsadás olyan szolgáltatás, amelyet szerződés alapján, független, és tárgyilagos módon nyújtanak ügyfelüknek, problémáik elemzésére, e problémák megoldására, és igény esetén segítenek a megvalósításukban”.

Ebből következik, hogy a szakértő általában informatikai biztonsági szakértéssel, tanácsadással foglalkozó vállalatnál, vagy önállóan dolgozik. Ez biztosítja a függetlenségét. Ha más profilú vállalatok alkalmazásában áll (különösen informatikai, vagy informatikai gyártónál),

függetlensége kétséges. Ilyenkor vállalatoktól csak akkor tud megbízást kapni, az őt alkalmazó vállalatnál végzett napi munkája mellett, ha nem merül fel érdekütközés. Ugyanakkor a szakértői címe a vállalaton belül komoly szakmai presztízst jelent, és elvileg belső tanácsadóként való foglalkoztatását sem zárhatjuk ki.
A szakértői tevékenység általános folyamat ábrája:



Itt kell megemlíteni még, hogy a szakértő, tanácsadó fontos feladata a helyezet felmérés során a megrendelő vállalat fogadó készségének (biztonsági tudatosságának) feltárása, amely nem szükségszerűen megfelelő színvonalú. Természetesen ennek részbeni, vagy teljes hiánya esetén meg kell terveznie ennek megteremtését, pl. irányított megbeszélésekkel, felvilágosítással, esetleg oktatással.
Végül felhívjuk a figyelmet arra, hogy a független szakértő, tanácsadó igénybe vétele, nemcsak biztonsági események vizsgálatánál lehet indokolt, hanem egy biztonságkorszerűsítési program, vagy két, háromévenként biztonsági audit, átvilágítás is indokolhatja.

5.4. AZ ETIKAI KÓDEX

Az informatikai biztonsági vezető (menedzser), tanácsadó és a szakértő olyan munkakört lát el, amely együtt jár a gazdasági szervezet (szervezetek) titkainak megismerésével, és azok védelmének felelősségével. Ezért munkája során szigorú etikai követelményeknek kell megfelelnie. Ezek az etikai követelmények egyébként megjelennek a

CISM minősítést elnyerőkkel szemben is. Az alábbiak az ISACA által megadott etikai követelmények alapján készültek.

AZ INFORMATIKAI SZAKÉRTŐ, TANÁCSADÓ, MENEDZSERNEK

- ***Meg kell őriznie függetlenségét. Korrekt, és tárgyilagos módon kell végeznie tevékenységét, kerülnie kell az olyan helyzeteket, amelyek fenyegetik a függetlenségét.***
- ***Nem vehet részt illegális vagy nem korrekt tevékenységben.***
- ***Védenie kell a feltárt információk bizalmasságát, és azokat saját előnyére nem használhatja fel.***
- ***Magas követelményeket kell, magatartását, és jellemét illetően maga elé állítania mind a szakmai, mind a magán életében.***
- ***Szakmai kompetenciája alapján kell megközelítenie a kapcsolódó szakterületeket.***
- ***Elegendő ténnyel kell a következtetéseit, és a javaslatait alátámasztania.***

6. AZ IT BIZTONSÁGMENEDZSMENT TERÜLETEI (CISM)

Ez a fejezet az ISACA Certified Information Security Manager, CISM (okleveles informatikai biztonság menedzser) vizsga anyaga [8] alapján készült. Tehát áttekintést nyújt a minősítő vizsga anyagáról, a végzendő tevékenységek öt szakterületéről, egyben az anyag az IBV teendőinek meghatározása is. A CISM vizsga anyag szerint az öt szakterület:

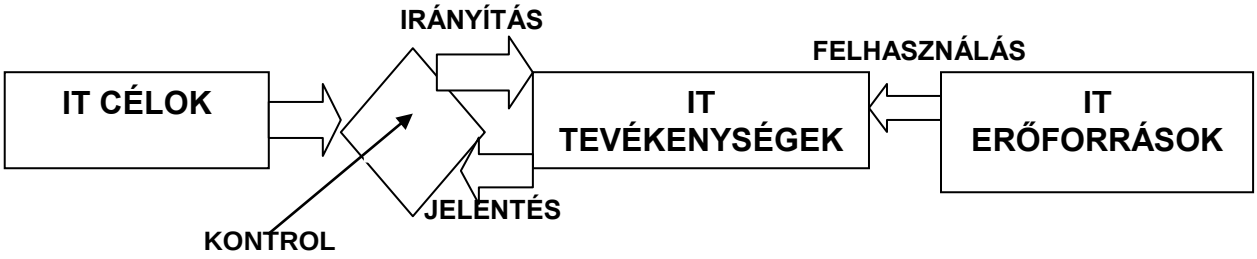
- IT biztonságirányítás,
- IT kockázat menedzsment,
- IT biztonsági program menedzsment,
- IT biztonságmenedzsment,
- IT válasz menedzsment.

6.1. AZ IT BIZTONSÁGIRÁNYÍTÁS

Az IT biztonságirányítás definíciója: Rendszer készítése, és karbantartása, gondoskodás a garanciákról, hogy a Biztonsági Stratégia megfeleljen az üzleti céloknak, és legyen konzisztens a törvényekkel, és szabályokkal.

Az IT biztonságirányítás célja: összpontosítani arra a szükségletre, hogy stabil irányítási program álljon rendelkezésre, így minden biztonsági stratégia, és folyamat tervezhető, implementálható, üzemeltethető és karbantartható legyen.

Az IT Biztonságirányítás funkcionális modellje:



AZ IT CÉLOK

- Az üzlet lehetővé tétele, és maximalizálása
- Az IT erőforrások felelősséggel való használata
- Az IT kockázatok megfelelő menedzselése

AZ IT TEVÉKENYSÉGEK

- Kockázat menedzsment (biztonság, gondoskodás az információkról, megfelelősség),
- Haszon realizálása az automatizálás hatékonyságával, és a költségek csökkentése az eredményesség elősegítésére.

Az IT erőforrások az előző pontban szerepelnek.

6.1.1. AZ ELVÉGZENDŐ FELADATOK

Az **IT biztonságirányítás** (IT SECURITY GOVERNANCE) tevékenységében a következők kiemelten meghatározóak:

- Az információk sértetlensége,
- A szolgáltatások folyamatossága, és
- Az informatikai erőforrások védelme.

Feladatok:

1. Az IT biztonsági stratégia fejlesztése az üzleti stratégiát, és irányítást szolgálva.
2. A menedzsment kötelezettségének, és támogatásának a megszerzése az IT biztonsághoz, a vállalat minden területén.
3. Gondoskodás arról, hogy a szerepek, és felelősségek meghatározása, mindenhol a vállalatnál, tartalmazza az IT biztonságirányítási tevékenységeket.
4. Jelentő, és kommunikációs csatornák kiépítése, amelyek támogatják az IT biztonságirányítási tevékenységet.
5. Azonosítja a jelenlegi, és lehetséges törvényi, és szabályozási témákat, amelyek hathatnak az IT biztonságra, és értékeli a vállalatra gyakorolt hatásukat.
6. Az IT biztonsági politikák támogatása, amelyek az üzleti célt, és előirányzatokat szolgálják.
7. Gondoskodás a folyamatok, és irányelvek fejlesztéséről, amelyek támogatják az IT biztonsági politikákat.
8. Üzleti esemény, és vállalati érték elemzést fejlesztése, amely támogatja az IT biztonsági program beruházásokat.

6.1.2. MAGYARÁZATOK A FELADATOKHOZ

1.-hez. A körültekintő üzleti gyakorlat megköveteli, hogy az IT folyamatok és irányelvek kövessék az üzleti folyamatokat, és célokat. Az igazgatóságtól elvárás, hogy az IT biztonság integrált része legyen a vállalatirányításnak. Az üzleti tevékenység növekedésének kulcs tényezője az IT. A kockázatok, a biztonság megsértésének növekedése jelentős, de igen sok feltáratlan marad. **A biztonsági folyamatok, módszerek, eszközök, és technikák együtt képezik a biztonsági stratégiát.** Az IT biztonsági menedzsernek kell gondoskodni arról, hogy a folyamatok, termékek, és szolgáltatások rendelkezésre álljanak a politikákhoz, architektúrákhoz, hitelesítéshez, jogosultság megadáshoz, az adminisztrációhoz, és a visszaállításhoz, az üzlet minden területén.

A biztonsági stratégia fő elemei:

- Kapcsolat az üzleti stratégiával,
- Politikák (követelmény szinten),
- Hitelesítés,
- Jogosultság menedzsment,
- Adminisztráció,
- Visszaállítás,
- Támogató szolgáltatások,
- Technológiák.

2.-höz.
A felső vezetés elkötelezettsége nélkül a biztonság nem valósítható meg, a vállalat minden területén.
A felső vezetés elkötelezettsége vonatkozik elsősorban:

- A vállalatirányításban magas szabványok elérésére.
- Az üzleti biztonság kezelése, mint egy kritikus üzleti ügy, pozitív biztonsági környezet kialakítására.
- A harmadik felek felé annak demonstrálására, hogy az IT biztonsággal a szervezet profi módon foglalkozik.
- Olyan alapelvek alkalmazására, mint felelősség vállalása az IT biztonságért, ellenőrzések implementálása, amelyek arányosak a kockázatokkal, és az egyéni számon kérhetőség elérése.

3.-hoz.

- A munkatársak felelőssége a munkaköri leírásokban meg kell, hogy jelenjen, a biztonság irányítás kihangsúlyozására. Az IT

biztonsági menedzsernek együtt kell kidolgoznia a humánpolitikai vezetővel ezeket a követelményeket.

4.-hez.

- Ki kell alakítani a jelentés csatornáját az IT biztonsági menedzser számára, a felső vezetés felé.

5.-höz

- Az IT biztonsági vezető feladata, hogy a jogi, és egyéb szabályozásoknak feleljen meg a biztonság, és mérje fel a vállalatra gyakorolt hatásukat.

6.-hoz.

- A biztonsági politikák fejlesztése, és karbantartása számára ki kell a megfelelő eljárást alakítani (figyelembe véve a szabványokat, (mint BS7799, MSZ ISO/IEC 17799-2002)

7.-hez.

- Gondoskodni kell folyamatokról, és irányelvekről, amelyek támogatják az IT biztonsági politikákat. Éspedig:

  - Háttér, és visszaállítás,
  - A politikák érvényesítése a meg nem felelősségre (pl. behatolás jelzés, audit).
  - A megfelelősség monitorozása.
  - Hálózati biztonsági politikák.
  - Rendszer sw politikák. Továbbá
  - Felügyeleti folyamatok.
  - Kockázat azonosítási folyamatok.
  - Biztonsági eseményekre válasz folyamatok.

8.-hoz.

- A beruházások hozam elemzése (Return on Investment, ROI), és a műveletek teljes költségének elemzése (Total Cost of Operation, TCO) a két alapvető vizsgálati cél egy projekt eldöntéséhez.
- Az IT biztonsági menedzsernek fejleszteni kel e két eljárást, a beruházások alátámasztáshoz.

A vállalatok igen gyakran az informatikai biztonsággal, mint technológiai kérdéssel foglalkoznak csak, kevés figyelmet fordítva a vállalat priorításaira, és követelményeire. A biztonság hatékonyságának az irányítása, és menedzselése felelősségét az üzemeltetési, és technikai menedzserekre korlátozzák.

Az IT biztonságirányításnak kell megteremteni a kapcsolatot az IT és az üzleti stratégia között.

Az „Information Security Governance: Guidance for Board of Directors and Executive Management” [lásd 32] az IT biztonsági vezetési

tevékenységeket, a fentiek figyelembe vételével a következők szerint határozza meg:

A felső vezetési szint IT biztonságirányítási tevékenységei (stratégiai):

- Folyamatosan informált a biztonságról.
- Megszabja az irányítást, vagyis politikát, és stratégiát működtet, és meghatározza a globális kockázati profilt.
- Erőforrásokat biztosít az IT biztonság eredményességéhez.
- Kijelöli a menedzsment felelősségeit.
- Meghatározza a prioritásokat.
- Támogatja a változásokat.
- Meghatározza a kulturális értékeket a biztonsági tudatosság vonatkozásában.
- Garanciákat szerez be a belső, és külső ellenőrzéstől.
- Ragaszkodik ahhoz, hogy a menedzsment a biztonsági beruházásokat, és a fejlesztéseket mérhetően végezze, valamint kövesse figyelemmel azok hatékonyságát.

A menedzser szint tevékenységei (taktikai):

- Biztonsági politikát ír, üzleti inputokkal.
- Gondoskodik arról, hogy az egyéni szerepek, felelősségek, és jogosultságok világosan legyenek kommunikálva, és mindenki értse meg.
- Azonosítja a fenyegetéseket, elemzi a sebezhetőségeket, és figyelembe veszi az általános gyakorlatot.
- Létrehozza a biztonsági infrastruktúrát.
- Fejleszt egy biztonsági, és ellenőrzési rendszert, amely szabványokat, mértékeket, gyakorlatot, és folyamatokat tartalmaz, és a szervezet irányító testülete egy politika alapján hagyja jóvá, valamint a szerepeket, és felelősségeket eszerint jelöli ki.
- Dönt, hogy milyen erőforrások álljanak rendelkezésre, meghatározza a lehetséges védelmi intézkedések fontossági sorrendjét, és implementálja a magas prioritású védelmi intézkedések közül azokat, amelyeket a vállalat tud biztosítani.
- Monitorozza a biztonsági eseményeket, és biztosítja azok kezelését.
- Periodikus vizsgálatokat, és teszteket végez.
- Biztosítja a biztonsági tudatosságot, oktatást, tréningeket.

- Biztosítja, hogy a biztonság integrált része legyen a rendszer életciklusának.
- Felhasználja az érettségi szint (maturity level) értékelési módszert (lásd melléklet) az önértékelésre.

6.2. IT KOCKÁZAT MENEDZSMENT

Az informatikai kockázat menedzsment definíciója: Az üzleti célok elérése érdekében azonosítja, és menedzseli az informatikai kockázatokat.

Az informatikai kockázat menedzsment célja: a biztonsági kockázatok azonosítása, és menedzselése az üzleti célok elérésére egy sor feladattal, amelyek hasznosítják a biztonsági menedzserek ismereteit a kulcs kockázat menedzsment technikákról.

6.2.1. AZ ELVÉGZENDŐ FELADATOK

1. Szisztematikus, elemzése, és folyamatos fejlesztése a kockázat menedzsmentnek.
2. Gondoskodás a kockázat azonosítás, elemzés, és csökkentési tevékenységek élet ciklusba integrálásáról.
3. Kockázat elemzési, és azonosítási módszerek alkalmazása.
4. A vállalat számára elfogadható kockázati szintcsökkentési stratégia, és választási lehetőségek fontossági sorrendjének megállapítása.
5. A szignifikáns kockázat változás jelentése rendszeresen, és esemény bázison, a menedzsment megfelelő szintjére.

Az informatikai kockázat menedzsment, a következő tevékenységeket jelenti:

- A veszélyforrások feltárása, vagy használják a veszélyforrások azonosítása meghatározást is,
- A kockázatok elemzése,
- Döntés a védelemről,
- A védelmi intézkedések specifikálása.

6.2.2.MAGYARÁZATOK A FELADATOKHOZ

1.-hez:

- A kockázat menedzsment folyamatos és dinamikus tevékenység legyen, amely gondoskodik a biztonsági program adaptálásáról, úgy, hogy folyamatosan védje a szervezet kritikus információit.

2.-höz:

- A kockázat menedzsment folyamatnak be kell épülnie a vállalat életciklusába.
- A vállalat életciklusában különösen fontos a változások követése, mivel egy-egy változás újabb kockázatokat jelenthet. A szervezetben, illetve az IT hálózatban, hw.-ben, alkalmazásokban bármely változás, változást jelent a kockázatokban is.
- A változás menedzsment követés a szervezet életciklusában egy megelőző tevékenység, amely lehetővé teszi a biztonsági vezető számára a biztonsági politika tervezését, és implementálását a szervezet üzleti céljainak megfelelően.

3.-hoz:

- A kockázat azonosítás, és elemzés a biztonsági vezető számára lehetővé teszi a kockázati veszélyforrások csökkentési stratégiájának kidolgozását. Az azonosítás, és elemzés magába foglalja a következőket:

    - Kockázati esemény (egy lehetséges esemény)
    - Valószínűség (a kockázat bekövetkezésének valószínűsége egy időn belül).
    - Várható érték (a kockázati esemény számszerűsíthető következménye).

4.-hez:

- Az IT biztonsági menedzser kulcs feladata a kockázatok csökkentése. Az azonosítás, és fontossági sorrend megállapítás lehetővé teszi a biztonsági menedzser számára a biztonsági stratégia kiigazítását, és a kockázatok csökkentését. A védelmi intézkedések lehetnek:

    - Elrettentő, a szándékos támadások csökkentésére.
    - Megelőző, a támadás sikertelensége, illetve a hatása csökkentése érdekében.
    - Javító a támadás hatásának csökkentésére.
    - Feltáró, a támadás feltárására, és megelőző vagy javító védelmi intézkedés indítására.

5.-höz:

- A szervezeten belüli változások következtében a kockázat menedzsmentnek is változnia kell, ezért a biztonsági menedzsernek időnként a naprakészség céljából értekezletet kell szerveznie, folyamatosan követni kell a kockázatok alakulását.

6.3. IT BIZTONSÁGI PROGRAM MENEDZSMENT

Az informatikai biztonsági program menedzsment definíciója: Az IT biztonság irányítási program fejlesztése, tervezése, és menedzselése az IT biztonság irányítási rendszer implementálása érdekében.

Az informatikai biztonsági program menedzsment célja: az IT biztonsági program tervezése, fejlesztése, és menedzselése annak érdekében, hogy az IT biztonsági irányítási rendszert implementálják, néhány feladattal tesztelve, amelyek használják a biztonsági menedzser tudását a kockázat elemzésről, a projekt menedzsmentről, és más technikákról.

6.3.1. AZ ELVÉGZENDŐ FELADATOK

1. Az IT biztonság irányítási rendszer implementálására tervek, program készítése, és karbantartása.
2. Az IT biztonsági alapok fejlesztése.
3. Folyamatok, és irányelvek fejlesztése a biztonsági kockázatok figyelembe vételével az üzleti folyamatokról történő gondoskodás céljából.
4. Folyamatok, és irányelvek fejlesztése gondoskodás arról, hogy az IT infrastruktúra tevékenységei feleljenek meg az IT Biztonsági Politikának.
5. IT biztonsági program követelményeinek integrálása a szervezet életciklus tevékenységeibe.
6. Az informatikai biztonsági követelményeknek megfelelő módszerek fejlesztése a végfelhasználókra gyakorolt hatás felismerésére.
7. Az üzleti folyamatok tulajdonosai, és mások számon kérhetőségének támogatása az IT biztonsági kockázatok menedzselésében.
8. Mérések meghatározása az IT biztonság irányítási rendszer menedzselésére.
9. Gondoskodás az informatikai biztonság külső, és belső erőforrásainak azonosításáról, megfelelősségéről, és menedzseléséről.

6.3.2. MAGYARÁZATOK A FELADATOKHOZ

1.-hez:

- Az IT biztonsági program sikeres végrehajtása azt igényli a biztonsági menedzsertől, hogy készítsen tervet:
  - Határozza meg a biztonságirányítási rendszert
  - Hagyassa jóvá a felső vezetéssel
  - Implementálja

  - Kövesse a teljesülését, és ha szükséges módosítsa.
- Az IT biztonsági menedzser felelős a terv végrehajtásáért, de nagyobb szervezetnél az IT, illetve a biztonsági szervezethez delegálhat belőle feladatokat.

2.-höz:

- A biztonsági politika, a biztonsági folyamatok implementálása után az IT biztonsági menedzsernek meg kell határozni az alapvető, minimális biztonsági szintet, amelyen védi az erőforrásokat (pl. MSZ ISO/IEC 17799-2002).

3.-hoz:

- A leghatékonyabb IT biztonságprogram, ahol, a biztonság minden üzleti folyamatban figyelembe van véve. Ez az általános biztonsági program kifejezi a szervezet üzleti követelményeit.
- Az IT biztonsági menedzsernek együtt kell dolgoznia az üzleti menedzserekkel, az üzleti folyamatok tulajdonosaival, és irányelveket kell kidolgoznia, amelyet támogat a felső vezetés.

4.-hez:

- Az IT infrastruktúra szervezetenként eltérhet, de általában a következő:
  - Folyamatok,
  - Fizikai infrastruktúra,
  - Platformok (op. rendszerek, alkalmazások), és
  - Hálózati infrastruktúra.
- Az IT biztonsági menedzsernek ki kell dolgoznia a folyamatokat, és irányelveket, amelyek biztosítják az IT infrastruktúrában a biztonsági politika érvényesítését.

5.-höz:

- Az IT biztonsági menedzsernek gondoskodni kell arról, hogy minden életciklus fázisban megvalósuljanak a biztonsági követelmények.

6.-hoz:

- A biztonság hatását a végfelhasználóra a biztonsági politikának figyelembe kell vennie.

7.-hez:

- Biztosítani kell az üzleti folyamatok, és más tulajdonosok felelősségének számon kérhetőségét az IT biztonsági kockázatok menedzselésében.
- Az IT biztonsági menedzsernek oktatni kell a tulajdonosoknak, és más felelősöknek a biztonsági tudatosságot.

8.-hoz:

- Az IT menedzser tudja legjobban felmérni, és kiigazítani, hogy mennyire teljesül a biztonsági politika, és menedzselni a biztonságirányítást.
- Az IT menedzsernek szükséges kialakítani, hogyan méri (mennyiségileg, minőségileg) a kockázat, a teljesítmény nagyságát, a munkavállalók tudatosságát, és adottságait

9.-hez:

- Az IT rendszerek alkalmaznak belső, és külső (szállítók, szervizek, konzultánsok, kutatók, szabványosítók) erőforrásokat, amelyeket egyaránt kezelni kell, amelyek biztonsági szempontból az IT biztonsági menedzser feladatkörébe tartoznak.

Az IT Biztonsági Program siker tényezőinek kritikus, és kiegészítő elemei a 10. sz. mellékletben találhatók.

6.4. IT BIZTONSÁGMENEDZSMENT

Az informatikai biztonságmenedzsment definíciója: Az IT biztonsági tevékenységek ellenőrzése, és irányítása, a biztonsági program végrehajtása érdekében.

Az informatikai biztonságmenedzsment célja: Összpontosítás azokra a feladatokra, és ismeretekre, amelyek a szervezeten belül a hatékony informatikai biztonságmenedzseléshez szükségesek, a biztonsági menedzserek számára.

6.4.1. AZ ELVÉGZENDŐ FELADATOK

1. Gondoskodás arról, hogy az IR használatának szabályai feleljenek meg az IT Biztonsági Politikájának.
2. Gondoskodás arról, hogy az IT adminisztratív folyamatok az Informatikai Biztonsági Politikával konzisztensek legyenek.
3. Gondoskodás arról, hogy a más vállalatok szolgáltatásai, beleértve az erőforrás kihelyezést, feleljenek meg az IT Biztonsági Politikának.
4. Az IT biztonsági védelmi intézkedések hatékonyságáról, és az IT Biztonsági Politika megfelelősségéről a mérés, monitorozás, és jelentéshez mértékek használata.
5. Gondoskodás arról, hogy az IT biztonság ne sérüljön a program csere menedzsment folyamatban.
6. Gondoskodás arról, hogy a sebezhetőség felbecsülését végrehajtsák a működő védelmi intézkedések hatékonyságának értékelésében.

7. Gondoskodás arról, hogy a meg nem felelősségeket, és más változásokat időben megoldják.
8. Gondoskodás arról (beleértve az IT biztonság oktatását, és a biztonsági tudatosságot), hogy a tevékenységek fejlesztése, és szállítása kedvezően befolyásolja az állomány kultúráját, és magatartást,

6.4.2. MAGYARÁZATOK A FELADATOKHOZ

1.-hez:
- A jól menedzselt szervezetben sok szabály, eljárás rend stb. létezik. Ezek a felhasználás minimális szabályai.
- Ezeknek a szabályzásoknak meg kell felelniük az IT biztonsági politikának.

2.-höz:
- Az adminisztratív szabályoknak is meg kell felelniük az IT biztonsági politikának.

3.-hoz:
- Az erőforrás kihelyezésnél érvényesíteni kell a biztonsági politikát (outsourcing),
- Az IT biztonsági menedzsernek gondoskodni kell e szabály betartásának a monitorozásról a harmadik félnél is.
- A harmadikféllel kötött szolgáltatási szerződést ellenőrizni kell, tartalmazza-e a biztonsági követelményeket.

4.-hez:
- Ellenőrizni, monitorozni, és mérni kell, hogy a védelmi intézkedések hatékonysága, és eredményessége kielégítő-e, valamint megfelel-e a biztonsági politikának.
- Feltétlenül fontos, hogy az előbbiekben említettek védelmi tevékenységet eredményezzenek.

5.-höz:
- A változtatások, az esetleges megkerülések feltárása fontos feladat.
- A távoli munkahelyek változtatásai, és a központi változások követése szintén fontos feladat.

6.-hoz:
- A működő védelmi intézkedések sebezhetősége esetleges változásának a folyamatos felbecsülése a biztonsági vezető feladatai közé tartozik.
- A biztonsági vezető erre a feladatra külső konzulenst vehet igénybe, amely az objektivitást biztosítja.

7.-hez:

- Gondoskodni kell, hogy megfelelő időben megtörténjen a meg nem felelősség, és más ellentmondás feltárása. Ehhez szabályozott követő rendszer szükséges.

8.-hoz:

- Az IT biztonsági vezetőnek gondoskodni kell arról, hogy a biztonsági tudatosság, a biztonsági oktatás, biztosítsa a szervezet biztonsági kultúráját, a biztonsági céllal való azonosulást.
- A tudatosság azt jelenti, hogy jól tájékozottak vagyunk, törődünk, és tudatában vagyunk egy speciális dolognak, és ez magába foglalja e dolog ismeretét, és megértését, valamint, hogy ennek megfelelően cselekszünk [20].
- A biztonsági tudatosság a mértéke annak, hogy egy szervezet minden tagja, és akik hozzáférhetnek a szervezet információihoz, miként értette meg [20]:
    - A biztonság, és a biztonsági szint szervezeti megfelelősségét,
    - a biztonság fontosságát, és a biztonsági hiányosságok következményeit,
    - a biztonsági felelősségét, és az ennek megfelelő cselekvését.
- E tevékenységnél a visszacsatolás biztosíthatja a folyamatos tökéletesítést.

6.5. VÁLASZ MENEDZSMENT

A válasz menedzsment definíciója: A bomlasztó, és romboló biztonsági események megválaszolására, és a visszaállításra fejleszti, és menedzseli a rendszer képességeit.

A válasz menedzsment célja: A biztonsági menedzserek számára szükséges információk, és tevékenységekre összpontosítva támogatni, hogy a szervezet válaszoljon, és visszaállítson a bomlasztó, és romboló informatikai biztonsági eseményekre.

6.5.1. AZ ELVÉGZENDŐ FELADATOK

1. Folyamatok fejlesztése, és implementálása a biztonsági események észlelésére, azonosítására, és elemzésére (Biztonsági események kezelési rendje, ÜFT).
2. Válasz, és visszaállítási terv fejlesztése a teamek képzését, gyakorlását, és szervezését beleértve.

3. Gondoskodás a válasz, és visszaállítási terveknek a periodikus teszteléséről.
4. Gondoskodás a követelményeknek megfelelő végrehajtásáról a válasz, és visszaállítási terveknek.
5. A biztonsági események következetes dokumentálása, s ha szükséges bírósági eljárás indítása.
6. Az eseményeket követően az okok, és javító tevékenységek azonosításának menedzselése.

6.5.2. MAGYARÁZATOK A FELADATOKHOZ

1.-hez:

- A kockázat menedzsmentben definiált szükségesség alapján, a fejlesztése, és az implementálása folyamatoknak, amelyek észlelik, azonosítják, elemzik, az informatikai erőforrásokra kedvezőtlenül ható biztonsági eseményeket.
- Az elemzések eredményeképpen az IT menedzser módosítani tudja, ha szükséges, az informatikai biztonsági programot.

2.-hez:

- Tekintettel arra, hogy nincs garancia arra, hogy az erőforrások bizalmassága, sértetlensége, és rendelkezésre állását fenyegető kockázatok megszüntethetőek, az IT biztonsági menedzsernek ellenőrizni kell a válasz, és visszaállítási terv fejlesztését.
- A felső vezetés jóváhagyja, az IT biztonsági menedzser felügyeli a terv fejlesztését.
- Az IT biztonsági menedzser gondoskodik arról, hogy a team tagok megismerjék, és folyamatosan kövessék a tervet.

3.-hoz

- A tervet rendszeresen tesztelni kell, és erre az IT biztonsági menedzser tervet készít, amely a következőket tartalmazza:
  - Fejlesztés
  - Végrehajtás
  - Értékelés
  - Ajánlások a tovább fejlesztésre
  - Követési folyamat implementálása.
- A nem tesztelt terv kockázatot képez, ezen kívül a tesztet független harmadikféllel monitoroztatni, és értékeltetni is kell.

4.-hez:

- Gondoskodni kel arról, hogy a terv végrehajtásra kerüljön, amelyhez szükséges egy koordinátor.
- Az IT biztonsági menedzser nem lehet a koordinátor, de meg kell figyelnie neki is a végrehajtást.

- A végrehajtást követően egy utólagos értékelést kell készíteni a koordinátornak, és az IT biztonsági vezetőnek.

5.-höz:

- A biztonsági szervezetnek dokumentálni kell a biztonsági eseményeket, és jelentést kell készíteni azokról.
- Amennyiben szükséges a jelentést továbbítani kell a bűnüldöző szervek felé.

6.6. A SZAKTERÜLETEK FŐ FELADATAI

Az öt CISM szakterület főfeladatai:

1. Biztonsági Stratégia készítése, menedzselése
2. Kockázat menedzsment
3. Programkészítés, és menedzsment
4. Biztonsági politikakészítés, és menedzselés
5. Válasz menedzsment.

7. AZ IT BIZTONSÁGSZERVEZÉS

7.1. AZ INFORMATIKAI BIZTONSÁGMENEDZSMENT RENDSZER, ISMS

7.1.1. AZ ISMS

Az elmúlt évben megjelent a BS 7799-2 szabvány továbbfejlesztett változatának magyar fordítása „az MSZ-ISO/IEC27001: 2006 Information Security Management System. Requirements" című szabvány, az ISMS. A szabvány az informatikai biztonságmenedzsment rendszer (gyakorlatilag ez a 4.6 Biztonsági rendszer c. fejezet biztonsági rendszer fogalmából az informatikai biztonsági rendszer) kiépítéséhez, üzemeltetéséhez, fenntartásához a folyamat megközelítés elvét alkalmazza, amely annak a felismerésén alapul, hogy

- Egy szervezet informatikai biztonsági követelményeit, és az informatikai biztonság céljait először meg kell érteni,
- Implementálni és üzemeltetni kell védelmi intézkedéseket az informatikai biztonság kezelésére, összhangban a szervezet üzleti kockázataival,
- Követni, felülvizsgálni kell az ISMS teljesítményét, és hatékonyságát,
- Objektív mérések alapján, folyamatosan tökéletesíteni kell.

Az ISO 2700-es szabvány család eddig megjelent tagjai:

- ISO 27001 - **The Information Security Management System requirements.** Magyar megfelelője MSZ-ISO/IEC 27001:2006, a korábbi BS 7799 part 2 megfelelője.
- ISO 27002 (az ISO 17799, illetve a BS 7799 part 1 megfelelője) – **Information Sercurity Mangement, Code of Practice**

Az alábbiak 2008 körül jelennek meg:

- ISO 27003 - **implementation guide** (implementálási irányelvek)
- ISO 27004 - **Metrics and Measurement** (mértékek és mérés)
- ISO 27005 - **Risk Management** (a BS 7799 Part-3 megfelelője) kockázat menedzsment
- ISO 27006 - **guide to the accreditation process** (az akkreditálási folyamat irányelvei)

Az ISMS a „PLAN-DO-CHECK-ACT”, „TERVEZÉS-MEGVALÓSÍTÁS-ELLENŐRZÉS-INTÉZKEDÉS” modellt használja, amely a következő folyamatokat kapcsolja rendszerbe:

- Tervezés,
- Üzemeltetés,
- Követés, felülvizsgálat,
- Karbantartás,
- Fejlesztés.

A PDCA modell:

- *PLAN (tervezés)*

Az ISMS politika, célok, folyamatok, és eljárások megalapozása, a kockázat menedzsmentnek megfelelően, és az informatikai biztonság fejlesztése eredmények elérésére a szervezet általános politikájának, és céljainak megfelelően.

- *DO (megvalósítás)*

Az ISMS politikák, célok, folyamatok, és eljárások megvalósítása, és működtetése.

- *CHECK (ellenőrzés)*

A folyamatok teljesítményének, értékelése, ahol lehet mérése az ISMS politika, célok, és a gyakorlati tapasztalatok alapján, és a menedzsment tájékoztatása.

- *ACT (intézkedés)*

Javító, és megelőző akciók az ISMS belső ellenőrzése, és a menedzsmentnek adott jelentés, illetve más relevans információk alapján, az ISMS folyamatos fejlesztése érdekében.

7.1.2. AZ ISMS ÉS MÁS SZABVÁNYOK

Az ISMS megfelel az ISO 9001: 2000, és az ISO 14001: 2004 minőség biztosítási szabványok követelményeinek, így várható, hogy a jövőben az ennek való megfelelősséget fogják preferálni, illetve tanúsítatni.

Az ISMS a biztonságirányítás, és kezelés keretrendszere, amely kimondja, hogy a megvalósításhoz az ISO/IEC 17799 (magyar megfelelője az MSZ-ISO/IEC 17799:2004) szükséges, illetve a szabvány szerint nélkülözhetetlen a megvalósításhoz. Ez azt jelenti, hogy az ISO 27001 tanúsítás, még nem jelenti, hogy a követelményeknek, elvárásoknak megfelelő az IT biztonság, hanem az MSZ-ISO/IEC 17799-nek is meg kell felelni.

Az alábbiakban ismertetett SMM módszertan, és az ISMS összefüggései *(az SMM az ISMS megvalósításának módszertanaként alkalmazható, figyelembe véve az ISO/IEC 17799, és COBIT4 megfelelősségét is)* a következők:

- *PLAN* ➔ Kockázat menedzsment (Helyzetfeltárás, Veszélyforrás elemzés, Védelmi intézkedések specifikálása, Szervezet, és Működés szabályozása),
- *DO* ➔ Implementálás, Üzemeltetés, Karbantartás,
- *CHECK* ➔ Ellenőrzés,
- *ACT* ➔ Intézkedés (válasz) az ellenőrzés alapján

Az ISMS célokat az SMM-ben a Biztonsági program fogja össze, illetve határozza meg.

7.2. AZ INFORMATIKAI BIZTONSÁGMENEDZSMENT MÓDSZERTANA (SMM)

A módszertan a biztonsági rendszer, és alrendszerek kiépítésére, a biztonsági rendszer menedzsmentjére, a biztonsági rendszer rendszerszervezés útján való megvalósítására (mind a három biztonsági alrendszerben) szolgál.

A rendszer fogalma a következő:

A rendszer egymással valamilyen kapcsolatban álló elemek összessége.

Rendszer például egy számítógép, vagy bármely technikai eszköz, illetve egy gazdasági szervezet, egy intézmény. A rendszereken belül csoportokat, alrendszereket képezhetünk. Így például egy gazdasági szervezeten belül lehet termelési, üzleti, informatikai, de biztonsági rendszer is. A rendszerek maguk állandó mozgásban, változásban vannak. A gazdasági rendszerek, ezen belül az információ-rendszer, a bonyolult rendszerek, közé tartozik. Ezeket az jellemzi, hogy az elemeik között végtelen sok korreláció létezik. Ebből az következik, hogy egy elem megváltozásának más elemekre gyakorolt hatását exakt módszerekkel nem lehet meghatározni. Biztonsági szempontból ez annyit jelent, hogy például egy támadás, amely egy elemet fenyeget, ha bekövetkezik, további elemekre is gyakorolhat hatást. Mindebből az következik, hogy a biztonsági alrendszert eredményesen csak rendszer szemlélettel lehet megszervezni. A szervezést, pedig felülről lefelé (top down) kell végezni. Azaz az üzleti követelményekből kiindulva, a gyakorlatot felmérve, lehet, és kell a védelmi intézkedéseket kidolgozni. A felülről lefelé elv megkerülése, az alulról felfelé elv (amely jellemző gyakorlat), a biztonsági alrendszer hatékonyságát teszi kétségessé.
A biztonsági alrendszer szervezését a biztonsági rendszerszervező végzi.

Rendszerszervezésen a szervezetben végbemenő folyamatok, valamint irányításuk, és ellenőrzésük kidolgozását értjük.

Feltétlenül fel kell hívni a figyelmet arra, hogy a biztonságszervezés, a biztonságmenedzsment érdekütközésekkel jár, járhat. Az IBV-nek erre munkája során oda kell figyelnie. A biztonsági célkitűzések megvalósítása nem függhet attól, hogy valakinek ellentétes érdekei vannak. Kérdés mi a megoldása ennek a problémának. Egy részről

törekedni kell a biztonsági tudatosság, az intézkedés indokoltságának elfogadtatására, másrészt a vállalat menedzsmentjének bevonásával meg kell találni a módját az „elvett” kompenzálására. Ne felejtsük el, hogy az ember a biztonság kemény tényezője, minden döntésnél ezt a tényt figyelembe kell venni.

A biztonságmenedzsment folyamatban természetesen minden menedzser arra törekszik, hogy a legjobb megoldásokat valósítsa meg. Ezt a törekvést fejezi ki **a legjobb gyakorlat, BEST PRACTICE** folyamatos figyelembevétele az alkalmazók számára. Az irodalmi hivatkozások szerint, jelenleg a legjobb gyakorlatot tartalmazza

- Az MSZ-ISO/IEC 27001:2006 Informatikai Biztonságmenedzsment Rendszer, Követelmények,
- Az ISO/IEC 17799, illetve magyar megfelelője, az MSZ ISO/IEC 17799, és az MSZ-ISO/IEC 27001:2006.
- A COBIT 3, és 4.

Ugyanakkor a független INFORMATIKAI BIZTONSÁGI FORUM (London), már hosszabb ideje foglalkozik azzal, hogy feldolgozza, és kiadja azt. Legutóbbi kiadványa

- az Information Security Forum Good Practice for Information Security. Version 4.1. 2005.

Várhatóan a jövőben ez terjedni fog. Ez a könyv olyan megoldásokat tartalmaz, amelyek döntő többsége megfelel a fenti szabványnak, illetve a COBIT-nak. Azokban az esetekben, amikor ezt nem állíthatjuk, azt kijelenthetjük, hogy a szerző a hazai, és külföldi tapasztalatokat a könyv megírásakor figyelembe vette.

7.2.1. AZ IT BIZTONSÁGMENEDZSMENT VÉGREHAJTÓI

Az IT biztonságmenedzsment, szervezés végrehajtói elsősorban a biztonsági szervezet munkatársai, az IT biztonság menedzser irányításával, esetleg külső szakértők, tanácsadók bevonásával
Ugyanakkor a biztonsági tevékenységet, de az informatikai tevékenységeket is csak a feladat szétválasztás elve betartásával lehet munkaköri feladatként kiadni. Minimálisan szét kell választani a következő feladatokat (lásd COBIT 3):

- az adatvédelmi, és az IT biztonsági munkakörök,
- az IT biztonsági, és informatikai munkakörök,

- informatikai fejlesztés, és üzemeltetés,
- az informatikai üzemeltetés, és az adatellenőrzés,
- az informatikai üzemeltetés, és karbantartás,
- az informatikai üzemeltetés, és a felhasználás.

7.2.2. AZ IT BIZTONSÁGMENEDZSMENT FOLYAMAT

A biztonságmenedzsment tevékenység egy folyamat, amelynek táblázatos bemutatása az alábbi ábrán látható. A biztonság értékelés módszereit meghatározó Common Criteria 2.1 (MSZ ISO/IEC 15408 1,2,3) felhasználásával mutatjuk be, hogy miből kiindulva, milyen feladatot kell megoldani a biztonságszervezőnek. A biztonsági környezet megadja azokat a feltételeket, amelyek között az információ-rendszernek dolgoznia kell. Az erőforrások azok az emberek, és eszközök, amelyekkel az információ-rendszernek az üzleti követelményeket ki kell elégítenie. A biztonsági környezet, és a fenyegetések együtt képezik a valós helyzetet. A kockázatok elemzése az alapja a biztonsági követelmények meghatározásának, amelyek megvalósítását a kockázatok csökkentésére teendő védelmi intézkedések specifikálása kell, hogy tükrözzön. Végül a védelmi intézkedések implementálása vezet a biztonsági alrendszer üzemeltetéséhez. A biztonságszervezésnek ezt a folyamatot kell követnie.

A biztonságmenedzsment folyamat a táblázatban feltüntetett dokumentumokban, és egyéb dokumentumokban testet, öltő szabályozásokat is jelent. A biztonságmenedzsment folyamat értelmezése, a biztonságszervezés folyamata, a tevékenységek, a témák, és a végtermékek a következő ábrán láthatók. Felhívjuk a figyelmet arra a biztonságszervezési folyamat egyes lépéseinek sorrendje nem változtatható meg, illetve nem lehet egy lépést a korábbiak megtétele nélkül megtenni, mert ez az egyenszilárdság elvének a megsértéséhez vezet.

TEVÉKENYSÉG → / TEVÉKENYSÉG TÁRGYA ↓	HELYZET FELTÁRÁS	VESZÉLY FORRÁS FELTÁRÁS KOCKÁZAT MGM	VEDELMI KÖVETELMÉNYEK	VÉDELMI INTÉZKEDÉSEK SPECIFIKÁCIÓJA RÉSZLEGES	VÉDELMI INTÉZKEDÉSEK SPECIFIKÁCIÓJA ÁTFOGÓ	SZABÁLYOZÁS	IMPLEMENTÁCIÓ	ÜZEMELTETÉS	ELLENŐRZÉS	RENDSZER KÖVETÉS
BIZTONSÁGI KÖRNYEZET *Szervezési környezet* *Erőforrások* *Védelmi intézkedések* *Fenyegetettség*	x x x x	X								
KOCKÁZAT *Szervezési veszélyforrások,* *Technikai veszélyforrások* *Kockázatai*		X X			x x					
BIZTONSÁGI CÉL *Bizalmasság* *Sértetlenség* *Rendelkezésre állás* *Számon kérhetőség* *Garanciák*			x x x x x		x x x					
BIZTONSÁGI KÖVETELMÉNYEK *Szervezési* *Technikai*			x x							x x
VÉDELMI INTÉZKEDÉSEK **Szervezési** **Technikai** **Fizikai** **Logikai**				X X X	X X X	X X X	X X X		X X X	X X X

VÉGTERMÉK	IT BIZTONSÁGI PROGRAM								
	TERVEZÉS					MEGVALÓSÍTÁS		ELLEN.	INTÉZK.
	Biztonsági átvilágítási Jelentés	B.-i Stratégia	B.-i Politika	ÜFT	Bizt.-i Szabály-zat	Működő B.-i Rendszer	Üzemelő B.-i rendszer	Ellenőr-zés	Intézkedések

A BIZTONSÁG SZERVEZÉSI FOLYAMAT ELVI LÉPÉSEI

AZ ALAP	**A FELADAT**	**AZ EREDMÉNY**
	❶ LÉPÉS	
JOGSZABÁLYOK, ŰZLETI STRATÉGIA **BELSŐ SZABÁLYOK ERŐFORRÁSOK MŰKÖDŐ VÉDELEM**	⇨ Mit kíván az üzleti *ér*dek?	⇨ **BIZTONSÁGI KÖRNYEZET**
	❷LÉPÉS	
BIZT.-I KÖRNYEZET FENYEGETÉSEK	⇨ Mi a gyakorlat?	⇨ **KOCKÁZATOK**
	❸LÉPÉS	
KOCKÁZATOK	⇨ Mit kell elérni ?	⇨ **BIZTONSÁGI *KÖVETELMÉNYEK***
	❹LÉPÉS	
BIZTONSÁGI KÖVETELMÉNYEK	⇨Mit,hogyan kell védeni?	⇨ **VÉDELMI INTÉZK. SPECIFIKÁCIÓJA**
	❺ LÉPÉS	
VÉDELMI INT.	⇨Hogyan kell megvalósítani?	⇨ **IT. BIZT. ALREND IMPLEMENTÁLÁSA**

7.2.3. AZ IT BIZTONSÁGI ALRENDSZER GAZDÁI

SZERVEZÉSI BIZTONSÁG

• Szervezet és működés szabályozása	Titkárság
• Biztonságszervezési dokumentumok	Biztonsági vezető
• Titok (adat) védelem szabályozása	Adatvédelmi, Biztonsági Vezető
• Iratkezelés szabályozása	Titkárság
• Humán politika	Humán erőforrások vezető
• Szerződések (Kockázat áthárítás)	Gazdasági vezető

TECHNIKAI BIZTONSÁG

• Fizikai biztonság	
➢ Hozzáférés védelem	Vagyonbiztonsági vezető
➢ Rendelkezésre állás	Vagyon bizt. vezető
• LOGIKAI BIZTONSÁG	
➢ Hozzáférés védelem	Inf.-i biztonsági vez.
➢ Rendelkezésre állás	Inf.-i biztonsági vez.
➢ Hálózati védelem	Inf.-i biztonsági vez.
➢ Védelem az életciklus során	Inf.-i biztonsági vez.

7.2.4. SZABÁLYOZÁSI FELADATOKRA PÉLDÁK AZ IRÁNYÍTÁS SZINTJEIN

Az egyes szinteknél feltüntetett szabályozásokat egy a szinteken elhelyezkedő vezető adja ki, írja alá, de nem ő készíti el, viszont ő (ők) a felelős(-ek) a megfelelősségéért, és a magvalósulásáért.

STRATÉGIAI SZINT: Üzleti célok, küldetés, a főbb elvek összessége, hosszú távú: Üzleti, Informatikai, Termelési, és Biztonsági Stratégia (Igazgatóság, Vezérigazgató).

TAKTIKAI SZINT: rövid távú: a stratégiát megvalósító módszerek követelmények, erőforrások, védelmi intézkedések meghatározása, mint Üzletpolitika, Informatikai Fejlesztési Terv, Termelési Fejlesztési Terv, Biztonsági Politika, Üzletmenet folytonossági Terv (BCP), Biztonsági Szabályzat, és az Akció tervek, az Adatvédelmi és Adatbiztonsági Szabályzatok, és Titokvédelmi Utasítás, Iratkezelési Szabályzat, Selejtezési Szabályzat (biztonsági, üzleti, termelési, informatikai menedzserek).

SZABÁLYOZÁSI SZINT napi szintű végrehajtási rendelkezések:
Informatikai, üzleti, biztonsági (életciklus szabályozás), termelési szabályozások (osztályvezetők, csoportvezetők)

MÚVELETI SZINT a folyamatos feladat végrehajtás szintjén az eljárás rendek, de gyakorlatilag minden szabályozás érinti (munkatársak).

7.2.5. A BIZTONSÁGMENEDZSMENT FOLYAMAT TEVÉKENYSÉGEI

A biztonságmenedzsment, a biztonsági alrendszerek szervezése, a tevékenységek a biztonsági dokumentumokban öltenek formát. Ezek valójában tartalmazzák mindazt, amit a biztonság megteremtése, üzemeltetése, a biztonsági követelmények kikényszerítése érdekében tenni kell. A biztonsági dokumentumokban testet öltő intézkedések, feladatok sokféleképpen csoportosíthatóak. Jelenleg sem hazánkban, sem az elérhető szabványokban, ajánlásokban nem található egységes előírás. Egyet azonban nyugodtan rögzíthetünk mindazt, amit az alábbi csoportosításban a biztonsági dokumentumok tartalmaznak, a hatékony, és eredményes védelem eléréséért meg kell tenni.

7.2.5.1. BIZTONSÁGI ÁTVILÁGÍTÁS

A Biztonsági Átvilágítás a következő tevékenységekből áll:

- Helyzetfeltárás
- Veszélyforrás elemzés
- Kockázat elemzés

HELZETFELTÁRÁS

A HELYZETFELTÁRÁS CÉLJA

A veszélyforrás elemzéshez az információ-rendszer gyengeségeinek, a veszélyforrásoknak a feltárása (és nem a felmérése).

A HELYZETFELTÁRÁS TÁRGYA

- a biztonsági környezet, amelyen belül:
  - az információ-rendszerrel szembeni üzleti elvárások,
  - a jogi feltételek (jogszabályok, és belső szabályzatok),
  - a szervezet és működés,
  - a humán politika,
- a gazdasági szervezet küldetésének teljesítéséhez biztosított informatikai erőforrások, és
- a megtett, már működő védelmi intézkedések, és újabb veszélyforrások, kockázatok feltárása.

A biztonsági környezet megszabja azokat a feltételeket, amelyek szerint az informatikai szolgáltatásokat a felhasználóknak nyújtani kell. Az informatikai erőforrások a biztonsági környezet által meghatározott feltételek, követelmények megvalósításához a tulajdonos által rendelkezésre bocsátott erőforrások, míg a védelmi intézkedések az erőforrások védelmére, a kockázatok csökkentésre szolgálnak.
A helyzet feltárás során elemi követelmény, hogy csak tények kerüljenek rögzítésre, mivel az ezekből levont következtetések a veszélyforrásokon keresztül elvezetnek a védelmi intézkedésekhez, és eleve meghatározzák az eredményt a szervezendő biztonsági alrendszert.

A HELYZETFELTÁRÁS MÓDSZERE

- az ellenőrzési listák adaptálása,
- interjúk készítése,
- dokumentumok tanulmányozása, és
- szemlék.

ELLENŐRZÉSI LISTA

A helyzetfeltárás megkezdése előtt rendelkezésre állnak az átvilágítás általános ellenőrzési szempontjai. Az általános ellenőrzési szempontokat az átvilágítás megkezdése előtt adaptálni kell. A védelmi intézkedések, átvilágításához fel kell használni a 15. pontban megadott „Védelmi intézkedések köre" tárgyú táblázatot. Az általános ellenőrzési lista adaptálása az alábbi lépésekből áll.

- 1. Lépés. Megközelítés

A következő anyagokat kell a biztonsági rendszerszervezőnek megismernie:

- üzleti (igazgatási szervezetnél küldetésből adódó) követelmények,
- szervezet és működés,
- jogszabályok, szabályzatok,
- erőforrások,
- alkalmazott védelmi módszerek,
- biztonságmenedzsment, és
- biztonsági dokumentumok (korábbi biztonsági átvilágítási jelentés, Biztonsági Politika, ÜFT, Biztonsági Szabályzat, és biztonsági események naplói)

- 2. Lépés. Alkalmazás

A következőket kell végrehajtani:

- az általános ellenőrzési lista alkalmazása a kijelölt átvilágítási területre (ÜR és /vagy IR),
- a tanulmányozandó dokumentumok meghatározása,
- a mintavétel elve alapján szervezeti egységek kijelölése, és
- az interjú alanyok kijelölése.

- 3. Lépés. Specifikálás

A következőket kell az ellenőrzési listán átvezetni:

- szektor specifikus követelmények,
- szabványok,
- megvalósítás specifikus követelmények (pl. informatikánál: platformfüggő követelmények).

7.2.5.2. ELLENŐRZÉSI LISTÁK

AZ ÜZLETI RENDSZER ELLENŐRZÉSI LISTÁJA

(Sablon, magas szintű szempontokkal)

Szervezési helyzetfeltárás

- Biztonsági szervezet
- Adat, és titokvédelem
- Szerződések

Az üzleti rendszer technikai helyzetfeltárása

- A folyamatok, és az általuk felhasznált erőforrások
- Fizikai helyzetfeltárás
- Logikai helyzetfeltárás

A hálózatok

Életciklus

AZ INFORMÁCIÓ RENDSZER ELLENŐRZÉSI LISTÁJA

(Sablon, magas szintű szempontokkal)

SZERVEZÉSI HELYZETFELTÁRÁS

A vállalati üzleti stratégia

- Az üzleti cél
- Az üzleti követelmények

Szabályzások

- Szervezet és működés szabályozása
- Biztonsági infrastruktúra szabályozása
- Tűzvédelmi szervezet, és működés szabályozása
- Polgári védelmi szervezet, és működés szabályozása
- Biztonsági alapdokumentumok
- Adatvédelem, és Adatbiztonság szabályozása
- Titokvédelem szabályozása
- Iratkezelés szabályozása

Humánpolitikai intézkedések

- Szerződések
- A szolgáltatási szint megállapodás megfelelősség
- A biztonsági események kezelésének rendje

Technikai helyzetfeltárás

Erőforrások

- A korábbiakban megadottak szerinti.

Fizikai hozzáférés védelem

- Alkalmazzák-e a Titokvédelmi Utasítás osztályozását
- Aktív támadás elleni fizikai védelem
- Passzív támadás elleni fizikai védelem

Fizikai rendelkezésre állás

- Energiaellátás
- Tűzvédelem
- Villámvédelem
- Klimatizálás
- Számítóközpont stratégiai elhelyezése
- Megbízhatóság
- Redundancia
- Beszéd kommunikációs eszközök
- Dokumentáció
- Karbantartást ellátók
- Felügyeleti rendszer

Logikai hozzáférés védelem

- Alkalmazzák-e a Titokvédelmi Utasítás osztályozását
- Aktív támadások elleni védelem
- Passzív támadás elleni hozzáférés védelem

Logikai rendelkezésre állás

- Redundancia
- Vírusvédelem
- Mentés, újraindítás
- Logikai rombolás
- Dokumentáció

Hálózatok

- Típusok, alkalmazási helyük
- Nem bizalmas hálózati kapcsolatok (Internet, Extranet, INTRANET)
- Védelem a LAN-ban
- Védelem a WAN-ban

Védelem az IR életciklus során

- Fejlesztés
- Átadás/átvétel
- Üzemeltetés
- Selejtezés

Számon kérhetőség

- Erőforrások leltárai
- Naplók (beléptetés tárolók tevékenység naplói, audit trailek)

DOKUMENTUMOK

A Megbízónak az átvilágítás megkezdésekor az alapvető dokumentumokat rendelkezésre kell bocsátani, valamint az átvilágítás során felmerülő további eseti dokumentum igényeket is biztosítania kell. Az induláskor rendelkezésre bocsátandó dokumentumok a következők (amelyeknek tartalma, és védelme vizsgálandó):

- *Üzleti stratégia (igazgatási szervezetnél küldetés)*
- *Informatikai stratégia*
- *Szervezeti és működési szabályzat,*
- *Iratkezelési utasítás,*
- *Adatvédelmi Szabályzatok,*
- *Titokvédelmi utasítás,*
- *Tűzvédelmi szabályzat,*
- *Polgári védelmi szabályzat,*
- *biztonsági dokumentumok (korábbi átvilágítási jelentés, Biztonsági Program, Biztonsági Politika, Katasztrófaterv, Biztonsági Szabályzat, Konfigurációkezelési Utasítás, Programváltozás kezelési eljárás rend, biztonsági események kezelési rendje, és naplói), és*
- *Információ-rendszer dokumentációi (rsw, asw-ek, stb)*

A helyzetfeltáráshoz felhasznált dokumentumok jegyzékét az Átvilágítási jelentésben rögzíteni kell.

INTERJÚK

A helyzetfeltárás egyik fontos eszköze az interjúkészítés. Ennek alapja az ellenőrzési lista. A több egységgel rendelkező szervezetek esetében az átvilágítás a mintavétel elve alapján történik. A különböző szintű szervezeti egységekből legalább egynek a mintában szerepelni kell. Az interjú alanyok első megközelítésben a következők:

- a. top menedzsment vizsgált területért felelős tagja,
- a humánpolitikai vezető,
- a biztonsági vezető (vagyon és az IT biztonságért felelős),
- a titokvédelemi felelős,

- az iratkezelésért felelős vezető,
- az informatikai vezető,
- az informatika fejlesztésért felelős vezető,
- az informatika üzemeltetéséért felelős vezető,
- a beszéd és adattávközlésért felelős vezető,
- az átvilágításba bevont egységek vezetői,
- az ÜR-ben alkalmazott berendezések, eszközök üzemeltetésért felelős vezető.

Az interjúk során tett megállapításokat az átvilágítónak saját részére rögzítenie kell, továbbá az Átvilágítási jelentésben szerepeltetni kell, nem a válaszaiknál, hanem összevonva, az interjút adó személyek nevét, és beosztását.

SZEMLÉK

Az átvilágítás szerves részét képezi az erőforrások, és a védelmi intézkedések üzemeltetésének helyszíni tanulmányozása. A szemlék tárgya a technikai védelmi intézkedések üzemeltetési gyakorlatának feltárása. A szemlék tárgyát, és helyét a 2.4.2.ben ismertetettek szerint kell meghatározni. A szemléknél alkalmazható módszerek a következők:

- *megfigyelés, amely történhet*
  - *helyszínbejárással,*
  - *az üzemeltető által működés közben bemutatott védelmi intézkedés megtekintésével,*

- *tesztelés, amely történhet*
- *a védelmi intézkedés megkerülési kísérletével,*
- *védelmi intézkedés feltörési kísérlettel,ellenőrző programmal (Computer Assisted Audit Techniques, pl. Internet, és bizalmas számítástechnikai bázis scannerek), méréssel.*

Az egyes módszerek például a következő védelmi intézkedéseknél alkalmazhatók:

- *belépés, és mozgás ellenőrzés,*
- *behatolás védelem,*
- *logika hfv. biztonsági környezete,*
- *fizikai rendelkezésre állás (mentések, eredeti programok, forrásnyelvi változatok tárolása),*
- *tartalomhitelesítés,*
- *rejtjelezés,*

- *mentések,*
- *akusztikus kisugárzás,*
- *elektromágneses kisugárzás.*

VESZÉLYFORRÁS ELEMZÉS

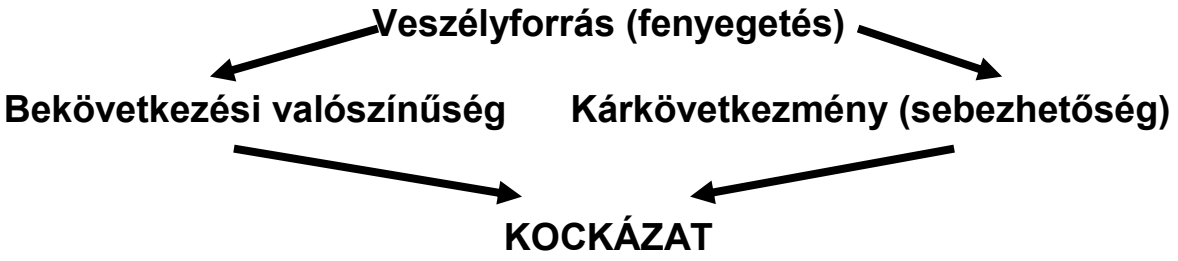
A VESZÉLYFORRÁS ELEMZÉS CÉLJA:

a helyzetfeltárás alapján meghatározza az erőforrások bizalmasságát, sértetlenségét, és rendelkezésre állását, fenyegető gyengeségeket, amelyek következtében egy támadás eredményeképpen nem kívánt állapot jöhet létre. A veszélyforrásokra példákat a 7sz. Melléklet tartalmaz.

A VESZÉLYFORRÁS ELEMZÉS TÁRGYA:

- A helyzetfeltárásban rögzített tények jelentenek-e fenyegetést az informatikai erőforrások bizalmassága és/vagy sértetlensége és/vagy rendelkezésre állására.
- Amennyiben vannak megtett védelmi intézkedések
  - vizsgálni kell a védelmi intézkedések megfelelősségét, azaz azt, hogy a védelmi követelményeknek eleget tesznek-e, és a védelmi intézkedések megfelelő erősségűek-e,
  - amennyiben korábban készült biztonsági átvilágítás, mi történt a feltárt veszélyforrásokkal,
  - ha van érvényes Biztonsági Szabályzat (Politika), és Katasztrófaterv, a specifikált védelmi intézkedések kikényszerítik-e az azokban meghatározott védelmi követelményeket,
- vizsgálni kell a megvalósítást, azaz azt, hogy
  - a védelmi intézkedések gyakorlata nem gyengíti-e a kitűzött védelmi követelményeket,
  - amennyiben van érvényes Biztonsági Szabályzat az a gyakorlatban végrehajtásra kerül-e, és
- a feltárt védelmi gyengeségeket, veszélyforrásokat a jelentésben rögzíteni kell.

A kockázat (az üzleti hatás) elemzés célja: a feltárt veszélyforrások azonosítása után, annak megállapítása, hogy a veszélyforrásból kiinduló sikeres támadásnak mekkora a valószínűsége, és milyen kárkövetkezményekkel járhat. *A kockázat az erőforrások sérülésének, a támadás bekövetkezésének a valószínűsége.*



A kockázat elemzés tehát egy eljárás, amelynek célja, hogy veszélyforrásonként meghatározzuk a veszélyforrások bekövetkezési valószínűsége, és a kárkövetkezmények összefüggését, a támadás üzleti hatását. A korábbiakban már szó volt arról, hogy egy veszélyforrás bekövetkezése, azaz a bekövetkezési valószínűség csökkentése különböző erősségű védelmi intézkedésekkel történhet. A menedzsment joga eldönteni, hogy milyen erősségű védelemre tart igényt. A szervező kötelessége az egyenszilárdság elvének megfelelő védelem biztosítása.
A kockázatot meghatározó tényezők a fenyegetettség, a bekövetkezési valószínűség, és a sebezhetőség. Ezek a következők:

- A fenyegetettség (T)

A fenyegetettség fogalma: az erőforrások, a veszélyforrás bekövetkezés esetén felfedésre és/vagy módosításra, és/vagy elpusztításra kerülhetnek, amely fenyegetést jelenthet az erőforrások bizalmasságára, sértetlenségére, és\vagy rendelkezésre állására nézve.

- A bekövetkezési valószínűség (P)

Bekövetkezési valószínűségen azt értjük mekkora az esélye annak, hogy a veszélyforrás képezte fenyegetettség támadás formájában, realizálódjon, azaz bekövetkezzen.

A bekövetkezési valószínűség lehet:

- igen kicsi **(VS),**
- kicsi **(S),**
- közepes **(M)** vagy
- nagy **(L),**
- igen nagy **(XL).**

A *bekövetkezési valószínűséget* a támadási potenciálból (amely valójában a támadó motivációja) kiindulva, a CEM (Common Evaluatin Methodology) szerint, exakt módszerekkel meghatározni igen nehéz. Továbbá a bekövetkezett támadásokról sem áll rendelkezésre statisztika (egyrészt nem vezetnek statisztikát, másrészt, ha vezetnek, nem hozzák

azt nyilvánosságra), így idősor hiányában a valószínűség számítási módszer sem alkalmazható. Ebből következik, hogy a bekövetkezési valószínűséget kénytelenek vagyunk becsülni.

Először a támadási potenciált kell meghatározni.

A *támadási potenciál* a sikeres támadás esélye.

A támadási potenciál a CEM szerint a következő tényezőktől függ:

- a védelem erősségétől,
- a támadási cél értékétől,
- a sikeres támadáshoz szükséges szakértelemtől,
- a sikeres támadáshoz szükséges erőforrásoktól
- a sikeres támadáshoz szükséges időtartamtól.

A támadási cél *védelmének erőssége* a támadás esélyeit meghatározza.
A támadási cél *értéke* azt fejezi ki, hogy érdemes-e a támadást végrehajtani.
A támadó *szakértelme* lehet: *laikus* (hozzá nem értő), *profi* (aki ismeri a rendszer tulajdonságait), *szakértő* (aki részleteiben ismeri a rendszerben alkalmazott védelmi intézkedéseket, és képes speciális eszközöket használni a támadáshoz).
A támadás *erőforrásai: a támadás eszköze, és az idő*. Az eszköz lehet *nem támogatott* (azaz nem szükséges eszköz a támadáshoz), *házi* (azaz a támadás célját képező rendszer egy erőforrása), és *speciális eszköz* (amely nem kapható civil forgalomban). A sikeres támadáshoz folyamatosan felhasználandó *időtartam* lehet: kevesebb, mint egy *óra*, kevesebb, mint egy *nap*, legalább egy *hónap*.

A támadási potenciál összetevőit sem lehet exakt módszerrel meghatározni. A CEM például az értékről azt mondja, hogy az szubjektív valami, amely nagymértékben függ attól, hogy az adott esetben a támadó számára, milyen értéket képvisel. Adott esetben tehát egy adat a támadó számára nagyobb értéket képviselhet, mint az adat tulajdonos számára. Hasonlóképen igaz ez a támadási potenciált meghatározó további tényezőkre is.
A CEM a támadási potenciál meghatározására a következő becslésen alapuló, eljárást ajánlja:
A támadási potenciál annál kisebb mennél

- *kisebb* a támadási cél értéke,
- kisebb a támadó szükséges szakértelme,
- *gyengébb* a védelem,
- egyszerűbb a sikeres támadáshoz szükséges eszköz,

- nagyobb a sikeres támadás végrehajtásához szükséges idő.
- Tehát ezek becsléssel történő elemzése alapján lehet egy veszélyforrás sikeres realizálódásához szükséges támadási potenciált (T_p) meghatározni, amely lehet:

  - kicsi **(S),**
  - közepes **(M),**
  - nagy **(L)**
  - gyakorlat feletti **(B).**

A bekövetkezési valószínűség (P) pedig annál nagyobb, mennél kisebb a támadási potenciál (T_p).

Az összefüggés az alábbi táblán található:

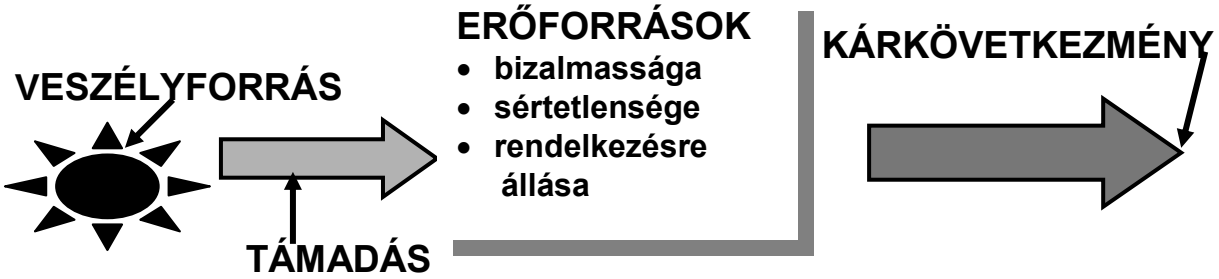
T_p	P
(B)	VS
(L)	S
(M)	M
(S)	L

- A sebezhetőség (V).

A sebezhetőség sikeres támadás esetén az erőforrások lehetséges sérülése. A támadás bekövetkezésekor a teljes rendszer vagy egy eleme sérülhet (a lehetséges kárkövetkezmény). Így a sebezhetőség lehet

- globális **(G)** azaz az összes erőforrás folyamatos működése szakad meg, vagy
- részleges **(R),** azaz egyes erőforrások sérülnek.

A fenyegetést, és bekövetkezése esetén, a hatását az alábbi ábrán értelmezzük:



- A kockázat (K).

A kockázatot (**K**) (a táblázatban, a szürke mezőben) ezek után a bekövetkezési valószínűség (P) és a sebezhetőség (V) becsült értékeinek logikai egybevetésével kaphatjuk meg, amelyet az alábbi táblázaton szereplő kockázati mátrix mutat

P	*V=R*	*V=G*
VS	**VS**	**S**
S	**S**	**S,M**
M	**M**	**M,L**
L	**L**	**L,XL**
XL	**XL**	**XL**

A kockázat elemzés alapján dönthet a menedzsment a védelmi intézkedésekről. A döntés a kockázatok tudatos felvállalása, azaz a menedzsment eldönti, hogy mely veszélyforrások ellen tesz védelmi intézkedést, és a védelmi intézkedés milyen erősségű lesz. Az egyenszilárdság elve alapján azonban a védelem ellenálló képességét mindig a leggyengébb védelmi intézkedés határozza meg.
Az eddigiekben ismertetett eljárás kvalitatív, vannak azonban kvantitatív eljárások is. A kvantitatív módszereket azért bírálják, mert erőltetik a precíz, matematikailag megalapozott eljárásokat, olyan esetekben, amikor nincs precíz, reális input adat. A gyakorlatban a kvantitatív módszerek egyrészt tényekre, másrészt spekulatív, azaz becsült adatokra támaszkodnak. Egyes szerzők ezért a kvantitatív módszereket látványosnak tartják, amelyek valójában nem nyújtanak pontosabb eredményeket a kvalitatív módszereknél. A FIPS (FEDERAL INFORMATION PROCESSING STANDARDS) PUBLICATION 65 megállapítja, hogy a hatáselemzés, illetve a bekövetkezési valószínűség exakt módszerekkel nem állapítható meg. Ugyanis a bekövetkezési valószínűség számításához nem állnak rendelkezésre statisztikai adatok, míg a kárkövetkezményeknél a vagyoni károk számíthatók, a nem vagyoni károk (pl. üzleti megítélés romlása, piaci részesedés csökkenése) azonban csak becsülhetőek.

A kockázat tehát egy kárkövetkezmény bekövetkezési valószínűségét fejezi ki. A kárkövetkezmény lehet vagyoni, és nem vagyoni kár. A vagyoni kár a vállalat adatai alapján számítható, a nem vagyoni kár (pl. piacvesztés, kártérítési igények, image romlása, tőzsde árfolyamesés) nem számítható. Ezért a megoldás, hogy ilyen igény esetén kockázatonként külön adunk választ a vagyoni, és a nem vagyoni kárra. A vagyoni kár osztályozása természetesen függ a vállalat

állóeszközeinek összértékétől. Tehát például egy nagyvállalatnál a vagyoni kár lehet:

RS	0-5MFt	GS	0-10MFt
RM	5-50MFt	GM	10-100MFt
RL	>50MFt	GL	>100MFt

A nem vagyoni kár nem függ össze a vagyoni kár nagyságával, mert lehet egy kis vagyoni kár mellett igen jelentős nem vagyoni kár. Ezért a nem vagyoni kárt külön adjuk meg, amely lehet kismértékű (RS, vagy GS), jelentős (RM, vagy GM), és igen jelentős (RL, vagy GL). A kárkövetkezmény megállapításánál mindig a nagyobbat kell figyelembe venni, tehát, ha a vagyoni kár például GS, a nem vagyoni kár GM, akkor a kárkövetkezmény GM.

A kockázat elemzés eredményét egy táblázatban lehet összefoglalni (konkrét kockázati mátrix), amely tartalmazza, hogy javasolt vagy nem javasolt védelmi intézkedés, illetve újabb, vagy erősebb javasolt. Például:

Veszély for.neve	**Fenyege-Tettség**	**Beköv. Valósz.**	**Sebez-hetőség**	**Kockázat**	**Javasolt védelmi intézkedés**	**Maradék kockázat**
Tűz	Rend. állás	M	GL	L	tűzvédelem	S

A maradék kockázat az a kockázat, amely fennáll a védelmi intézkedések ellenére.
Végül rá kell mutatnunk arra, hogy a kockázat elemzés a kockázat menedzsment fontos része, amelyet a védelmi intézkedések specifikálása egészít ki. Tehát a kockázat menedzsment a helyzetfeltárás, veszélyforrás elemzés alapján végrehajtott kockázat elemzésből, és a védelmi intézkedések specifikációiból [Biztonsági Szabályzat (Politika)] áll.

7.2.5.3. PÉLDÁK AZ ÜZLETI RENDSZER VESZÉLYFORRÁSAIRA

(Magas szintű példák)

Az üzleti, és támogató folyamatok, képezte veszélyforrások biztonsági szempontból a működési veszélyforrások (kockázatok) közé tartoznak, amelyek elsősorban

- *nem megfelelően végrehajtott vagy*

- *kiesett üzleti folyamatok, és*
- *az infrastruktúra kiesése,*

amelyek emberek, rendszerek, és az üzleti folyamatok végzését lehetővé tevő infrastruktúra kiesése, vagy külső események miatt következnek be, és üzleti veszteséghez vezetnek.

Informatikai veszélyforrások

SZERVEZÉSI VESZÉLYFORRÁSOK (RÉSZLEGES)

Szabályzatok

- Szervezet és működés nem a biztonsági követelmények szerint szabályozott
- Szervezet, és a működési gyakorlat nem felel meg a biztonsági követelményeknek
- Biztonsági szervezet és működés nem felel meg a biztonsági követelményeknek
- Tűzvédelmi szervezet és működés nem felel meg a tv-nek
- Polgári védelmi szervezet és működés nem felel meg a tv-nek
- *Biztonság naprakészen nem rendszerszervezett*
- Iratkezelés szabályozása nem naprakész, mind a papír, mind az elektronikus alapú iratoknál

Humánpolitikai intézkedések

- Munkaviszony létesítés és megszüntetés naprakészen nem felel meg a biztonsági követelményeknek
- Feladatok meghatározása és szétválasztása elméletben, és gyakorlatban nem felel meg a biztonsági követelményeknek
- Teljesítménykövetés nem terjed ki minden munkatársra
- Csalás elleni politika elméletben, és gyakorlatban nem felel meg a biztonsági követelményeknek
- Az ipari kémkedés elleni politika nem megfelelő
- Oktatás nem naprakész

Szerződések

- Szerződés harmadikféllel nem felel meg a biztonsági követelményeknek
- Kockázat áthárítás nem naprakészen teljes körű
- Nincs a biztonsági események kezelése szabályozva

TECHNIKAI VESZÉLYFORRÁSOK (RÉSZLEGES)

Fizikai hozzáférés védelem

Aktív támadás elleni hozzáférés-védelem nem teljes körűen korlátozza a hozzáférést, a következőknél:

- Épületautomatika
- Belépés és mozgás ellenőrzés
- Behatolás-védelem
- Értéktárolás, értékszállítás
- Üres íróasztal politika, sötét képernyő

Passzív támadás elleni hozzáférés-védelem nem teljes körűen korlátozza a hozzáférést, a következőknél:

- Elektromágneses kisugárzás
- Akusztikus kisugárzás
- Hulladékmegsemmisítés

Fizikai rendelkezésre állás

- Energiaellátás nem biztosítja a folyamatos rendelkezésre állást
- Tűzvédelem nem rendeltetésszerű
- Beszéd kommunikáció nem biztosítja rendeltetésszerűen a biztonsági követelményeket
- Klimatizálás nem biztosítja a folyamatos rendelkezésre állást
- Megbízhatóság nincs megfelelő redundanciával biztosítva
- Dokumentáció nem naprakész, és teljes körű
- Karbantartást ellátókkal szemben nincsenek maradéktalanul érvényesítve a biztonsági követelmények

Logikai hozzáférés védelem

Aktív támadás elleni hozzáférés-védelem nem korlátozza megfelelően a hozzáférést, a következőknél:

- Jelszó és jogosultsági rendszer
- Hitelességvédelem
- Time out
- Logikai behatolás jelzés, védelem

Passzív támadás elleni hozzáférés –védelem nem felel meg a biztonsági követelményeknek

Logikai rendelkezésre állás

- A rosszindulatú szoftverek (pl. vírusvédelem)elleni védelem nem biztosítja a zavartalan, folyamatos rendelkezésre állást

- A rendszer határai nincsenek meghatározva
- Mentés, újraindítás, erőforrás felhasználás nem biztosítja a rendelkezésre állást
- Dokumentáció nem naprakész, nem teljes körű
- Rendszerkövetés nem megfelelően szervezett

Hálózatok

- LAN nem biztosítja megfelelően a biztonsági követelményeket
- Jogosulatlan LAN hozzáférés
- Helytelen LAN erőforrás hozzáférés (jogosulatlan, jogosult)
- Adatok felfedése
- Adatok, szoftverek módosítása jogosulatlanul
- LAN forgalom felfedése
- LAN forgalom becsapása (spoofing)
- LAN Funkciók megszakítása
- WAN nem biztosítja megfelelően a biztonsági követelményeket, pl. a héjvédelmet
- Adatok nem védettek
- Beszéd hálózat nem megfelelően védett
- Az elektronikus hitelesítés nem teljes körű

Az IR életciklus

- Fejlesztés során nem érvényesülnek a biztonsági követelmények
- Fejlesztési környezet
- Biztonsági követelmények a fejlesztendő rendszerben
- A harmadik félnél fejlesztett rendszereknek nincs biztosítva a szállítás alatti biztonsága
- Átadás/átvétel során nem érvényesülnek a biztonsági követelmények megfelelően
- Megfelelősség ellenőrzése
- A védelmi intézkedések végrehajtásának ellenőrzése
- Üzemeltetés során nem érvényesülnek megfelelően a biztonsági követelmények
- Selejtezés nem biztosítja a biztonságkritikus anyagok bizalmas megsemmisítését
- A biztonsági technológia védelmének hiánya, vagy meg nem felelőssége.

ÁTFOGÓ VESZÉLYFORRÁSOK

Szervezési

- Szervezet és működés nem biztosítja a biztonsági követelményeket
- Humánvédelem nem biztosítja a folyamatos működés humán feltételeit
- Szerződések nem érvényesítik megfelelően a biztonsági követelményeket

Fizikai

- Fizikai hozzáférés -védelem nem véd megfelelően
- Fizikai rendelkezésre állás nem biztosítja a növelt rendelkezésre állást

Logikai

- Logikai hozzáférés –védelem nem megfelelő színvonalú
- Logikai rendelkezésre állás nem biztosítja a megfelelő növelt rendelkezésre állást

7.2.5.4. BIZTONSÁGI STRATÉGIA

A Biztonsági Stratégia: az elérendő biztonsági cél, és a biztonsági követelmények meghatározása, amelyek az üzleti célhoz (eredményesség, hatékonyság), és az üzleti követelményekhez (minőség, megbízhatóság, biztonság), azaz az üzleti stratégiához kapcsolódnak.

A Biztonsági Cél: a menedzsment elkötelezettségét kinyilvánítja az informatikai erőforrások védelmére, a következők szerint

- az informatikai erőforrások folyamatos, és rendeltetésszerű működésének biztosítása, avagy
- a bizalmasság, sértetlenség, rendelkezésre állás (továbbá egyes országok szabványai szerint a számon kérhetőség, és garanciák a rendeltetésszerű működés) biztosítására.

A Biztonsági Követelményeknek azt kell meghatározni, hogy az informatikai erőforrások védelmének, a kockázatok minimalizálása érdekében mit kell kielégíteniük. Ennek megfelelően a biztonsági követelmények a következőkből állnak:

Funkcionális biztonsági követelmények, amelyek célja a biztonsági stratégiában meghatározott stratégiai célok eléréséhez szükséges követelmények meghatározása. Például:

- Szervezési biztonsági követelmények
  - Ellenálló képesség.
  - Biztonsági szervezet.
  - Adatok, és Titkok biztonságérzékenység szerinti osztályozása
  - Humánpolitika
  - Iratkezelés
  - Szerződések
- Technikai biztonsági követelmények
  - Hozzáférés-védelem (fizikai, és logikai)
  - Rendelkezésre állás védelme (fizikai, és logikai)
  - Hálózatok védelme
  - Védelem az informatikai erőforrások életciklusa során
  - Biztonsági események kezelése.

Garanciális biztonsági követelmények, amelyek célja annak a biztosítása, hogy a funkcionális követelmények kikényszerítsék a biztonsági követelményeket. Például:

- Számon kérhetőség
- Meg nem kerülhetőség

PÉLDAKÉPEN NÉHÁNY BIZTONSÁGI KÖVETELMÉNY

Funkcionális.
A biztonsági rendszer ellenálló képességének meghatározása
Az integrált biztonsági szervezet.
Az alkalmazottak megbízhatósága.
A fizikai, és logikai belépés, és mozgás ellenőrzés
Az erőforrások fizikai, és logikai rendelkezésre állása.

Garanciális:
A tevékenységek (naplózás), és erőforrások (leltárak) utólagos számon kérhetősége.
Életciklus alatti védelem.

7.2.5.5. BIZTONSÁGI POLITIKA

A BIZTONSÁGI POLITIKA CÉLJA:

az erőforrások fenyegetettségének, a sikeres támadás valószínűségének, a kockázatoknak a csökkentésére részleges védelmi intézkedések specifikálása. A védelmi intézkedések körére ad útmutatást a 15.sz. pontban megadott ábra.

A védelmi intézkedések lehetnek részlegesek (egyes erőforrások védelmére szolgálnak), és lehetnek átfogóak (az egész Információ rendszer folyamatos működésének biztosítására szolgálnak), mint a veszélyforrások. A védelmi intézkedések, tehát nem lehetnek 100%-osak, minden védelmi intézkedés maradéktalan végrehajtása esetén is van *maradék kockázat*.

A BIZTONSÁGI POLITIKA TÁRGYA:

a részleges védelmi intézkedések specifikálása.

A gazdasági szervezet Biztonsági politikája az ITSEC szerint:

- *törvények, szabályok, és a gyakorlat alapján a biztonsági követelmények érvényesítése, az erőforrások menedzselésére, védelmére, és elosztására.*

A védelmi intézkedések a következő főbb védelmi csoportokban dolgozandók ki:

- Szervezési védelmi intézkedések
  - Biztonsági szervezet,
  - Humánpolitika,
  - Titokvédelem,
  - Iratkezelés, és
  - Szerződések.
- Technikai védelmi intézkedések
  - Fizikai, logikai hozzáférés-védelem,
  - Fizikai, logikai rendelkezésére állás védelme,
  - Az információ-rendszer életciklusa alatti védelem,
  - Hálózatok védelme.
  - Életciklus alatti védelem.

A védelmi intézkedéseket úgy kell specifikálni, hogy azok alapján a tervezés, beszerzés, kivitelezés végrehajtható legyen. A védelmi intézkedések specifikációja nem lehet konkrét termék specifikációja.

A Biztonsági Politika szervezési védelmi intézkedései a törvények, szabályok, és a gyakorlat alapján szabályozzák, hogy a szervezet miként menedzselje, védje, és ossza el az erőforrásokat, miként teljesítse, a szervezet a biztonsági követelményeit.

A Biztonsági Politika az erőforrások biztonság érzékenysége, az osztályozásuk (lásd az ISO/IEC 17799-2002 szabványt) alapján meghatározza, specifikálja a védelmi intézkedéseket, azaz azt, hogy miként kell a biztonsági követelményeket érvényesíteni. Az osztályozás tehát eligazít abban, hogy a különböző erősségű védelmi intézkedések közül, melyeket használjuk, figyelembe véve a rendszer védelmi erősségének, ellenálló képességének követelményét, azaz, az egyenszilárdság elve alapján ennél gyengébb védelmi intézkedés nem használható.

A védelmi osztályozás elve:

Védelmi osztályok	***Védendő***		***Hozzáférés***	
	Bizalmasság	***Sértetlenség***	***Belső***	***Külső***
1.	***Igen kritikus***	***Életbevágó***	***Erősen korlátozott***	***Erősen korlátozott***
2.	***Kritikus***	***Életbevágó***	***Korlátozott***	***Erősen korlátozott***
3.	***Nem kritikus***	***Fontos***	***Nem korlátozott***	***Korlátozott***
4.	***Nem kritikus***	***Nem életbevágó***	***Nem korlátozott***	***Nem korlátozott***

A VÉDELMI INTÉZKEDÉSEK MEGVALÓSÍTÁSA

A védelmi intézkedések megvalósítása lehetséges
- Szervezési intézkedésekkel
- Technikai intézkedésekkel, amely lehet
  - hardware megoldás
  - software megoldás
- Szervezési, és technikai egyaránt

A VÁLASZ MENEDZSMENT

A válasz menedzsment, a biztonsági eseményekre adandó válasz tevékenységek, feladatok, amelyeket a Biztonsági Politika tartalmaz.

Biztonsági esemény mindaz, ami a biztonságra fenyegetést jelent, vagy jelenthet. *(mindaz az esemény, amikor a védelmi intézkedések nem tudják kikényszeríteni az erőforrások bizalmasságának, sértetlenségének, rendelkezésre állásának védelmét).*

A BIZTONSÁGI ESEMÉNYEK KEZELÉSÉNEK CÉLJA

Felkészülés a biztonsági esemény bekövetkezésére, és a gyors, hatékony válasz feltételeinek biztosítása.

A BIZTONSÁGI ESEMÉNYEK VÁLTOZATAI

a) amikor a biztonsági esemény a rendszerre részleges fenyegetést jelent, vagy jelenthet.
b) amikor a biztonsági esemény a teljes rendszer leállásához vezet, vagy vezethet

Az a) esetben a kárkövetkezmények csökkentésére a „Biztonsági események kezelési eljárás rendje szolgál.(lásd 3. fejezet). A b) esetben a kárkövetkezmények csökkentésére az ÜFT szolgál.(lásd 4, és 5. fejezet).

A BIZTONSÁGI ESEMÉNYEK KEZELÉSE

A kezelés fázisai:

- A felkészülési fázis
  Amelyben
  - A Biztonsági események kezelésének eljárás rendje elkészül
  - A tesztelések megtörténnek
  - A karbantartást terv szerint végrehajtják
  - Az oktatást rendszeresen megtartják
  - A tartalék eljárásokat, erőforrásokat (tartalék eszközök, mentett adatok, programok, rendszer beállítások) biztosítják

- Az észlelési fázis
  Amelyben az eseményt észlelik, és az arra jogosult, és kötelezett személy azt jelenti a koordinátornak (aki általában az ÜFT-ben meghatározott Katasztrófa menedzser).
- Az értékelési fázis

Amelyben a koordinátor azonosítja az eseményt, és dönt a megteendő intézkedésekről. Ezek lehetnek részleges katasztrófa esetén a visszaállítás, vagy átfogó katasztrófa esetén az ÜFT indítása. Itt a visszaállítás az eredeti állapot helyreállítását jelenti, a tartalék erőforrások felhasználásával.

- A visszaállítási fázis
  Amelyben a koordinátor intézkedései nyomán a Visszaállítási team (ugyanaz, mint az ÜFT-ben) visszaállítja az eredeti állapotot.
- Az intézkedési fázis
  Amelyben az értékelés alapján a koordinátor dönt arról, hogy szükséges-e a visszaállításon kívül egyéb intézkedést tenni (pl. a védelmi intézkedést korszerűsíteni, lecserélni).
- Számon kérési fázis
  Amelyben a koordinátor
  - Gondoskodik a bizonyítékok megőrzéséről
  - Meghatározza az esetleges felelősöket
  - Dönt belső ellenőrzési vizsgálat, vagy belső, illetve külső jogi eljárás kezdeményezéséről.

A KOORDINÁTOR SZEREPE

A koordinátor (általában az ÜFT katasztrófa menedzser) felelős a biztonsági események kezelésének menedzseléséért, és e tevékenységét a Vezérigazgató képviseletében, a biztonsági szervezetben látja el.

A SZÁMÍTÓGÉPES BIZTONSÁGI ESEMÉNY VÁLASZ TEAM (CSIRT)

Az USA-ban a Computer Emergency Response Team (CERT)-ek bázisán kialakult, és nemzetközivé vált a Számítógépes Biztonsági Események Válasz Teamje (Computer Security Incident Response Team) Csoportja, amely ma már kiterjed szerte a világon. A CSIRT-ek felépítése, működése sok hasonlóságot mutat a tűzoltóság(-ok) rendszeréhez. Ebből következik, hogy a biztonsági struktúrában jöhetnek létre a CSIRT vállalati Csoportjai, amelyeket koordinációs csoportok kötnek össze, ezek együttműködve nyújtják a következő szolgáltatásokat (lásd a következő oldalon a táblázatot):

A CSIRT KÖZÖS SZOLGÁLTATÁSAI

Reagáló szolgáltatás	Megelőző Szolgáltatás	Minőség Menedzsment szolg.
Riasztás, figyelmeztetés Eseménykezelés • esemény analízis • válasz az eseményre a helyszínen • esemény, válasz, támogatás • esemény - válasz koordináció • Sebezhetőség kezelés • sebezhetőség anallízis • sebezhetőség válasz • sebezhetőség válasz koordináció Fenyegetéskezelés • fenyegetés analízis • fenyegetés válasz • fenyegetés - válasz koordináció	Közlemény Technológia felügyelet Biztonsági audit Konfiguráció Biztonsági karbantartás Biztonsági eszközök fejlesztése Behatolás jelzés szolgáltatása Biztonsági információk közzététele	Kockázat elemzés Üzletmenet folytonossági terv Biztonsági konzultáció Tudatosság képzés Oktatás/gyakorlat Termékértékelés, vagy tanúsítás

7.2.5.6. ÜZLETMENET FOLYTONOSSÁGI TERV

A KATASZTRÓFATERVEZÉS CÉLJA

Az üzleti tevékenység folyamatos és rendeltetésszerű működése biztosítási feltételeinek kidolgozása. A továbbiakban egyszerűség kedvéért, nem üzletmenet folytonossági tervről (BCP, ÜFT), hanem katasztrófa tervről beszélünk

A KATASZTRÓFA TERVEZÉS TÁRGYA

Védelmi intézkedések meghatározása a katasztrófa bekövetkezése esetén a kárkövetkezmények csökkentésére. A katasztrófaterv (BCP=ÜFT), tehát nem a katasztrófa bekövetkezési valószínűségének csökkentésére szolgál, a kockázat csökkentésére a Biztonsági Szabályzatban (Politikában) kell védelmi intézkedéseket meghatározni.

A katasztrófa tervezés során kidolgozott védelmi intézkedések átfogó védelmi intézkedések, amelyek tehát az egész információ rendszernek a rendelkezésre állása biztosítására szolgálnak.

A KATASZTRÓFA FOGALMÁNAK MEGHATÁROZÁSA

A vállalatok esetében a katasztrófa fogalma az üzleti tevékenység megszakadása. Azonban ezt pontosítani kell az adott vállalatra nézve. A katasztrófákat, az erőforrások rendelkezésre állásának megszakadását az alábbiak szerint osztályozhatjuk:

- I. Kategória. Az erőforrások nem állnak rendelkezésre, az információ-rendszer működése megszakad. (pl. tűz, bombariadó, vírusfertőzés, túszejtés következtében).
- II. Kategória. Egyes erőforrások nem állnak rendelkezésre, és az információ-rendszer működése megszakad (pl. az energiaellátás teljes kiesése).
- III. Kategória. Csak erőforrás elem sérül, de az információ-rendszer működése folyamatos (pl. egy diszk esik ki, ez a Biztonsági Szabályzat (Politika) tárgya.

A katasztrófa fogalmát használja, az 1999. évi. LXXIV: tv. az állami, önkormányzati katasztrófa védelemről, amelynek megfelelően Dr. Rohács professzor a katasztrófa, a veszélyhelyzet fogalmát a következőképen adja meg [24]: *A veszélyhelyzet olyan nem szándékolt és nem kívánt körülmény, esemény kialakulása, amely hátrányosan hatással, hatásokkal van, azaz veszélyezteti*

- *az emberi életet,*
- *az anyagi javakat,*
- *a kulturális értékeket,*
- *az élővilágot, a természetet, valamint*
- *a kialakult társadalmi rendet.*

A törvény a veszélyhelyzetre a természeti, biológiai eredetű illetve tűz okozta példákat, adja meg.
Esetünkben azonban a vállalatok (kivéve a veszélyes ipari üzemeket, és létesítményeket) üzletmenet folytonosságával kapcsolatosan az üzletmenet megszakadásakor előálló veszélyhelyzetre, a teendők meghatározására, az első értelmezés az irányt adó.

A KATASZTRÓFATERVEZÉS KIINDULÓ FELTÉTELEI

Amennyiben a Megbízó nem rendelkezik Biztonsági Politikával ezt az anyagban fel, kell tüntetni, és rá kell mutatni a keresztösszefüggésre. Ugyanis a katasztrófa bekövetkezése után, a visszaállítás, és a helyreállítás során, illetve befejezésekor legalább az eredeti védelmet garantálni kell.

A KATASZTRÓFATERVEZÉS ALAPJA

A katasztrófatervezés alapja a veszélyforrás elemzés során a teljes rendszer működését fenyegető, feltárt átfogó veszélyforrások kockázatai, az üzleti hatások.

AZ ÜZLETI HATÁSOK, KOCKÁZATOK ELEMZÉSE

Az üzleti hatások, a kockázatok elemzése a veszélyforrás elemzésben feltárt átfogó veszélyforrásokra nézve hajtandó végre.

A VISSZAÁLLÍTÁSI STRATÉGIA

Az információ-rendszerben az alkalmazások folyamatos és rendeltetésszerű működését kell biztosítani. A tervezéshez tehát az alkalmazások erőforrás igényére, valamint a felhasználók nyilatkozatára van szükség, az üzleti tevékenységük informatika függőségéről. Az alkalmazások informatika függőségét a sebezhetőségi ablakok adják meg.

A visszaállításhoz felhasználható időnek, amelyet egyébként egyes szerzők KÍVÁNT IDŐTARTAM-nak, neveznek, kisebbnek, vagy legrosszabb esetben egyenlőnek kell lennie, azzal az idővel, amit az üzletmenet megszakadás nélkül, tartalék megoldással KIBÍR. Tehát ez alatt az idő alatt a visszaállításnak meg kell történnie.

Ezt a KÍVÁNT IDŐTARTAMOT több feleképpen nevezik:

- **Sebezhetőségi ablak (window of vulnerability):** A katasztrófa bekövetkezése esetén az üzletmenet megszakadása nélkül elviselhető időtartam.
- **Visszaállítási idő célkitűzés (recovery time objective, RTO):** A katasztrófa esetén az időtartam, amelyet az üzleti funkciók a visszaállításra igényelnek.

A visszaállításhoz felhasznált tényleges idő, pedig

- **A Visszaállítási idő (Recovery time).**

A sebezhetőségi ablakok a következő kategóriákba sorolhatók:

- I. kategória. Küldetés kritikus alkalmazások (sebezhetőségi ablak 0-1 óra).
- II. kategória. Lényeges alkalmazások (sebezhetőségi ablak 1-8 óra).
- III. kategória. Szükséges alkalmazások (sebezhetőségi ablak 8-24 óra).
- IV. kategória. Kívánatos alkalmazások (sebezhetőségi ablak $>$ 24 óra).

A többszintű informatikai hálózatoknál vizsgálni kell az egyes szintek alkalmazásainak egymástól való függőségét, mivel nem zárható ki egy csak a központra vagy csak egy közép szintre vagy csak egy alsó szintre vonatkozó katasztrófa helyzet bekövetkezése. Ilyenkor azonban az egyéb szintek alkalmazásai is kieshetnek, így a katasztrófa kiterjedhet. Például egy erősen a központi rendszerre épített információ-rendszerben a központ kiesése ellehetetlenítheti az alsóbb szinteket is.

A **sebezhetőségi ablakok** alapján lehet eldönteni, kiválasztani a háttér típusát. Az informatikai szolgáltatások ideiglenes visszaállításához szükséges (kívánatos) időnek kisebbnek kell lennie, mint azoknak az alkalmazásoknak a sebezhetőségi ablakai, amelyeknek a hátterét kívánjuk kiválasztani. A háttereket az alábbi jellemzők alapján választhatjuk ki:

- A hátterek típusai a konfiguráció szerint:

➢ Hideg háttér, több hetes sebezhetőségi ablak megvalósításához. Ez egy infrastruktúrával ellátott üres gépterem. A szállítókkal kötött szerződésekben kell a soron kívüli szállító készséget biztosítani.
➢ Meleg háttér, a legkritikusabb, úgy nevezett küldetés kritikus alkalmazások hátthereként, a kivitelétől függően egy – néhány órás sebezhetőségi ablak megvalósításához, amely nem automatikusan induló, hanem manuális újraindítást igénylő rendszerrel építhető ki (ez lehet az eredeti konfiguráció csökkentett változata manuális átvitelt feltételezve vagy lokális, illetve távoli passzív redundans rendszer).
➢ Forró háttér, az összes alkalmazások hátthereként, egy – néhány órás sebezhetőségi ablak megvalósításához, amely újraindítást igénylő rendszerrel építhető ki (ez lehet az eredeti

konfigurációval megegyező konfiguráció vagy lokális, illetve távoli passzív redundans rendszer).

- Katasztrófatűrő háttér, az eredeti rendszer tűkörképeként, folyamatos működés megvalósításához, amely távoli aktív redundans rendszerrel építhető ki, ahol az át, és a visszakapcsolás a háttérre, illetve az eredeti rendszerre nem igényel manuális beavatkozást.

- A növelt rendelkezésre állás szerinti háttér megoldások

két alapvető változata ismert (a fizikai rendelkezésre állás részleges védelménél ismertetett tartalék berendezés biztosítás mellett), éspedig

- az adatok rendelkezésre állását biztosító, részleges védelmi intézkedés, és
- a rendszerrendelkezésre állást biztosító átfogó védelmi intézkedés.

Az adatok rendelkezésre állásának biztosításához a diszk tükrözés elvét alkalmazzák. Ennek egyik igen elterjedt változata a RAID (redundant array of independent disks, független diszkek redundáns sorozata) technológia. A rendszer lényege, hogy a diszkeket többszörözik, és ugyanazt az adatot szimultán írják/olvassák több diszkre/diszkről. Így egy diszk kiesése esetén nincs adatvesztés, és a rendszer tovább képes folytatni a feldolgozást. Valójában ez a megoldás az adott konfigurációban a diszkek, és ezzel az adatok rendelkezésére állását növeli meg. A RAID technológiának több változata létezik ezek RAID 1. 2., 3., 4., 5., 6., 7., 10., 53. A diszk tükrözés alkalmazása a rendelkezésre állás részleges (azaz egy diszk) sérülése ellen nyújt védelmet. Hangsúlyozni kell, hogy a mentéseket nem teszi feleslegessé, mivel a gyakorlatban előfordulhat, és elő is fordul, hogy egy operátori vagy egyéb hiba következtében, a többszörözött adatállomány egyaránt megsérül, vagy megsemmisül.

Az átfogó veszélyforrások elleni védelemre a háttér rendszerek két változata szolgál:

- a passzív redundans rendszerek, és
- az aktív redundans rendszerek.

A passzív redundans rendszereknél a háttér rendszer nem vesz részt az eredeti rendszeren folyamatban, lévő feladatban. Az eredeti rendszerben fellépő hiba esetén a passzív hátteret aktiválni kell, a hiányzó elemek betöltésével, pedig módosítani. Az átálláshoz a háttér rendszerre, a szükséges idő figyelemre méltó, így a megszakadás jelentős.

A passzív redundans rendszer lehet:

- off line vagy
- visszaállítás bázisú rendszer.

Az Off line változatnál az adatok manuális átvitele, a betáplálás és újra indítás képez időigényt. A visszaállítás bázisú rendszerek periodikusan átmásolják a fileokat a háttérre, hiba esetén, pedig a hátter az utolsó mentéstől automatikusan indul. Ez is időigényes, és az utolsó mentés és a háttér indítása közötti időszak adatai elvesznek. Az alkalmazások, és a felhasználók érzékelik a kiesést. A passzív redundans rendszerek magas *rendelkezésre állást* biztosítanak.

Az aktív redundans rendszerek minimálisan egy háttér processzort alkalmaznak, amely ugyanazon adatokon, ugyan abban az időpontban, ugyanazt a műveletet hajtja végre, mint az eredeti rendszer. Az aktív redundans rendszer lehet:

- hibatűrő rendszer vagy
- túlélő hibatűrő rendszer.

A hibatűrő rendszerek alapja processzor párok alkalmazása. A rendszer működését egy hiba fellépése esetén automatikusan állítják vissza, nem áthidalják azt. Így nincs szükség az alkalmazások újraindítására, az adatbázis visszaállítására. Továbbá folyamatosan integritás ellenőrzést végeznek a mikroprocesszoroknál, a belső buszoknál, és a meghajtóknál. Hiba észlelése esetén mielőtt az a folyamatban kárt okozna, a hibát elszigetelik. A hibatűrő rendszereknél átállási idő (a másodperc törtrésze) nem érzékelhető. A túlélő hibatűrő rendszereknél jelentősebb átállási idő van (másodperc). Ebből következik, hogy a túlélő hibatűrő rendszerek „csak gyakorlatilag” biztosítják, hogy a hiba fellépése ne legyen érzékelhető. A túlélő hibatűrő rendszerekben a folyamatos működést egy speciális szoftver irányítja, szemben a hibatűrő rendszerekkel, ahol a hw, és a rendszer szoftver is speciális. A túlélő hibatűrő rendszer a speciális szoftveren kívül szokványos, kereskedelemben elérhető hw, és rendszerszoftver elemekből áll, ezért az ára is kedvezőbb. Az aktív redundans rendszerek *folyamatos rendelkezésre állást* biztosítanak.

- Az elhelyezés szerinti háttér megoldások

  - A háttér lokális, az eredeti konfigurációval azonos helyen történő elhelyezésével.
  - A háttér az eredetitől földrajzilag megfelelően távoli elhelyezésével.

A meleg, illetve forró háttérnek a passzív, és a lokális aktív rendszerek, míg a katasztrófatűrőnek a távoli aktív rendszerek felelnek meg. A lokális

aktív rendszerek, az eredeti rendszerrel azonos biztonsági környezet miatt, nem elégítik ki a katasztrófatűrő hátterekkel szembeni biztonsági követelményeket. Például tűz esetén az eredeti és háttér konfiguráció egyaránt sérülhet, de az objektum környezetéből adódó kockázatok is azonosak. A lokális aktív redundans rendszerek részleges védelmet, de magasabb rendelkezésre állást biztosítanak. A távoli aktív redundans rendszerek átfogó védelmet, és folyamatos rendelkezésére állást biztosítanak.
A passzív, és az aktív redundáns rendszerek sem teszik az adat, és a programmentéseket feleslegessé, hanem a folyamatos működés különböző szintű biztosításával annak felhasználási valószínűségét csökkentik.

Összefoglalva az információ-rendszernek a rendelkezésre állása biztosítására a következő, a felsorolás sorrendjében növekvő erősségű, redundáns megoldások alkalmazhatók:

- Nagy megbízhatóságú (MTBF értékű) hw eszközök alkalmazása, és hideg tartalék berendezések biztosítása (ezzel a fizikai rendelkezésére állásnál foglalkozunk),
- Magas rendelkezésre állást biztosító rendszer alkalmazása (passzív, illetve lokális aktív redundans rendszer),
- Folyamatos rendelkezésre állást biztosító rendszer alkalmazása (távoli aktív redundans rendszer).

A HELYREÁLLÍTÁSI STRATÉGIA

A helyreállítási stratégia célja az eredeti konfiguráció, általában az eredeti helyen történő újjáépítése. Ennek során

- fel kell mérni a keletkezett károkat,
- ki kell dolgozni az újjáépítésnek a tervét, és költségvetést,
- dönteni kell,
- végre kall hajtani az építést, beszerzéseket,
- az eredeti konfigurációnak megfelelő konfiguráción az újraindítást,
- a háttér rendszer leállítását.

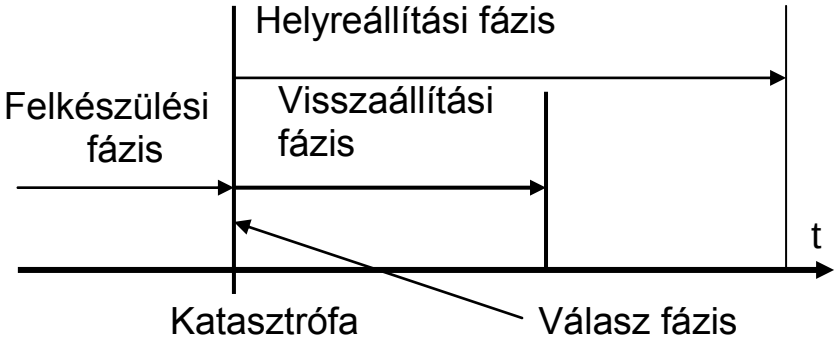
A SZÁLLÍTÓI STRATÉGIA

A katasztrófa tervezés során meg kell határozni, hogy a szállítók felé, milyen szerződéses kötelezettségeket kell érvényesíteni. Például katasztrófa esetén szakértői közreműködés, rendkívüli szállítás (vannak olyan világcégek, amelyek vállalják nemcsak az azonnali szállítást, hanem gördülő háttér (roll in replacement) biztosítását.

A KATASZTRÓFAKEZELŐ KÖZPONT

A katasztrófakezelő központ a katasztrófa team munkahelye, amelyet úgy kell kialakítani, hogy a team munkájának minden előfeltétele adva legyen. Ezek alternatív kommunikációs lehetőségek, számítástechnikai, és ügyviteli eszközök, a Katasztrófaterv egy példánya, munkatársak, és szállítók címlistái, szerződések. A Katasztrófa kezelő központ a felkészülési fázisban a team munkáját már kiszolgálja. Ezért létszámot is kell hozzá biztosítani.

A KATASZTRÓFA ELHÁRÍTÁS FOLYAMATA



A katasztrófa elhárítása a következő fázisokból áll:

- *Felkészülési fázis,* amelyben a katasztrófa bekövetkezése előtti feladatokat kell megoldani (a katasztrófa elhárítási részleges védelmi intézkedések, az ÜFT karbantartása, tesztelése, oktatása).
- *Válasz fázis*, amelyben a katasztrófa bekövetkezését követő legrövidebb időn belül meg kell kezdeni a katasztrófa kihirdetését, a kárkövetkezmények csökkentését, és a visszaállítás megkezdését.
- *Visszaállítási fázis,* amelyben a szolgáltatásokat a háttér felhasználásával (átmenetileg) újra kell indítani.

MSZ ISO/IEC 17799 a 11.1.3. C). pontban írja: Ajánlatos megfontolni a tartalékra kapcsolás eljárásait, ezek azokat a tevékenységeket írják le, amelyekben lényeges üzleti tevékenységeket vagy a támogató szolgáltatásokat ideiglenesen áthelyezik alternatív helyekre, és az üzleti tevékenységeket kívánt időn belül ismét üzembe helyeznek.

- *Helyreállítási fázis*, amelyben a kárkövetkezmények felmérése, és az újjáépítés után, a szolgáltatásokat az eredeti helyen kell újraindítani.

MSZ ISO/IEC 17799 a 11.1.3. D). pontban írja: Ajánlatos megfontolni az újrakezdés/folytatás azon eljárásait, amelyek a rendes üzleti működéshez való visszatérést, megvalósító tevékenységeket írják le.

A KATASZTRÓFA TERVEZÉS KÖLTSÉGEI:

A katasztrófatervezésnél természetesen nem lehet megkerülni a megvalósításának költségei, és a katasztrófa esetén bekövetkező kár összehasonlítását. A problémát az képezi, hogy a katasztrófa bekövetkezése esetén a kárkövetkezmények lehetnek

- vagyoni károk, és
- nem vagyoni károk.

A vagyoni károk, azaz az eszközökben bekövetkező károk szinte pontosan megbecsülhetők. A nem vagyoni károk, mint például a piaci részesedés csökkenése, a gazdasági szervezet megítélésének negatív megváltozása, illetve adott esetben részvények tőzsdei árfolyamának csökkenése, semmilyen módon nem becsülhető. A nemzetközi tapasztalat, és az irodalom szerint minden olyan módszer, amely „számításokon alapul” csak a menedzsment számára készített, látványos produkció értékű. J. Butler azt írja, hogy *a katasztrófa kockázatának quantitatív meghatározása többnyire kevés realitással bír.* Továbbá *a kár nagysága általában a kiesett idővel rohamosan növekszik,* amely felkészülés hiányában igen hosszú lehet. A bankoknál a kár növekedési arányait mutatja a következő elvi példa: 1. nap 9MUSD, 2. nap 25MUSD, 3. nap 34MUSD. Azaz nem kell sok idő ahhoz, hogy egy bank, esetleg egy vállalat kiessen teljesen az üzletből.

B. Menkus ismertet egy 1993-ban, az USA-ban (Clifton, New Jersey) bekövetkezett katasztrófát, amikor az épület összeomlása miatt az EDS bankkártyás központja vált üzemképtelenné. Az USA-ban üzemelő ATM-ek 6%-a esett ki. A nem megfelelő háttér következtében két hét volt szükséges a háttérközpont újraindításához. A keletkezett kár messze meghaladta egy jó Katasztrófaterv, egy jó háttér költségeit.

A Katasztrófatervvel rendelkező, és nem rendelkező vállalatok költségeinek összehasonlítására J.Butler alapján, a katasztrófaterv nélküli esetben a kárkövetkezmények rendkívül magasak, és egy időpontban jelentkeznek. A Katasztrófatervvel rendelkező vállalatnál egyszeri beruházási költség, üzemeltetési költség, és a visszaállítási költség jelentkezik.

ÖSSZEFOGLALVA

A katasztrófaterv megvalósítási költségei messze alatta maradnak egy olyan katasztrófa költségeinek, amelynél a kárkövetkezmények csökkentésére a gazdasági szervezet nem rendelkezik katasztrófatervvel.

7.2.5.7. BIZTONSÁGI SZABÁLYZAT

A Biztonsági Szabályzat, a biztonsági Szervezet és Működés Szabályozása, és a védelmi intézkedések Üzemeltetési Rendje. (itt is utalunk arra, hogy az ISO/IEC 17799-2002 szabvány magyar fordítása a Security Policyt- Biztonsági Politika Biztonsági Szabályzatnak fordítja, ezzel a két szabályzatot összevonja).

A CÉLJA: a védelmi intézkedések életciklusának minden fázisában a feladatok és felelősségek szabályozása, annak érdekében, hogy a védelmi intézkedések szabályozása a gyakorlatban a védelmi követelmények, kikényszerítését szolgálja, és ehhez a biztonsági szervezet, és infrastruktúra meghatározása
A biztonsági szervezet szabályozása a gazdasági szervezet Szervezeti és Működési szabályzatának része. Az egyenszilárdság elvének megfelelő megoldás, amikor a gazdasági szervezetben a biztonságmenedzsment egy kézben van, és az egyenszilárdság elvének megfelelően a vagyon, és az informatikai biztonságot egységes rendszerként kezelik.

A TÁRGYA: a biztonsági alrendszerek működésének szabályozása, gyakorlatilag a védelmi intézkedések üzemeltetési rendje, amely azt jelenti, hogy a Biztonsági Szabályzatban (Politikában), és a Katasztrófatervben meghatározott védelmi intézkedések üzemeltetési rendjét kell kidolgozni. Az Informatikai Biztonsági Szabályzat a vállalat Biztonsági Szabályzatának része.

A VÉDELMI TECHNIKÁK ÉLETCIKLUSA: a védelmi technikáknál természetesen jól elkülöníthetők az életciklusuk egyes szakaszai, amelyeket célszerű, ha a Szabályzat követ. Ezek a következők

- Fejlesztés/beszerzés, amelynek során a szervezési védelmi intézkedéseket kidolgozzák (pl. humán politika, Titokvédelmi utasítás), a technikai védelmi intézkedésekhez, pedig az eszközöket fejlesztik vagy beszerzik.
- Az átadás/átvétel során a kitűzött vagy szerződött követelmények teljesítését ellenőrzik.
- Az üzemeltetés során a szervezési védelmi intézkedéseket végre kell hajtani, a technikai védelmi intézkedéseket üzemeltetni kell. Az üzemeltetés során meg kell határozni a lehetséges szereplők feladatát, és felelősségét. A szereplők az üzemeltetők, karbantartók, felhasználók. A szereplők feladatainak meghatározásánál alkalmazni kell a feladat szétválasztás elvét. A védelmi intézkedések alkalmazását regisztrációhoz kell kötni. Azaz

csak a Szabályzatban rögzített módon lehet védelmi intézkedéseket bevezetni, a vállalat biztonsági vezetőjének hatáskörében.
- Külön szabályozni kell a biztonsági események kezelésének rendjét.
- A védelmi intézkedések megszüntetése a biztonsági vezető hatáskörébe tartozik. A védelmi eszközök selejtezésénél a szabályozásnak biztosítania kell, hogy a bizalmasság követelménye kikényszerítésre kerüljön.

MONITORING

A védelmi intézkedések hatékonyságának, eredményességének folyamatos követésére, figyelésére például a naplók, és a különféle jelentések alapján rendszert kell kiépíteni, a gyors intézkedések biztosítása céljából.

A BIZTONSÁGI ÜZEMELTETÉSI RENDNEK TEHÁT KÖVETKEZŐ FŐ PONTOKBÓL KELL ÁLLNIA

- A védelmi technikák fejlesztésének rendje.
- Szervezési védelmi intézkedések végrehajtási rendje.
- Garanciális intézkedések üzemeltetési rendje.
- Technikai védelmi intézkedések üzemeltetési rendje.
- Biztonsági események kezelési rendje (ez a hazai gyakorlatban ide tartozik).
- A Biztonsági Szabályzás végrehajtási rendje.

A biztonsági szabályozásnak az üzemeltetési feladatok kiosztásánál a feladat szétválasztás elvét érvényesítenie kell.

7.2.5.8. A BIZTONSÁG ELLENŐRZÉSE

A biztonság folyamatos ellenőrzése lehetőséget ad arra, hogy a biztonságról, mint üzleti követelményről folyamatosan gondoskodjunk, hiszen a veszélyforrások, a kockázatok is folyamatosan változnak. Az úgy nevezett monitoring, vagy rendszerfigyelés funkció nem valósul meg ellenőrzés nélkül. Az ellenőrzés lehet

- belső, vagy
- független külső ellenőrzés.

A belső ellenőrzés maga is független, tehát nem tartózhat az IBV hatáskörébe sem. Ugyan akkor a belső ellenőrzési célok, feladatok meghatározásában részt kell vennie az IBV-nek, és a jelentéseket meg kell kapnia.

A belső biztonsági ellenőrzés lehet:

- folyamatos (speciális esetekben, pl. naplók értékelése),
- terv szerinti, és
- cél vizsgálat, biztonsági események értékeléséhez.

A nemzetközi gyakorlat célszerűnek tartja a biztonság háromévenkénti független külső ellenőrzését.

A COBIT 3 szerint az ellenőrzésnek általában két fő célja van:

- a védelmi intézkedések jogszabályi, illetve belső szabályzatoknak való megfelelőssége, és
- a védelmi intézkedések rendeltetésszerű megvalósítása.

A biztonság belső ellenőrzését adott esetben megfelelő képzettségű szakembernek kell végeznie, és erről nem lehet mindig a belső munkatársak közül gondoskodni.

A BIZTONSÁG BELSŐ ELLENŐRZÉSÉNEK HELYE A VÁLLALATI SZERVEZETBEN

A biztonság belső ellenőrzését a vállalat belső ellenőrzésének szervezetében, és működésében szükséges szervezetileg elhelyezni.

BELSŐ ELLENŐRZÉS

A belső ellenőrzést a vállalat saját belső ellenőrzési munkatársai hajtják végre.

KÜLSŐ ELLENŐRZÉS

Mindazokban az esetekben, amikor egy speciális probléma merül fel külső szakértőt célszerű igénybe venni. Ilyen igény merülhet fel, például az elektromágneses kompatibilitás, a rejtjelezés, vagy például a tartalomhitelesítés területén. Továbbá indokolt legalább háromévenként független, külső szakértőkkel a biztonsági rendszert auditáltatni.

A BELSŐ ELLENŐR KÖVETELMÉNYEI

A biztonsági belső ellenőrnek a következő követelményeknek kell eleget tenni-e

- A vizsgált területtől, és a biztonsági termékek forgalmazóitól függetlennek kell lennie.
- Rendelkeznie kell szakmai kompetenciával.
- A feladatának, szerepének, és felelősségének dokumentumban kell rögzítve lennie, általában, és a konkrét vizsgálatra nézve.
- A vizsgálatot költség hatékonyan, határidőre, minőségileg jól, és megfelelően dokumentálva kell elvégeznie.
- Rendelkeznie kell a vizsgálat idejére a szükséges fizikai, és logikai hozzáférési jogosultságokkal.

A SARBANES OXLEY TÖRVÉNY

A SOX az USA-ban egy világ cégnél bekövetkezett pénzügyi botrány hatására, annak a megismétlődése elkerülésére 2002-ben megjelent törvény, (amelyet követett 2004-ben egy EU Direktíva), a gazdasági társaságok éves beszámolóinak ellenőrzését, és annak valódisága biztosításának követelményeit szabályozza. Megadja a gazdasági szervezet pénzügyi ellenőrzésének (belső, és külső), és az éves mérlegbeszámoló, értékelő jelentés, valamint az üzleti jelentés valódiságának, jogszerűségének ellenőrzési, értékelési követelményeit. A hazai vonatkozó jogszabály szerint (1997.évi. CXLIV.tv. V. fejezet. A gazdasági társaságok törvényes működésének biztosítékai.) a beszámolókat az Igazgatóság a társaság választott könyvvizsgálójával, auditorával köteles a valódiság, és jogszerűség szempontjából ellenőriztetni. Szükséges rögzíteni, hogy a pénzügyi ellenőrzés valódisága nagymértékben függ az informatikai környezet ellenőrzésének realitásától, a biztonsági intézkedések, pl. számon

kérhetőség, védelem a fehérgalléros bűnözés, és a csalás ellen, hatékonyságától

A biztonsági szempontból a legfontosabb követelmények a következők:

- Az Igazgatóság éves vállalati pénzügyi helyzetértékelési kötelezettsége, amelyben a biztonsági helyzet értékelésének is benne kell lennie.
- A pénzügyi, és biztonsági ellenőrzés (külső, belső) megerősítése.
- Az auditorok függetlenségének és etikus magatartásának garantálása, az auditorok regisztrációja, és rotálása.
- Az ellenőrzési, és pénzügyi jelentések minőség ellenőrzése.
- Auditálási Bizottság alakítása.
- A számvitel átláthatóságának biztosítása.
- A pénzügyi rendszerben a valódiság, az adatok, alkalmazások sértetlensége, a biztonság érzékenység alapján meghatározott védelme. (A számon kérhetőség, és a hitelesség következetes biztosítása).
- Független tagok bevonása a boardba.

Továbbá „Az IT ellenőrzési célok a SARBANES-OAXLEY (ITGI kiadvány) megfelelősségre”, több biztonsági ellenőrzési célt is tartalmaznak (Pl. a 19, 23, 36, 39, 41, 59-es ellenőrzési célok), amelyek jól mutatják a pénzügyi, üzleti és az informatikai folyamatok, és biztonságuk kölcsön hatását. Példaként kiemeljük a 25, és a 26-os ellenőrzési célt:

> *25. Az IT menedzsment összhangban a vállalati biztonsági, és adatvédelmi politikával határozta-e meg, az adatok osztályozásának szabályait.*
> *26. Az adatok osztályozásánál minden adatra meg van-e határozva, implementálva, és karbantartva a biztonsági szint? Ezek a biztonsági szintek minden osztályozásnál a megfelelő biztonsági szintet képviselik-e? Rendszeresen újra értékelik-e, ennek megfelelően módosítják-e?*

Ezekből az IT ellenőrzési célokból természetesen meg lehet határozni, hogy mi az, ami biztonsági szempontból fontos, amit biztosítani kell a **SARBANES OAXLEY megfelelősséghez**. *Végül mindezek a védelmi intézkedések, és ellenőrzési célok természetesen nemcsak az információ rendszerre, hanem az üzleti rendszerre, azaz az egész vállalatra, és a teljes biztonsági rendszerre is vonatkoznak.*

Az IT Control Objectives for Sarbanes Oaxley C. melléklete 16-22.-es pontjai ellenőrzési listák a törvénynek való megfelelősség biztonsági ellenőrzéséhez. Az ellenőrzés célja az ésszerű ellenőrzés biztosítása, hogy a pénzügyi jelentés és alrendszer megfelelően biztonságos-e, megelőzi-e az adatok jogosulatlan használatát, felfedését, módosítását, megrongálását, vagy elvesztését, mivel ezek szignifikánsan befolyásolhatják a pénzügyi jelentést.

Összefoglalva:

A SOX, és az EU Direktíva

A gazdasági társaságok éves mérlegbeszámolójának, éves eredmény értékelésének, és üzleti jelentésének valódiságával, jogszerűségével kapcsolatban, új, vagy már meglévő, de fokozott követelményeket állít a gazdasági társaságok elé,

- A könyvvizsgálói, auditorai,
- igazgatóságai, és Felügyelő bizottságai,
- a belső ellenőrzése, és
- a biztonság, ezen belül az informatikai biztonság elé.

Továbbá a SOX (404 paragrafusa) a felső vezetéstől, és az üzleti folyamatok gazdáitól nem pusztán egy megfelelő belső ellenőrzési struktúra létrehozását, hanem a hatékonysága éves bázison történő értékelését is előírja.

7.2.5.9. AKCIÓTERVEK, BIZTONSÁGI PROGRAM

Az Akció Tervek a Biztonsági Politikában, és az ÜFT-ben kidolgozott védelmi intézkedések végrehajtása, megvalósítása, és a Biztonsági Szabályzat szerinti rendeltetésszerű üzemeltetésük biztosítására készülnek. Az Akció Tervek feladatokat, felelősöket (a munkaköröket szabad csak megadni!), és határidőket tartalmaznak, valamint meghatározzák a munkaköri, és befejezés esetén érvényes jelentési kötelezettségeket. Végeredményben az Akció Tervek együttesen egy Biztonsági Programot (a biztonsági rendszer elkészítésére, vagy rekonstrukciójára) alkotnak. Ide tartozik természetesen a fejlesztés/beszerzés szakmai irányítása, amely néhány kritikus oldalát a 10. sz. Melléklet tartalmazza, valamint a biztonság ellenőrzése, és ennek alapján az intézkedése (tervezés, megvalósítás, ellenőrzés, intézkedés, PDCA modell).

7.3. AZ IT BIZTONSÁG ERŐSSÉGE

Természetesen a védelmi intézkedéseknek erősség szempontjából, azaz abból a szempontból, hogy egy rendszer milyen erősségű támadásnak tud ellenállni, több változata is lehetséges. Ebből következően a kockázat menedzsment végrehajtása után, a kockázati mátrix birtokában, az informatikai biztonsági vezető javaslatát figyelembe véve, a top menedzsmentnek el kell döntenie, hogy milyen erősségű védelmet kíván. Fontos, hogy az egyenszilárdság elve alapján ennél gyengébb a védelmi intézkedés egyik biztonsági alrendszerben sem lehetséges. A termékek ellenálló képességét az MSZ/ISO/IEC 15408 szabvány alapján lehet meghatározni, amelyet akkreditált szervezetek tanúsíthatnak. Jelenleg hazánkban ilyen szervezet létrehozása folyamatban van. Az értékelés lehetséges értékei EAL-0, EAL-1, EAL-2, EAL-3, EAl-4, EAL-5, EAL-6, EAL-7, ahol az EAL = Evaluation Assurance Level, az értékelés garanciális szintjei.. A kereskedelmi gyakorlatban az EAL-3, és EAL-4 szintek a használatos legmagasabbak, míg az ennél magasabb szinteket, a biztonsági szervezetek, az államigazgatási szervek alkalmazzák. Továbbá a nemzetközi gyakorlatban egymás akkreditált szervezeteinek tanúsításait is a kereskedelmi szintekig fogadják el az egyes országok.

A korábbiakban használatos biztonságértékelési módszerek az AMERIKAI TCSEC (Trusted Computer Security Evaluation), az EUROPAI ITSEC (IT Security Evaluation), és az ezekből készült CC (Common Criteria), illetve az ISO/IEC 15408-1,2,3, és a magyar fordítása az MSZ ISO IEC 15408-1,2,3 Az informatikai biztonság értékelésének közös szempontrendszere).

CC *MSZ ISO/IEC 15408*	*TCSEC*	*ITSEC*
EAL0	***D***	***E0***
EAL1		
EAL2	***C1***	***E1***
EAL3	***C2***	***E2***
EAL4	***B1***	***E3***
EAL5	***B2***	***E4***
EAL6	***B3***	***E5***
EAL7	***A1***	***E6***

Az információ rendszer biztonságának értékelésére a COBIT 3–ban megadott „érettségi modell” szolgál, amely szerint egy rendszer biztonsága lehet (ezt az értékelést minden szervezet maga elvégezheti):
0 Nem létező
1 Kezdő / ad hoc

2 Intuitív
3 Definiált folyamatok
4 Menedzselt, mérhető
5 Optimalizált

AZ ÉRETTSÉGI SZINT MODELL (COBIT3)

A biztonság értékelésére fentiekben megadott különböző eljárások, szabványok, módszertanok részletesebben. Történelmileg a legelső a Trusted Computer Security Evaluation Criteria (TCSEC) az USA-ban készült el a nyolcvanas években. Ezt követte az europai Information Technology Security Evaluation Criteria (ITSEC). Majd az amerikai, kanadai, és nyugat europai szabványügyi hivatalok együttes munkájával megszületett a Common Criteria for Information Technology Security Evaluation (ehhez később kiadták a Common Evaluation Methodology-t), amelynek volt különböző változata, míg a 2.1 változat lett az ISO/IEC 15408-as szabvány (Magyar megfelelője az MSZ-ISO/IEC 15408-1,2,3) Ezeket a szabványokat akkreditált szervezetek jogosultak használni, azaz a biztonság erősségéről tanúsítványt kiállítani. Hazánk 2003. szeptemberben csatlakozott a Common Criteriához, jelenleg nincs akrreditált szervezet. A Cobit 3 Érettségi szint modell (Maturity Model) bárki által használható, tehát egy vállalat saját alkalmazásával megvizsgálhatja, hogy hová sorolható be a megvalósított biztonsága.

Az érettségi modell szintjeit azért nem feleltetjük meg, mert a három szabvány egy részletesen kidolgozott értékelési módszer valójában, míg az érettségi modell ehhez képest egy nagy vonalú eljárás. Ezért az IBV-nek ügyelni kell arra, hogy az érettségi modell nem helyettesítheti a szabványokat, csak tájékoztató jellegű következtetések levonására, önértékelésre alkalmas. A COBIT 4 már minden ellenőrzési folyamatra (34 van) alkalmazza az érettségi modellt.

Az alábbiakban megadjuk az egyes szintek értelmezését az érettségi modell szerint

- **0 szint. Nem létező.** A szervezet nem ismerte fel az IT biztonság szükségességét. Nincsenek felelőségek kijelölve a biztonság érvényesítésre. Az IT biztonságot nem támogatják védelmi intézkedések. Nincs biztonsági jelentés. Nincs válasz a biztonsági eseményekre. A rendszer biztonsági adminisztráció teljes hiánya.
- **1 szint. Kezdő/ad hoc.** A biztonsági tudatosság az egyénektől függ. Az IT biztonság reaktív alapú, nem mért. Az IT biztonsági eseményeket, ha jelzik, véletlen válaszokat adnak, mivel nem tisztázottak a felelősségek. Az IT biztonsági eseményekre a válaszok előre nem láthatóak.

- **2 szint. Ismételhető/intuitív.** A felelősségek és a számon kérhetőség az IT koordinátorokra van kijelölve, menedzselési jogosultságok nélkül. A biztonsági tudatosság osztott, korlátozott. IT biztonsági információk készülnek, de nem elemzik. A biztonsági megoldások a biztonsági eseményekre válaszként irányulnak. A Biztonsági Politikát fejlesztik. Nem megfelelő gyakorlat, és eszközök. Az IT biztonság nem teljes, megtévesztő, nem helyénvaló.
- **3 szint. Definiált folyamatok.** Biztonsági tudatosság fennáll, és a menedzsment előmozdítja, szabványosítva van, és formalizált**.** Az IT biztonsági folyamatok definiálva vannak és megfelelnek a Biztonsági Politikának. A felelősségek ki vannak jelölve, de nincsenek konzisztensen kikényszerítve. A Biztonsági Politika kockázat elemzésen alapuló védelmi intézkedésekből áll. Az IT biztonsági jelentés IT nem üzlet orientált. Ad hoc behatolás elemzés van.
- **4 szint. Menedzselt/mérhető**. Az IT biztonsági felelősségek világosan kijelöltek. A biztonsági jelentések üzlet orientáltak. A biztonsági tudatosság biztosítása kötelező. Biztonsági specialitásokra is kitér a Biztonsági Politika. Felhasználó azonosítás, hitelesítés, jogosultság menedzsment szabványosítva van. Behatolás ellenőrzés szabványosított, formalizált folyamat.
- **5 szint. Optimalizált**. Az IT biztonság közös felelőssége az üzleti és az IT menedzsmentnek. Az IT biztonság integrálva van a vállalati biztonsági (üzleti) célokkal. Az IT biztonsági követelmények világosan definiáltak, optimalizáltak és megfelelnek egy ellenőrzött biztonsági tervnek. A biztonság a rendszerbe beépített, nem hozzáadott. A számon kérhetőség ki van alakítva a felhasználók számára. Az IT biztonsági jelentések korai figyelmeztetést adnak a változó, és növekvő kockázatokról, monitorozva a küldetés kritikus rendszereket. A biztonsági eseményekre azonnal van válasz, automatikus rendszerekkel. Periodikus biztonsági felmérés értékeli az implementált biztonsági rendszert. Az új fenyegetéseket és sebezhetőségeket rendszeresen gyűjtik, elemzik, és megfelelő ellenőrzések mérsékelik. Behatolás tesztelés, a biztonsági események elemzése, és a kockázatok proaktív azonosítása az alapja a folyamatos fejlesztésnek. A biztonsági folyamatok és technológiák integráltak vállalat szerte. Automatikus központi felhasználó menedzsment rendszer van implementálva. A másik oldalon bemutatunk egy táblázatos összefoglalást az egyes szintek fő jellemzőiről.

Jellemző érettségi szint	Biztonsági tudatosság	Felelelősségek kijelőlése	Védelmi intézkedések, és gyakorlat	Biztonsági események kezelése
0 Nem létező	Nem ismerték fel	Nincsenek kijelölve	Nincsenek	Nem kezelik, és nincs admin. sem
1 Kezdő/ad hoc	Egyéntől függő	Nincs	Nem szervezett, nem mérhető	Ha jelzik, véletlenszerű válasz
2 Intuitív	Osztott, korlátozott	IT koordinátorok menedzselési jog nélkül	Bizt. Pol. Van, Nem teljes, nem megfelelő eszközök, és gyakorlat	Jelentés van, értékelés nincs
3 Definiált folyamatok	Van, szabályozott, mgm támogatja	Definiált folyamatok, kikényszerítés nem konzisztens	A Bp. kockázat elemzésen alapul, ad hoc behatolás ellenőrzés	A jelentések nem üzlet orientáltak
4 Menedzselt, mérhető	Tudatosság szervezése szabályozott, és megvalósul	Egyértelműen kijelölve	A Bp. specialitásokra is, Felhasználó azonosítás, hitelesítés, jogosultság szabályozva Behatolás ellenőrzés szabályozott	Jelentések üzlet orientáltak
5 Optimalizált		Az IT és az üzleti mgm közös felelőssége a biztonság. Számon kérhetőség ki van alakítva	Követelmények definiáltak, a biztonság nem hozzá adott, hanem beépített	Kezelik. A biztonsági eseményekre van válasz, azokat periodikusan elemzik, intézkednek, a fejlesztés folyamatos

A COBIT SECURITY BASELINE

A Cobit Security Baseline (CSB) a Cobit 3 alapján kidolgozott biztonsági irányelveket tartalmazza, jól felhasználható a korlátozott lehetőségekkel rendelkező kis vállalatok biztonsági követelményeinek meghatározására.

Többek között tartalmazza:

Informatikai biztonság meghatározását

Kockázatokat

39 lépést az informatikai biztonsághoz (a COBIT 3 összesen 318 ellenőrzési szempontot tartalmaz).

Biztonsági intézkedéseket az otthoni felhasználók, professzionális felhasználók, menedzserek, végrehajtók, és az igazgatóság részére.

A 15. sz. melléklet bemutatja a CSB alapján, hogy az miként felel meg az ISO/IEC 17799-es szabványnak.

VÉDELMI INTÉZKEDÉSEK ERŐSSÉGÉNEK MEGHATÁROZÁSA

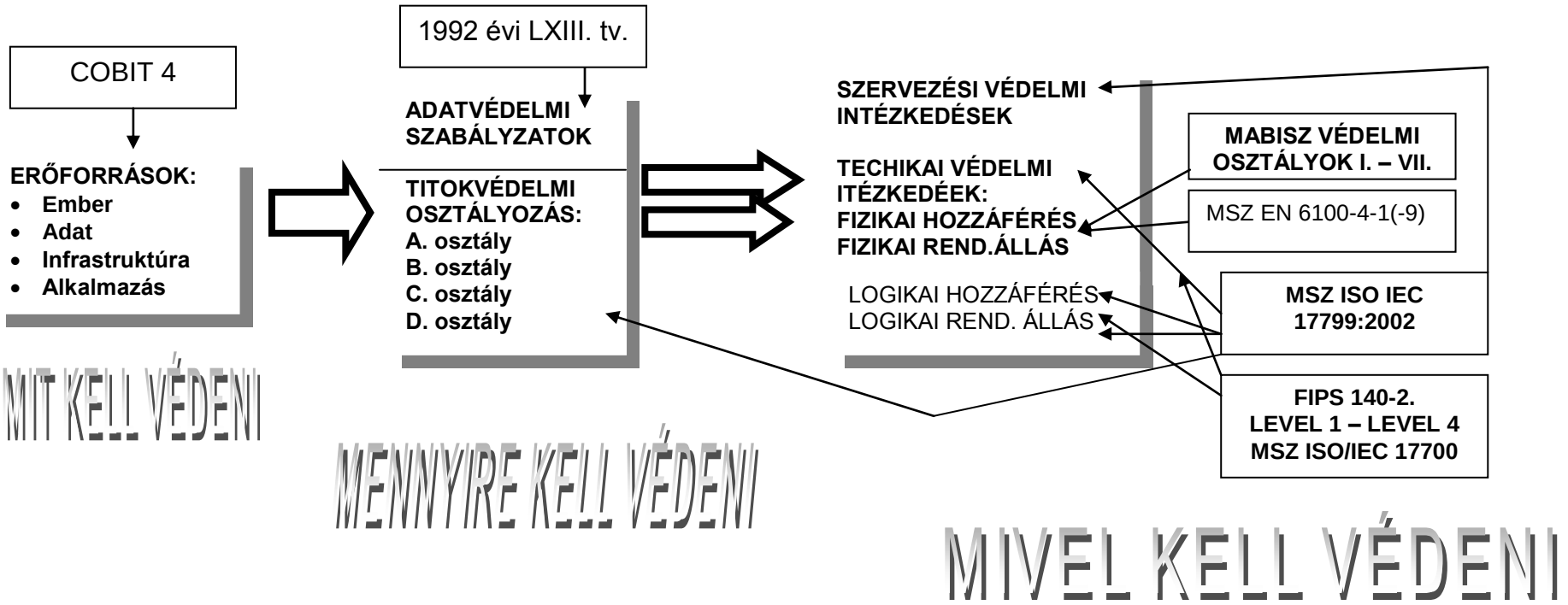
Az informatikai biztonság szervezésénél az adatokat, alkalmazásokat, eszközöket és helyiségeket osztályozni kell. Az osztályozás célja, hogy egyértelműen meghatározza, mit, és milyen mértékben kell megvédeni. A védelem mértékét a hatályos jogszabályok, és a vállalat üzleti érdekei, a védendő rendszer, erőforrás biztonság érzékenysége alapján határozhatjuk meg, azaz egy több szintű biztonsági politikát (multilevel security policy) kell alkalmazni. Az egyes védelmi osztályokhoz, az adott gazdasági szervezet, erőforrás biztonság érzékenysége szerint hozzá kell rendelni a védelmi követelményeket (például a hozzáférési jogosultságokat), amelyekből pedig a védelmi intézkedések specifikálhatók. A védelmi osztályozást az alábbi ábrán mutatjuk be, amely alapul szolgál az adatok, alkalmazások, eszközök, és helyiségek védelmi osztályozásához (az MSZ ISO/IEC 17799 szabvány mondja ki, hogy ezt az osztályozást el kell végezni, és alapul kell venni).

Védelmi osztályok	*A védendő*		*A hozzáférés*	
	Bizalmasság	*Sértetlenség*	*Belső**	*Külső***
A. osztály	***Igen kritikus***	***Életbevágó***	***Erősen korlátozott***	***Erősen korlátozott***
B. osztály	***Kritikus***	***Életbevágó***	***Korlátozott***	***Erősen korlátozott***
C. osztály	***Nem kritikus***	***Fontos***	***Nem korlátozott***	***Korlátozott***
D-. osztály	***Nem kritikus***	***Nem életbevágó***	***Nem korlátozott***	***Nem korlátozott***

* bizalmas hálózaton belül ** nem bizalmas hálózat felé

VÉDELMI OSZTÁLYOZÁS

A védelmi intézkedés erősségének meghatározásához az általános elvi összefüggést az alábbi ábra mutatja


COBIT 4
ERŐFORRÁSOK:
• Ember
• Adat
• Infrastruktúra
• Alkalmazás
MIT KELL VÉDENI
1992 évi LXIII. tv.
ADATVÉDELMI SZABÁLYZATOK
TITOKVÉDELMI OSZTÁLYOZÁS:
A. osztály
B. osztály
C. osztály
D. osztály
MENNYIRE KELL VÉDENI
SZERVEZÉSI VÉDELMI INTÉZKEDÉSEK
TECHIKAI VÉDELMI ITÉZKEDÉEK:
FIZIKAI HOZZÁFÉRÉS
FIZIKAI REND.ÁLLÁS
LOGIKAI HOZZÁFÉRÉS
LOGIKAI REND. ÁLLÁS
MABISZ VÉDELMI OSZTÁLYOK I. – VII.
MSZ EN 6100-4-1(-9)
MSZ ISO IEC 17799:2002
FIPS 140-2.
LEVEL 1 – LEVEL 4
MSZ ISO/IEC 17700
MIVEL KELL VÉDENI

ADATOK VÉDELMI OSZTÁLYOZÁSA

Az adatok védelmi osztályozása a titokvédelemre kötelezett szervezeteknél a titokvédelemről szóló törvény, a titokvédelemre nem kötelezett gazdasági szervezeteknél, pedig az üzleti titokról, és a személyes adatok, illetve a banktitok, a biztosítási titok, és az értékpapírtitok védelméről szóló jogszabályok, végrehajtását szolgálja.

- Üzleti titok mind az, aminek a védelméhez a gazdasági szervezetnek méltányolható érdeke fűződik, és a védelmére a gazdasági szervezet, intézkedéseket tett.

- Személyes adat a meghatározott személlyel kapcsolatba hozható adat, az adatból levonható, az érintettre vonatkozó következtetés. A személyes adat mindaddig megőrzi e minőségét, amíg a kapcsolata az érintettel helyreállítható.

- A banktitok minden olyan, az egyes ügyfelektől a banknak a rendelkezésre álló adat, amely az ügyfél személyére, adataira, vagyoni helyzetére, kereskedésére, valamint a bank és az ügyfél között kötött szerződés(ek)re vonatkozik.

Az adatokat, tehát a biztonság érzékenységük szerint kell osztályozni.

- A biztonság érzékenység az adatnak egy arra jogosult személy által meghatározott azon tulajdonsága, amely szerint azt védeni kell, mert a jogosulatlan felfedése, módosítása, elvesztése vagy rombolása valakinek vagy valaminek kárt okoz.

Az osztályozást az alábbi ábra szerint kell elvégezni.

Védelmi Osztály	A védelmi osztály Megnevezése	A védelmi osztályba sorolt adatok (pl.)	
		Minősítésre kötelezett szerv.	Gazdasági szerv.
A	Titkos	Államtitok	Üzleti titok
B	Bizalmas	Szolgálati titok	Személyes adatok
C	Belső használatra	Belső használatra	Belső használatra
D	Nyilvános	Nyilvános	Nyilvános

Adatok védelmi osztályai.

Az egyes védelmi osztályokhoz tartozó adatokat, a hozzáférés védelmi rendszerben, különböző erősségű védelemmel kell ellátni.

ALKALMAZÁSOK VÉDELMI OSZTÁLYOZÁSA

Az alkalmazásokat annak függvényében kell a védelmi osztályokba besorolni, hogy milyen adatokat kezelnek, állítanak elő. Amennyiben egy alkalmazás több védelmi osztályba sorolt adatot kezel vagy állít elő, a legerősebb védelmi osztály a meghatározó.

ESZKÖZÖK VÉDELMI OSZTÁLYOZÁSA

Az eszközök lehetnek hardver, és szoftver eszközök, azaz az alkalmazott technológia elemei. A védelmi osztályba sorolás azt határozza meg, hogy az eszköz bizalmassága, és sértetlensége mennyire biztonságkritikus. Az ábrán az eszközök védelmi osztályai találhatók. Az A osztályba tartozik például a rejtjelező gép (bontásvédett kivitelben kell alkalmazni). A B. osztályba tartozik például a fizikai, és a logikai hozzáférés-védelmi szoftver, amelyeket megfelelő erősségű hozzáférés-védelemmel kell védeni. A C osztályba például a kereskedelmi forgalomban kapható, közismert eszközök tartoznak. A D osztályba a nyilvánosan használt eszközök (pl. pénzkiadó automata) tartoznak.

Védelmi Osztály	A védelmi osztály Megnevezése	A védelmi osztályba sorolt eszközök (pl.)
A	Titkos	Speciális hw
B	Bizalmas	Speciális rsw
C	Belső használatra	Egyéb hw, és rsw
D	Nyilvános	Közterületen üzemeltetett

Eszközök védelmi osztályai

A FIPS PUB 140-2 amerikai szabvány a biztonsági követelményeket határozza meg nem minősített, biztonság érzékeny információk rejtjelezése esetében, (tehát nem állam vagy szolgálati titkot képező információk) számítógépes, illetve távközlési rendszerekben alkalmazott rejtjelező modulok védelmére. Azaz a rejtjelező gépek esetében, az A védelmi osztályba sorolás mellett, a szabvány négy lehetséges védelmi erősségi szintet ad meg, éspedig Level 1, Level 2, Level 3, Level 4 (növekvő erősségű sorrendben). A biztonsági követelmények kiterjednek a rejtjelező modul bizalmas tervezésére, és implementálására. Többek között:
A rejtjelező modul tervezését, a portokat, és interface-ket; szerepeket, szolgáltatásokat, és a hitelesítést, a fizikai biztonságot, a rejtjelezési kulcs menedzsmentet, a működési környezetet, az elektromágneses interferencia/ elektromágneses kompatibilitás (EMI/EMC) védelmét (47 Code of Federal Regulations Part 15, Subpart B, unintentional Radiators, Digitel Devices, Class A for business use, Class B for home use) határozza meg.

Az egyes szintek követelményei részletesebben:

- **Level 1.**

A legalsó szint, amelyre az alapvető biztonsági követelmények vonatkoznak, például egy PC, egy nem értékelt operációs rendszert használva. Az egyéb követelmények, mint fizikai biztonság, hálózati biztonság, és adminisztratív biztonság korlátozottan vagy egyáltalán nincsenek. EMI/EMC üzleti környezetben való alkalmazáshoz.

- **Level 2.**

Itt megjelenik a modul bontás védett kivitele, a modul mozgatható falainak, és ajtójának ellenálló zárása a jogosulatlan behatolás ellen, és minimális szerep bázisú (felhasználó, rejtjelező adminisztrátor, karbantartó), hitelesítést igényel az operátor esetében. A Level 2 megengedi, hogy a software, firmware elemek egy általános célú számítástechnikai rendszert, operációs rendszert használjanak. A biztonságértékelési követelmény EAL 2 (CC). EMI/EMC üzleti környezetben való alkalmazáshoz

- **Level 3.**

Az előbbieken túlmenően itt elő van írva, olyan bontás védettség, amely erőszakos behatolás esetén a biztonság kritikus információkat megsemmisíti. Az operátor hitelesítése azonosítás bázisú, és ellenőrzi, hogy milyen tevékenységre vonatkoznak az operátor jogosultságai. A nyilvános szöveg input, és output útvonala bizalmas útvonal kell legyen elkülönített portra. A Level 2–vel azonos feltételekkel használhat softwaret, és firmwaret, azzal, hogy az operációs rendszer EAL 3 értékelésű legyen. EMI/EMC otthoni környezetben való alkalmazáshoz.

- **Level 4.**

A legmagasabb szint, amelynek komplett fizikai védelmet kell biztosítani a modul körül, fizikai támadásjelző képességgel. A jelzet támadás esetén minden nyílt szöveget meg kell, hogy semmisítsen. Alkalmazható fizikailag nem védett környezetben. Az operátor hitelesítése azonosítás bázisú. Az operációs rendszernek az EAL 4 követelményeit kell teljesíteni. EMI/EMC otthoni környezetben való alkalmazáshoz.

HELYISÉGEK VÉDELMI OSZTÁLYOZÁSA

A helyiségeket a funkciójuk szerint kell osztályozni. Az alábbi ábrán, bemutatjuk a helyiségek védelmi osztályait.

Védelmi Osztály	A védelmi osztály Megnevezése	A védelmi osztályba sorolt helyiségek (pl.)
A	Zárt	WAN kpt.-i rendszer
B	Kiemelten ellenőrzött	LAN szerver
C	Ellenőrzött	Iroda helyiségek
D	Nyilvános	Ügyfélszolgálat

Helyiségek védelmi osztályai.

A zárt terület csak ellenőrzött területre nyílhat. A belépés ellenőrzés, a mozgás ellenőrzés, a behatolás védelem, az akusztikus és elektromágneses kisugárzás védelem erőssége a védelmi osztályok szerint alakítandó ki. A zárt területen mindegyik, míg a nyilvános területen gyakorlatilag csak az élőerős őrzésvédelmet alkalmazzák. Az alkalmazott védelem a B és C védelmi osztályban elsősorban attól függ, hogy az objektum elhelyezkedése milyen kockázatokat képez. Például az objektumnak vannak más épületekkel közös falai indokolt a közös falakat behatolás érzékelőkkel ellátni.

VÉDELMI OSZTÁLYOZÁS MINTA

A védelmi osztályba sorolást a védendő erőforrás a jogszabályokban meghatározott kötelezettségei, illetve a vállalat üzleti érdekei lapján meghatározott bizalmassági, és sértetlenségi követelményei alapján kell elvégezni. Az osztályozás célja a védelmi intézkedések specifikálásához a védelem erősségének, mint követelménynek a meghatározása. A védelmi osztályok a következők:

Védelmi osztályok	***Védendő***		***Hozzáférés***	
	Bizalmasság	***Sértetlenség***	***Belső***	***Külső***
1.	***Igen kritikus***	***Életbevágó***	***Erősen korlátozott***	***Erősen korlátozott***
2.	***Kritikus***	***Életbevágó***	***Korlátozott***	***Erősen korlátozott***
3.	***Nem kritikus***	***Fontos***	***Nem korlátozott***	***Korlátozott***
4.	***Nem kritikus***	***Nem életbevágó***	***Nem korlátozott***	***Nem korlátozott***

*Az adatok osztályozása a titokvédelemre kötelezett szervezeteknél a titokvédelmi minősítés, a titokvédelemre nem kötelezett gazdasági szervezeteknél, pedig az üzleti titokról („üzleti titok mind az, aminek a védelméhez a gazdasági szervezetnek méltányolható érdeke fűződik, és **a védelmére a gazdasági szervezet, intézkedéseket tett**”), és a személyes adatok, illetve a banktitok, és az értékpapírtitok védelméről szóló jogszabályok végrehatása érdekében védelmi osztályozást kell készíteni.*

Adatok védelmi osztályai:

1. Osztály. Titkos adatok. Ide sorolandók azok az adatok, amelyekhez a belső, és külső hozzáférés t erősen korlátozni kell, és a sértetlenségük életbevágó. Pl.:

- az erősen védendő üzleti titkok,
- az erősen védendő ügyféladatok (bank-, biztosítási, értékpapírtitok).

2. Osztály Bizalmas adatok. Ide sorolandók azok az adatok, amelyekhez a belső, és külső hozzáférést korlátozni kell, és sértetlenségük életbevágó. Pl.:

- a közepesen védendő üzleti titkok,

- az ügyféladatok (banktitkok, biztosítási titok, értékpapír titok),
- a munkatársak személyes adatai.

3. Osztály. Belső adatok. Ide sorolandók azok az adatok, amelyeknek a felfedése nem kritikus, csak a külső hozzáférés t kell korlátozni. A sértetlenségük fontos, de nem életbevágó. Pl.:

- ***a csak belső felhasználásra szolgáló szolgálati adatok,***
- a csak belső felhasználásra szolgáló üzleti adatok,
- a harmadik felek munkatársainak adatai.

4. Osztály. Nem osztályozott adatok. Ide sorolandók azok az adatok, amelyeknek a felfedése nem kritikus, sebezhetőségük nem életbevágó, a védelmet nem igénylő adatok.

Az állam-, és a szolgálati titok a titokvédelmi törvény alapján minősítésre kötelezett szervezetekre vonatkozik.

Az osztályozást az adat megőrzi teljes életciklusa alatt, és akár papír, akár elektronikus adathordozón van rögzítve, fel kell tüntetni.

Folyamatok, alkalmazások védelmi osztályai.

A védelmi osztályokba a folyamatokat, az alkalmazásokat a szerint kell besorolni, hogy az alkalmazások által kezelt, illetve előállított adatok milyen védelmi osztályba vannak sorolva. Amennyiben az alkalmazás több védelmi osztályba sorolt adatot kezel a legerősebb védelmi osztály a mértékadó.

Helyiségek védelmi osztályai:

1. Osztály. Zárt helyiségek*, ahová csak erősen korlátozott számú személyek léphetnek be, akiknek erre jogosultságuk van. Ide tartoznak, a számítóközpontok, adathordozó raktárak, az épület felügyeleti és biztonsági felügyeleti rendszer központi berendezéseinek helyiségei. A zárt terület csak ellenőrzött területről nyílhat.*

2. Osztály. Kiemelten ellenőrzött helyiségek, *ahová a saját munkatársak belépése korlátozva van. Például LAN-ok szerverei elhelyezésre szolgáló helyiségek, az üzemi helyiségek, energiaellátó berendezések, távközlési és energiaellátó kábelek csatlakozási pontjai és az elosztók, raktárak, klimatizáló berendezések helyiségei, dokumentumtárak, pénztárak.*

3. Osztály. Ellenőrzött helyiségek, *ahová a munkatársak, illetve a látogatók ellenőrzés után léphetnek be. Például az irodák.*

4. Osztály. Nem osztályozott helyiségek, *ahová bárki minden további nélkül beléphet. Idetartoznak az ügyfélszolgálatot ellátó irodák, bankfiókok ügyfélkiszolgáló helyiségei.*

Eszközök, eljárások, értékek védelmi osztályai:

1. Osztály. Titkos eszközök. Ide tartoznak azok a speciális eszközök, berendezések, amelyek hozzáférés e kiemelten korlátozott kell legyen. Pl. rejtjelező gépek.

2. Osztály. Bizalmas eszközök. A fizikai, és a logikai hozzáférés -védelmi szoftver**.** Egyes eljárások (pl. know how alapján alkalmazott eljárás, gyártási titok, fejlesztés, új üzletág), és az azokat realizáló eszközök, berendezések, valamint értékek (anyagok, félkész, és késztermékek, készpénz, értékpapírok, értéktárgyak).

3. Osztály. Belső használatra szolgáló eszközök. Egyéb hw, és rsw-ek.

4. Osztály. Nem osztályozott eszközök. Nyilvános helyen üzemeltetett berendezések.

A VÉDELMI OSZTÁLYOZÁS ALKALMAZÁSA

A védelmi osztályozást a fizikai hozzáférés védelemnél, valamint a logikai hozzáférés védelemnél kell alkalmazni. Mégpedig a következőképen

A fizikai hozzáférés-védelemnél a helyiségek védelmét az osztályozás alapján legalább az egyes osztályokban a következőképpen kell kialakítani:

Védelmi Osztály	Belépés ellenőr-zés	Mozgás ellenőr zés	Beha tolás vé-delem	Tűz-véde-lem	Lég állapot vé-delem	EMC EMI véd.	Felü-gyelet
I. zárt	E	E	E	E	T	T	T
II. kiemelt	R	R	R	N	R	-	T
III. ellenőrzött	M	M	M	N	R	-	T
IV. nem oszt.	É	M	-	N	-	-	É

A jelölések: E= erősített, É= élőerővel, M= minimális, N= normál, R= részleges, T= teljes.

Az objektumok informatikai területeinek, illetve helyiségeinek védelmi osztályba sorolása (példa):

I. zárt terület: számítóközpont, integrált felügyeleti központ, távközlési központ,

II. kiemelt terület**:** terminál szobák**,** elektronikus adathordozó, és berendezés raktár, szünetmentes áramellátó, klíma központ, energia és távközlési becsatlakozások, elosztók, papír alapú adathordozó raktár, pincék, expedíció,

III. ellenőrzött terület: irodák, folyosók, emeleti előterek, udvar,

IV. nem osztályozott terület: főbejárati előtér, ügyfélszolgálat

A zárt, és a kiemelt terület nem nyílhat nyílt területről. Az I-III. kategóriájú területen belül megengedett további azonos vagy más I-III. kategóriába sorolt terület kialakítása, a belépési jogosultságok korlátozása, a belépés, és a mozgás ellenőrzése céljából.

A belépés ellenőrzés az egyes védelmi osztályokban:

I. Zárt terület.
A zárt terület hátárán kétirányú elektronikus, és mechanikai ellenőrzés, a területen belül leválasztott zárt területeken kétirányú elektronikus ellenőrzés.
II. Kiemelt terület.
Kétirányú elektronikus ellenőrzés.
III. Ellenőrzött terület.
A belépés elektronikus ellenőrzése.
IV. Nem osztályozott terület.
Ellenőrzés élőerővel.

A mozgás ellenőrzés az egyes védelmi osztályokban:

I. Zárt terület.
Teljes körű térvédelem. Zártláncú videó rendszerhez csatlakozó videó kamerák a terület határán, és a biztonságkritikus pontokon.
II. Kiemelt terület.
Részleges térvédelem. A terület határán videó kamerák.
III. Ellenőrzött terület.
A terület határán videó kamerák.
IV. Nem osztályozott terület.
A terület videó kamerákkal ellenőrzött.

Fizikai behatolás védelem az egyes védelmi osztályokban:

I. Zárt terület.
Erősített felületvédelem,
II. Kiemelt terület.
Minimális felületvédelem utcai fronton, és szomszédos épülettel közös falon.
III. Ellenőrzött terület.
Felületvédelem a szomszédos épülettel közös falon.
IV. Nem osztályozott terület.
Nincs behatolás védelem.

Tűzvédelem az egyes védelmi osztályokban:

A hatósági előírások szerint.

Elektromágneses kompatibilitás védelem az egyes védelmi osztályokban:

A zárt területen.

Integrált felügyeleti rendszer az egyes védelmi osztályokban:
Az integrált felügyeleti rendszer irányítja, és ellenőrzi az épületautomatikai, és a biztonságtechnikai felügyeleti rendszert, és a következőket foglalja magába:

Épületautomatika:

- *Villamos energiaellátó rendszer,*
- *szünetmentes áramellátó rendszer,*
- *fő-, és installációs elosztó berendezés ellenőrzése,*
- *villamos kapcsolások, liftek,*
- *fogyasztásmérés, energiaoptimalizálás,*
- *hő központ, hűtési rendszer,*
- *fűtési rendszer,*
- *füst, és tűzjelző rendszer,*
- *automatikus tűzoltó rendszer.*

Biztonsági rendszer:

- *belépés ellenőrző rendszer,*
- *mozgás ellenőrző rendszer,*
- *behatolás védelmi rendszer,*
- *zártláncú videó rendszer,*
- *kapcsolat a hatóságok felé (rendőrség, tűzoltók, mentők).*

Az integrált felügyeleti rendszer központja az egyes rendszer elemekkel strukturált univerzális hálózattal kacsolódik. A hálózat, és végpontok elemeit fizikai hozzáférés -védelemmel kell ellátni. A felügyeleti rendszer központ számítástechnikai erőforrásai logikai hozzáférés-védelmére, és a részleges rendelkezésre állásának a biztosítására intézkedéseket kell tenni.

A logikai hozzáférés -védelemnél az egyes védelmi osztályokban a jelszórendszer, és a jogosultsági rendszer erősségét a következőképpen kell meghatározni:

Védelmi osztályok	***Hozzáférés***	
	Belső	***Külső***
1.	***Erősen korlátozott***	***Erősen korlátozott***
2.	***Korlátozott***	***Erősen korlátozott***
3.	***Nem korlátozott***	***Korlátozott***
4.	***Nem korlátozott***	***Nem korlátozott***

A BELSŐ HOZZÁFÉRÉS KORLÁTOZÁSA AZT JELENTI, HOGY

az 1. Véd. Osztályban, legalább egyszer használatos jelszót, államtitkok esetén titokmegosztást is alkalmazni kell, a jogosultsággal csak szűk kör rendelkezhet a betekintési jogokat figyelembe véve, ami az emberileg olvasható outputok elérésének korlátozását, valamint elérési jogosultság esetén a hard copyk kezelésének szigorú szabályozását jelenti.
A 2. Véd. Osztályban, alkalmazható többször használatos jelszó, de a szükséges tudás elve alapján adott jogosultságokkal.

A KÜLSŐ HOZZÁFÉRÉS KORLÁTOZÁSA AZT JELENTI, HOGY

Az erősen korlátozott esetben (a minősített adatoknál az 1. Védelmi osztályban) nem férhet hozzá senki, a korlátozott adatoknál (például dial in porton keresztül) csak egyszer használatos jelszóval, és az emberileg olvasható outputok kinyomtatási, illetve adathordozóra másolási jogosultsága nem engedhető meg. A 2. védelmi osztályban külső hozzáférés szigorú felhasználó azonosítás (egyszer használatos jelszó), és a port védelme mellett engedélyezhető.

7.4. AZ IT BIZTONSÁG PRODUKTIVITÁSÁNAK MÉRÉSE

A LEGJOBB GYAKORLAT

Az IT biztonsági alrendszerünk, az informatikai biztonságmenedzsment tevékenységünk teljesítményének, azaz annak, hogy mennyire volt eredményes a megállapítása nem tartozik az egyszerű feladatok közé. Ugyanis a nemzetközi gyakorlatban nem ismert olyan eljárás, amellyel exakt módszerekkel lehet a biztonsági alrendszer produktivitását meghatározni. A jelenlegi legelterjedtebb eljárás az összehasonlítás „LEGJOBB GYAKORLAT”-tal (best practice), amely azt jelenti, hogy a gazdasági szervezet adottságait, pl. a rendszer biztonság érzékenységét figyelembe véve megállapítok mérhető mutatókat, amelyek a biztonság a gazdasági szervezettel azonos szerveztek mutatóival, vagy az általános gyakorlatával hasonlítok össze. A mérhetőség azt jelenti, hogy időszakonként vizsgálok (pl. évenként) olyan mutatókat, amelyek az előfordulást számszerűen is mutatják. Például

- A biztonsági események száma
- A sikeres behatolások száma.
- A vírus fertőzések száma.
- Az ismertté vált csalások száma.
- Az Üzletmenet folytonosság zavarainak, megszakadásainak száma

A COBIT 4 magas szintű ellenőrzési elvei például a legjobb gyakorlaton alapulnak, ezért folyamatos a kiadvány korszerűsítése (lásd az alábbiakban példaként megadott IT biztonság, és IT biztonságirányítás sikertényezői pontokat).

Továbbá a legjobb gyakorlatot tartalmazza az MSZ-ISO/IEC 17799:2000, az MSZ-ISO/IEC 27001:2006 szabvány, és a COBIT 4. Így a biztonsági rendszerünk megfelelősségének megállapítása e szabvánnyal, és ennek alapján, a biztonsági rendszeren módosítások végrehajtása a legjobb gyakorlat figyelembe vételét jelenti

Természetesen az összehasonlításra a COBIT Érettségi Modell is lehetőséget ad. Továbbá az Information Security Forum, amely egy tagsággal rendelkező szervezet, kiadott egy szabványt e témában, amely nem tagoknak is elérhető [lásd Mellékletek, Szabványok)].

AZ IT BIZTONSÁG SIKERTÉNYEZŐI

- Semmilyen esemény nem okozott nyilvános zavart, a biztonsági események száma nem jelentős.
- Az új implementációk kis száma késett biztonsági zavar miatt.
- A küldetés kritikus üzleti folyamatokat kiszolgáló IT rendelkezik ÜFT-vel.
- A kritikus infrastruktúra elemeinek rendelkezésre állását automatikusan felügyelik.
- Az alkalmazottak tudatossága mérhető fejlődést mutat (rendszer biztonsági elvek, és a feladatok teljesítménye etikai, és biztonsági oldalról).
- Az üzleti, és az informatikai biztonság integrációja.

AZ IT BIZTONSÁGIRÁNYÍTÁS SIKERTÉNYEZŐI

- Teljes megfelelés vagy megegyezéses, és rögzített eltérés a minimális biztonsági követelményektől.
- A fejlesztett, és dokumentált IT tervek, és politikák meghatározott százaléka megfelel az IT biztonsági küldetésnek, elgondolásnak, céloknak, értékeknek, és a vezetés szabályainak.
- Az IT biztonsági tervek, és politikák meghatározott százalékát a részvényesek ismerik.

8. HÁLÓZATI BIZTONSÁG

*Ez fejezet a Control Objective for Net Centric Technology (**CONCT**), az INFORMATION SYSTEM AUDIT and CONTROL FOUNDATION kiadványa alapján készült [Hálózat Centrikus Technológia **(HCT**)].*

A hálózatok annak a függvényében, hogy magán (bizalmas), vagy nyilvános (nem bizalmas) hálózatról van szó, különböző védelmet igényelnek. Az INTERNET megjelenése, felhasználása új fenyegetéseket jelent, amelyekre új védelmi intézkedésekkel kell válaszolni.

Néhány alapvető hálózat típus:

- A hagyományos, bérelt vonalakkal dolgozó privát hálózatok gyakorlatilag zárt hálózatot jelentenek (általában pont-pont összeköttetésekből állnak), amelynek használata kevesebb kockázattal jár.
- Az INTRANET egy olyan belső vállalati hálózat, amely az INTERNET technológiával (TCP/IP) működik.
- Az INTERNET, amelyet az jellemez, hogy a kommunikáló feleknek a tér, az idő, és a távolság nem jelentenek korlátozást, az informatikai hálózatok részévé vált.
- Az EXTRANET, az INTRANET kiterjesztése az INTERNET-en keresztül a felhasználói (kliens) végpontok felé. Itt fellépnek az INTERNET jelentette kockázatok is.
- A virtuális magán hálózat (Virtual Privat Network, VPN) a magán hálózatot a távoli felhasználói végpontokkal az INTERNETen keresztül, bizalmas csatornán kapcsolja össze. Ez esetben tehát jelentkeznek egyes INTERNET képezte kockázatok.

Az idézett anyag tárgyalt megoldásai elsősorban a logikai hozzáférés védelemmel foglalkoznak, például nem foglalkoznak az emberrel, mint erőforrással, vagy a kisegítő berendezésekkel sem.
Az anyagból a felhasznált ellenőrzési célok, és az ellenőrzési irányelvek valójában, biztonsági követelményeket, és az azokat realizáló védelmi intézkedéseket határoznak meg, pontosabban írnak elő.

A BIZTONSÁG ELLENŐRZÉSI SZEMPONTOK A HCT-BEN

A HCT-ben a biztonság ellenőrzési szempontok a következő pontokban vannak megadva:

1. A magas szintű biztonság ellenőrzési célok
2. Az ellenőrzés biztonsági célja
3. Az ellenőrzés biztonsági irányelvei
4. Az információs objektumokhoz kapcsolódó üzleti objektumok biztonságmenedzsmentje

Ezekből, **az üzleti követelmények szerint**, az alábbi biztonsági intézkedések szükségessége adódik (hiszen, ha ellenőrzik, akkor a meglétét, és rendeltetésszerű üzemelését vizsgálják).

OBJEKTUM BIZTONSÁGI MENEDZSMENT

Üzleti követelmény, hogy az informatikai objektumok védelmét a jogosulatlan hozzáféréstől biztosítani kell. A következő biztonsági követelményeket kell figyelembe venni

- az információs objektumok adatainak rejtjelezése
- az informatikai környezet fizikai, és logikai védelme
- hozzáférés védelem
- hitelesítés
- jogosultság kezelés,

amely megvalósítható a következőkkel

- a felhasználói azonosító, és jelszó regisztráció, és karbantartás
- a hozzáférés naplózás, és a megsértés jelentése
- a rejtjelezési módszer és kulcs menedzsment (tartalom, alkalmazási szint, stb)
- tűzfal
- eseménykövetés.

HÁLÓZATI BIZTONSÁGI MENEDZSMENT

Az üzleti követelmény a távközlési hálózat hozzáférés védelme, azaz a következő biztonsági követelményeket kell figyelembe venni

- A hálózati erőforrások hozzáférés védelme
- A biztonsági információk archiválása, és visszakeresése
- A rejtjelezési folyamatok, és a digitális aláírás menedzselése, és ellenőrzése
- Hitelesítés, és jogosultság kezelés
- Le nem tagadhatóság szolgáltatás,

amely megvalósítható a következőkkel

- A digitális aláírás
- A tűzfal (csomópont cím szint/alkalmazási kapu proxy routert/ alkalmazási réteg protokoll
- Hozzáférés ellenőrzés, és jogosultsági rendszer
- Rejtjelezés, és kulcs menedzsment/ bizalmas szerver
- Hitelesítés, egyszer használatos jelszó, és tanúsítás
- Az üzenet eredetének, és szállításának bizonyítása
- Biztonsági napló
- Leszívás/ biztonsági eseménykövetés

VÉDELMI BIZTONSÁGI MENEDZSMENT

Az üzleti követelmény a HCT komponensek védelme a jogosulatlan hozzáféréstől, és a fejlesztési, valamint karbantartási fázis alatti cserétől, azaz a következő biztonsági követelményeket kell figyelembe venni

- A fizikai komponensek védelme
- A sw komponensek védelme
- A hálózati komponensek védelme
- Az objektumok védelme
- A hitelesítési objektumok
- A jogosultsági objektumok,

amely megvalósítható a következőkkel

- Vírus védelem
- Fizikai azonosító szám naplózás
- Software package betöltés. és változat platform szám érvényesítés
- Könyvtári software package jogosulatlan csere ellen
- Feladat szétválasztás
- Megsértés monitoring
- Megengedő szintek
- Belépési kulcsok

AZ ÜZEMELTETÉSI BIZTONSÁGI MENEDZSMENT

Az üzleti követelmény a HCT komponensek üzemeltetés alatti jogosulatlan cserétől való védelme, azaz a következő biztonsági követelményeket kell figyelembe venni

- A fizikai hozzáférés védelem
- A logikai hozzáférés védelem
- A vírus védelem
- A hitelesítés,
- A jogosultság kezelés,

amely megvalósítható a következőkkel

- szerver fizikai környezet védelme
- logikai hozzáférés védelem a klienshez, és terminálhoz
    - jelszó/ ID
    - hozzáférés naplózás
    - terminál kikapcsolás
- az objektumok rejtjelezése
- a hálózati távbeszélő hozzáférés számcseréje
- on line vírus védelem

*Mindezek a követelmények az **alábbi védelmi intézkedések megtételét**, és rendeltetésszerű üzemeltetést igénylik:*

OBJEKTUM BIZTONSÁGI MENEDZSMENT

Itt első sorban az informatikai objektumok hozzáférés védelméről van szó, amely a következő védelmi intézkedéseket jelenti:

- A három (Mit tudsz?, Mi van a birtokodban?, Ki vagy?) hozzáférés védelmi eljárás kombinációjának alkalmazása.
- A biztonsági mechanizmusnak megfelelő információk osztályozása.
- A magasan biztonság érzékeny adatok erős rejtjelezési eljárással való rejtjelezése.
- Biztosítsa, hogy csak jogosult web helylátogatók kaphassanak hozzáférést a logikai erőforrásokhoz, mint pl. hálózati objektumok, tűzfal táblák, web alkalmazások.
- A biztonsági események real time jelzésére monitoring eszközök alkalmazása.

- A hozzáférő személyek naplózására monitoring eszközök használata, és automatikus válasz biztosítása.
- A biztonság kritikus eszközök fizikai védelme fizikai akadályokkal, mint zárak, kábelárnyékolás, biometriai hozzáférés védelem.
- A szervezet magán hálózatának védelme jogosulatlan belső, és külső hozzá féréstől.
- Digitális tanúsítvány használata hitelesítéshez, mint pl.
- Web hely látogatók nyilvános kulcsai,
- Web hely sértetlensége,
- Kliens programok sértetlensége.
- A web hely objektumok pontosságának, és teljességének (sértetlenség) periodikus hitelesítése.
- A web helyre beadott partner információk pontosságának, és teljességének (sértetlenségének) real time hitelesítése.
- A Biztonsági Politika szerint a végrehajtott szolgáltatások érvényességének hitelesítése.

HÁLÓZATI BIZTONSÁGMENEDZSMENT

A hálózati biztonságmenedzsment gondoskodjon arról, hogy a hálózati hozzáférés védelem csak jogosultak számára engedélyezzen tevékenységeket, és adatokhoz hozzáférést. Éspedig

- Biztonsági Politika, amely gondoskodik az adatok osztályozásáról, és meghatározza a szükséges védelem minimális szintjét.
- Felhasználó hitelesítés a három hozzáférési eljárás kombinációja alapján.
- Felhasználó adminisztrációs eljárás, amely támogatja a felhasználói jogok esetenkénti hozzáadását, módosítását, és visszavonását.
- A hálózati biztonság periodikus felmérése, pl. behatolás teszttel.
- A felhasználói jogosultságok periodikus felülvizsgálata.
- A hálózati adminisztráció jogosultságainak korlátozása.
- Az érzékeny, és bizalmas adatok rejtjelezése.
- Digitális aláírás, és nyilvános kulcsú infrastruktúra használata az adatok jogosulatlan módosításának, és a tranzakció letagadásának megelőzésére.
- A kulcs hálózati komponensek fizikai biztonságának biztosítása (szerver, hub, kapcsolók)

- A szükséges tudás elve alapján az érzékeny, és bizalmas adatok hozzáférésének korlátozása.
- Vírus felismerő szoftver alkalmazása az adatok megfertőzésének jelzésére, megelőzésére.
- Tűzfal alkalmazása az Internet, és a belső vállalati forgalom szűrésére.
- Behatolás jelző eszközök alkalmazása a behatolás real time jelzésére.
- Tartalom szkenner alkalmazása jogosulatlan információ ki, illetve bevitelének megelőzésre.
- Minden hálózati behatolás naplózása, és a napló rendszeres értékelése.
- A web hely független tanúsításának biztosítása.
- Gondoskodás a küldés, és fogadás le nem tagadhatóságáról.

VÉDELEM BIZTONSÁGI MENEDZSMENT

A rendszerfejlesztés alatt a hálózati környezet védelme a jogosulatlan hozzáféréstől, éspedig

- Hozzáférés hitelesítés, és erőforrás elérés jogosultság.
- Fizikai hozzáférés védelem alkalmazása a hálózati objektumokra, mint web szerver, szerverek, és router (táblák).
- A hw elemek biztonságos helyen tartása.
- A sw objektumok bizalmas könyvtárban tartása, a hozzáférés korlátozása.
- A kliens sw-ek védelme
- Program kivonattal, és a programozó digitális tanúsítványával
- Idő, és napbélyegzéssel
- a kliens hozzáférések ellenőrzésével
- Automatikus biztonsági monitoring eszközök alkalmazása a biztonsági események jelzésére, és a tranzakció feldolgozó erőforrások jelzésére.
- A forrás, és az objekt kódok hozzáférés ellenőrzése, és az objekt kódképzés, valamint az egymást követő cserék ellenőrzése verzió ellenőrző sw-rel.
- A hw, sw, nw objektumok automatikus leltározása.
- A hozzáférés korlátozása hozzáférés védelemmel a távoli sw elosztó sw-hez.
- A hozzáférés a kliens, a szerver, és a nw objektum file-okhoz a hozzáférés és a directory engedélyezés védelme.
- A forrás objektumok rejtjelezése.

- Az ellenőrzés, és hozzáférés engedélyezésnél feladat szétválasztás.
- A fejlesztők számára az üzemi környezethez a hozzáférés korlátozása.
- A tranzakció feldolgozó eszközökhöz a hozzáférés korlátozása.
- A szükséges tudás elve alapján az adatbázisokhoz a hozzáférés korlátozása.
- Hacker támadásra válasz eljárás alkalmazása.
- A tűzfalaknál, a szerver, és a kliens szinteken vírus szkenner alkalmazása.
- A három hozzáférési eljárás alkalmazása.

ÜZEMELTETÉSI BIZTONSÁGI MENEDZSMENT

Az hálózati komponensek védelme a jogosulatlan cserétől a rendszer műveleti állapotában, éspedig

- A rendszer műveletek alatt az I/E/I komponensek logikai hozzáférés védelme, mint
- Jelszó / ID
- Bejelentkezés
- Tétlen terminálok kikapcsolása
- Vírusvédelem alkalmazása
- A felesleges portok, és lehetséges hozzáférési módszerek kikapcsolása
- A szerver hw biztonságos területen történő elhelyezése (zárt, kondicionált környezet, és minden hozzáférés számon kérhető)
- A szolgáltatások védelme, a szolgáltatásokat megszakító támadásoktól.
- A file letöltésekor a felesleges nyilvános hozzáférés megszakítása.
- Hálózati szintű védelem alkalmazása, mint tűzfal, proxy szerver, szűrő router, protokoll elrejtő stb.
- Felhasználó név és jelszó hitelesítés, valamint alkalmazás hozzáférés alkalmazása a web szerverben.
- CA szerver használata I/E web alkalmazások hitelesítéséhez.
- A szerver konzol jelszóval védett.

HÁLÓZAT RENDELKEZÉSRE ÁLLÁSA

Végül e tárgykörben szólni kell a hálózat folyamatos rendelkezésre állásának biztosításáról.
A védelmi intézkedések két változata ismert

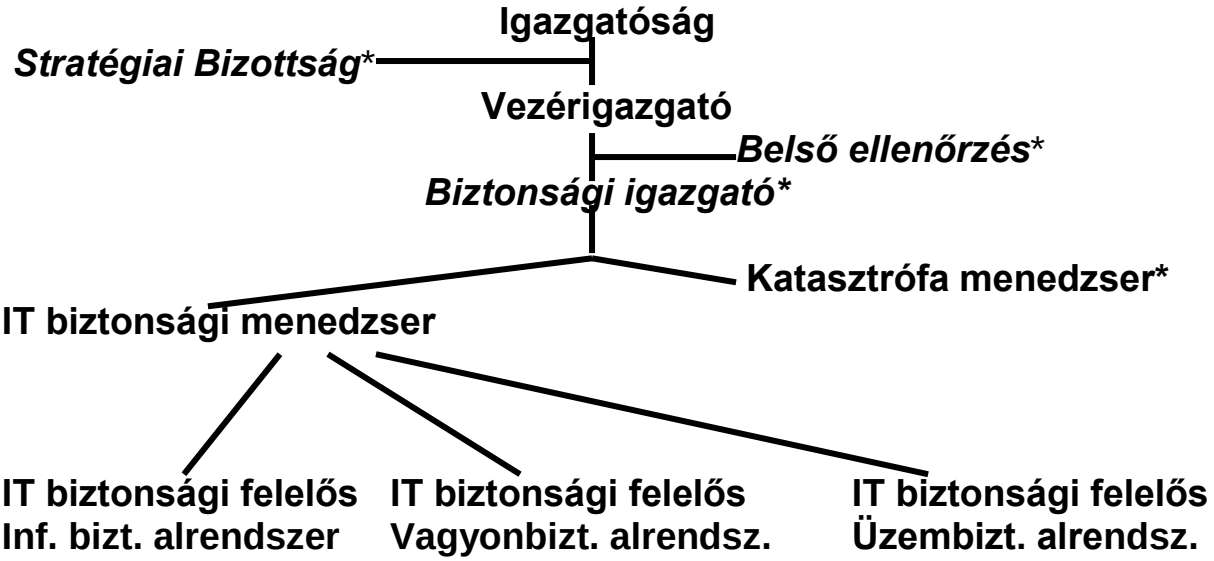
- Egyes erőforrások kiesése elleni védelem, a hálózat egyes pontjain tartalék erőforrások biztosításával, és
- Alternatív útvonalak, illetve alternatív távközlési módok biztosítása, a teljes kiesés elleni védelemre.

9. ÖSZEFOGLALÁS

9.1. IT BIZTONSÁGIRÁNYÍTÁS, ÉS MENEDZSMENT

A biztonságirányítás, és a biztonságmenedzsment a vállalati szervezeti struktúrában integrált, a biztonsági alrendszerek irányítását, és menedzsmentjét egyaránt magába foglaló, és a felső vezetéshez közvetlenül alárendelt szervezet. Feladata a vállalat üzleti tevékenysége, az üzleti cél sikeres megvalósításához szükséges biztonsági feltételek folyamatos, költség hatékony biztosítása, amely kizárja, hogy bármely üzleti, vagy támogató folyamat, illetve az ezeket kiszolgáló informatika partikuláris érdekeinek alárendelve működjön.

Az IT biztonságirányítás, és menedzsment szervezeti struktúrája:



*Az IT biztonságirányításban, és menedzsmentben részt vesz, de a másik két biztonsági alrendszert is irányítja.

9.2. A HUMÁN ERŐFORRÁSOK SZEREPE A BIZTONSÁGIRÁNYÍTÁSBAN

A fenti struktúra egyes szintjein emberek állnak, akik a munkakörükből adódó feladatokat, és felelősségeket folyamatok, és erőforrások (köztük humán erőforrások) felhasználásával látják el. Ebből levonhatjuk azt a következtetést, hogy az informatikai biztonságirányítás, és menedzsment az azt megvalósító humán erőforrásokon alapul. Ennek a ténynek a kiemelését az indokolja, hogy a biztonsági rendszer, illetve az azt felépítő biztonsági alrendszerek jogszabályi, belső szabályzati

megfelelőssége, rendeltetésszerű megvalósulása, azaz az, hogy a védelmi intézkedések naprakészen kikényszerítsék a biztonsági követelményeket. Ehhez magas szintű biztonsági tudatosságra, és az etikai kódex betartására, betartatására van szükség a struktúra minden szintjén. A biztonságtechnika tapasztalatai, és az irodalom azt hangsúlyozza, hogy az informatikai, és általában a biztonság leggyengébb pontja nem a technika, hanem az ember (tudatos, illetve véletlen kárkövetkezménnyel járó tevékenységek miatt). Ebből pedig nem az következik, hogy senkiben nem lehet megbízni, hanem az, hogy a biztonságirányítás, és menedzsment fontos feladata a MEGBÍZHATÓ munkatársak, MEGBIZHATÓSÁGA fenntartásának feltételeit biztosítani. Ennek módja

- Az etikai kódex betartatása,
- A biztonsági tudatosság oktatása, elfogadtatása, ébrentartása,
- A vállalatvezetés elszántságának bizonyítása a felelősségek érvényesítésére (a papíralapú, és az elektronikus irodában egyaránt) a számon kérhetőség, a számonkérés biztosításával, valamint
- A rendszeres belső, és időszakonkénti külső, független ellenőrzéssel.

9.3. TÍZ AXIÓMA A BIZTONSÁGMENEDZSMENTRŐL

1. Nincs 100%-os védelem, így mindig van maradék kockázat.
2. Az adat (információ) védelme a személyes adatok védelmét jelenti. Az adatbiztonság két jelentéssel bír vagy a személyes adatok biztonságát, vagy minden adat (személyes adat, üzleti adat, stb.) biztonságát jelenti.
3. Csak az integrált, egész vállalatot átfogó egyenszilárdságú biztonsági rendszer nyújt hatékony védelmet.
4. A gazdasági szervezet mikró gazdasági rendszer, amely az üzleti, termelési (ha van), és az informatikai rendszerből áll.
5. A vagyonbiztonság, termelési biztonság, és informatikai biztonság egyaránt a bizalmasság, sértetlenség, és rendelkezésre állástól függ.
6. A veszélyforrások, kockázatok nem állandóak, ezért rendszeresen vizsgálni kell őket.
7. Az üzletmenet folytonosság csak, ha az egész mikró gazdasági rendszerre kiterjed, biztosítható.
8. A biztonságszervezés csak a Biztonsági Átvilágítástól indulva, és szisztematikusan végezve lehet eredményes.
9. Az erőforrásokat kell védeni a biztonsági alrendszerekben.
10. A biztonság külön szakma, nem is egy.

MELLÉKLETEK

10. AZ IT BIZTONSÁGI PROGRAM SIKERTÉNYEZŐI KRITIKUS ELEMEI

Az informatikai biztonsági program, és ezzel az It biztonság megvalósításának sikere több tényezőtől függ. Az ISACA „Az informatikai biztonsági program kritikus siker tényezőit" a következők szerint határozza meg [19]:

- A felső vezetés elkötelezettsége az IT biztonsági irányelvek mellett.
- A menedzsmentnek a megértése az IT biztonság kérdéseivel.
- Az új technológia implementálásánál elsődleges az IT biztonság.
- *Az üzleti, és az IT biztonság integrációja.*
- Az IT biztonság összhangja a szervezet céljaival.
- Az IT biztonság implementálására, megfigyelésére, és támogatására vonatkozóan, a menedzsment tulajdonossága, és számon kérhetősége.

Ezen kívül a kiegészítő sikertényezők:

- A munkatársak megfelelő oktatása, az informatikai erőforrások védelmének tudatossága.
- Az IT Biztonsági Politikáknak, és szabványoknak a Konzisztens kikényszerítése.
- Az IT biztonság elhelyezése a szervezeti hierarchián belül.
- Az IT biztonsági stratégiai, és taktikai terv költségvetése.
- Konzisztencia a board és a végrehajtó menedzsment között az IT biztonsági priorítások tekintetében.
- Figyelem arra, hogy a rövid távú célok hosszú távon gyengeségeket eredményezhetnek.
- Általánosan elfogadott a legjobb IT biztonsági gyakorlat, és mérések.

11. IRODALOMJEGYZÉK

[1] Horváth, Lukács, Tuzson, Vasvári. Informatikai Biztonsági Rendszerek. E&Y. BMF KANDÓ KAR. 2001.
[2] COBIT 3rd Edition. AUDIT Guidelines. July 2000. ITGI
[3] CISA Review Technical Information Manual 1998. ISACA Inc. 1998.
[4] Control Objectives for Enterprise Governance. ITGI. 2003.
[5] IT Governance Executive Summary. IT Governance Institute 2003.
[6] Information Security Governance: Guidance for Boards of Directors and Executive Management. IT Governance Institute. 2003.
[7] Security awaraness. ISACA. 2005.
[8] CISM Review Manual. ISACA. 2003.
[9] COBIT Security Baseline. IT Gouvernance Institute.2004.
[10] COBIT Quickstart.IT Gouvernance Insitute.2004.
[11] M. Kubr. Vezetési tanácsadás. Nemzetközi Munkaűgyi Hivatal. Genf. 1986.
[12] Sla Toolkit, Service Level Agreement. 2002. Easytech.
[13]Dr. Lukács György: Új vagyon védelmi nagykönyv. CEDIT 2000 Kft.
[14]Kevin D. Mitnick: A legendás hacker, a megtévesztés művészete. Perfekt-Pro Kft. 2003.
[15] Control Objectives for Enterprise Governance. ITGI.1999.
[16] Handbook for Computer Security Incident Response Team. CMU/SEI-2003-HB-002
[17] A. Targowski, és T.RIENZO: ENTERPRISE INFORMATION INFRASTRUCTURE. WESTERN MICHIGAN UNIVERSITY. 2004,
[18] Control Objectives for Net Centric Technology (Volume I.-IV.). ISACF: 1999.
[19] Critical Elements of Inform. Security Program Succes. ISACA 2005.
[20] How to Make Your Organisation Aware of IT Security. European Security Forum. London. 1993.
[21] F. Björck: Security Scandinavian Style. Stockholm Universíty. 2001.
[22] P. Beynon Davies: Information Systems. Palgrave. 2002.
[23] Bakacsi Gy.: Minőség és biztonsági kultúra. BME. Ergonómiai Tanszék.
[24] Dr. Rohács József: A veszélyhelyzet menedzsment technológiai alapjai. Veszélyhelyzet menedzsment konferencia. 2003. HM Ei Rt. .
[25] A. Mizzi: Return on Information Security investment. http://www.geocities.com/amz/ .
[26] S.Niels Physical Security in Mission Critical systems. APC White Paper. 82. 2004
[27] Return on Security Investment. ISACA Auditing Draft Guideline 2006.

12. SZABVÁNYOK

Megjelent magyar szabványok (amelyeket figyelembe vettünk)::

- MSZ ISO/IEC 9594-8-2004 Informatika. Nyílt rendszerek összekapcsolása.
- MSZ ISO/IEC 15408-1,2,3 Az informatikai biztonság értékelésének közös szempont rendszere.
- MSZ ISO/IEC 17700-1 Biztonságtechnika, kulcsgondozás.
- MSZ ISO/IEC 17799: 2002 Informatikai biztonság menedzselésének eljárás rendje.
- MSZ E- 15100-1 Informatikai szolgáltatás irányítása (elő szabvány).
- MSZ ISO/IEC 27001: 2006. Az információbiztonság irányítási rendszerei. Követelmények.

Az alábbiakban néhány külföldi, illetve nemzetközi biztonsági szabványt példaképen megadunk:

- BS 7799-1:2000, Information technology — Code of practice for information security management.
- BS 7799-2:2002, Information security management systems — Specification with guidance for use..
- *ISO/IEC 17799:2003 Code of practice for information Security Management*
- *ISO/IEC 17799-2:2004. Information security management system.*
- *ISO/IEC 27001:2005. Information security management system. Requirements.*
- *Information Security Forum: The Standard of Good Practice. Version 4.1. 2005. www.isfsecuritystandard.com*

13. BIZTONSÁGI SZEMPONTBÓL KIEMELT SZABÁLYOZÁSOK

UTASÍTÁSOK

Humán Politika
Titokvédelmi Utasítás
Iratkezelési Utasítás
Selejtezési Utasítás
Tűzvédelmi Utasítás
Outsourcing Utasítás

IT SZABÁLYZATOK

Adatvédelmi, és Adatbiztonsági Utasítások
IT Biztonsági Szabályzat (Politika)
IT Üzletmenet Folytonossági Terv
IT Működési Szabályzat
IT Fejlesztési Szabályzat
Vírusvédelmi Szabályzat

IT ELJÁRÁS RENDEK

Jelszó és Jogosultság Kezelés Rendje
Az Alkalmazások Eljárás Rendjei (mentési, és újraindítási rend beleértve)
Átadás-átvételi Rend
Help Desk Eljárás Rend
Szoftver Licensz Nyilvántartási Rend
Program Változás Kezelés Rendje
Hálózat Üzemeltetés Eljárás rendje
Védelmi Intézkedések Nyilvántartási Rendje
Konfiguráció Kezelési Rend
Átadás/átvételi Eljárási Rend

14. BIZTONSÁGI SZEMPONTOK EGYES SZABÁLYOZÁSOKHOZ

Az alábbi szabályozások készítése nem képezi a Biztonsági vezető feladatát, a készítésében általában nem vesz részt, de véleményezésre meg kell kapnia, a biztonsági követelmények érvényesítése érdekében. Ehhez néhány, a legfontosabb szabályozásnál az IT biztonsági vezető részéről képviselendő biztonsági követelményt, az alábbiakban megadunk.

ADAT, ÉS TITOKVÉDELMI UTASÍTÁSOK

Az 1992. évi LXIII. tv. A személyes adatok védelméről, 2004. január 1.-én hatályba lépett változata szerint az országos hatósági, munkaügyi, vagy bűnügyi adatállományt kezelőknél, pénzügyi szervezeteknél, és távközlési, közüzemi szolgáltatóknál az első számú vezetőhöz tartozó adatvédelmi felelőst kell megbízni, aki készíti az Adatvédelmi, és Adatbiztonsági Szabályzatokat. Ezek a természetes személyek személyes adatairól szólnak. Az MSZ ISO/IEC 17799-es szabvány szerint, pedig az adatokat (itt ez minden adatot jelent, a személyes adatokat is), a helyiségeket, és az eszközöket biztonság érzékenységük szerint osztályozni kell, amelyre készül a Titokvédelmi Utasítás, amely tartalmazza a titokvédelemmel kapcsolatos szabályokat, valamint a titokköri jegyzéket, azaz az adatok, helyiségek, eszközök biztonság érzékenységük szerinti osztályozását.
Természetesen ezek a szabályzatok, utasítás készítése ajánlott minden gazdasági szervezet számára is.

IRATKEZELÉSI UTASÍTÁS

Készül a titkárság, elsősorban a jogtanácsos irányitásával. Az Iratkezelési Utasításnak ki kell térnie egyrészt a papíralapú, másrészt az elektronikus iratokra egyaránt. Át kell fognia az iratok keletkezésétől, a kezelésükön keresztül, a selejtezésükig a teljes életciklust. Gondoskodni kel arról, hogy megfelelő védelmi intézkedések garantálják az egyikből, a másikba, illetve fordítva, az átment esetében, hogy az iratok megőrizzék biztonsági osztályozásukat.

SELEJTEZÉSI UTASÍTÁS

Készül a titkárság, elsőssorban a jogtanácsos irányításával. A Selejtezési Utasításnak ki kell térnie bármely papír vagy elektronikus

adathordozó, illetve bármely erőforrás selejtezési szabályaira. A fő biztonsági szabályok:

- A selejtezés csak bizottság előtt történhet, amely a tevékenységéről jegyzőkönyvet köteles felvenni.
- A selejtezés bármilyen mennyiségről van szó, nem történhet csak egyenként.
- Az adathordozókat (papír, elektronikus) a selejtezés előtt érvényteleníteni kell.
- Gondoskodni kell arról, hogy a leselejtezett eszközökkel jogosulatlanul ne juthasson senki bizalmas adatok birtokába. Ez mágneses adathordozók esetében jelentheti azt, hogy az adathordozót nem lehet értékesíteni (pl. egy PC értékesítésekor a törölt winchester is biztonsági kockázatot jelent).

OUTSOURCING UTASÍTÁS

Készül a jogtanácsos rányitásával. Az outsourcing (erőforrás kihelyezés) veszélyforrást képez, mivel a harmadikféltől csak a szerződésben rögzített kötelezettségek kérhetők számon, azok sem túl egyszerűen. A biztonsági követelményeket a szerződésnek feltétlenül tartalmazni kell. Ezek a következők:

- Mire vonatkozik a szerződés (külső fejlesztés, belső fejlesztés, üzemeltetés kiadása, munkaerőbérlés stb).
- Köteles-e a felhasználó megbízásából elvégzett tevékenységeinél minden jogi követelményt, illetve szabályt, és szabványt alkalmazni,
- Biztosítva van-e a szerződésben a felhasználó ellenőrzési jogosultsága a szolgáltató minden szerződéses tevékenységénél saját, és a szolgáltató telephelyein,
- Van-e a szerződésben „biztonsági szolgáltatási szint megállapodás”, és megfelel-e legalább a Felhasználó Biztonsági Politikájának.
- Ki van-e kötve a felhasználó humán politikai irány elveinek alkalmazási kötelezettsége.
- Ki van-e kötve a szolgáltatói tevékenység folyamatos monitoringja.
- Ki van-e kötve a felelősség, a felelősök a szerződés végrehajtásáért.

A COBIT 3 előírja, hogy az outsourcing szerződésben szerepelni kell az SLA-nak (Service Level Agreement) Szolgáltatási Szint Megállapodásnak, és legalább az alábbi követelményeknek:

- a szolgáltatás meghatározása
- a szolgáltatás költsége
- a számszerűsíthető minimális szolgáltatási szint
- az informatikai funkció által nyújtott támogatás szintje

- rendelkezésre állás, megbízhatóság, bővítési kapacitás
- az üzemfolytonosság tervezése
- biztonsági követelmények
- megállapodás bármely pontjának módosítása esetén a követendő eljárás
- az érvényességi idő és annak felülvizsgálata/megújítása/ a megújítás kizárása
- a teljesítési jelentések gyakorisága és tartalma, valamint a szolgáltatási díjfizetések, azok reális volta
- a díjtételek számításának módja
- a szolgáltatás javítására tett kötelezettségvállalás.

Az MSZ-E-15000 a szolgáltatási szint irányítása, magyar előszabvány szerint a szolgáltatási szintet tervezni és azt végrehajtani kell (SLM = service level management).

ÁTADÁS/ÁTVÉTELI ELJÁRÁS REND

Készül az informatikai vezető irányításával. Az Átadás/átvételkor érvényesítendő biztonsági követelmények:

- Az átadás/átvétel során meg kell győződni arról, hogy a fejlesztés/beszerzés elindításakor megadott biztonsági követelmények teljesülnek-e. Ide tartozik, amennyiben a szállításra is voltak megadva biztonsági követelmények, azok megvalósulását is ellenőrizni kell.
- Az eljárás folyamán gondoskodni kell arról, hogy éles adatokhoz jogosulatlanul ne lehessen hozzáférni. Lehetséges az átadónak hozzáférési jogosultságot adni, de azt az eljárás befejezése után vissza kell vonni.
- A szállító, amennyiben harmadik fél „fenyegetés mentességi” nyilatkozatot kell írásban adnia, amelyet a szerződéskötéskor elő
- kell írni, továbbá nyilatkoznia kell arról, hogy a leszállított termék jog tiszta.

PROGRAM VÁLTOZÁSKEZELÉS REND

Készül az informatikai vezető irányításával. A programokon változtatni csak az erre jogosult személy változtathat. Gondoskodni kell arról. Hogy

- A változtatási jogosultság nem lehet örök érvényű. Különösen nem, ha azt a fejlesztő, programozó kapja meg. Ebben az esetben, csak meghatározott rövid időre vonatkozhat.
- A változtatásra jogosult köteles
  - A változtatást a dokumentációkon átvezetni
  - Gondoskodnia arról, hogy az új változat mindenütt, ahol az IR-ben alkalmazzák az adott programot, átvezetésre kerüljön.
  - Az új változat teszteléséhez felhasznált éles adatok nem kerülhetnek vissza az éles rendszerbe.
- A feladat szétválasztás elve alapján a programváltoztatásra jogosult nem lehet a rendszer gazda.
- A program korábbi változatát, a lecserélt változatot archiválni kell.

KONFIGURÁCIÓ KEZELÉSI REND

Készül az informatikai vezető irányításával. A konfiguráció változtatása a legkülönbözőbb okok miatt válhat szükségessé. Alapvető biztonsági követelmény, hogy a változtatás végrehajtásakor meg kell győződni arról, hogy az új elemek kielégítik a biztonsági követelményeket, amely a technológia minden elemére létezik.

SZOFTVEREK REGISZTRÁCIÓS NYILVÁNTARTÁSA

Készül az informatikai vezető irányításával. A vásárolt szoftverek jogtisztaságáról a szállítónak nyilatkozni kell, majd azok regisztráltatását nem csak végre kell hajtani, hanem nyilván is kell tartani. Ez jelenti a vállalat regisztrációs kérelmét, és a regisztrálás tényét elismerő szállítói nyilatkozatot. Előfordul az, hogy a regisztrálás meghatározott feltételek mellett áll fenn, és pl. határidőhöz is kötött. A nyilvántartásnak gondoskodni kell arról, hogy ez a határidő ne járjon le.
A nem jogszerűen használt szoftver komoly veszélyforrást képez, hiszen sem hitelességét, sem karbantartást, sem megsemmisülés esetén pótolhatóságára nincs garancia.

VÉDELMI INTÉZKEDÉSEK NYILVÁNTARTÁSI RENDJE

Készül a biztonsági vezető irányításával. Védelmi intézkedések bevezetése, és törlése csak a biztonsági vezető engedélyével történhet. Ezért az engedélyezett védelmi intézkedésekről, és azok törléséről vagy módosításáról a biztonsági szervezetnek nyilvántartást kell vezetnie.

15. VÉDELMI INTÉZKEDÉSEK KÖRE I (A BIZTONSÁGI ALRENDSZEREKBEN)

RÉSZLEGES VÉDELMI INTÉZKEDÉSEK

I. SZERVEZÉSI

1. **szabályozás**
   - ***titokvédelmi osztályozás***
   - biztonsági szervezet
   - biztonsági dokumentumok
   - ***Iratkezelés***
2. **humán politikai védelmi intézkedések**
   - megbízhatóság munkaviszony létesítéskor,
   - megbízhatóság munkaviszony megszűntekor
   - megbízhatóság alkalmazás alatt
     - teljesítménykövetés
     - feladat szétválasztás
     - oktatás,
     - biztonságtudatosítás
     - megtévesztés elleni védelem
3. **szerződések**
   - vagyonbiztosítás
   - ***biztonsági követelmények a harmadikfél felé***

II. TECHNIKAI

fizikai védelmi int.-ek

1. aktív támadás elleni hfv

- ***objektum védelem***
- ***belépés és mozgás ellenőrzés***
- ***behatolás védelem***
- ***értéktárolás védelem***
- ***értékszállítás védelem***
- üres íróasztal, és képernyő politika

2. passzív támadás elleni hfv

- kisugárzás elleni védelem (akusztikus, el. mágneses)

3. rendelkezésre állás

- megbízhatóság
- redundancia
- energiaellátás
- villámvédelem
- tűzvédelem
- dokumentáció

4. számon kérhetőség biztosítása

logikai védelmi int.-ek

1. aktív tám. elleni hfv

- ***vállalati szintű azonosság mgm***
- ***jelszó mgm***
- ***jogosultság mgm***
- ***hitelesítés***
- ***tanúsítás***
- időbélyegzés
- behatolás jelzés
- tűzfal

2. passzív tám. elleni hfv

- rejtjelezés
- titokmegosztás

3. rendelkezésre állás

- mentés, újraindítás
- vírusvédelem
- logikai rombolás
- **dokumentáció**

4. számon kérhetőség biztosítása

hálózat védelmi int.-ek

1. logikai hfv

- személyhitelesítés
- tulajdonság hitelesítés
- tartalomhitelesítés
- letagadhatatlanság
- eszközhitelesítés
- **eredet,tulajdonság tanúsítás, pki**
- ***bizalmas útvonal***
- **tűzfal**
- **behatolás jelzés**

2. fizikai hfv.

- **rendelkezésre állás**
  - √ **fizikai r. áll.**

3. IR életciklus véd.

- ***fejlesztés/beszerzés***
- ***átadás/átvétel***
- ***üzemeltetés***
- ***selejtezés***

a biztonsági technológia védelme

- *A bizalmas számítástechnikai bázis fizikai, és logikai védelme*
- *A rejtjelező eszközök, kulcsok fizikai, és logikai védelme*
- *Fizikai, és logikai naplók védelme*

B. ÁTFOGÓ VÉDELMI INTÉZKEDÉSEK

I. SZERVEZÉSI

1. <u>szabályozás</u>

- katasztrófa menedzser megbízása
- katasztrófaminősítés
- katasztrófa teamek szervezése
- A katasztrófa- terv karbantartása
- oktatás

2. <u>szerződés</u>

- biztosítás a folyamatos működésre
- üzemi háttérszerződés
- szállítói háttérszerződés

II. TECHNIKAI

1.rendelkezésre állás

- visszaállítás
- hátterek, háttér eljárások
- Katasztrófakezelő központ
- helyreállítás
- biztonsági események kezelése

A BETŰTÍPUSOK JELENTÉSE
(a védelmi intézkedés mit véd?):

Ariel black = címsor
Ariel = bizalmasság
<u>Ariel</u> = <u>sértetlenség</u>
ARIEL = bizalmasság és sértetlenség
Courier new = rendelkezésre állás
Courier new = mind a három

16. ÖSSZEHASONLÍTÁS A CSB ALAPJÁN

Tervezés és szervezés		
Ellenőrzési célok	**ISO 17799**	**COBIT**
Küldetés kritikus vállalati információk és szolgáltatások azonosítása, és azok biztonsági követelményei		PO1: 1.1, 1.8 PO2: 2.2, 2.3, 2.4,
Az IT szervezet és kapcsolatok meghatározása		
Az IT biztonsági felelősségek meghatározása, és megértetése	4.1,6.1,8.1	PO4:4.5, 4.6, 4.9.4.10
A menedzsment célok és iránymutatások		
A menedzsment célok és iránymutatások megfelelő meghatározása és körözése	3.1,4.1,6.1,7.2,8.7,9.3,9.4, 12.1,	PO6: 6.2, 6.3, 6.8, 6.,9, 6.11,
Emberi erőforrások menedzselése		
Az It biztonságnak megfelelő funkciókról gondoskodás	6.1,	PO7:7.1, 7.2, 7.6,
Gondoskodás s külső követelményekről		
Gondoskodás arról, hogy az IT követelmények megfeleljenek az alkalmazandó törvényeknek, szabályozásoknak és más külső követelményeknek	8.7,12.1,	PO8: 8.2, 8.3,8.5,8.6 DS12: 12.4
Kockázatok elemzése		
A biztonsági kockázatok feltárása, és fontosságának megállapítása és tudatosítása	4.1, 4.2,5.2, 10.1, 3.1, 4.1, 6.3,	PO9: 9.1, 9.3, DS5: 5.6, PO9: 9.5 AI1: 1.9, DS7: 7.3

Beszerzés, és implementálás		
Az automatikus megoldások azonosítása		
A biztonság figyelembe vétele az automatikus megoldások azonosításánál		AI1:1.1,
A technológiai infrastruktúra beszerzése, és karbantartása		
A beszerzés, és karbantartásnál a biztonság figyelembe vétele	7.2,7.3,8.7,9.3,9.4,9.5,	AI3: 3.1,3.2, 3.3, 3.4, 3.5, 3.6 DS8: 8.1, PO11: 11.9
Folyamatok fejlesztése, és karbantartása		
Gondoskodás a biztonság a fejlesztés, és a karbantartásnál	6.2,	AI4: 4.2, 4.3,4.4, DS:7 7.1
Rendszerek installálása és akkreditálása		
Gondoskodás arról, hogy minden új rendszer, és változtatás csak megfelelő biztonsági teszt után lesz elfogadva	4.1, 5.1,	AI5: 5.75.11, 5.12,
Valamint a tesztek eredménye az üzleti céloknak és biztonsági követelményeknek megfelel	8.2, 10.5,	AI5: 5.9, 5.13, 5.14,
Változtatás kezelés		
Gondoskodás arról, hogy minden változtatás megfelel a vállalati céloknak biztonsági szempontból.	8.1,10.5	AI5: 5.7, AI6:6.4
A szolgáltatás színvonalának meghatározása, és menedzselése		
A szolgáltatás színvonalának meghatározása biztonsági szempontból	4.2,4.3, 6.1, 10.5	DS1: 1.2,1.5, DS2: 2.3, 2.8, AI4: 4.1,
Harmadik felek szolgáltatásainak menedzselése		
A harmadik felek szolgáltatásainak menedzselése biztonsági szempontból	4.2, 4.3,6.1,6.3,8.1,8.7, 10.5	DS2: 2.4, 2.5, 2.6, 2.7,

Gondoskodás a szolgáltatás folyamatosságáról		
Gondoskodás arról, hogy a vállalat az üzleti tevékenységét folyamatosan el tudja látni.	6.3, 7.1, 7.2, 8.4, 11.1, 11.3, 12.1,	DS4: 4.2, 4.3,4.4,.4.6, 4.9, 4.10, 4.12, DS10: 10.1, 10.2, DS11: 11.23,11.24, 11.25 DS12:12.6
Gondoskodás a rendszer biztonságról		
Gondoskodás arról, hogy az automatikus folyamatokat csak jogosult személyek/ rendszerek használhassák üzleti célra	4.2,4.3,6.3, 7.2, 8.5, 8.6, 8.7, 9.2, 9.4, 9.6,10.5, 12.1, 12.3,	DS5: 5.3,5.4,5.5,5.7, 5.11, 5.13, 5.14,5.19. 5.20, 5.21 DS9: 9.5
Konfiguráció menedzsment		
Gondoskodás arról, hogy minden erőforrás biztonsági kockázata minimalizálva van	4.2,8.7, 10.4,	DS9: 9.1, 9.2, 9.3, 9.4, 9.5, 98,
Adat menedzsment		
Gondoskodás arról , hogy minden adat legyen teljes, pontos, érvényes, az input, feldolgozás, tárolás, és elosztás során.	7.2, 8.6, 8.7, 10.2, 10.3	DS11: 11.3, 11.4, 11.7, 11.8, 11.911.10, 11.11, 11.211.13, 11.14. 11.15, 11.16, 11.18, 11.19,11.20, 11.26,
Támogatások menedzselése		
Az IT berendezések védelme a sérüléstől	7.1, 7.2,	DS12: 12.1, 12.5, 12.6

Ellenőriz, és értékel		
A folyamatok monitorozása – a belső ellenőrzés megfelelőségének ellenőrzése		
Az informatikai biztonság hatékonyságának rendszeres ellenőrzése		M1: 1.2, 1.3, 1.4, M2: 2.1,
Független ellenőrzés		
Bizalom elérése a biztonságban megbízható, és független ellenőrzéssel		M3: 3.3, 3.4, 3.5, 3.6, 3.7,

A COBIT oszlopban megadott pontokat felfoghatjuk úgy is, hogy az a COBIT biztonsági vonatkozású szempont gyűjteménye, amit check listként is használhatunk. Az ISO 17799 oszlopból kiderül, hogy a COBIT 3-4 pont kivételével, tartalmazza az ISO 17799 pontjainak megfelelő ellenőrzési szempontokat, illetve biztonsági követelményeket.

17. BESZERZÉS NÉHÁNY KRITIKUS PONTJA

A beszerzés (itt most nem a közbeszerzésekről lesz szó, mert ezt az eljárást törvény szabályozza) számtalan biztonsági szempontból kritikus pontot tartalmaz, amelyekből a legfontosabbakat az alábbiakban tárgyaljuk. A közbeszerzési törvény hatálya alá nem eső beszerzési eljárások, amelyek vonatkozhatnak termékekre és/vagy szolgáltatásokra, történhetnek több lehetséges szállítótól történő ajánlatkéréssel, vagy pályáztatással.

A biztonsági termékek, szolgáltatások harmadikféltől történő beszerzését, csak az informatikai biztonsági vezető, vagy a biztonsági menedzser irányíthatja, és a biztonsági apparátus vehet részt benne. Természetesen a kiíró egyéb informatikai szakértője személyes megbízás alapján (esetleg külső szakértő is), a titoktartási kötelezettségeknek alárendelve, részt vehet benne. Ki kell tehát mondani, hogy a biztonsági rendszer, alrendszerek, az egyes védelmi intézkedések megvalósítása nem az informatikai vezető hatáskörébe tartozó feladat! Különösen fontos ez akkor, ha a kiírás a teljes biztonsági rendszert, alrendszert érinti, mert annak minden adata szigorúan titkos kell legyen.

A teljes ajánlatkérési, illetve pályáztatási (tenderezési) folyamat tisztaságának, befolyás mentességének biztosítása.
A hazai tapasztalatok azt bizonyítják, hogy a legtöbb támadás a beszerzési eljárást lefolytató céget a döntése nyilvánosságra hozatala után e területen éri. Ezért javasolt az alábbiak betartása.

- Az eljárással bármely szinten foglalkozó vállalati munkatársak, vagy külső szakértők számának a lehetséges minimumon tartása azzal, hogy az eljárás bármely szakaszában résztvevők, és az azok birtokába jutott adatok üzleti tikot képeznek. A pályázók egy része ugyanis a nevek ismeretében keresni kezdi azt a személyt, aki részéről befolyásolható. Továbbá a pályázók számára nagy fontossággal bír a kiíró cég által a beszerzésre szánt maximális összeg megismerése.
- Mind a saját munkatársak mind a pályázók számára egyértelműen kinyilvánított követelményként kell szabni, hogy a kiíró bármely munkatársával a kiírástól a döntés nyilvánosságra hozásáig, sem személyes, sem bármely távközlési módon kapcsolat nem vehető fel. A kiírásban meg kell adni a lehetőséget, hogy a pályázók írásban, vagy távközlési eszközökön keresztül kérdéseket tehessenek fel a kiírásban

megadott címre azzal, hogy azt a szintén írásbeli válasszal együtt minden pályázó megkapja. Ezen kívül lehetséges az összes pályázó számára egy alkalommal, *egyszerre konzultációt tartani.*

- A beszerzés tárgyát képező terméket, szolgáltatást úgy kell a kiírásban specifikálni, hogy az ne legyen egy szállítóra nézve specifikus.

Néhány egyéb biztonsági szempont:

- *A pályázatok, ajánlatok könnyebb értékelhetősége érdekében elő kell írni, hogy*
  - *A pályázatok felépítése milyen legyen, azt is biztosítva, hogy a megajánlott termékek, szolgáltatások prospektus szintű ismertetése az anyag mellékleteként szerepeljen.*
  - *Ki kell kötni, hogy a pályázatok (ajánlatok), nem tartalmazhatnak alternatívákat, hanem egy csak egy változatot, és egy árat.*
  - *A szállítónak garantálni kell, hogy a termék, szolgáltatás leszállítása alatt nem történhet semmi, ami a szállítmány eredeti állapotát akár csak részben is megváltoztatja.*
  - *Hazánkban még nem gyakorlat, de el kell érni, hogy a szállító az átadás/átvételkor nyilatkozzon, hogy az átadásra kerülő termék, szolgáltatás nem tartalmaz a megrendelő számára fenyegetést jelentő megoldást, elemet. Ez „a fenyegetés mentességi nyilatkozat”.*
  - *Szoftver szállítása esetén a szállítónak vállalni kell a szokásos garanciák, rendszerkövetés mellett, hogy a forrás nyelvi változatot közjegyzőnél letétbe helyezi arra az esetre, ha bármilyen okból (megszűnés, átalakulás) a kiíró számára elérhetetlenné válik, azaz nem tudja rendszerkövetési kötelezettségét teljesíteni.*

A fentiekben megadott szempontok betartandók a nem biztonsági termékek, szolgáltatások beszerzésénél is. Ezért a biztonsági szervezetnek ezeket ilyenkor is érvényesíteni kell.

18. NÉHÁNY VÁLLALATOK ELLENI BÜNCSELEKMÉNY

Néhány a vállalatok, és/vagy alkalmazottaik ellen, illetve alkalmazottaik által elkövethető bűncselekmény, az „1978. évi. IV. tv. (többször módosított) a büntető törvénykönyvről” alapján:

- 318.§. **Csalást** követ el, aki jogtalan haszonszerzés végett mást tévedésbe ejt vagy tévedésben tart, és ezzel kárt okoz.
- 300/C. §. **Számítástechnikai rendszer, illetve adatok elleni bűncselekményt követ el**, aki a számítástechnikai rendszerbe a számítástechnikai rendszer védelmét szolgáló intézkedés megsértésével, vagy kijátszásával jogtalanul belép, vagy belépési jogosultsága kereteit túllépi.
- 137.§ **Felfegyverkezve** elkövetés akkor állapítható meg, ha az elkövető az élet kioltására alkalmas eszközt az ellenállás leküzdése, vagy megakadályozása érdekében tartja magánál.
- 321.§. **Rablást** követ el, aki idegen dolgot eltulajdonítás végett úgy vesz el valakitől, hogy evégből valaki ellen erőszakot vagy élet vagy testi épség elleni közvetlen fenyegetést alkalmaz, illetőleg valakit öntudatlan vagy védekezésre képtelen állapotba helyez.
- 142.§. **Rombolást** követ el, aki fontos vagyontárgyat megsemmisít, használhatatlanná tesz, vagy megrongál.
- 175.§. **Túszejtést** követ el, aki mást személyi szabadságától megfoszt.
- 317.§ **Sikkasztást** követ el, aki rábízott idegen dolgot jogtalanul eltulajdonít, vagy azzal sajátjaként rendelkezik.
- 323.§. **Zsarolást** követel, aki jogtalan haszonszerzés végett mást erőszakkal vagy fenyegetéssel arra kényszerít, hogy valamit tegyen, ne tegyen, eltűrjön, és ezzel kárt okoz.

A fentiek nem tartalmazzák az **adatok védelmének, az adatbiztonságnak a sérelmére elkövethető bűncselekményeket,** amellyel a „Személyes adatok védelméről szóló, 1992. évi. LXIII. Törvény” foglalkozik.