

ALMA MATER

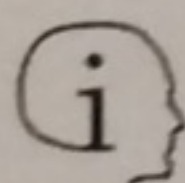
Válogatott tanulmányok a vállalati biztonság témaköréből



Információs Társadalomért Alapítvány

ALMA MATER

VÁLOGATOTT TANULMÁNYOK A VÁLLALATI BIZTONSÁG TÉMAKÖRÉBŐL



Információs Társadalomért Alapítvány

Sorozatszerkesztő / Series editor: Dr. Kiss Ferenc, a Szerkesztőbizottság vezetője /
Head of Editorial Board

Szerkesztő / Editor: Dr. Kiss Ferenc

Technikai szerkesztő / Technical editor: Bender Zoltán, Szanyi István

Lektorok / Review Committee:

Dr. Kiss Ferenc, a lektori bizottság vezetője / Head of the Review Committee

Dr. Bassa Lia

Prof. Dobay Péter

Dr. Horváth Attila

Dr. Kupás Tibor

Dr. Székely Iván

Hon. Assoc. Prof. Vasvári György

© Vasvári György CISM, Lengyel Csaba, 2011

ISSN 1587-2386

ISBN 978-963-87788-9-5

Első kiadás / First edition

A kiadvány szerzői jogvédelem alatt áll. A kiadványt, illetve annak részeit másolni, reprodukálni, adatrögzítő rendszerben tárolni bármilyen formában vagy eszközzel – elektronikus úton vagy más módon – a kiadó és a szerzők előzetes írásbeli engedélye nélkül tilos.

All copyrights reserved. Neither the publication nor any part of it may be copied, reproduced, stored in any data recording system in any form or by any means – electronically or by other methods – without prior written permission from the publisher and the authors.

Kiadó / Publisher:

Információs Társadalomért Alapítvány

1507 Budapest, Pf. 213

Web: <http://www.infota.org>

E-mail: info@infota.org

Tel.: +36-1-279-1510 Fax.: +36-1-279-1511

Felelős kiadó / Responsible for the Publication: az Alapítvány Kuratóriumának elnöke /
the Chairman of the Curatorium

Budapest, 2011. november / November 2011

Az ALMA MATER sorozat eddig megjelent kötetei / Published in the series of ALMA MATER

Tanulmányok az örökségmenedzsmentről 2. – Kulturális örökségek kezelése, 2011. október

Studies on Heritage Management 1. – World Heritage and its Management, 2010. október

The capital of intelligence – the intelligence of capital, 2009. március

Tanulmányok az örökségmenedzsmentről 1. – Világörökség és kezelése, 2009. március

Szabad adatok, védett adatok 2. (Open Data, Protected Data 2.), 2008. augusztus

Studies on Information and Knowledge Processes 13., 2008. március

Studies in Theory of Information Retrieval, 2007. október

Alma Mater sorozat az információ- és tudásfolyamatokról 12. (Alma Mater Series on Information and Knowledge Processes 12.), 2007. március

Alma Mater sorozat az információ- és tudásfolyamatokról 11. (Alma Mater Series on Information and Knowledge Processes 11.), 2006. október

Studies in Simulation, 2006. július

Alma Mater sorozat az információ- és tudásfolyamatokról 10. (Alma Mater Series on Information and Knowledge Processes 10.), 2006. március

Alma Mater sorozat az információ- és tudásfolyamatokról 9. (Alma Mater Series on Information and Knowledge Processes 9.), 2005. október

Szabad adatok, védett adatok (Open Data, Protected Data), 2005. március

Selected Papers from the Alma Mater Series 1-8., 2004. szeptember

Tanulmányok az információ- és tudásfolyamatok világából 8. (Essays from the World of Information and Knowledge Processes 8.), 2004. szeptember

Logisztika, információmenedzsment, szoftvertechnológia (Logistics, Information Management, Software Technology), 2004. március

Üzlet, folyamat, monitoring (Business, Process, Monitoring), 2003. szeptember

Szervezeti kihívások – Informatikai megoldások (Organizational Challenges – IT Solutions), 2003. március

Vállalat, információ, tudomány (Company, Information, Science), 2002. szeptember

Sokszínű e-világ (Colourful e-world), 2002. február

Intelligens rendszerek, hatékony alkalmazások (Intelligent Systems, Efficient Applications), 2001. augusztus

TARTALOMJEGYZÉK

Nagyon magas stressz fenyegetettségnek kitett informatikai munkakörök <i>Vasvári György CISM</i>	1
Kisvállalatok biztonsági keretrendszere <i>Vasvári György CISM – Lengyel Csaba</i>	15
Irányítás, kockázat, megfelelőség (GRC) <i>Vasvári György CISM</i>	35
Információs társadalom, információs hadviselés <i>Vasvári György CISM</i>	45
Az IT virtualizáció <i>Vasvári György CISM</i>	57
Tévhitek az információról, a biztonságról – „Errare humanum est” <i>Vasvári György CISM</i>	81
Informatikai biztonsági kockázat példatár <i>Vasvári György CISM</i>	101

Nagyon magas stressz fenyegetettségnek kitett informatikai munkakörök

Vasvári György CISM

Információs Társadalomért Alapítvány
1507 Budapest, Pf. 213
Telefon: +36-1-279-1510, Fax: +36-1-279-1511
e-mail: gvasvári@tiphaz.hu

Absztrakt

Az informatikai munkakörök között vannak olyan munkakörök, amelyek az azt betöltő munkatárs és így a szervezet számára komoly kockázatot jelentenek. A váratlanul bekövetkező katasztrófa, biztonsági esemény önmagában az ilyenkor intézkedésre felkészített munkatársban stressz hatást válthat ki. Ehhez hozzájöhet, az adott munkatárs személyiség jegyei függvényében egy plusz negatív hatás, a döntés, intézkedés kényszerben lévő munkatársban a felelősség érzés félelmet kelthet az esetleges helytelen intézkedése miatt. Ez a két hatás a munkatárs tevékenységét blokkolhatja. Így a szervezet megfelelő védelmi intézkedés nélkül maradhat. A munkatárs kiválasztásánál, képzésénél, ezért a személyiség jegyeket, illetve azok a szervezet számára kedvező irányú megváltoztatására kell, hogy készítsék.

Kulcsszavak: speciális munkakörök (special positions), stressz hatás (stress effect), tevékenység leblokkolása (blocking activity), védelmi oktatás (proactiv education)

1. A nagyon magas stressz fenyegetett IT munkakörök

Az IT munkaköröket betöltőket stressz hatások fenyegetik a munkahelyi környezetből és a munkaköri feladatból adódóan. Az IT területen ki kell emelni az alábbi, nagyon magas stressz fenyegetettségnek kitett munkaköröket. Ilyenek:

- a működésfolytonosság menedzsment, (katasztrófa menedzsment, help desk munkatárs),
- a hardver, szoftverkarbantartó,
- hardver, szoftver hibaelhárító munkakörök.

E munkakörökben a nagyon magas stressz fenyegetettséget a munkahelyi környezetből adódó stressz hatásokon felül az képezi, hogy működési zavarkor, az IT munkatárs gyors, és helyes, szakszerű döntéseitől, intézkedéseitől az információrendszer zavartalan, folyamatos működése függ, azaz az intézkedés tétje a lehetséges okozott kár, igen magas lehet.

2. A működésfolytonosság zavarai

A működési zavarok, az időszakos megszakadás elleni védelem problémájával foglalkozunk amely, az információrendszerek kiemelt feladata. Ma már az információ rendszerek annyira beépültek a szervezetek, vállalatok alaptevékenységébe, hogy a legkisebb működésfolytonossági zavar is az alaptevékenység ellehetetlenüléséhez vezethet.

Éppen ezért, a hatályos jogszabályok igen magas szintű rendelkezésreállást követelnek meg. Pl. az elektronikus aláírással kapcsolatos szolgáltatókra a 3/2005. (III. 18) IHM rendelet 17.§.(1). 99,9%-os rendelkezésreállást ír elő, és az eseti szolgáltatás kiesést 3 órában maximálja. Hasonlóan szigorúak a bankközi elszámolás–forgalmi rendszerek (GIRO, SZOFTVERIFT), termelési folyamat vagy légiforgalom–irányító számítástechnikai rendszerek követelményei.

A működésfolytonosság megszakadása külső vagy belső támadás hatására bekövetkező biztonsági esemény. Ilyen esemény lehet pl.:

- a hardver vagy a szoftver meghibásodása,
- tudatos vagy véletlen emberi hiba,
- áramellátás kimaradása,
- légállapot szabályozás kiesése,
- természeti katasztrófa,
- tűz,
- árvíz, vízbetörés,
- terrortámadás,
- elektronikus támadás (információs hadviselés), például logikai rombolás, rosszindulatú szoftver támadás,
- hacker támadás,
- szabotázs.

A működésfolytonosság zavarai, megszakadása negatív hatást kiváltó biztonsági eseménynek tekintendő. Az ilyen események következményeiket tekintve különböző mértékűek lehetnek:

- Érzékeny esemény: az eredeti helyzet helyreállításáig, a folyamatos működés hosszabb időre áthidalható,
- Alapvető esemény: megszakadás csak rövid időre hidalható át,
- Kritikus esemény: az eredeti állapot csak hosszabb idő elteltével állítható helyre.

A visszaállítás a működés folytonosság ideiglenes biztosítása, a felkészülés során kiépített háttér rendszerrel történik, míg a helyreállítás az eredeti rendszer, eredeti helyén történő, a katasztrófa bekövetkezése előtti állapotnak megfelelő, eredeti állapot újra kiépítése, a rendszer működőképessé tétele.

Az egyes alkalmazói rendszerek pedig, a visszaállítás időtartamára (lásd 1. ábra) különböző mértékben érzékenyek. Így a következő változatok fordulhatnak elő:

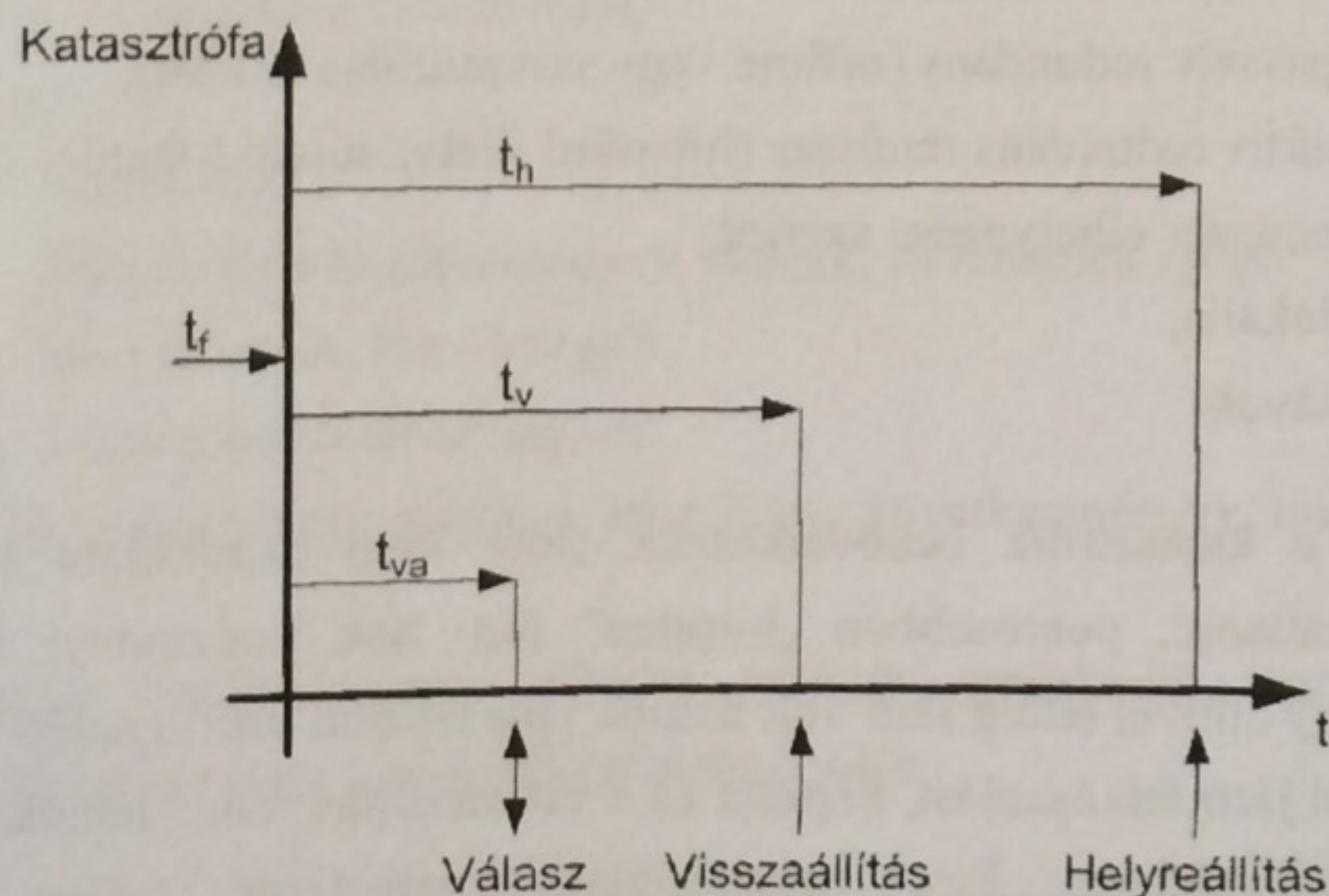
- A megszakadást egyáltalán nem tűri el (pl. pénzforgalmi rendszerek, légi irányítási rendszerek) vagy
- rövidebb időre eltűri (pl. gazdálkodási rendszerek) vagy
- hosszabb időre eltűri (pl. személyzeti, munkaügyi nyilvántartó rendszerek).

Ezeket az időtartamokat az egyes alkalmazások sebezhetőségi ablakának nevezik, amelyek tehát azt határozzák meg, hogy az alkalmazás mekkora időtartamot tud áthidalni megszakadt IT működésfolytonosság mellett. Ami egyúttal azt is jelenti, hogy a katasztrófa bekövetkezésére a válaszingtezkedésnek úgy kell megtörténnie, hogy a visszaállítás a sebezhetőségi ablakon belül menjen végbe.

A katasztrófa bekövetkezésével kapcsolatos idődiagramot az 1. ábrán adjuk meg.

t_f = felkészülési idő, t_v = visszaállítási idő, t_h = helyreállítási idő,

t_{va} = válaszadási idő (igen rövid időtartam célszerű).



1. ábra: Idődiagram

A működésfolytonosság megszakadásának néhány jellemzője:

- A megszakadás bekövetkezési valószínűsége csak becsülhető, és a bekövetkezése nem zárható ki, a valószínűsége nem lehet zéró.
- A válasz intézkedés megtételének a lehető legrövidebb időn belül kell megtörténnie annak érdekében, hogy a további kárkövetkezmények mennél kisebbek legyenek.

A számítóközpontokban általában minden műszakban van egy a katasztrófamenedzselésért felelős munkatárs, aki a katasztrófa bekövetkezésekor köteles és jogosult

- a katasztrófát azonosítani,
- a válaszintézkedésekről dönteni, és azokat megtenni, azaz
 - amennyiben szükséges, a munkatársak életének mentéséről gondoskodni, a kiürítési terv végrehajtását elrendelni,
 - intézkedni a visszaállítás és a helyreállítás megkezdéséről, a teameket riasztani,
- a menedzsmentet értesíteni,
- az eseményt dokumentálni.

A háttér lehet:

- a konfiguráció szerint:
 - hideg (üres számítógép terem, infrastruktúrával ellátva),
 - meleg (nem automatikusan induló, újraindítandó a küldetéskritikus alkalmazásokra),
 - forró (minden alkalmazásra).
- növelt rendelkezésreállású, az egész rendszert fenyegető katasztrófa elleni védelemre alkalmas hátterek:
 - passzív redundáns (offline vagy visszaállítás bázisú),
 - aktív redundáns rendszer (hibatűrő illetve túlélő hibatűrő rendszer).
- a háttér rendszer elhelyezése szerint:
 - lokális,
 - távoli.

Továbbá, mivel a katasztrófa bekövetkezése előre nem számítható ki, valójában a bekövetkezés váratlanul, pontosabban „hirtelen” jön. Sok intézményi vezető abban a tévhitben van, hogy „mivel eddig sem volt nálunk katasztrófa, ezért ezután sem lesz”. Így a jelentős költséggel járó felkészülést, képzést és a visszaállítás feltételeinek megteremtésére nem hajlandó beruházni. Egy nagyvállalati menedzser pedig a katasztrófa következményeinek elhárítási tervét készítve, azt kérdezte: „atomtámadásra készülünk fel?”

Ez a magatartás súlyosan sérti a szervezet biztonsági, üzleti érdekeit, nehezíti a válaszadásért felelős munkatárs helyzetét, intézkedési alternatíváit pedig csökkenti.

3. A humán erőforrások szerepe

Az információrendszerek egyik erőforrása a humán erőforrás, amely e témában gyakorlatilag a főszerepet játssza, ezért nézzük meg először, általában milyen feladatokat látnak el a biztonsági szervezet egyes munkatársai:

- IT védelmi intézkedések menedzselése, üzemeltetése.
- A védelmi intézkedések jogszabályi, belső szabályozási megfelelőségének folyamatos biztosítása.
- Gondoskodás arról, hogy a védelmi intézkedések kikényszerítsék a biztonsági követelmények teljesülését.
- A kockázatok folyamatos feltárása, értékelése és a szervezet kockázati tűrőképességének megfelelő szinten tartása.
- A biztonsági események megoldása, dokumentálása.

A működésfolytonosságért felelős személy(-ek), a folytonosság megszakadása, katasztrófa esetén egyedül jogosult és kötelezett intézkedni. Hasonló a helyzet a help desk munkatársakkal, akik az információrendszer bármely pontján kialakult zavar, vészhelyzet, katasztrófa esetén jogosultak és felelősek a megfelelő intézkedések végrehajtásáért. Tehát ezen munkakörök betöltőitől magas stressztűrő képességet várnak el, amely jelentős kockázatot hordoz.

Ezek után nézzük meg, hogy a katasztrófa menedzser, milyen folyamatok él át a katasztrófa bekövetkezése után:

- Felismeri, azonosítja a katasztrófát,
- Átgondolja:
 - Mi történt?
 - Milyen kárkövetkezmények vannak, és lehetnek még?
 - Mi a feladata, felelőssége?
 - Milyen intézkedést tegyen?
- A teendő intézkedések súlya, a lehetséges következmények miatt megijed, félni kezd.
- A félelmet részben vagy teljesen leküzd, intézkedik vagy az eluralkodó félelemnek a hatására cselekvőképtelenné válik.

Tehát annak a kockázata, fenyegetése jelentős, hogy az a személy, aki eddig tisztában volt a rá váró feladattal, felkészült a katasztrófa bekövetkezésekor ráháruló felelősségre, mikor

szembe kerül ezzel a helyzettel, a rá nehezedő terhelés alatt félni kezd. A félelmet nem tudja leküzdeni, leblokkol. Ennek következtében újabb károk keletkeznek, a működésfolytonosság visszaállítása a sebezhetőségi ablakon belül nem történik meg. E folyamat egy stresszor (a stressz oka) hatása alatt megy végbe.

4. A szervezet, szervezeti kultúra a katasztrófa menedzser környezete

A katasztrófa menedzser a munkahelyi és a szervezeti kultúra által létrehozott környezetben, dolgozik, szocializálódik. E környezet pszichoszociális kockázatokat jelent az egyén számára, amely a feladata végrehajtása során jelentkezhet nála. A katasztrófa menedzsernek az összterhelése azaz, amit fel kell dolgoznia a válasz megtételéhez, ezzel is növekszik. Ez nem kevesebbet jelent mint azt, hogy a környezet képezte kockázatok a helyes, hatékony válasz megtételének feltétlenül nem elhanyagolható motiváló tényezőjét képezik. Erre célszerű oda figyelni. Ki kell emelni, hogy a környezet stresszhatása folyamatos, hosszabb ideje hathat (okozhat az egyénben feszültséget), míg a katasztrófa, mint stresszor hirtelen, váratlanul jelentkezik, és az általa kiváltott félelem ráépül a környezet okozta feszültséghez. Így az egyén feladatai megoldásához mind a kettőt le kell küzdenie. Nem lehet tehát kizárni, hogy az így kialakult összterhelést már az egyén szervezete részben vagy egészében nem tudja leküzdeni. Továbbá olyan környezetben, amely magas pszichoszociális kockázatokat jelent, ugyanaz az egyén más hatékonysággal intézkedik, adhatja meg a katasztrófára a választ [11].

5. Katasztrófák hazánkban

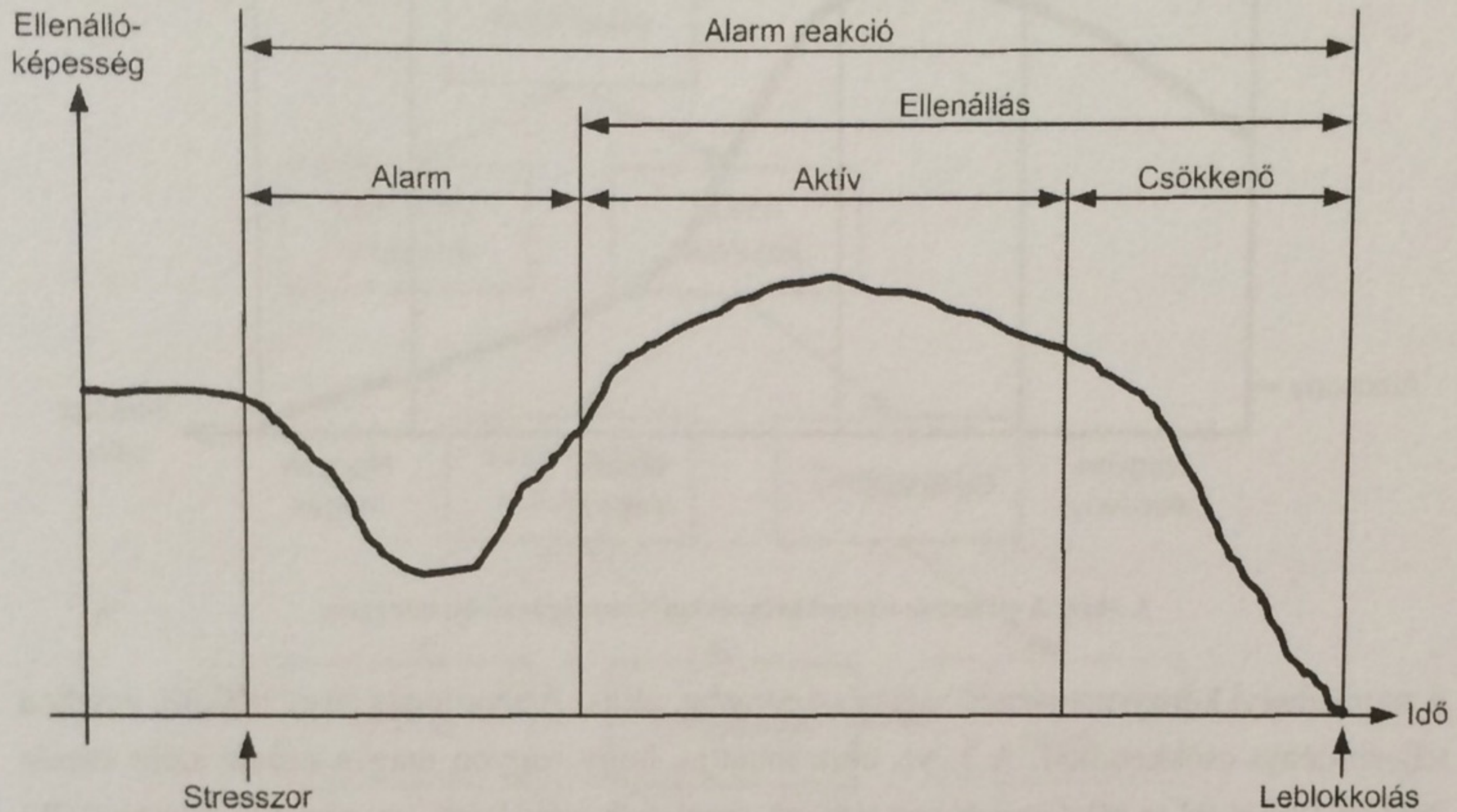
A katasztrófa bekövetkezését megelőzően rendszeresen végzett kockázatelemzések kimutatják, hogy egy katasztrófa bekövetkezésének valószínűsége közel nulla, de nem kizárt. A felkészülési fázis keretében folyik az oktatás, a háttérrendszerek és egyéb védelmi intézkedések létrehozása és működőképes állapotban tartás. Ugyanakkor a katasztrófa bekövetkezésének nincs konkrét időpontja. Néhány katasztrófa hazánkban, amely 1970 és 1990 között zajlott le. Egy számítóközpontban a klimatizálás leállása vagy máshol a központifűtés csövek megrepedése miatt bekövetkezett vízbetörés vagy egy harmadik számítóközpontban kitört tűz.

6. A stressz

Selye szerint: a stressz a humán szervezet nem - specifikus válasza bármely igénybevételre, amely a stresszorok (stresszt kiváltó okok) által okozott hatások következtében jelentkezik. Cooper (1976) szerint: a stressz egy pszichológiai állapot, amely egy személy és a munkakörnyezete közötti folyamat interakciójának része, illetve válasz arra. A stresszor az

emberi szervezetben sokkot válthat ki, aminek következtében a szervezet ellenálló képességének a csökkenése miatt nem képes leküzdeni, a szervezet leblokkol.

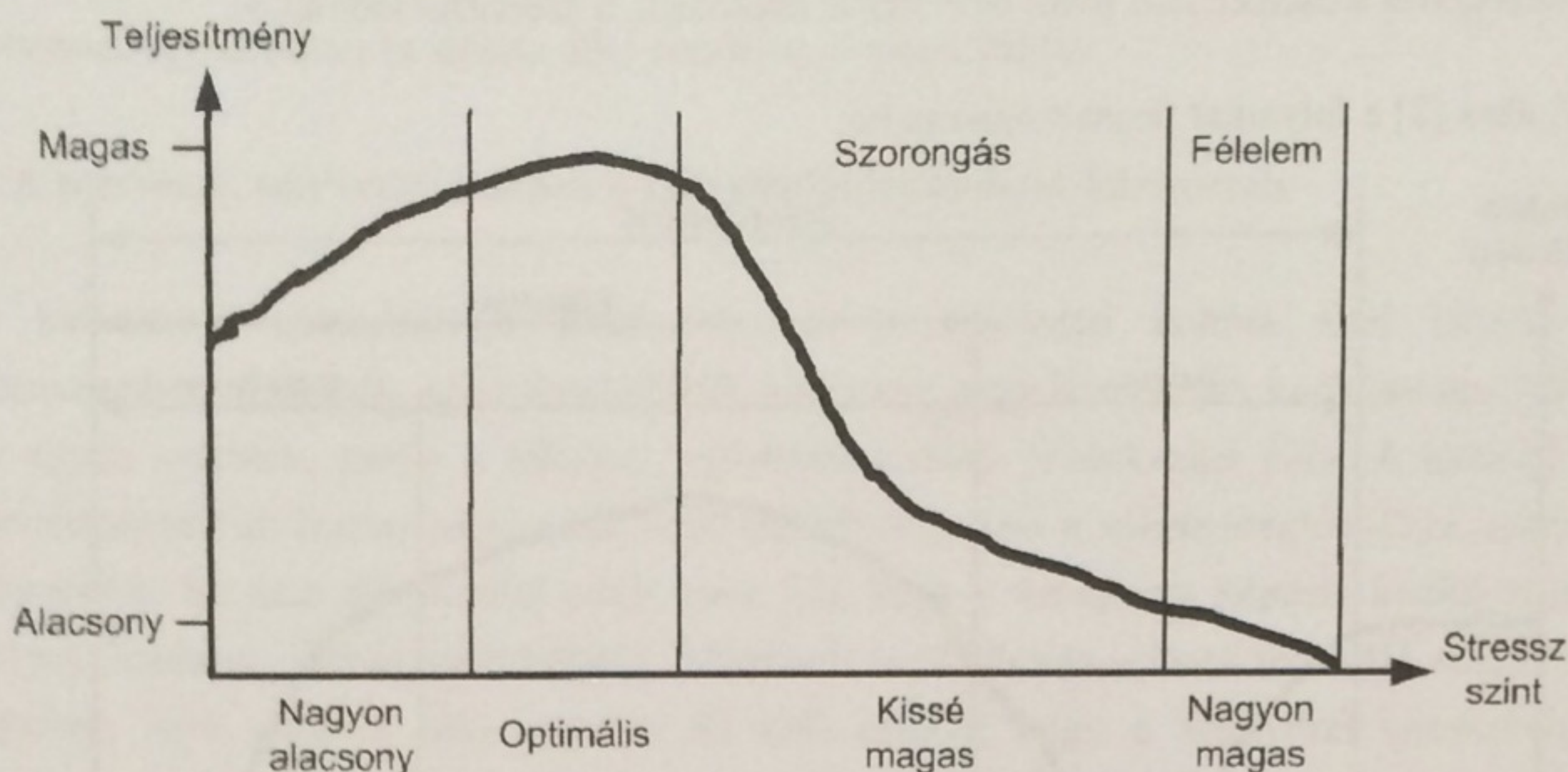
A 2. ábra [2] e folyamat fázisait mutatja be:



2. ábra: A stressz folyamata

Az alarm reakció alatt megy végbe a katasztrófa azonosítása, a helyzet értékelése, döntés az intézkedésekről. Az aktív ellenállás az adott személy ellenállóképességének a függvényében kíséri meg a félelmet leküzdeni. Előfordulhat azonban az, hogy ez az ellenállóképesség a leküzdéshez már nem elegendő, így előállhat egy olyan helyzet, amikor a személy cselekvőképessége nullára csökken. Ugyanakkor lehetnek olyan esetek is, amikor az ellenálló képesség csak részbeni leküzdést tesz lehetővé, amikor is hibás intézkedés (-ek) születhetnek.

A stressz és a munkavégzés hatékonyságának összefüggését a 3. ábra [2, 10] szemlélteti.

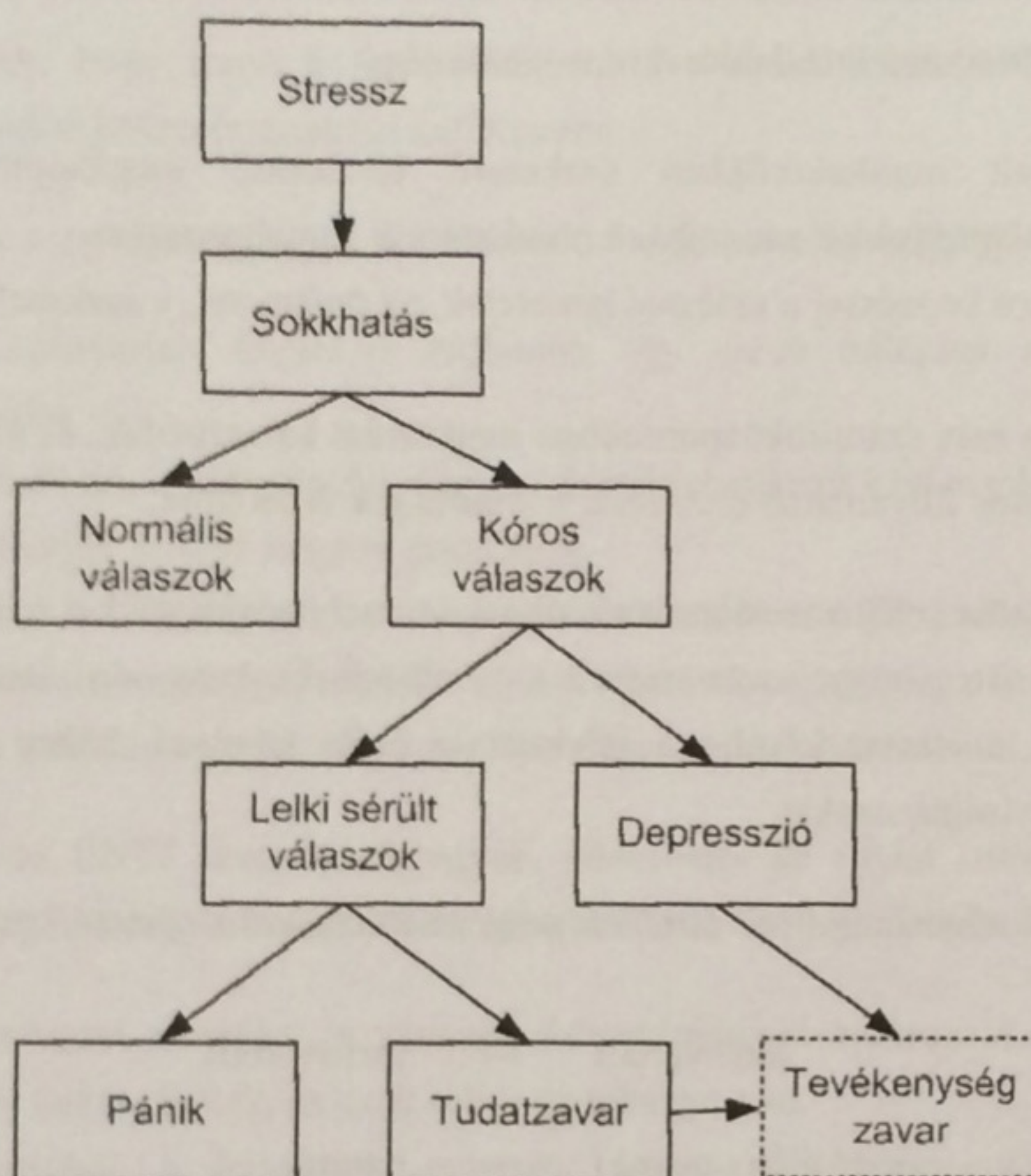


3. ábra: A stressz és a munkavégzés hatékonyságának összefüggése

A munkahelyi környezet stresszhatása szorongást okoz. A szorongás tárgy nélküli, amely a teljesítményt csökkentheti. A 3. sz. ábra mutatja, hogy nagyon magas stressz szint esetén félelem léphet fel (a félelemnek van tárgya), amelynek hatására, emocionális trauma (lelki sérülés), tudatzavar alakulhat ki, amely az egyén munka teljesítményét akár nullára is csökkentheti (leblokkolhatja). Mint másik változatot meg kell említeni a normális hibamentes cselekvőképességet, amely akkor következik be, ha az egyén szervezete, aktív ellenálló képessége le tudja küzdeni a stressz hatását, a félelmet. Az állami katasztrófavédelem foglalkozik a stressz hatására létrejövő [3]-ban a humán reakciók típusaival. A Szerző véleménye szerint esetünkben a hisztériás reakciókhoz tartozó tudatzavar kialakulásának tudható be a tevékenységi zavar, esetleg a teljes cselekvés képtelenség (lásd a [3] alapján a 4. ábrát). Ugyanakkor rögzítenünk kell, hogy e reakció nem azonos minden embernél, hiszen az emberek személyisége, kompetenciája igen különböző.

R. Ryckman [6]-ban azt írja, hogy a személyiség, az egyén tulajdonságainak egy dinamikus és szervezett készlete, amely egyedül képes befolyásolni különböző helyzetekben az egyén ismereteit, motivációit, magatartását. Ezt kiegészíti az egyén kompetencia szintje, azaz a személyiségjegyek mellett, a szakmai tudásának, tapasztalatainak és nem utolsósorban önismeretének, azaz (esetünkben) szakmai magabiztosságának szintje.

A katasztrófa menedzser személyiség jegyei a stressz hatására különböző válaszokat adnak az emocionális trauma mértékének függvényében normál választól a cselekvési zavaron át a cselekvés képtelenségig. Vagyis cselekvési zavar mértéke meghatározza a cselekvés megfelelőségének, helyességének mértékét, és a súlyos emocionális trauma esetén ez vezethet a teljes cselekvés képtelenséghez.



4. ábra: A tevékenységi zavar kialakulása

A pánik (roham) szorongással járó pszichés zavar, amely kiszámíthatatlan és elemi erejű félelemmel jár, valamint testi tüneteket is produkál. Ennek azonban nincs valószínűsége esetünkben, ugyanis az emocionális trauma bekövetkezése a tapasztalatok szerint döntésképtelenséget von maga után, amely cselekvésképtelenséget eredményezhet. A katasztrófa menedzselésért felelős személy nem képes a feladatának megfelelően intézkedni.

7. A stressz kockázatának a csökkentése

A szervezetek, vállalatok működésfolytonosságának optimális biztosítása elemi üzleti érdek. Ugyanakkor, mint már erről szó volt, nem minden felsővezetés ismeri ezt fel. Ezt a nézetet erősíti a kockázatok csökkentésének költsége, valamint „a nálunk ez már előfordult, még egyszer nem fordulhat elő” nézet. Valójában a biztonsági kultúra, biztonsági tudatosság nem megfelelő szintjéről van szó.

A biztonsági követelmények (szabványok, a legjobb gyakorlat) ezzel szemben elvárja a kockázatok folyamatos elemzését, és csökkentésükre az intézkedések megtételét.

Összefoglalva a következő intézkedésekre van szükség:

- A tárgyalt munkakörökben szakszerű tesztekkel megállapított, megfelelő személyiségjegyekkel rendelkező munkatársak foglalkoztatása.
- Folyamatos képzéssel a szakmai ismeretek, az önismeret, a szakmai magabiztosság erősítése.
- A saját és más számítóközpontokban megtörtént katasztrófák, és az azokat követő intézkedések folyamatos elemzése, a tanulságok értékelése.

Összefoglalva a katasztrófa menedzsernek olyan személyiségjegyekkel kell rendelkeznie, amely valószínűsíti, hogy szervezete a működésfolytonosság megszakadásának bekövetkezésekor, a stressz kiváltotta félelmet le tudja küzdeni. Ehhez nézzük meg a különböző személyiségtípusokat.

A személyiség típusokat Jung típus elmélete négy ellentétpárra alapozza, ezek:

I	introvertált	↔	extrovertált	E
S	érzékelő (sensing)	↔	intuitív	N
T	gondolkodó (thinking)	↔	érző (feeling)	F
J	megítélő (judging)	↔	észlelő (perceiving)	P

- **I:** introvertált, tartózkodó, befelé forduló, akinek a lelki energiaforrása belülről származik, és aki szorongásra, félelemre hajlamos.
- **E:** extrovertált, társaságkedvelő, kifelé forduló, akinek a lelki energiaforrása kívülről származik.
- **S:** érzékelő, arra alapoz, amit az érzékszervei közvetítenek.
- **N:** intuitív, aki a kívülről nyert információkat belül rendezi, és ennek alapján dönt.
- **T:** gondolkodó, aki az értelmére, a gondolkodására hallgat, amikor cselekszik.
- **F:** érző, akinél az ösztönei határozzák meg a reflexióit, cselekedeteit.
- **J:** megítélő, aki gyorsan képes döntést hozni.
- **P:** észlelő, aki észleléseit megfontolva dönt.

Jung az alaptípusokból 16 személyiség típust határoz meg és azokat a vastagon írt betűkből kialakított betű négyesekkel jelöli.

Megvizsgálva a katasztrófa menedzser munkakör követelményeit a megfelelő személyiségjegyeket e munkakörhöz az ENTJ – kifelé forduló, intuitív, gondolkodó, megítélő típusban látjuk.

Ebből következik, hogy mind a felvételnél, mind a munkakörök betöltőinél ezeket a személyiségjegyeket követelményként kell kezelni.

A kimaradt négy személyiségjegy, a stresszhatás, a tudatzavar kialakulását segítené. Ezek:

- Az **I** introvertált félelemre hajlamos, így eleve felléphet a félelmi állapot kialakulása.
- Az **S** érzékelő, a katasztrófák nagy részénél jelentkező kárkövetkezmények erősen motiválhatják fellépő negatív gondolata.
- Az **F** érző, a keletkezett károk kedvezőtlenül motiválhatják cselekvőképességét.
- A **P** fontolva döntő a negatív következtetések súlya negatív szerepet játszhat („hátha mégsem vagyok erre képes”) a döntések meghozatalánál.

Ezzel szemben az ENTJ személyiségjegyek, növelhetik az egyén stresszhatást leküzdő, ellenálló képességét, a helyes intézkedések megtételének valószínűségét. Mivel:

- **E** a szervezet elvárásai, a szakmai követelmények határozzák meg cselekvését, amelyre felkészítették, és azok teljes birtokában van.
- **N** intuitívnál, a fejlesztett, erősített „képes vagyok megoldani”, a szakmai magabiztosság tudata döntő szerepet játszik.
- **T** gondolkodónál a szakmai ismeretei, a lehetséges következmények lépnek előtérbe („ha nem intézkedem, mi történik”).
- **J** gyorsan döntőnél, az előbbieket segítik a döntés, elhatározás gyors megtörténtét (a rövid időn belüli válaszingtezkedést).

A biztonsági szervezetek a katasztrófák kárkövetkezményeinek csökkentésére Működésfolytonossági Terveket készítenek. E tervek kitérnek többek között

- a felkészülési időszakban teendő fizikai, logikai védelmi intézkedésekre,
- humán védelmi intézkedésekre, mint
 - oktatás, szakmai önismeret erősítése,
 - megfelelő személyiség jegyű katasztrófa menedzserek biztosítása,
 - felkészülési, visszaállítási, helyreállítási teamek megszervezése,
- a katasztrófa bekövetkezését követő védelmi intézkedések:
 - a további kárkövetkezmények csökkentésére,
 - a visszaállításra és
 - a helyreállításra,

természetesen az 1. pontban megadott mind a három esemény változatra.

8. Stressz szimuláció

A felvételnél az egyén alkalmasságát a katasztrófa menedzser munkakörre, stressz interjúval tesztelik. [9] írja, hogy „Minden interjú stresszel, kényelmetlenséggel jár, de nem minden interjú stresszinterjú! A stresszinterjú során az interjú készítője szándékosan intenzív nyomással terhelt légkört teremt, a pályázót kényelmetlen, szokatlan kérdésekkel bombázza. Célja és feladata ezzel az, hogy megfigyelje a jelölt reakcióját és teljesítményét olyan feszültség, bizonytalanság esetén, amit - ha felveszik - a munkája során tapasztalni fog”.

Kétségtelen, hogy az említett stresszinterjú, egy olyan módszer, mely a majdani munkakörben jelentkező feszültséghez hasonló helyzetben vizsgálja a jelölt várható reakcióját, teljesítményét. Ezzel szemben esetünkben, mint a fentiekben rámutattunk ennél „keményebb” stressz (félelem stressz) leküzdését várják el a jelölttől. Esetünkben egy adott személy katasztrófa utáni válaszára kényszerhelyzetében várható viselkedését, magatartását, cselekvéseit, feltehetőleg csak egy katasztrófa utáni helyzethez hasonló helyzetben lehet korrekten megítélni. Felmerül a kérdés, hogy vajon egy ilyen szituáció szimulálható-e egy stresszinterjúval vagy más eljárásra van szükség a katasztrófa utáni helyzet teszt célokra történő előállítására? Erre a kérdésre a választ a pszichológusok adhatják meg. Addig is, míg a szimulált katasztrófa környezetben történő tesztelést nem oldják meg, a személy (felvételre jelölt, katasztrófa menedzseri munkakörben dolgozó) megfelelőségének a megállapítása az előbbieken említett stressz interjú eljárással történhet.

Megállapíthatjuk, hogy a tesztek minden fajtája végeredményben általános, nehezen található bennük egy adott (főleg kritikus) „élethelyzetben” várható magatartás prognózisa. Általában ezek az adott helyre és adott időpontra választ adó módszerek. Ezekben a személyiség képe jelenik meg, amiből áttételesen következtethető egy, a kritikus helyzetben tanúsított magatartás (aktivitás, helytállás stb.).

Végül az amerikai Burleson Consulting tanácsadó cég írja honlapján [12]:

Sok szervezetnél nincsenek tekintettel arra, hogy egyes számítógépes szakembereknek magas feladat stressztűrőképességgel kell rendelkezniük. A működésfolytonosság megszakadása például, jelenthet 100.000 \$/óra veszteséget is. Ez pedig hatalmas terhelést, nyomást jelent azokra a szakemberekre, akiknek választ kell adniuk egy biztonsági eseményre. Mivel a magas stresszfenyegetésnek kitett munkakörökre történő alkalmasság megállapítására nincs kielégítő megoldás, ezért törekedni kell olyan szakembereket felvenni, akik magas stressztűrőképességet igénylő munkakörökben már más szakterületen, tapasztalatot szereztek.

Irodalomjegyzék

- [1] Vasvári György: Vállalati biztonságirányítás. Time Clock Kft. 2007.
- [2] Antalovics M., Izsó L.: Bevezetés az információergonómiába. Jegyzet. BME 2000.
- [3] Vészhelyzet pszichés hatásai. Országos Katasztrófavédelmi Főigazgatóság. 2009. július.
- [4] L. Schnech. D. Dyck: Dealing with Stress and Traume. Eastern Mannonite University. 2007.
- [5] Stresssz. Wikipedia.
- [6] R. Ryckman. Wikipedia. 2004.
- [7] dr. Poor György: Stressz. HR. Portál. 2009.
- [8] Vasvári György: A biztonsági kultúra és az egyén. ITA Biztonságmenedzsment Kutatócsoport. 2007.
- [9] Ing. Peter Zajíček: Stressz interjú. P&Bert Management Consulting Group. 2009.
- [10] Tózsér Dávid: Szervezeti magatartásformák okainak és következményeinek vizsgálata, különös tekintettel a stressz hatásának elemzésére. Diplomamunka. Debreceni Egyetem Közgazdaságtudományi Kar. 2007.
- [11] Szegény György: A szervezeti kultúra, mint pszichoszociális kockázat. Humán Szemle. 2007.
- [12] Hiring for high stress job. Burleson Consulting. Home page. 2009.

Kisvállalatok biztonsági keretrendszer

Vasvári György CISM

Információs Társadalomért Alapítvány
1507 Budapest, Pf. 213
Telefon: +36-1-279-1510, Fax: +36-1-279-1511
e-mail: gvasvari@tiphaz.hu

Lengyel Csaba

biztonsági menedzser
Központi Elszámolóház és Értéktár (Budapest) Zrt.
1075 Budapest, Asbóth u. 9-11.
Telefon: +36-1-483-6100 Fax: +36-1-342-3539
e-mail: lengyi84@chello.hu

Absztrakt

A kis vállalat anyagai forrásai korlátozottak, ezért meg kell találni azt a megoldást, amely biztonsági szempontból elfogadható. Ehhez nyújt segítséget a COBIT SECURITY BASELINE, valamint a hatályos szabványok. A kockázatokat elemezni kell, és azt hogy milyen fenyegetést jelentenek a kis vállalat számára az előbbieken megadott irányelvek szerint kell meghatározni. A szükséges és elégséges biztonsághoz a kockázatokat és a teendő védelmi intézkedéseket a biztonság szempontjából kielégítő szinten kell meghatározni, figyelembe véve a kis vállalat teherbíró képességét és a minimálisan szükséges biztonság biztosításának igényét.

Kulcsszavak: biztonsági követelmények (security requirements), veszélyforrások (exposures), kockázati matrix (risk matrix), védelmi intézkedések (protectiv measures), biztonság menedzsment (security management)

1. Bevezetés

A kisvállalatok az elmúlt években felismerték, hogy nekik is tenni kell a vállalati biztonságért (a vagyon-, üzem- és informatikai biztonságért), ugyanakkor mind anyagi, mind létszám szempontból a lehetőségeik igen korlátozottak. Ezt felismerte az ISACA

(Információ Ellenőrök Nemzetközi Szervezete) is, amikor elkezdett foglalkozni ezzel a témával, és végül kiadta a COBIT QUICKSTART és a COBIT SECURITY BASELINE (továbbiakban CSB) dokumentumokat. Ezen dokumentumok a kisvállalati sajátosságokat figyelembe véve határozzák meg az informatikai (továbbiakban: IT) auditálási szempontokat, illetve ezzel az IT biztonság minimális követelményeit, mivel az ismertetett auditálási szempontok úgy is értelmezhetők, hogy megadják, mit kell vizsgálni, melyek az elvárások, így ezek alapján a teendők is meghatározhatók.

„A Vállalati Biztonság Keretrendszere” tárgyú kutatási témánk folytatásaképpen most tehát a kisvállalati (kisszervezeti) biztonsággal kívánunk foglalkozni az alábbiak szerint (nem tárgyaljuk azokat a kisvállalatokat, amelyek termelő vagy technikai szolgáltató tevékenységet folytatnak, tehát nem foglalkozunk a vállalati biztonsági rendszeren belül az üzembiztonsági alrendszerrel, csak a vagyon- és IT biztonsági alrendszerekkel):

A) A kutatás célja

Kisvállalatok, illetve kisszervezetek (amelyek nem folytatnak termelést vagy technikai szolgáltatást, mint például a kereskedelmi, pénzügyi és szellemi szolgáltató kisvállalatok, vagy egyes államigazgatási, önkormányzati szervezetek) számára elfogadható anyagi és létszámterhet jelentő, a kompromisszumok ellenére elfogadható erősségű biztonsági keretrendszer és biztonsági követelmények kidolgozása.

Kisvállalat alatt olyan vállalatot értünk, amely kis nettó nyereséggel (néhányszor 10 millió Ft/év), kis költségvetési kerettel és korlátozott számú munkaerővel (néhányszor 10 fő) rendelkezik (a Nemzetközi Munkaügyi Szervezet anyaga még hozzáteszi a kis energiafogyasztást is.)

B) A kutatás tárgya

A kisvállalati biztonsági kockázat menedzsment és ezzel a minimális biztonsági követelmények meghatározása, amelyekből a kisvállalat eldöntheti, melyeket vezeti be, és melyek esetében vállalja annak a kockázatát, hogy nem védekezik.

A kutatómunka főbb szempontjai:

- a vállalati veszélyforrások, kockázatok feltárása,
- a vállalati biztonsági kockázati mátrix,
- a minimális IT, majd vállalati biztonsági követelmények meghatározása, CSB-t felhasználva,
- a javasolt védelmi intézkedések a CSB követelmények és az MSZ ISO/IEC 17799 alapján,
- a védelmi intézkedések kiterjesztése az egész vállalatra.

2. COBIT, COBITQUICKSTART ÉS COBITSECURITY BASELINE (CSB)

A CSB úgy illeszkedik a kisvállalatok lehetőségeihez, hogy míg a COBIT QUICKSTART például 62 IT auditálási szempontot ad meg a COBIT3 318 IT auditálási szempontjával szemben, addig a CSB 39 IT biztonsági auditálási szempontot határoz meg.

Összefoglalva a kontroll szempontok számát:

COBIT 3	COBIT QUICKSTART	COBIT SECURITY BASELINE
318	62	39

A COBIT QUICKSTART elsősorban arra szolgál, hogy megadja az induló vállalatok alapvető biztonsági teendőit, de felhasználható a kisvállalatok informatikai ellenőrzési céljaira. A CSB azokat a kulcs ellenőrzési szempontokat adja meg, amelyekből a kisvállalatok biztonsági követelményeit meghatározhatjuk. A 39 lépés a COBIT3-ból lett kiemelve annak érdekében, hogy a kisvállalatoknál is „jobb IT biztonságot” lehessen létrehozni.

3. ISO/IEC 17799 és CSB

A CSB (lásd az előző fejezetben) az ISO/IEC 17799-es szabványl pontjainak többségét lefedi, és ezt egy kimutatással támasztja alá.

4. A CSB szerinti IT biztonsági követelmények

Szervezési biztonsági követelmények

- Humán követelmények
 - A munkaköri kötelezettségek és felelősségek meghatározása személyre szóló munkaköri leírásban
 - A felhasználók képzése, a biztonsági tudatosság folyamatos biztosítása.
 - Gondoskodás felvételnél és vállalati foglalkoztatás alatt a megbízhatóságról.*
- Szervezési követelmények
 - A biztonsági infrastruktúra meghatározása;
- Biztonsági dokumentumok
 - A Biztonsági Szabályzat (Politika) kidolgozása;
 - Az Üzletmenet-folytonossági Terv kidolgozása;

- Titokvédelmi Utasítás
 - Az adatok, eszközök, helyiségek osztályozása;
- Szerződési követelmények
 - A harmadik felekkel kötött szerződések biztonsági követelményeinek meghatározása;

Technikai biztonsági követelmények

- Fizikai hozzáférési követelmények;
 - A fizikai hozzáférés-védelem biztosítása a létesítmények, helyiségek, irodabútorok, hardver és szoftver eszközök, környezeti infrastruktúra, azaz az IT és ügyviteli erőforrások esetében;
- Fizikai rendelkezésre állási követelmények
 - A hardver és szoftver (IT és ügyviteli erőforrások rendelkezésre állásának biztosítása;
 - A környezeti infrastruktúra (tápellátás, klíma, vagyonvédelem) működésének biztosítása;
 - Az üzletmenet-folytonosság biztosítása;
- Logikai hozzáférési követelmények
 - A felhasználó fizikai és logikai belépésének korlátozása, a felhasználó által az IT rendszerben végezhető tevékenységek meghatározása, beállítása;
 - Az operációs rendszerek hozzáférés-védelmének biztosítása;
 - A biztonság érzékeny adatok (papíralapú és elektronikus), rendszerek, eszközök hozzáférés-védelmének biztosítása;
- Logikai rendelkezésre állási követelmények
 - Az adatok hitelességének biztosítása;
 - A rosszindulatú szoftverek (vírusok) elleni védekezés az eszközök szintjén;*
 - Az üzletmenet-folytonosság biztosítása;
- Hálózati biztonsági követelmények
 - A hálózati hozzáférés korlátozása;
 - A rosszindulatú szoftverek (vírusok) elleni védekezés a hálózat szintjén;*
 - A hálózaton az adatok bizalmasságának biztosítása;
- Életciklus biztonsági követelmények
 - A fejlesztés/beszerzés biztonsága;
 - A napi és havi mentések biztonsága;
 - A hardver, szoftver és ügyviteli eszközök átadás/átvételének biztonsága;
 - Az üzemeltetés biztonsága;

- Biztonsági események kezelésére vonatkozó követelmények
 - A biztonsági események kezelése;
 - A biztonsági események naplózása;
 - Számonkérhetőség követelménye
 - Audit naplók működtetése;
 - A vagyoni felelősség biztosítása;
 - Ellenőrzési követelmény
 - (a rendszeres belső és eseti külső biztonsági audit);
- * *A rosszindulatú szoftverek elleni védekezés, valamint gondoskodás a felvételkor és a vállalati foglalkoztatottság alatt a megbízhatóságról, nem szerepel a CSB-ben, de a biztonság érdekében foglalkoznunk kell vele.*

5. Kisvállalati biztonsági veszélyforrások és védelmi intézkedések

A vagyon- és IT biztonság érdekében el kell végezni a veszélyforrások feltárását, majd ezek ismerete után kell megadnunk azok kockázatának csökkentésre szolgáló védelmi intézkedéseket a következő, a CSB által kiemelt biztonsági veszélyforrások figyelembe vételével:

- új veszélyforrások a technikai fejlődés eredményeképpen,
- új technikai megoldások késedelmes alkalmazása,
- növekvő hálózati és távoli hozzáférési (mobil) tevékenységek,
- védelmi intézkedések nem kielégítő alkalmazása,
- hackerek, csalók, bűnözők és terroristák új módszerei,
- hiányosságok a biztonsági tudatosság területén.

HUMÁN VESZÉLYFORRÁSOK

- A naprakész munkaköri leírás hiánya, amely a felelősségre vonás lehetőségét teszi kétségesse (V1).
- A folyamatos biztonsági képzés hiánya, ami a munkatársak gyenge biztonsági tudatosságát, a biztonsági kompetenciájuk elavulását eredményezi (V2).
- A felvételtől az alkalmaztatáson keresztül a munkaviszony megszüntetéséig átfogó humánpolitika hiánya, amely a megbízhatóság biztonsági követelményének érvényesítését kétségesse teszi (V3).

SZERVEZÉSI VESZÉLYFORRÁSOK

- A nem egységes biztonsági szervezet, valamint a nem a kisvállalat legfelső vezetője alá tartozó biztonsági szervezet a támadó számára sok lehetőséget nyújt (V4).

BIZTONSÁGI INTÉZKEDÉSI TERV, MINT VESZÉLYFORRÁS

- A biztonsági dokumentáció, a szabályzatok hiánya, illetve hiányosságai a védelmi feladatokkal kapcsolatban bizonytalanságot, eseti nem tervezett intézkedéseket eredményeznek, és nem teszik lehetővé a számon kérhetőséget (V5).

A TITOKVÉDELMI UTASÍTÁS HIÁNYA

- A hatályos jogszabályok szerint csak azért vonható bárki felelősségre, amit egy szabályzat, utasítás vagy eljárásrend tartalmaz, és arról az alkalmazott bizonyíthatóan tudomással bír (V6).

VÉDELEM A SZERZŐDÉSEKBEN

- A harmadik felekkel kötött szerződésekből a megbízó biztonsági követelményeinek hiánya az outsourcing, a fejlesztés, a beszerzés, a munkaerőbérlés esetén egyaránt jelentős kockázatot képez.
- A biztonsági követelmények szerződésekbe nem megfelelő beépítése, miután a megbízó követelményeit vita, nem teljesítés esetén csak jogi eljárás után érvényesítheti, további kockázatokat képezhet (V7).

FIZIKAI HOZZÁFÉRÉS LEHETŐSÉGE VESZÉLYFORRÁS

- Az erőforrásokhoz történő jogosulatlan fizikai hozzáférés lehetősége a támadó számára jelentős motivációs tényező (V8, V9).

FIZIKAI RENDELKEZÉSRE ÁLLÁS MEGSZAKADÁSA

- Az erőforrások sebezhetőek, amelynek bekövetkezése a kisvállalat számára az üzleti cél és követelmények teljesíthetőségét teszi kockázatosná (V10, V11).

LOGIKAI HOZZÁFÉRÉS LEHETŐSÉGE

- A logikai hozzáférés korlátozatlansága, feltételekhez kötöttségének hiánya a kisvállalat számára az üzleti cél és követelmények teljesíthetőségét teszi kockázatosná (V12, V13, V14).

LOGIKAI RENDELKEZÉSRE ÁLLÁS MEGSZAKADÁSA

- Az erőforrások részleges vagy átfogó rendelkezésre állásának megszakadása a kisvállalat számára az üzleti cél és követelmények teljesíthetőségét teszi kockázatosná (V16).

HÁLÓZATI VESZÉLYFORRÁSOK

- A hálózatok (a helyi és nagytávolságú hang, illetve adat hálózatok egyaránt) az erőforrások, üzenetek biztonságára nézve jelentenek komoly kockázatok (V17, V18).

ÉLETCIKLUS ALATTI VESZÉLYFORRÁSOK

- A hardver és szoftver, valamint ügyviteli eszközök fejlesztése, beszerzése, átadás/átvétele és üzemeltetése számtalan veszélyforrás jelentkezése mellett történik, amelyek hatásának a csökkentése nem nélkülözhető (V19, V20, V21).

A BIZTONSÁGI ESEMÉNYEK KEZELÉSÉNEK SZABÁLYOZATLANSÁGA

- A szabályozatlanság a nem tudatos, ötletszerű és így nem hatékony védekezés forrása (V22).

A SZÁMONKÉRHETŐSÉG HIÁNYA

- A számon kérhetőség hiánya az elrettentés hiányával jár, és ez a támadó motivációját növeli (V23).

A FOLYAMATOS, CÉLORIENTÁLT ELLENŐRZÉS HIÁNYA

- Az ellenőrzés hiánya lehetővé teszi a védelmi intézkedések elmaradását vagy nem rendeltetésszerű végrehajtását, kétséggé teszi azok naprakészségét (V24).

6. A kisvállalati biztonsági kockázati mátrix

A veszélyforrásokhoz hozzárendeljük azok becsült bekövetkezési valószínűségét (P), a bekövetkezésük esetén a becsült kárkövetkezményt (V, amely lehet R= részleges, és G= átfogó), valamint az alábbi táblázat alapján az adott veszélyforrás képezte kockázatok (K) becsült értékét.

A becslést az indokolja, hogy a bekövetkezési valószínűségek és a nem vagyoni károk egzakt, matematikai eszközökkel nem értékelhetők, csak a vagyoni károk.

Ezeket a kockázati értékeket (a fekete mezőben megadottakat) csökkentik a javasolt védelmi intézkedések, amelyek rendeltetésszerű megtétele esetén is mindig fennáll egy maradék kockázat. Cél a maradék kockázat alacsony szinten tartása. Mindezeket egy kockázati mátrixban ábrázoljuk. Ugyanakkor becsült értékekből kiindulva megadunk egy számszerűsített kockázatelemzési módszert is a következő oldalon.

P \ V	R	G
VS	VS	S
S	S	S
M	M	M
L	L	L
XL	XL	XL

1. ábra: Kockázati mátrix

Kockázatszámítás (0-8 skálán)

Fenyegetés mértéke (bekövetkezési valószínűség)		A			K			M		
Sérülékenység szintje (kárkövetkezmény)		A	K	M	A	K	M	A	K	M
A vagyon elemi értéke	0	0	1	2	1	2	2	2	3	4
	1	1	2	3	2	3	3	3	4	5
	2	2	3	4	3	4	4	4	5	6
	3	3	4	5	4	5	5	5	6	7
	4	4	5	6	5	6	6	6	7	8

1. példa:

Fenyegetés mértéke:

K

Sérülékenység szintje:

A

A vagyon elemi értéke:

2

Kockázat:

3

2. példa:

Fenyegetés mértéke:

M

Sérülékenység szintje:

K

A vagyon elemi értéke:

3

Kockázat:

6

VESZÉLYFORRÁS	P	V	K	VÉDELMI INTÉZKEDÉS	MARADÉK KOCKÁZAT
Humán	XL	R, G	XL	V1, V2, V3	M
Szervezési	XL	R, G	XL	V4	S
Biztonsági dokumentumok hiánya	M	R, G	M	V4, V5	M
Titokvédelmi utasítás hiánya	L	R	L	V6	S
Szerződésbeli hiányok	L	R	L	V7	S
Fizikai hozzáférés	L	R	L	V8, V9	S
Fizikai rendelkezésre állás megszakadása	L	R	L	V10, V11	S
Logikai hozzáférés	L	R	L	V12, V13, V14	S
Logikai rendelkezésre állás megszakadása	XL	R, G	XL	V15, 16	M
Hálózati	M	R, G	M	V17, V18	M
Életciklus	L	R	L	V19, V20, V21	S
Biztonsági események szabályozatlan kezelése	M	R, G	M	V22.	M
Számonkérhetőség hiánya	L	R	L	V23	S
Ellenőrzési hiányosságok	M	R, G	M	V24	L

7. Kisvállalati védelmi intézkedések az IT követelmények felhasználásával

AZ IT biztonsági követelményekből kiindulva kidolgozhatók a vállalati szintű vagyonbiztonságra (papíralapú iroda) és IT biztonságra (elektronikus iroda) vonatkozó biztonsági követelmények.

Szervezési biztonsági (funkcionális) védelmi intézkedések

A szervezési védelmi intézkedések mind a két biztonsági alrendszerben (vagyon és IT) előfordulnak.

- Humán védelem
 - V1.) A munkaköri kötelezettségek, jogok, felelősségek személyre szóló munkaköri leírásban történő naprakész meghatározása.
 - V2.) A felhasználók, munkatársak folyamatos biztonsági képzése, a biztonsági tudatosság naprakész biztosítása.
 - V3.) Gondoskodás megfelelő humánpolitika végrehajtásával, a felvételtől és a teljes vállalati foglalkoztatás alatt a munkatársak, illetve a szerződéssel munkát végzők megbízhatóságáról
- Szervezési védelem
 - V4.) A két biztonsági (vagyon és IT biztonsági) alrendszert egyaránt magába foglaló, integrált, és az első számú vezetőhöz közvetlenül tartozó biztonsági szervezet és működés kialakítása, amelyet a vállalat nagyságának megfelelően egy munkatárs is elláthat.
- Biztonsági Intézkedési Terv
 - V5.) A Biztonsági Intézkedési Terv kidolgozása a biztonsági rendszer (vagyon és IT) elkészítésére, karbantartásra, üzemeltetésére.
- Titokvédelmi Utasítás
 - V6.) Titokvédelmi Utasítás készítése, amely mindkét biztonsági alrendszerben a védelmi intézkedések kiválasztásához meghatározza a védendő titkokat, és a titokkört képező adatállományokat, valamint az adatok, eszközök, helyiségek osztályozását azok biztonság érzékenysége függvényében.
- Védelem a szerződésekben
 - V7.) A harmadik felekkel kötött szerződésekbe (szállítási, karbantartási, fejlesztési, rendszerkövetési) a Titokvédelmi Utasításnak is megfelelő biztonsági követelmények, valamint Szolgáltatási Szint Megállapodás (SLA) beépítése, azok naprakészen tartása és érvényesítése.

Technikai (funkcionális) védelmi intézkedések

A technikai védelmi intézkedések mindkét biztonsági alrendszerben előfordulhatnak, de a fizikai védelmi intézkedések elsősorban a vagyonvédelmi biztonsági alrendszert, míg a logikai védelmi intézkedések az IT biztonsági alrendszert érintik.

- Fizikai hozzáférés védelem
 - V8.) A létesítmények, helyiségek, és egyéb erőforrások esetében vagyonvédelmi rendszer működtetése, abban a belépési jogosultságok korlátozása, a belépések ellenőrzése és nyilvántartása, távfelügyeleti kapcsolat mellett.
 - V9.) A papíralapú és elektronikus irodák munkahelyein az üres íróasztal és a sötét képernyő politika érvényesítése. (A sötét képernyő alatt a szabvány a kikapcsolt gépet érti).
- Fizikai rendelkezésre állás védelme
 - V10.) Az egyes erőforrások rendelkezésre állásának biztosítása, gondoskodás tartalék berendezésekről, erőforrásokról, esetleg külső erőforrások bevonásáról, az SLA figyelembe vételével.
 - V11.) Az üzletmenet-folytonosság érdekében gondoskodás háttér, papíralapú és elektronikus háttér megoldásokról, rendszerről más helyszínen, továbbá a munka folytatásához szükséges naprakész dokumentumokról (papír és elektronikus) és járulékos eszközökről (telefon, fax, másolók stb.), valamint a papíralapú és az elektronikus adathordozók biztonságos külső tárolásáról, szervezett mentéséről.
- Logikai hozzáférés védelem
 - V12.) Az informatikai rendszerben a munkaköri feladatok ellátásához szükséges, jelszavas beléptetés, és a belépő jogosultságainak meghatározása és karbantartása.
 - V13.) Az operációs rendszerek jelszavas hozzáférés védelme a legszükségesebb (a munkakörök által indokolt) körre korlátozva a hozzáférési jogosultakat.
 - V14.) A biztonság érzékeny adatok (pl. jelszavak), rendszerek, eszközök hozzáférés védelme tárolás, felhasználás alatt.
- Logikai rendelkezésre állás védelme
 - V15.) A rosszindulatú szoftverek elleni aktív, védelmi (vírus ellenőrző és irtó) szoftverek alkalmazása és naprakészen tartása.
 - V16.) Az üzletmenet-folytonosság lehetséges biztosítása.

- Hálózati védelem
 - V17.) A hálózati hozzáférési jogosultságok jelszóhoz kötése és egyúttal technológiai, logikai korlátozása.
 - V18.) Az adatok bizalmasságának, sértetlenségének biztosítása a hálózaton, a biztonság érzékeny adatok esetében elektronikus aláírás és rejtjelezés alkalmazásával.

Technikai (garanciális) védelmi intézkedések

- Életciklus alatti védelem
 - V19.) A fejlesztés / beszerzés / tesztelés biztonságos környezetének (humán, fizikai, logikai leválasztás az éles rendszerről) igénylése, ellenőrzése. A fejlesztés tárgyával kapcsolatos biztonsági követelményeknek a fejlesztési/üzleti követelményekkel történő együttes megadása.
 - V20.) Az átadás/átvételnél a fejlesztett termékkel szembeni biztonsági követelmények ellenőrzése, az átadás megtörténtekor a fejlesztési jogosultságok visszavonása.
 - V21.) Az üzemeltetés humán, fizikai, logikai leválasztása a fejlesztéstől, valamint a program változáskezelésének szabályozása (a minimálisra korlátozott jogosultakkal).
- Biztonsági események kezelése
 - V22.) A vállalatnál bekövetkező biztonsági események kezelési rendjének meghatározása, tudatosítása, az azonosítás, jelentés, értékelés, intézkedés folyamatának biztosítása.
- Számon kérhetőség biztosítása
 - V23.) Vagyonleltár készítése az üzleti rendszer és az IT rendszer erőforrásairól, a gazdák meghatározásával. A vagyon és IT biztonsági alrendszere en belül, operációs rendszer és alkalmazói rendszereknél egyaránt a jogosultság-változásokról, a végrehajtott, vagy megkísérelt tevékenységekről és ellenőrzésükről naplók vezetése.
- Ellenőrzés
 - V24.) A belső és külső független ellenőrzés (audit) rendszeres működtetése a teljes vállalati biztonsági rendszerre.

A fentiekben szereplő védelmi intézkedéseken túl, még további jelentős számú védelmi intézkedést lehet tenni, hiszen maga a szabvány sem tartalmazza a lehetséges védelmi intézkedések teljes körét. Ezek meg nem tétele azt jelenti, hogy egyes védekezések elmaradásának kockázatát a kisvállalat menedzsmentjének a teljesíthetőség érdekében fel kell vállalnia.

8. Megvalósítás

A kisvállalat biztonsági keretrendszere olyan jellemzőkkel kell, hogy rendelkezzen, amelyek a kisvállalat anyagi, létszám korlátainak megfelelnek, azaz megvalósíthatóak. Vizsgáljuk meg, hogy a fentiekben meghatározott keretrendszer kielégíti-e ezt a követelményt.

- A biztonsági követelmények köre

A CSB követelményekből kiindulva megállapítható, hogy a kisvállalatok esetében, az anyagi és létszámkorlátok miatt, a megvalósítandó védelmi intézkedések köre a közép- és nagyvállalatok védelmi intézkedéseéhez képest jelentősen szűkebb. Ennek az a következménye, hogy a kisvállalat menedzsmentjének fel kell vállalnia azokat a kockázatokat, amelyek csökkentésre nem tesz védelmi intézkedést. Megállapítható tehát, hogy a kisvállalat biztonsági rendszere kompromisszumokon alapul, nem egyenszilárdságú, ezért megkerülhető.

- A kompromisszumok egyéb következménye

A kockázat felvállalása, azaz egy védelmi intézkedés meg nem tétele esetén lehetővé válik olyan megoldás, amely adott esetben más, újabb veszélyforrást képez. Például a biztonság érzékeny feladatok szétválasztása a kisvállalatoknál a korlátozott létszám lehetőség miatt nem realizálható. Előfordulhat azonban az, hogy egy munkatársat nem két, hanem, több feladattal bíznak meg, és egy munkatárs feladatai elérhetnek egy kritikus szintet, amikor már a feladatok rendeltetésszerű végrehajtását veszélyeztetik. Ezért a kisvállalat szervezeti Működési Szabályzatában feltételekhez kell kötni a több feladat egy munkatársnak történő kiadását. Például fél, egy évenként felül kell vizsgálni ezeket, hogy nem lépték-e valahol túl a tűréshatárt.

Azaz nem elég arról dönteni, hogy egy kockázatot a menedzsment felvállal, hanem vizsgálni kell a következményeket, azt, hogy nem jelenthetnek-e újabb veszélyforrást. Ennek következményeként pedig adott esetben intézkedni kell.

- A védelmi intézkedések beruházás igénye

A Szervezési védelmi intézkedések megvalósítása, üzemeltetése nem igényel csak saját munkatársak szellemi munkáját. Ugyanakkor egyes esetekben célszerű külső szakértőt igénybe venni.

A technikai védelmi intézkedések beruházás igényesek, de előfordulhat, hogy egyesek a vállalat már használt szoftverjeiben megtalálhatók, csak éppen nem

használják őket. Pl. az operációs rendszerek ma már tartalmazznak Bizalmas Számítástechnikai Bázist (Trusted Computing Base), amely az aktiválást (beállítást) követően védelmi intézkedések alkalmazását teszi lehetővé.

A javasolt technikai védelmi intézkedések, figyelembe véve a vállalat teherbíró képességét, egy hosszabb időszak alatt is megvalósíthatók. Ezt elősegítheti az a nemzetközileg elfogadott álláspont is, amely szerint a legjelentősebb veszélyforrások a humán veszélyforrások, nem a technikaiak. Ebből következik, hogy elsősorban a szervezési védelmi intézkedéseket kell megvalósítani (V1 - V8), amelyek a saját munkaerő ráfordítást, illetve egyes esetekben külső szakértő közreműködését igénylik, tehát nem beruházás igényesek. Előfordulhat ugyanakkor az is, hogy már meglévő és üzemelő szoftverben lehet (kell) egyes védelmi intézkedéseket aktiválni.

Tekintettel arra, hogy a kárkövetkezmények egzakt módszerekkel csak a vagyoni károkra határozhatók meg, a nem vagyoni károkra csak legjobb esetben is becsülhetők, így az azokat csökkentő védelmi intézkedés gazdaságossági célú összehasonlítása konkrétan nem elvégezhető. Abból kell tehát a döntéskor kiindulni, hogy a meg nem tett védelmi intézkedés a kárkövetkezmények bekövetkezésének kockázatát nem csökkenti, annak bekövetkezési valószínűsége nagyobbá válik.

- **Biztonsági Intézkedési Terv**

A kisvállalatoknál nem várható el, hogy a biztonság szervezés eredményeit úgy dokumentálja, mint egy közép- vagy nagyvállalat teszi. (Biztonsági Átvilágítási Jelentés, Biztonsági Stratégia, Biztonsági Politika, Üzletmenet Folytonossági Terv, Biztonsági Szabályzat). Ugyanakkor biztonsági szempontból az írásbeliség a számon kérhetőség lehetőségét biztosítja. Továbbá néhány biztonsági szabályozást is bár röviden, de el kell végezni. Ezeket tartalmazza, az a Biztonsági Intézkedési Terv vázlat, amelyet a Melléklet ajánl.

9. A kisvállalati biztonságirányítás

Természetesen a kisvállalaton belül annak biztonsági rendszerét is irányítani kell annak érdekében, hogy az irányító és ellenőrző folyamatok minimális kockázattal és költséggel, hatékonyan biztosítsák az üzleti cél biztonságos megvalósítását. Ezért egyértelműen meghatározott üzleti cél és üzleti stratégia, valamint ezekkel összefüggő biztonsági cél és biztonsági stratégia szükséges. Ezekből lehet levezetni a vagyonbiztonsági és informatikai biztonsági célokat és stratégiákat. A biztonsági tudatosság érdekében ezeket a munkatársakkal közölni és számukra folyamatosan elérhetővé kell tenni, továbbá azokat

velük meg kell értetni és általuk el kell fogadtatni. E feladat elvégzése kisvállalat esetében is a tulajdonosi vagy igazgatói (vezetői) körre hárul.

A kisvállalati biztonságirányítás olyan módon valósul meg, hogy

- a vállalati biztonságirányítást a top menedzsment szintjén kell ellátni, mivel a biztonsági célok és a biztonsági stratégia alapját az üzleti célok és üzleti stratégia képezik, míg
- a biztonság menedzselése (végrehajtása) a biztonsági vezető (menedzser) szintjén történik.

Tehát elfogadhatatlan az az álláspont, hogy a biztonsági vezető egyedül felelős a biztonság irányításáért és annak végrehajtásáért.

10. A kisvállalatok biztonsági auditálása

A biztonsági audit magas szintű auditálási szempontjait a 2. pontban említett CSB táblázatok 39 szempontja alapján lehet megállapítani. Az MSZ ISO/IEC 17799 szabványból pedig következnek azok az auditálási szempontok, amelyeket a 39 magas szintű auditálási szemponton túl érdemes még az auditor ellenőrzési listájára felvenni. Természetesen előfordulhat, hogy a kisvállalat menedzsmentje egyes szempontoknak megfelelő védelmi intézkedéseket nem tett meg, illetve ennek kockázatát a menedzsment felvállalta. Ezeket az audit kezdete előtt az auditorral a menedzsmentnek közölni kell.

A külső független biztonsági auditot célszerű 3-4 évenként elvégeztetni. A váratlan biztonsági események kapcsán felmerült ellenőrzéseket, az okok és a következmények feltárását, a belső ellenőr feladata elvégezni.

11. Kisvállalati biztonsági rendszer értékelése

A biztonsági rendszerben megvalósított védelmi intézkedések a kisvállalat számára meghatározható erősségű biztonságot biztosíthatnak. A biztonsági rendszer erősségétől függ, hogy milyen mértékű támadások visszaverésére képes. Az értékelésre az ISO/IEC 15408-1, 2, 3 szerinti, „Az IT biztonság értékelésének közös szempontrendszere” tárgyú szabvány szolgál. A szabvány a termékek biztonsági minősítését szolgálja (a Common Criteria 2.1 alapján készült, és magyar szabványként is kiadták, MSZ ISO/IEC 15408). Az értékelést és ezt követően a tanúsítást akkreditált szervezetek is végezhetik, amely szervezetek működését a szabvány kapcsán alakult nemzetközi bizottság hagyta jóvá. Ilyen szervezet, illetve annak módszertana, miután hazánk csatlakozott a nemzetközi együttműködéshez, Magyarországon előkészítés alatt áll.

A kisvállalatok azonban csak korlátozott lehetőségekkel rendelkeznek, így ezeket a követelményeket nem tudják teljesíteni. Számukra a CBS-ből kiindulva, csak kompromisszumok árán kialakított biztonsági rendszer érhető el.

A rendszerszintű biztonságot a COBIT 3 Érettségi Modell alapján lehet elvégezni. Hazánkban nagyon elterjedt a BS 7799, illetve az ISO/IEC 17799 megfeleléség igénylése. Az eddig írtak alapján belátható, hogy a kisvállalatok biztonsági rendszere erősségének értékelésére a CBS megfeleléség vizsgálata szolgálhat. A vizsgálat eredménye lehet a rendszer „megfelelő”, „nem teljesen megfelelő, de kielégítő”, és „nem megfelelő” minősítése.

12. Mellékletek

12.1. Biztonsági intézkedési terv

Az alábbi vázlat ajánlás a kisvállalatok Biztonsági Intézkedési Tervére (BIT), amely egyaránt vonatkozik a kisvállalat üzleti (papír alapú) és információ (elektronikus alapú) rendszereire.

VÁZLAT:

1. A kockázatok elemzése (szervezési, fizikai, logikai)
2. Az elhatározott védelmi intézkedések (szervezési, fizikai, logikai)
3. A védelmi intézkedések beszerzése, átvétele, üzemeltetése
4. Az üzletmenet-folytonosság biztosítása
5. A biztonsági szervezet és működése
6. A biztonság ellenőrzése (belső, külső)
7. A biztonsági események kezelése
8. További szabályozások:
 - Titokvédelmi osztályozás (személyes és közérdekű, valamint üzleti adatok, eszközök, helyiségek)
 - Programváltozás kezelés
 - Erőforrások selejtezése
9. ABIT
 - Oktatása
 - Karbantartása

A hatályba lépés időpontja

Dátum

Első számú vezető aláírása

12.2. Ellenőrzési lista interjúkhoz

Az interjúk ellenőrzési listáját, a szemlék ellenőrzési listáját, a szabályzatok ellenőrzési listáját a gyakorlatban teszteltük, és azok kiállták a próbát.

1. Azonosítani kell a kritikus üzleti folyamatokat.
 - Védni kell az IT rendszert a helytelen felhasználás és az adatvesztés ellen
 - Az üzleti szolgáltatások, amelyeknek rendelkezésre kell állni
 - A bizalmas üzleti tranzakciók, amelyeket védeni kell
2. Megfontolandó biztonsági követelmények:
 - Ki férhet hozzá és módosíthat adatokat?
 - Ki és milyen engedély alapján módosíthat egy jogosultság beállítást?
 - Milyen adatok megőrzése (mentése) történik?
 - Mentési rend? Mentések hány példányban készülnek?
 - Mentések őrzési helye?
 - Milyen informatikai háttér rendszer áll rendelkezésre, ill. biztosítása szükséges?
 - Milyen rendelkezésre állás van, illetve kell?
 - Az elektronikus tranzakcióknál, milyen hitelesítés, és ellenőrzés van?
3. Meg kell határozni a kisvállalati menedzsment és a biztonsági menedzsment felelősségeit:
 - A felelősségeket meghatározták-e, közzétették-e, és azt az érintettek megértették-e?
 - Ismerik-e annak a veszélyeit, ha egy személyhez koncentráltan túl sok szerepet és felelősséget rendelnek hozzá?
 - Gondoskodnak-e azokról az erőforrásokról, amelyek a felelősségek hatékony gyakorlásához kellenek?
4. Következétesen meg kell értetni és rendszeresen beszélni kell azokról az alapvető szabályokról, amelyek a biztonsági követelmények implementálása és a biztonsági események megválaszolása témákban merülnek fel. Megállapították-e a biztonsággal összefüggő folyamatosan elvégzendő feladatokat? Emlékeztetik-e az alkalmazottakat a biztonsági kockázatokra és az ő személyes felelősségükre? Van-e rendszeres oktatás?
5. Vizsgálják-e a szerződéssel foglalkoztatottak referencia adatait?
6. Ellenőrizik-e a szerződéseket, hogy azok a szükséges biztonsági követelményeknek megfelelnek-e?

7. Gondoskodnak-e arról, hogy az alapvető biztonsági feladatok ne egyetlen erőforrástól függjenek?
8. Azonosították-e, hogy minden vállalati intézkedés megfelel a biztonsági követelményeknek, a privacy-nak, a szellemi jogoknak és más jogi, szerződéses, biztosítási kötelezettségeknek? Tudatában van-e minden alkalmazott e területeken a saját felelősségével?
9. Készítettek-e kockázatkezelési tervet, és abban meghatározták-e a jelentős kockázatokat?
10. Biztosított-e az alkalmazottak biztonsági tudatossága?
11. Biztosítottak-e költséghatékony eszközök az azonosított kockázatok menedzselésre (háttér rendszer, hozzáférés ellenőrzés, vírusvédelem, tűzfalak stb.)?
12. Meghatározták-e a biztonságpolitikát, és az összhangban van-e az aktuális rendszerrel?
13. Biztosított-e külső támogatás (megfelelő referenciával rendelkező szerződéses szerviz /SLA/, tanácsadás)?
14. Megfelelően támogatja-e a technológiai infrastruktúra a biztonsági rendszert (automatizmusok)?
15. Biztosítva van-e a biztonsági infrastruktúrának a védelme? Távfelügyelet biztosított-e?
16. Azonosítják-e és monitorozzák-e a szükséges biztonsági patch-eket?
17. Megtörténik-e az állomány biztonsági oktatása? Vannak-e biztonsági gyakorlatok? Dokumentáltak-e ezek?
18. Tesztelik-e a biztonsági rendszer funkcionális és működési követelményeit változások esetén? Miként integrálódnak az új biztonsági megoldások a létező rendszerbe? A működő éles rendszert nem szabad tesztelni.
19. Összevetik-e a teszteredményeket az üzleti céllal és biztonsági követelményekkel a végső biztonsági megoldás elfogadását megelőző értékeléskor? Bevonják-e az állományt az értékelésekbe?
20. Értékelik-e minden változtatáskor (patch-ek telepítésekor is) az érzékeny adatok integritását és az adatvesztés kockázatát?
21. Naplózzák-e a változtatásokat a kritikus változásokat követően?

22. A belső és külső szolgáltatási szint megállapodások (SLA-k) kielégítik-e a biztonsági követelményeket?
23. Meghatározták-e a külső szolgáltató professzionális képességével szemben támasztott követelményeket?
24. Milyen módon és mértékben függ a külső szolgáltató a biztonsági követelményektől? Képes-e a külső szolgáltató a folyamatosságot biztosítani?
25. Azonosították-e a kritikus üzleti folyamatokat és információkat, valamint azok erőforrásait, amelyek szolgálják azokat. Biztosított-e az erőforrások rendelkezésre állása biztonsági esemény bekövetkezése esetén?
26. Megoldottak-e biztonsági események esetére az alternatív feldolgozási folyamatok, valamint a normál feldolgozás helyreállítása? Miként kommunikálják mindezt az ügyfelekkel és a szállítókkal?
27. Meghatározták-e a visszaállításhoz szükséges kritikus file-okat, dokumentációkat? Biztosított-e azok megfelelő védelem mellett történő külső tárolása).
28. Korlátozták-e az alkalmazottak és a szolgáltatók IT rendszerhez történő hozzáférését egy megfelelő jogosultsági rendszer kialakításával?
29. Milyen módon történik a felhasználók IT rendszer által történő hitelesítése (jelszavak erőssége, biztonsági tokenek alkalmazása)? Ellenőrizik-e az accountokat (azonos személy végzi-e).
30. Hol és védetten őrzik-e a jelszavakat?
31. Naplózzák-e és jelentik-e a biztonsági eseményeket?
32. Biztosított-e a partnerek felé az elektronikus tranzakciók esetében a hitelesség és a bizalmasság? Biztosított-e a szerződéses kötelezettségeknek való megfelelés?
33. Jogtiszta szoftvereket használnak-e? Aktív és naprakész-e a vírusvédelem?
34. Rendelkeznek-e licencnyilvántartással?
35. Meghatározták-e az elektronikus kommunikáció során megengedett üzeneteket? Megfelelően konfigurálták-e a tűzfalat?
36. A hardware és software erőforrásokról naprakész leltárt vezetnek-e?
37. Rendszeresen ellenőrzik-e, hogy az installált software-ek hitelesek és jogtiszták-e?

38. Ellenőrzik-e a beérkező adatok sértetlenségét (pontosságát, teljességét, érvényességét)?
Az ellenőrző tranzakciók hitelesek nem letagadhatók legyenek.
39. A biztonság-érzékeny outputokat csak a jogosultak kaphatják-e meg?
40. Meghatározták-e az archiválási kötelezettségeket a dokumentumokra, adatokra, software-ekre? Gondoskodtak-e az archivált adatok visszakereshetőségéről?
41. Gondoskodtak-e az IT rendszer fizikai biztonságáról? Esetleg külső tanácsadót is igénybe vesznek?
42. Kiterjed-e a fizikai védelem a mobil és adathordozó eszközökre? Hogyan védik ezeket megsemmisítés, lopás és véletlen elvesztés ellen?

Irányítás, kockázat, megfelelés (GRC)

Vasvári György CISM

Információs Társadalomért Alapítvány
1507 Budapest, Pf. 213
Telefon: +36-1-279-1510, Fax: +36-1-279-1511
e-mail: gvasvari@tiphaz.hu

Absztrakt

A korszerű szervezeti, vállalati biztonság holisztikus (teljes körűség) szemlélettel készülhet el. Azaz a vállalati szinten kell, átfogóan az irányítást (governance, G), a kockázat (risk, R) menedzsmentet, és a szabványoknak, jogszabályoknak való megfelelést (compliance, C) kidolgozni, biztosítani. Az integrált vállalati szintű GRC-t rendszeresen auditálni és éves terv alapján folyamatosan belső ellenőrizni kell.

Kulcsszavak: fogalmak (concepts), megvalósítás (compliance), GRC auditálás (GRC audit)

1. Bevezetés

Az utóbbi időben egyre több olyan esemény történt, hogy az események sora új helyzetet, új irányzatot jelzett a szervezetek, vállalatok életében. Ennek következtében egy paradigmaváltásra van szükség, és a világ erre a SOX (USA), BASEL II. (bankok) és az egyes országokban egy irányba mutató intézkedésekkel reagált. Új fogalmakkal, módszerekkel kellett megismerkedni és következtetéseket levonni.

A) Ilyenek például

- A vállalatnak, szervezetnek az irányítása (Governance),
- A kockázat menedzsment (Risk management),
- A megfelelés menedzsment (Compliance management).

B) Ennek megfelelően új igények jelentkeztek, mint például

- Az integrált GRC
- A vállalati szintű kockázat menedzsment (ERM),
- Vállalati szintű biztonságmenedzsment (ESM).

C) Az új intézkedések arra hivatottak, hogy szolgálják

- A vállalat hírnevének, a márkának a védelmét,
- Az érdekeltek (stakeholders), a beruházók, a jog és a szabályozások alkotói, a vevők, a fogyasztók megnövekedett igényeit,
- Az értékteremtés és így a teljesítmény növelés követelményeit,
- A vállalat, szervezet fokozott védelmét az üzletment zavarai, a működés megszakadása ellen és a válságmenedzselés lényeges javítását,
- A munkatársak kultúrájának (biztonsági kultúrájának) emelését.

2. A GRC értelmezése

GRC mozaik szó, amely az eddig függetlenül működő Governance, Risk és Compliance tevékenységek első betűiből áll.

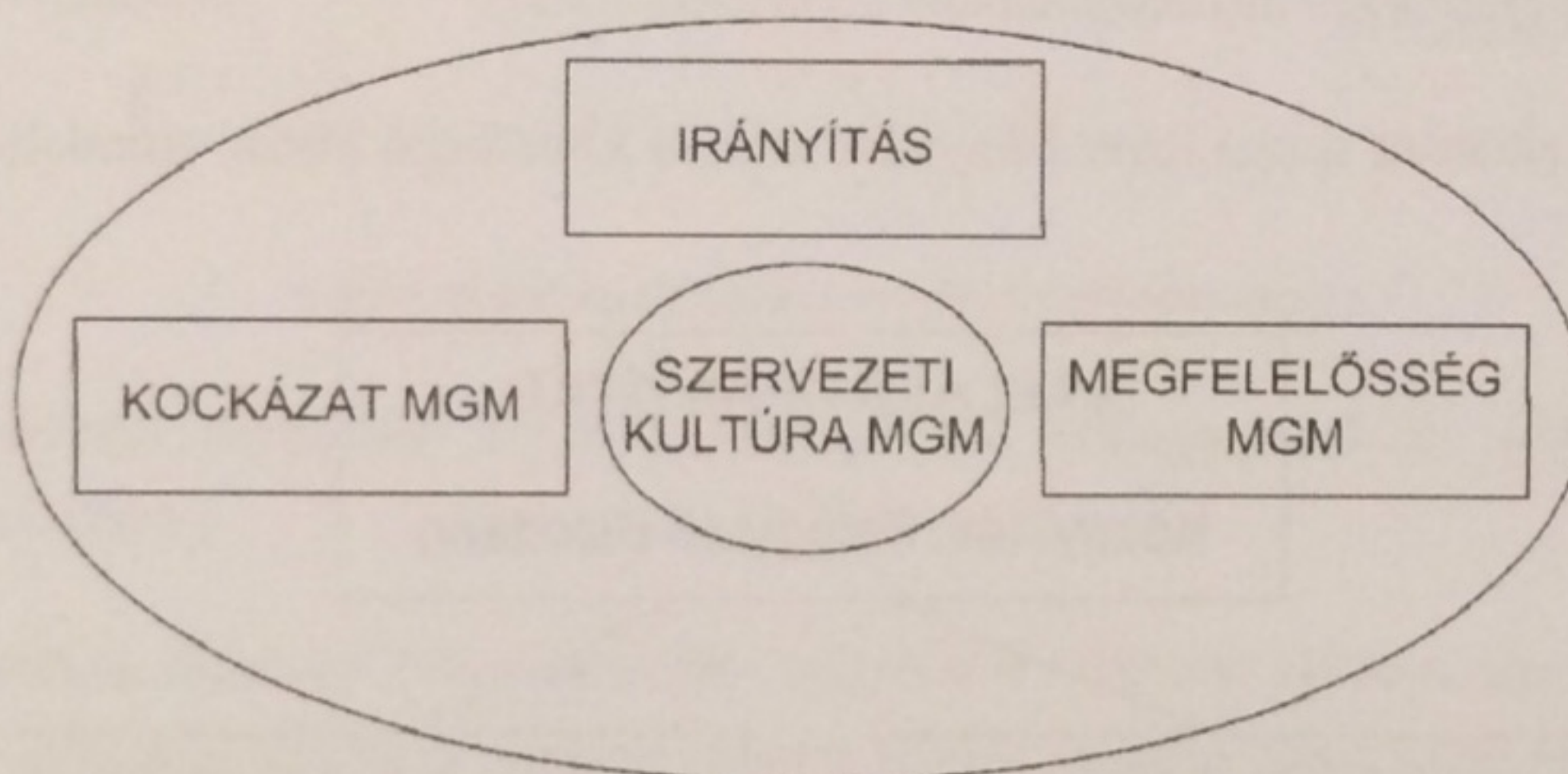
2.1. Alapfogalmak

- Irányítás (Governance) a menedzsment felelősségének és a szervezet átláthatóságának a megteremtése a szervezet által használt eljárások meghatározásával, a politikák és a folyamatok állandó kezelése és követése végett. A megfelelő irányítási stratégia szerint az üzleti tevékenységeket figyelő, követő rendszert hoznak létre, hogy biztosítsák a megfelelő intézkedéseket a meghatározott politikák szerint, és korrigálják a szabályok figyelembe nem vételét vagy félremagyarázását.
- Kockázat menedzsment (Risk management) egy folyamat, amelyben a szervezet meghatározza a kockázati étvágyat (risk appetite), a szervezet által elviselhető kockázatok összegét, azonosítja a lehetséges kockázatokat és az egyes kockázatok elviselhető mértékét (risk tolerance) a szervezet céljainak megfelelően. A kockázat menedzsment felhasználja a belső ellenőrzést a kockázatok vállalati szintű kezelése és csökkentése céljára.
- Megfelelőség (Compliance) a jogszabályoknak, az ipari követelményeknek és a belső szabályozásoknak való megfelelésegről gondoskodás a folyamatok, politikák és ellenőrzések rögzítésével és megfigyelésével.
- Integráció rendszerezett, a követelmények, politikák, ellenőrzések és a szabályok megsértésének összehangolt kezelése, a hatékony kommunikációt szolgálva, a szabályok megsértése lehetőségének kiküszöbölése céljából.
- Kultúra, etika az emberiség által létrehozott anyagi és szellemi értékek összege, egy civilizáció, egy ország, egy szervezet jellemző tulajdonságai, műveltségi színvonala és viselkedés kultúrája.

- Biztonság egy társadalom, szervezet kedvező állapota, amelynek megváltozása nem valószínű, de nem is kizárt. A szervezet küldetésének a teljesítése nemcsak a megtett intézkedésektől függ, hanem a munkatársak, egyének személyi sajátosságaitól (kultúra, etika). A nem biztonságos nem reális információk, magatartások katasztrofálisan befolyásolhatják a biztonságot, és azt hogy a szabályozások miként segítik a rendeltetésszerű végrehajtást.
- A tudatosság meghatározott kérdésekben a kérdés ismerete, tekintetbe vétele, az azzal való törődés, és az annak megfelelő cselekvés.

2.2. Az alapfogalmak összefüggése

Az OCEG (Open Compliance and Ethics Group) az összefüggéseket [5] az 1. ábrán mutatja be egy integrált GRC esetében. Látható, hogy a G, R és C egy körön belül helyezkedik el az integráltságra mutatva, míg a középen elhelyezett kultúra a szervezet, a szervezeti egységek, a munkatársak kultúrája, amely alapját képezi az integrált GRC működésének.



1. ábra: Összefüggések egy integrált GRC esetében

2.3. Az integrált GRC szerepe

A szervezet életében az irányítás, a kockázat menedzsment és a megfelelőség menedzsment az üzleti cél, a küldetés hatékony és eredményes megvalósítását szolgálják, amelyek mértékét a szervezeti kultúra, azon belül a szubkultúrák (pl. szervezeti egységek, szakmák kultúrája és a biztonsági kultúra) alapvetően befolyásolják. Azaz az integrált GRC létrehozása ezek összehangolt irányítását, integrálását indokolja, a küldetés megvalósítása, a működési zavarok, problémák minimálisra csökkentése érdekében.

2.4. Az integrálás hatása a szervezetben

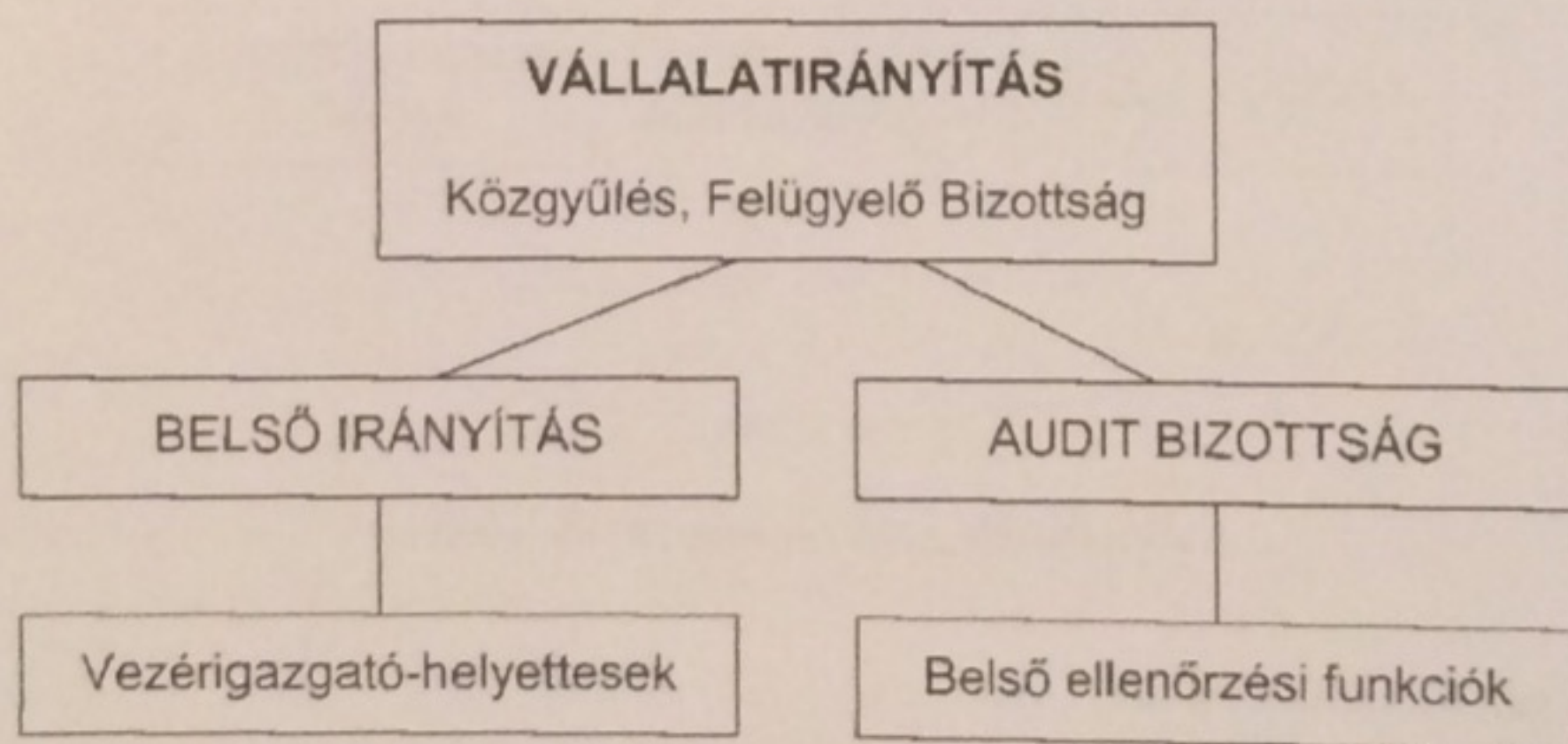
A GRC integrálása szervezeti intézkedéseket is igényel. Ezek az intézkedések egyértelműen a szervezetnek az irányításától a vezetési koncepció megváltoztatását igénylik. Azaz paradigmaváltást. Ezeket a szervezeti változtatásokat, az alábbi szervezeti ábrán mutatjuk be.

Az integrált vállalatirányítás (G), kockázatmenedzsment (R), megfelelőség (C) és vállalati kultúra elősegíti és támogatja a szervezet, vállalat teljesítményét, amelyet, mivel belső ellenőrzési funkciók, célszerű összekapcsolni a belső ellenőrzési tevékenységgel is. A belső ellenőrzési funkciókat, az Audit Bizottság irányítja, és a felső vezetéshez tartoznak közvetlenül.

A belső ellenőrzési funkciók:

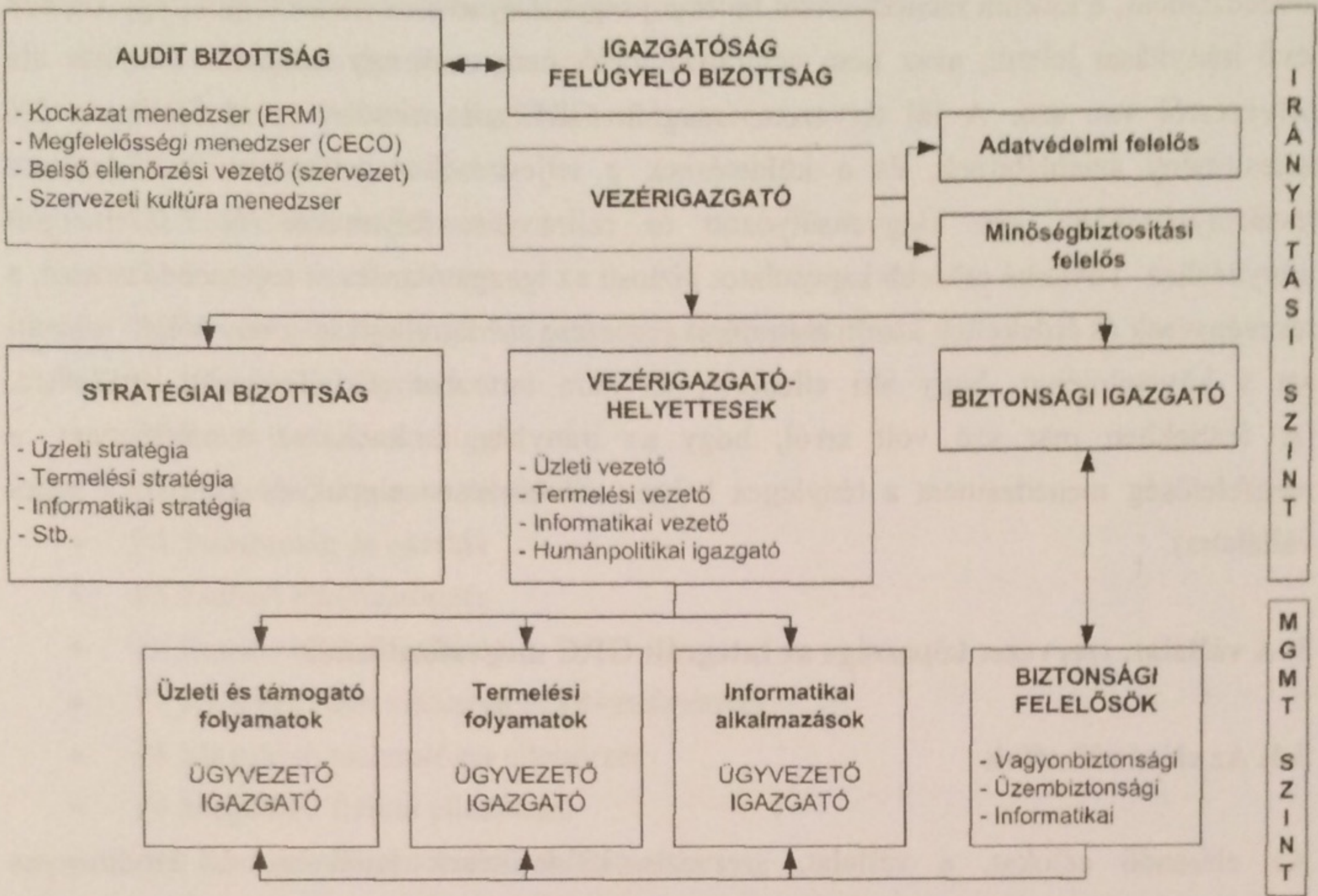
- Kockázat menedzsment,
- Megfelelőség menedzsment,
- Szervezeti kultúra menedzsment,
- Belső ellenőrzés menedzsment és szervezet.

Az integrálás hatására a szervezet irányítási része a következő ábrán szemléltetett módon alakul:



2. ábra: A szervezet irányítási része az integrálás hatására

A szervezetirányítás szintek szerinti megoldását mutatja be az alábbi ábra.



3. ábra: A szervezetirányítás szintek szerinti megoldása

Az ábrán található rövidítések: ERM (Enterprise Risk Manager), CECO (Chief Ethics and Compliance Officer).

Amint az ábrákon látható a vállalatirányítás egyrészt a belső irányításon, másrészt az Audit Bizottságon keresztül végzik a szakterületekért felelős vezérigazgató helyettesek, másrészt a belső ellenőrzési funkciókhoz tartozó menedzserek irányítását. Ez a szervezeti konstrukció tehát azon az elven épül fel, hogy a kockázat menedzsment, a megfelelőség menedzsment (amelyet a CECO, a Chief Ethics and Compliance Officer végez) és a kultúra menedzsment gyakorlatilag ellenőrzési tevékenységek, hiszen a kultúra, a megfelelőség és a kockázat menedzsment meghatározott helyzetek, állapotok, tevékenységek, szabályozások és azok megvalósításának ellenőrzésén alapulnak, míg a teendőket egy-egy programban határozzák meg, amelyet szintén ellenőrizni kell. A vezérigazgató (aki résztvevője a Közgyűlésnek is) végzi a belső irányítást végző vezérigazgató helyetteseken (esetleg közvetlen igazgatókon) keresztül a vállalat irányítását. Az Audit bizottság elnöke tagja a Felügyelő Bizottságnak és az Audit Bizottság tagjai pedig az egyes belső ellenőrzési funkciók vezetői.

Az ábra értelemszerűen nem tartalmazza a harmadik, a végrehajtási szintet, azaz az igazgatókat, osztályvezetőket és a munkatársakat.

A fentiekből egyértelműen az következik, hogy az integrálás, az irányítás, a megfelelőség menedzsment, a kultúra menedzsment tevékenységek folyamatos összehangolt, egy kézben lévő irányítását jelenti, azaz nem centralizációról, nem csak egy központi irányítás alá helyezésről van szó. A jól tervezett, integrált GRC utat biztosít az elvi alapon álló teljesítmény szemléletnek, és a küldetésnek a teljesítéséhez szükséges menedzsment tevékenységekhez, egy kiegyensúlyozott és célirányos, folyamatos és összehangolt irányításhoz. Továbbá erősebb kapcsolatot biztosít az igazgatótanács, a top menedzsment, a részvényesek és érdekeltek között a stratégia tervezése és végrehajtása során. Végül teljesíti azt a követelményt, hogy aki ellenőriz, az nem tartozhat az ellenőrzött területhez. (A fentiekben már szó volt arról, hogy az irányítás, a kockázat menedzsment, a megfelelőség menedzsment a tényleges helyzet ellenőrzésén alapul, és kiterjed a teljes vállalatra).

3. A vállalat, szervezet képessége az integrált GRC megvalósítására

3.1. Az elérendő célok

Az elérendő célokat, a vállalat, szervezet küldetésének hatékony és eredményes megvalósítását a szervezet stratégiája határozza meg. Ennek kidolgozása és a döntés erről a Board, a top menedzsment feladatát képezi. Mint az előbbiekben említettük, ehhez az integrált GRC alapvető segítséget nyújthat. Az OCEG (Open Compliance and Ethics Group) kidolgozta az úgynevezett képesség modellt [1], amely részletes, tapasztalatokon alapuló eljárást, intézkedés sort határoz meg.

3.2. A GRC képességi modell

A GRC képességi, a végrehajtásra, megvalósításra alkalmassá tétel modellje, a „Red book” (lásd [5]) a következő elemekkel, teendőkkel foglalkozik, amelyek az integrált GRC megvalósításához vezetnek.

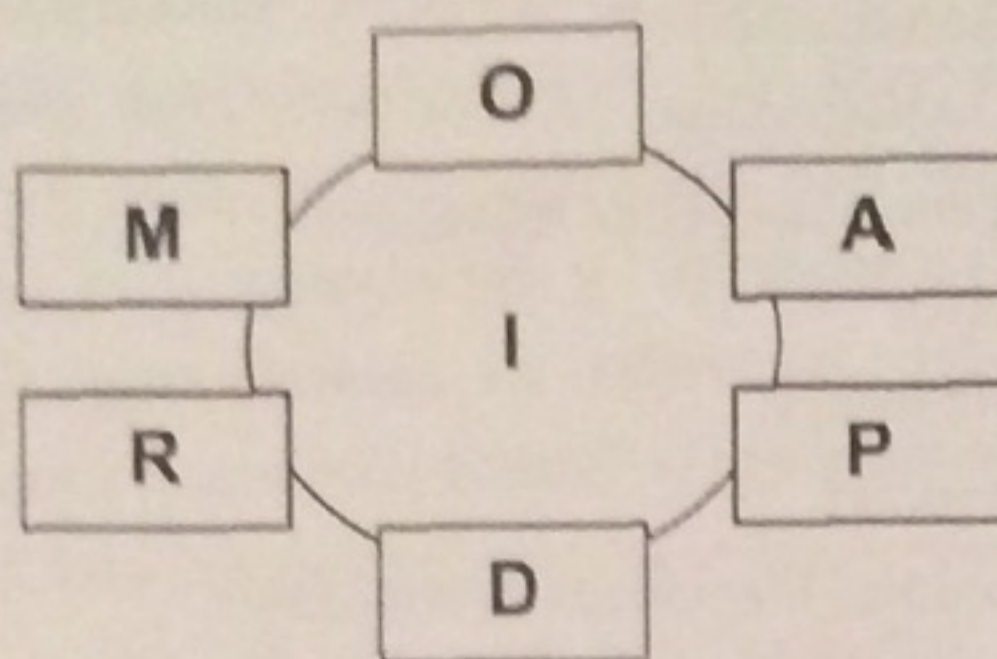
- M (Monitor and measure) Megfigyelés és mérés
- M1 Összefüggés megfigyelés
- M2 Teljesítmény megfigyelés, értékelés
- M3 Rendszeres fejlesztés
- R (Respond and resolve) Válaszadás és megoldás
- R1 Belső vizsgálat és kutatás
- R2 Harmadik fél érdeklődése és kutatása
- R3 Krízisre válasz és kutatás
- R4 Követés és fegyelem
- I (Inform and integrate) Informálás és integrálás

- I1 Információmenedzsment és dokumentáció
- I2 Belső és külső kommunikáció
- I3 Technológia és infrastruktúra
- D (Detect and discern) Észlelés és felismerés
- D1 Forródrót és jelzés
- D2 Érdeklődés és felmérés
- D3 Feltárás és ellenőrzés
- P (Prevent and promote) Megelőzés és támogatás
- P1 Vezetésszabályozás
- P2 Belső üzleti összefüggés
- P3 Megelőző folyamat ellenőrzés
- P4 Tudatosság és oktatás
- P5 Emberi tőkeösztönzés
- P6 Emberi tőke ellenőrzés
- P7 Az érdekelték viszonya és követelményei
- P8 Megelőző technológia ellenőrzés
- P9 Megelőző fizikai ellenőrzés
- P10 Kockázat finanszírozás és biztosítás
- A (Asses and align) Értékelés és fontossági sorba állítás
- A1 Kockázat azonosítás
- A2 Kockázat elemzés
- A3 Kockázat optimalizálás
- O (Organize and oversee) Szervezés és áttekintés
- O1 Eredmény és kötelezettség vállalás
- O2 Szerepek és felelősségek
- O3 Szemlélet és számonkérés
- C (Context and culture) Összefüggés és kultúra
- Külső üzleti összefüggés
- Belső üzleti összefüggés
- Kultúra
- Értékelés, célok

A GRC modell alkalmazásának várható eredményei:

- Üzleti célok elérése,
- Fejlett szervezeti kultúra,
- Az érdekelték növekvő bizalma,
- A szervezet felkészítése és védelme,
- A vezetés vizsgálata és motivációja.

A GRC modell az alábbi ábrán látható:



4. ábra: A GRC modell

A GRC képesség modell alkalmazásakor a 8 eleméhez rendelt egyes tevékenységekhez megadott feladatokat kell végrehajtani.

4. Az integrált GRC auditálása

4.1. A GRC program folyamatos, rendszeres ellenőrzése

Az igazgatótanácsnak és a menedzsmentnek rendszeresen értékelnie kell a GRC képességi modell tervezése és megvalósítása helyzetét. Ez naprakész követést, a tevékenységek megfigyelését, azaz a modell munkák, folyamatos, rendszeres ellenőrzését igényli. Azonban ez az ellenőrzés nem csak a modellel kapcsolatos munkák követését jelenti, hanem lehetőséget kínál a menedzsment tevékenységének fejlesztésére is.

4.2. A belső ellenőrzés célja

A cél természetesen, a GRC képesség modell hatékony alkalmazása, a szervezet stratégiájának megvalósítására. Ehhez szükséges, hogy a board és a menedzsment

- megerősítést kapjon arról, hogy megfelelően halad a képesség modell alkalmazása. Ugyanakkor a végrehajtóknak is szükségük van tevékenységük megfelelőségének a megerősítésére,
- ehhez világos, a szervezet stratégiájának megfelelő célkitűzésekre van szükség, amelyek megvalósítását a GRC képességi modell határozza meg,
- továbbá meg kell határozni az ellenőrzés hatáskörét, hogy mire terjed ki.

A kulcs célok kidolgozásánál érdemes a következőket is figyelembe venni:

- a képesség modell alkalmazási program megfelelő garanciát nyújt-e a szervezet stratégiai céljainak teljesítésére,
- a program menedzsment jól dokumentált-e, és megfelel-e a szervezet igényeinek,
- a program implementáció hatékony-e, és a jelentési rendszer szabályozott-e, illetve biztosítja-e a teljesítés pontos tükrözését.

4.3. A belső ellenőrzés lépései

A belső ellenőrzés következő fázisból áll:

- a lépések tervezése,
- a helyzetfeltárás,
- az értékelés és
- a szükséges intézkedések javaslatának kidolgozása.

A tervezési fázis alatt meg kell győződni arról, hogy

- az audit cél megfelel-e a szervezet garanciális kötelezettségeinek,
- a kulcs kockázatok az audit tervnek a készítésénél figyelembe vették-e,
- a tervezők jól értelmezték-e a GRC képesség modellt.

A végrehajtásnak a modell egyes elemeire és azokon belül a tevékenységek maradéktalan végrehajtására kell kiterjednie. Az értékelésnek a képesség modell megvalósítási programjának teljesülését kell vizsgálnia, és a feltárt hiányosságok megszüntetésére javaslatokat kell tennie.

4.4. A belső ellenőr szükséges képzettsége

A belső ellenőrnek CISA, vagy annak megfelelő, regisztrált minősítéssel kell rendelkeznie (Pl. NJSZT ellenőrzési szakértő).

5. A megvalósítás

5.1. A kockázatok

A megvalósításkor általánosságban, tehát szervezettől, vállalattól függetlenül, a következő kockázatok merülhetnek fel:

- Az integráció egyes munkatársak érdeksérelmével járhat. A sértett munkatársak nem segítik megfelelően a megvalósítást.
- Az integráció a szervezetben működési zavarokat okozhat.
- A működési zavarok komoly fenyegetést jelenthetnek a szervezet image-ére nézve.
- Csökkenhet a szervezet, vállalt éves eredménye.

5.2. A Megvalósítási program

- A megvalósításra programot, tervet kell készíteni.
- A sikeres megvalósítást fenyegető kockázatokat a tervkészítés megkezdése előtt fel kell mérni és értékelni kell.
- Képzést kell tartani, amely nem csak a megvalósításhoz szükséges, hanem lehetőséget ad a munkatársak reakcióiból megállapítani a várható kockázatokat.
- A tervnek a fokozatos lépések elvét kell követnie, és minden lépésnél tervezni kell háttér megoldásokat a működési problémák felmerülése esetére.

Irodalomjegyzék

- [1] Governance & Compliance Conference. Measuring value, Managing Risk Assuring Compliance. ISACA.
- [2] GRC Capability Model. OCEG.2008.
- [3] D. Swanson: Auditing Compliance & Ethic. ACCA Home Page.
- [4] ERM Integrated Framework Executive Summary. COSO. 2007.
- [5] Integrated Governance, Risk Management, Compliance, and Culture. OCEG. 2006.
- [6] Vasvári György: Vállalati (szervezeti) kockázat menedzsment. Információs Társadalomért Alapítvány. 2008.

Információs társadalom, információs hadviselés

Vasvári György CISM

Információs Társadalomért Alapítvány
1507 Budapest, Pf. 213
Telefon: +36-1-279-1510, Fax: +36-1-279-1511
e-mail: gvasvari@tiphaz.hu

Absztrakt

Az információs technológia gyors fejlődése, elterjedése, az információs társadalom alakulása a háborúk, a hadviselés egy új változatának a megjelenését eredményezte, amely a civil szférában, a gátlástalan feleket motiválta a katonai, politikai, célokön túl a gyakran sikeres civil célok elleni alkalmazásra. A civil célokat, fenyegeti a kiberterroristák agressziója is. Ugyanakkor ez a helyzet folyamatos védekezést igényel. A védekezés sikere az információs hadviselésben, igen erősen függ a társadalom, biztonsági kultúrájának színvonalától is.

Kulcsszavak: információs társadalom, információs háború, információs hadviselés, időhadviselés, kiberterrorizmus, biztonsági kultúra

1. Előzmények

Az ezredfordulóra kialakult az információs társadalom és mondhatjuk, hogy már nem csak a szakemberek, hanem a társadalom egyre nagyobb része a társadalom egyik erőforrásának tartja, és alkalmazza az információt, az információs rendszereket. Az lehet vita tárgya, hogy mit értünk információs társadalom alatt, csak a tény nem, hogy az informatika az üzleti, katonai, politikai, privát világot egyre jobban átszövi, egyre inkább nélkülözhetetlen eszköze lesz.

Az informatika elterjedésével, pedig új kihívásokkal, az új technológia felkínálta lehetőségekkel élők, visszaélők egyre számosabban lesznek. Az Institute for the Advanced Study of Information Warfare (IASIW) meghatározása szerint ma a következő tipikus fenyegetésekkel kell számolnunk:

- katonai hadviselés,
- terrorizmus és bűnözés,

- növekvő kockázatok,
- konfliktusok,
- járványok,
- környezeti problémák, túlnépesedés,
- információs hadviselés (information warfare).

Az információs háború (information war) a hagyományos háború támogatása, ha tetszik egyik, a szemben álló fél ellen alkalmazott, átfogó célú támadási módszer. A [4] szerint, pedig az információs háború a háborúval párhuzamosan folyik, a háború új fajtája, amelynek a célja a szemben álló fél távközlésének, számítógépes hálózatainak, számítógépeinek lekapcsolása, szétrombolása, valamint az áramellátás, elektronikus rendszerek, eszközök kikapcsolása.

Az információs hadviselés, az információs háború része, akár egyedi célpontok ellen is, az információs infrastruktúra, az információs rendszerek ellen irányuló támadás. Így a civil szférában ilyen támadás békében is megtörténhet, megtörténik.

Dr. Iván Goldberg (IASIW) az információs hadviselést a következőképpen határozta meg:

Az információs hadviselés az informatikának a támadó vagy védekező alkalmazása, az információ rendszerek leállítása, felhasználása, feltárása, egy ellenfél információs vagy információ bázisú folyamatának, információrendszerének rombolása, információ hamisnak nyilvánítása saját rendszerének a védelme mellett. Az ilyen akciókat az ellenféllel szemben tervezik, üzleti, katonai, politikai, privát haszon, előny elérésére.

2. Katonai információs hadviselés

Az információs hadviselés [4] szerint, a hagyományos háborúval párhuzamosan folyó támogató vagy védő jellegű információs háború céljaiért folyó információs műveletek összessége. Az informatikai eszközök katonai célokra történő felhasználása, egyértelműen a háború, a hadviselés új formáját, kiterjesztését jelenti, továbbá átfogó jelegű. A különböző hadviselési módokat [4] az alábbiak szerint adja meg, történelmileg előrehaladó sorrendben:

- szárazföldi hadviselés,
- tengeri hadviselés,
- tengeralattjáró hadviselés,
- légi hadviselés,
- légvédelmi hadviselés,
- különleges hadviselés,
- lélektani hadviselés,

- vegyi hadviselés,
- biológiai hadviselés,
- atom hadviselés,
- elektronikai hadviselés,
- kozmikus hadviselés,
- hadszíntéri ballisztikus rakétavédelem,
- ultrafejlett robotikai hadviselés,
- információs hadviselés.

A katona politikai vonatkozásra álljon itt csak néhány példa. Eszerint az 1992-ben a Kuvaitot megszállva tartó iraki csapatok, az ENSZ felszólítás ellenére nem távoztak, majd az USA haderejének támadását egy információs hadviselési eszközökkel végrehajtott akció előzte meg, amely eredményeképpen az iraki számítástechnikai és távközlési rendszerek működésképtelenné váltak. Így az Öböl-háborút tekintik az információs hadviselés első esetének. Továbbiak Koszovó, Csecsenföld, és egyesek szerint a grúziai orosz beavatkozás.

Az információs háború, tehát a ma és jövő háborúinak egy új módja. Azonban rá kell mutatni arra, hogy egész addig, míg nem jelenik meg egy új változat. A korábbi változatokkal szemben azonban törekvésének nem az emberek, az általuk épített világ elpusztítása a cél, hanem a szemben álló fél informatikai eszközeinek rombolással harcképtelenné tétele.

3. Civil információs hadviselés

A civil szférában ma már az informatikai eszközök, rendszerek felhasználása információs fölény megszerzésére gyakori esemény, például:

- anyagi előnyök szerzésére,
- versenytárrsal szembeni előny szerzésére,
- politikai előny szerzésére,
- személyes bosszú végrehajtására,
- kiber terrorcselekmény végrehajtására,
- személyes adatok megszerzésére.

Az információs hadviselésben a támadás az erőforrások (adatok, Infrastruktúra [technológia, támogató eszközök], alkalmazások, és az ember) bizalmassága, sértetlensége, és/vagy rendelkezésre állása ellen irányul, amelynek sikere a támadó (szervezet vagy egyén) támadási potenciáljától, azaz attól függ, hogy a támadó rendelkezésre álló eszközök, a motivációja, és a gyakorlata, milyen erősségűek, és a támadási cél védelme milyen erősségű. Fontos rámutatni arra is, hogy a védelmi módszerek és erősségük, a támadót motiváló tényező.

A támadás folyamata:

- a védelem, a védelem erősségének a felmérése után a támadási cél meghatározása,
- a támadás előkészítése,
- a támadás végrehajtása,
- a támadás eredményének (akár sikeres, akár nem sikeres) értékelése.

Az információs hadviselés lehetséges támadási eszközei ma már igen nagyszámúak. Így például:

- számítástechnikai eszközök (hardver, szoftver), például rosszindulatú szoftverek, mint a vírusok (amelyeknek soha be nem fejeződően megjelenő, új változatai vannak),
- elektronikus támadási eszközök, mint az elektromágneses zavarás, nagy energiájú elektromágneses impulzus besugárzás,
- elektromágneses kisugárzás lehallgatásához eszközök,
- hálózat lehallgatásához, hálózaton futó adatok manipulálásához eszközök.

A támadás lehet aktív, behatoló, mint a fenti felsorolás első két esete, vagy passzív, nem behatoló, mint a harmadik és negyedik példa. Továbbá a támadási célok lehetnek a következők:

- A rombolás:
 - fizikai rombolás (részleges vagy átfogó),
 - logikai rombolás (részleges vagy átfogó),
 - az információ rendszer, a hálózat működésének leállítása.
- Az adatok, programok támadása:
 - átfogó adat, program megsemmisítés,
 - célzott adatok, programok megsemmisítése,
 - célzott adatok, programok módosítása.
- Adatok megszerzése.
- Programok megszerzése.

Az információs hadviselés támadási célpontjait D. L. Carter csoportokba osztja, azt hangsúlyozva, hogy a bűnözés, a számítógépek elterjedésével együtt nő.

Ezek a csoportok a következők:

- a számítógép maga,
- a számítógép egy büntett eszköze,
- a számítógép más büntettel együtt.

A támadási célok, és módszerek rendkívül változatosak, és állandóan fejlődnek, a védelem fejlődését követve, illetve így megelőzve. A támadási módszerek egyes csoportjaira megadunk egy-két példát:

- Rombolás, működésleállítás
 - szabotázs,
 - terroristatámadás,
 - jogosulatlan hozzáférés, behatolás.
- Csalás
 - programmanipulálás,
 - jogosult folyamatok jogosulatlan felhasználása,
 - számlák átirányítása,
 - pénzmosás,
 - illegális tranzakció,
 - adatok megváltoztatása (pl. kórházban elhelyezett betegek adatainak megváltoztatása).
- Eltulajdonítás
 - szoftverek szerzői jogainak eltulajdonítása,
 - berendezések eltulajdonítása,
 - programok másolása harmadik fél részére.
- Emberek támadása
 - humán erőforrások elleni fizikai akciók,
 - személyes adatok megszerzése,
 - a „social engineering” alkalmazása.

Fontos hangsúlyozni, vállalva az esetleges ellenszenv kiváltását, hogy az elkövetők a civil szférában lehetnek szervezetek, vállalatok esetében külső, és belső személyek is.

A példák azt mutatják, hogy ezeket feltétlenül komolyan kell venni. Az emberek reagálása (hivatalos és privát) erre általában kétféle. Egyrészt valóban komolyan veszik, és átgondolt szakszerű, intézkedéseket tesznek, illetve várnak el az illetékesektől. Másrészt válasz nélkül hagyják „a nálam, nálunk ez nem fordulhat elő” nézet alapján. Természetesnek kell azonban venni az egyes emberek egyedi személyiség jegyeit, amelyek számításba vétele hozzásegíthet a helyes védelmi megoldások megtalálásához. Természetesen akkor, ha az információs társadalomban társadalmi, szervezeti, közösségi, egyéni szinteken a biztonsági kultúra felismeri az információs hadviselés milyen fenyegetést jelent, és szükségesnek tartja, elvárja az ellene teendő intézkedéseket. Meggyőződésem, hogy az információs társadalomért az információs hadviselés anyagi, fizikai, lelki összefüggéseinek a vizsgálata nélkül nem lehet célra vezetően tevékenykedni, azt vizsgálni, és következtetéseket levonni.

A fentiekben megadott támadási módszerek, egyben meghatározzák, a védelmi célokat, és ebből következően azt, hogy mire kell megtalálni a védelmi módszereket.

Az információs hadviselés védelmi oldala tehát megkívánja a védelmi intézkedések folyamatos naprakészen tartását, amelyhez alapot a tervszerű, rendszeres kockázatelemzés és a biztonsági szint rendszeres belső ellenőrzése, valamint független, külső auditja adhatja.

Lehet azt vitatni, hogy az információs hadviselés erős kifejezés helyett megfelelőbb a kibernetikai, a cyber bűnözés. Azt azonban, hogy létezik, hogy védekezni kell ellene, vitatni már nem célszerű, pontosabban igen nagy kockázat felvállalását jelent. Az információrendszerek, távközlési hálózatok védelme, napjainkban már számottevő tudományág, amely igen jelentős ipari háttérrel rendelkezik.

Fel kell figyelni arra is, hogy az információs társadalom és az információs hadviselés kölcsönhatásban vannak egymással. Egyrészt mind a kettőt a folyamatos változás jellemzi, másrészt az egyiknél bekövetkezett események, a másiknál is eseményeket vonnak maguk után.

Szükséges felvetni azt, hogy a biztonsági eseményeknél egyesek következetesen kitartanak amellett, hogy egy esemény, egy biztonsági esemény bekövetkezését előre meg lehet egzakt módszerekkel határozni. A „jósnő” kategóriájába tartozó embereket, óriási felelősség terheli a valóságtól eltérő tevékenységük miatt, amely számtalan negatív következménnyel járhat. A valóság viszont az, hogy a társadalomban, de az információs hadviselésben (támadás, védekezés) is, nem a kiszámítottság, hanem a valószínűség határozza meg a kockázat bekövetkezését.

Az információs hadviselés területén a támadási módszerek egyre veszélyesebbek lesznek, amelynek következtében egyre fejlődni fog a védekezés módszere, technikája is. Ez természetesen nem csak technológiai, hanem humán következményekkel is jár, amely kivetül a társadalomra is.

4. Időhadviselés

Az információs hadviselés keretében ma, az időért folyó intenzív küzdelmet az időhadviselés keretében vívják. A szervezeteknek, vállalatok menedzsmentjének döntés előkészítése, döntése és a döntései végrehajtása szempontjából az időigény összessége az időhadviselés tárgya. Ezt nagymértékben befolyásolja a menedzsment biztonsági kultúrája. Természetesen felmerül az időfölény, az előny megszerzésének a témája a lehetséges támadókkal szemben, és ennek eszköze az időigény csökkentése. Az időhadviselés célja tehát a szemben álló féllel, azaz a támadókkal szemben időfölény elérése, a döntés-előkészítés, a döntés, és annak végrehajtásához szükséges idők csökkentése révén.

A támadók például, általában nemcsak a cél ismeretében, hanem adott esetben a hely ismeretében is előnyt szerezhhetnek. Például a profi bankrabló miután mindezeket megismerte, hajtja végre a támadást, amelynek egyaránt lehet fizikai vagy logikai célja. Ugyanakkor azt is tudja, hogy a jogosulatlan behatolás után várhatóan mennyi idő áll rendelkezésére a támadás végrehajtására, a védelmet ellátó erők megérkezéséig.

Erre negatív példa, hogy egy bankrablásnál Budapesten, egy kerületi rendőrkapitányság melletti bankfiókban, a riasztó rendszer egy igen távoli őrző-védő vállalathoz volt bekötve.

A támadás végrehajtására, a támadó rendelkezésére álló idő az alapvető motivációs tényezők egyike. Nem vitás, hogy védelemre a támadó új támadási módszerrel válaszol, és nem mindegy az az idő, amely alatt a támadási cél védelme erre is felkészül. Várható tehát, hogy a jövőben az időhadviselés határozottan megjelenik az információs hadviselés mellett.

5. Kiberterrorizmus

Ma már sajnos nem lehet kizárni, a terrorizmus kibernetikai változatát. Léteznek jól képzett emberekből álló, és jól szervezett terrorista csoportok, amelyek kiberterrorista támadás végrehajtására vállalkoznak, amely egy informatikai agresszió, és irányulhat egy szervezet, vállalat információ rendszere, hálózata vagy annak részei ellen. Okai feltehetően az anyagi, gazdasági, politikai előnyök elérésének szándékai lehetnek. Eredménye fizikai, pénzügyi és/vagy humán károk lehetnek.

A kiberterrorizmus valamely előre megfontolt, politikailag, gazdaságilag motivált támadás információk, számítógép rendszerek, programok és adatok ellen. Valójában elektronikus terrorizmus vagy információs agresszió, amely fizikai vagy extrém pénzügyi, illetve humán kárt okoz. Például fizikai rombolást kívülről elektromágneses impulzus bombával (EMP BOMBS) végrehajtott támadás eredményezheti, amelyben tűz keletkezik, és emberek eshetnek áldozatul.

Később, a 7. pontban megadunk [2] felhasználásával, néhány az információs hadviselés körébe tartozó szakkifejezést, azzal a céllal, hogy konkrét támadó műveletekkel mutassuk be, milyen támadásokra lehet az általánosan ismert vírustámadásokon túlszámítani.

6. Az információs hadviselés és a biztonsági kultúra

A biztonsági kultúra a szervezetek, vállalatok, közösségek, egyének kultúrájának összetevője, a társadalmi kultúra egyik alakítója.

A társadalmi biztonsági kultúra struktúrájának mint a nemzeti biztonsági kultúra egyik elemének egy nagyvonalakban megadott megközelítése, a következő:

NEMZETI KULTÚRA:

- Nemzeti biztonsági kultúra:
 - Rendvédelem,
 - Honvédelem.
- Társadalmi kultúra:
 - Közösségek kultúrája,
 - Szervezetek kultúrája.
- Egyének biztonsági kultúrája:
 - Egyének biztonsági tudatossága,
 - Egyének etikussága,
 - Egyének személyiség jegyei.

A biztonsági kultúra az, amikor az egyének ismerik a biztonsággal kapcsolatos jogaikat, kötelességeiket és érvényesítik ezeket, tesznek érte. Ugyanakkor felismerik a biztonságot fenyegető kockázatokat, és elfogadják az ezek csökkentésére tett intézkedéseket. A biztonsági kultúra meghatározó eleme egy szervezet, amely a társadalom ellenálló képességének kialakítására törekszik.

A biztonsági kultúrát, a biztonsági tudatosságot befolyásoló tényezők:

- a jogszabályok,
- a közösségek elfogadott szabályai,
- a kormányzati intézkedések,
- a közvélemény,
- a politikai és gazdasági hatások,
- a kis közösségek, családok, ahol élnek az emberek,
- az egyének biztonsági ismeretei.

Az egyének kultúrája, biztonsági tudatossága mint a biztonsági kultúrának az alakítója, az információs hadviselés védelmi intézkedéseit tartja szem előtt (ismerve azok be nem tartásának, el nem fogadásának következményeit), elítéli mások részéről az elutasítást, készek álláspontjuk képviselésére, azok alapján az elutasítás elítélésére. A biztonsági tudat velejárója az erkölcsös, etikus viselkedéskultúra is.

Mindebből levonható az a következtetés, hogy az információs hadviselés a védelem oldalán, a társadalom, illetve szervezeteinek, ellenálló képessége az egyének, a társadalom tagjainak, közösségeinek, szervezeteinek a biztonsági kultúráján alapul. A társadalom tehát folyamatosan érdekelt abban, hogy az egyének biztonsági tudatossága megfelelő szinten maradjon, amely az oktatáson, a médián keresztül a szakszerű, a valóságot nem a média anyagi érdekeit szolgáló szenzációhajhászó befolyásoláson nyugszik.

Amennyiben a társadalom képes az információs hadviselést mint a tudomány legújabb eredményeinek alkalmazását, és ezen eredményeknek az életminőséget is javító oldalát felismerni, meg van minden okunk arra, hogy bízzunk az információs hadviselés sikeres megvívásában az egyéntől, a szervezeteken, vállalatokon, és közösségeken keresztül.

Az emberiség történelme folyamán a tudomány előrehaladását, sokszor kemény áron, de végül mindig a maga javára fordította, így az informatika tudománya sem lehet az emberiség boldogulásának megrontója, és ha jól használjuk, akkor napjainkban sem az. Elég talán arra hivatkozni, hogy az informatikával támogatott bankműveletek elterjedése bizonyítja, hogy az azok elleni sikeres támadások ellenére rohamosan növekszik az elektronikus bankműveleteket alkalmazók száma.

A biztonsági kultúra magas színvonalon tartása mellett, az Információ Technológia folyamatosan megjelenő újabb eredményei (például szoftverrel megoldott védelmi intézkedések kivitelezése hardverrel) lehetővé teszik, hogy a szervezetek, vállalatok az információs hadviselésben a védelmüket olyan színvonalon tartsák, amely az információs hadviselésben az ellenük végrehajtható sikeres támadások kockázatát minimálisra csökkenti. A jövő kutatási kérdésének tartom, hogy a Faraday háló milyen erősségű elektromágneses besugárzás (EMP bomba vagy HERF fegyver) ellen véd. Ugyanis egyrészt a hazai informatikai rendszerek elhelyezése ezt a védelmet igen gyakran nélkülözi, másrészt szükséges lenne tisztázni, hogy ezt a kockázatot a jelenleg alkalmazott módszerrel lehetséges-e a minimálisra csökkenteni.

Az információs hadviselésben a védelem alapvető kérdése, hogy a szervezetek, vállalatok Biztonsági Politikájukat, a biztonsági eseményekre válaszoló képességüket naprakészen tartják-e, mennyi és milyen erőforrásokat fordítanak ennek megoldására. A szervezetek biztonsági kultúrája a társadalmi biztonsági kultúra része-e és alakítója-e.

7. Az információs hadviselés néhány jellemző támadó művelete a szakkifejezések tükrében

- **Cracking** (kreking): Illegális belépő az információ rendszerbe, kár okozás céljából.
- **Cyberspace** (kiber tér): Globálisan egymással összekapcsolt számítógépek, számítógéprendszerek.
- **Cyberwar** (kiber hadviselés): A kibernetikai háború, az információs háború szinonimája.
- **Chernobyl Virus**: Elpusztít minden tárolt adatot, amikor a fertőzött fájlt megnyitják.
- **DNS spoofing** (DNS becsapás): Más rendszerének a jogosulatlan használata.

- **DOS** (Denial of service, szolgáltatás letiltása): Az ellenfél letiltása egy program, egy rendszer használatáról.
- **Dumster diving** (guberálás): Hozzáférés az ellenfél információihoz a szemét-tartályok vizsgálatával.
- **Echelon**: Nemzetközi lehallgató hálózat az elektronikus távközlés bármely formájának kulcsszavak alapján történő elfogására.
- **Van ECK monitoring** (van ECK megfigyelés): Egy számítógép vagy egy elektronikus berendezés alacsony szintű kisugárzásának elfogása.
- **ECM**: Aktív vagy passzív, elektronikus védelmi intézkedés az ellenfél érzékelő/leolvasó berendezései és távközlési forgalma eltérítésére, zavarására.
- **EMP bomb** (EMP bomba): Elektronikus hálózat (integrált áramkörök) rombolására szolgáló készülék.
- **Hacker** (hekker): Egy személy, aki betör egy rendszerbe, amelyre nincs jogosultsága vagy szándékosan átlépi saját jogosultságának határát, adat keresés, lopás, módosítás vagy más hozzáférésének és az informatikai szolgáltatásoknak a megakadályozása céljából.
- **HERF** (High Energy Radio Frequency): A HERF fegyver, amely egy digitális készülék működését megállítja.
- **Killer's** (gyilkosok): Lepakcsolják a biztonsági programokat például a tűzfal vagy vírusvédő rendszereket.
- **Logic bomb** (logikai bomba): Jogosulatlan számítógép kód, gyakran e-mailen küldve, amely ha meghatározott előfeltételeket ellenőrizve indítják, behatolást vagy rombolást okoz.
- **Sigint**: Elektronikus jelek elfogása.
- **Social engineering** (megtévesztés): A támadó a támadást segítő célokra az alkalmazottakat, egyéneket megtevesztő, tudományosan módszert dolgoz ki.
- **Zombie army** (zombi hadsereg): Több, a támadó által vírus fertőzött, és így beállított számítógép, amely számítógéprendszer, üzenet és utasítás továbbítására alkalmas, amely így egy a támadó által uralt, rosszindulatú hálózatot képez.

8. Összefoglalás

Az ismerttetett információs hadviselés kétségtelenül a figyelembe veendő veszélyforrások között szerepel a szervezetek, vállalatok védelmének kialakításakor, és a biztonság szintjének fenntartásához elengedhetetlen. Ugyanakkor azonban a munkatársak képzésekor fel kell hívni a figyelmet arra, hogy az információs támadás esetleges bekövetkezéséről nem félni, hanem arra megfelelően fel kell készülni.

Irodalomjegyzék

- [1] Galvin, J.: Info War: Targeting your business. www.zdnet.com.au
- [2] Dr. Goldberg, I.: Global Security Matrix: Printable Definitions. The Watson Institute. 2001.
- [3] Computer crime categories: How-Techno criminals Operate. School of Criminal Justice. Michigan State University. 1995.
- [4] Dr. Várhegyi, Dr. Makkay: Információs korszak, információs háború, biztonságkultúra. OMIKK. 2000.
- [5] Dr. Munk S.: Katonai informatika a XXI. Század elején. Zrínyi Kiadó. 2007.
- [6] Cohen, F.: World War. F. Cohen & Associates. 2008.

Az IT virtualizáció

Vasvári György CISM

Információs Társadalomért Alapítvány
1507 Budapest, Pf. 213
Telefon: +36-1-279-1510, Fax: +36-1-279-1511
e-mail: gvasvari@tiphaz.hu

Absztrakt

A modern információ rendszerek többek között gazdaságos kialakításának, a minimális eszköz igénynek a célját szolgálja a virtualizáció. Ez az eljárás az eszközök optimális és folyamatos kihasználását biztosítja a korábbi technológiával szemben. Ezzel az eszközök jelentős részének használaton kívül helyezését eredményezi. A virtualizáció az informatikai technológia széles területein alkalmazható. Természetesen az alkalmazás új kockázatokat is hoz, amelyek figyelembe vételével kell az új védelmi intézkedéseket meghatározni. A virtualizációs környezet folyamatos belső ellenőrzést és rendszeres független auditálást igényel.

Kulcsszavak: fogalmak (concepts), alkalmazás (application), biztonság (security), virtualizációs környezet védelme (protection of virtualization environment), kockázatok (risks)

1. A probléma

A virtualizáció az elmúlt évek igen jelentős technológiája. Sokan sokféle képen határozzák meg, és a virtualizáció a növekvő vállalatok, felhasználók számára, sok előnyt kínál. Ma az IT-ben egy állandó van, a változás. Az új stratégiákkal, mint a konszolidáció és a virtualizáció, a változás jól kiszolgálható. Egyszerűbb, jobban skálázható, költség-hatékonyabb IT infrastruktúra érhető el, amely rugalmasabban követheti a változásokat. Az üzleti célok szempontjából ki kell emelni, hogy az energia, és a hely igénye kisebb.

2. A virtualizáció fogalma

A virtualizáció egy keretrendszer vagy módszer a számítógép erőforrásainak felosztására, egy többszörös megvalósító környezetre, alkalmazva egy vagy több koncepciót vagy

technológiát, mint a hardver és szoftver felosztás, az időosztás, a részleges vagy teljes gép szimuláció, emuláció, minőségi szolgáltatás, konszolidáció, és sok más.

A HP szerint a virtualizáció egy alkalmazkodó infrastruktúrának a létrehozásra alkalmas, az erőforrások szükség szerinti felhasználása, a szükség szerinti munkaterhelés erőforrások közötti elosztása, és a magas rendelkezésre állás területén, valamint elősegíti az erőforrásokkal való ellátás kiegyensúlyozottságának biztosítását, a túlzott vagy alábecsült ellátás elkerülését.

Néhány további példa az ismert definíciók közül:

- A virtualizáció valaminek egy látszólagos verziója (szoftverrel megosztott hardver).
- A virtualizáció a folyamatok elválasztása az Operációs Rendszertől a fizikai gépen.
- A virtualizáció számítógép a számítógépben, szoftvert alkalmazva.
- A virtualizáció egy hardver megosztása, több virtuális, látszólagos részre.
- A virtualizáció
 - több egységre bontja, ami egy,
 - egynek láttatja, ami több részből áll.
- A virtualizáció paradigmaváltás a vállalati háttér iroda (backend) fejlesztési koncepciójában és architektúrájában.

A Wikipedia szerint a virtualizáció egy tág szakkifejezés, amely valójában a számítógépes erőforrások absztrakciója. Így az lehet:

- Platform virtualizáció, azaz az operációs rendszer szeparálása, az alárendelt platform erőforrásoktól.
- Erőforrás virtualizáció, azaz speciális erőforrások virtualizálása.
- Alkalmazás virtualizáció, azaz idegen hardver/szoftver alkalmazás befogadása.
- Desktop virtualizáció, azaz a desktop távoli kezelése.

A virtualizáció a környezetet két részre bontja:

- A frontend (előtér) a környezet azon része, amely közvetlenül kommunikál a felhasználóval, míg
- A backend (háttér) tartalmazza a komponenseket, amelyek a frontend outputját dolgozzák fel.

Ez, tehát egy absztrakció, amely a hagyományos környezet elemeinek szétválasztását valósítja meg. A virtualizáció a gyorsan növekvő IT szolgáltatások revíziója, adaptálása vagy fejlesztése, amely sok fizikai szervert, sok logikai szerverré konszolidál kevesebb

fizikai szerverrel. Mindez csökkenő költségeket, növekvő alkalmazkodó képességet, és rugalmasságot, egyszerűbb menedzsmentet, és az automatizálás következtében növelt erőt jelent.

3. A virtualizáció fejlődésének fázisai

A virtualizációnak az állandó változás, fejlődés jegyében, a következő fázisai voltak:

- A VM-ek telepítése, tesztelése és fejlesztése,
- A feldolgozási környezet egyszerűsítése, a szerverek konszolidációjával,
- Az erőforrások egyesítése, a teljes adatközpont virtualizálásával, majd automatizálásával,
- A felhő számítástechnika alkalmazása, a „felszabadítási” fázis.

4. A virtualizáció indokai

A vállalatok, szervezetek állandóan növekvő változó igényei, a jelenlegi technológiával, csak növekvő költségek mellett elégíthetők ki. Ugyanakkor a fejlesztések – az állandó hardver beállítások miatt – alacsony kihasználtságot eredményeznek.

A virtualizáció top készletői:

- Alacsonyan kihasznált hardver,
- Az adatközpontokban a hely hiánya,
- A növekvő energia költségek,
- Az adminisztratív költségek szignifikáns növekedése.

5. A virtualizáció lehetséges alkalmazási területei

- Hardver,
- Szoftverek (alkalmazások, operációs rendszerek),
- Szerverek,
- Tárolók,
- Hypervisor,
- Hálózat,
- Felhasználói munkaállomások.

6. Adatközpont virtualizáció

A dinamikus adatközpontok (számítóközpontok) az alkalmazkodó számítástechnika új lehetőségeit nyitják meg a virtualizációs, és az automatizálási technológiák alkalmazásával. Az automatizálás biztosítja, az IT erőforrások automatikus allokációját a szolgáltatások részére.

A virtualizáció és automatizálás következményei az adatközpontban:

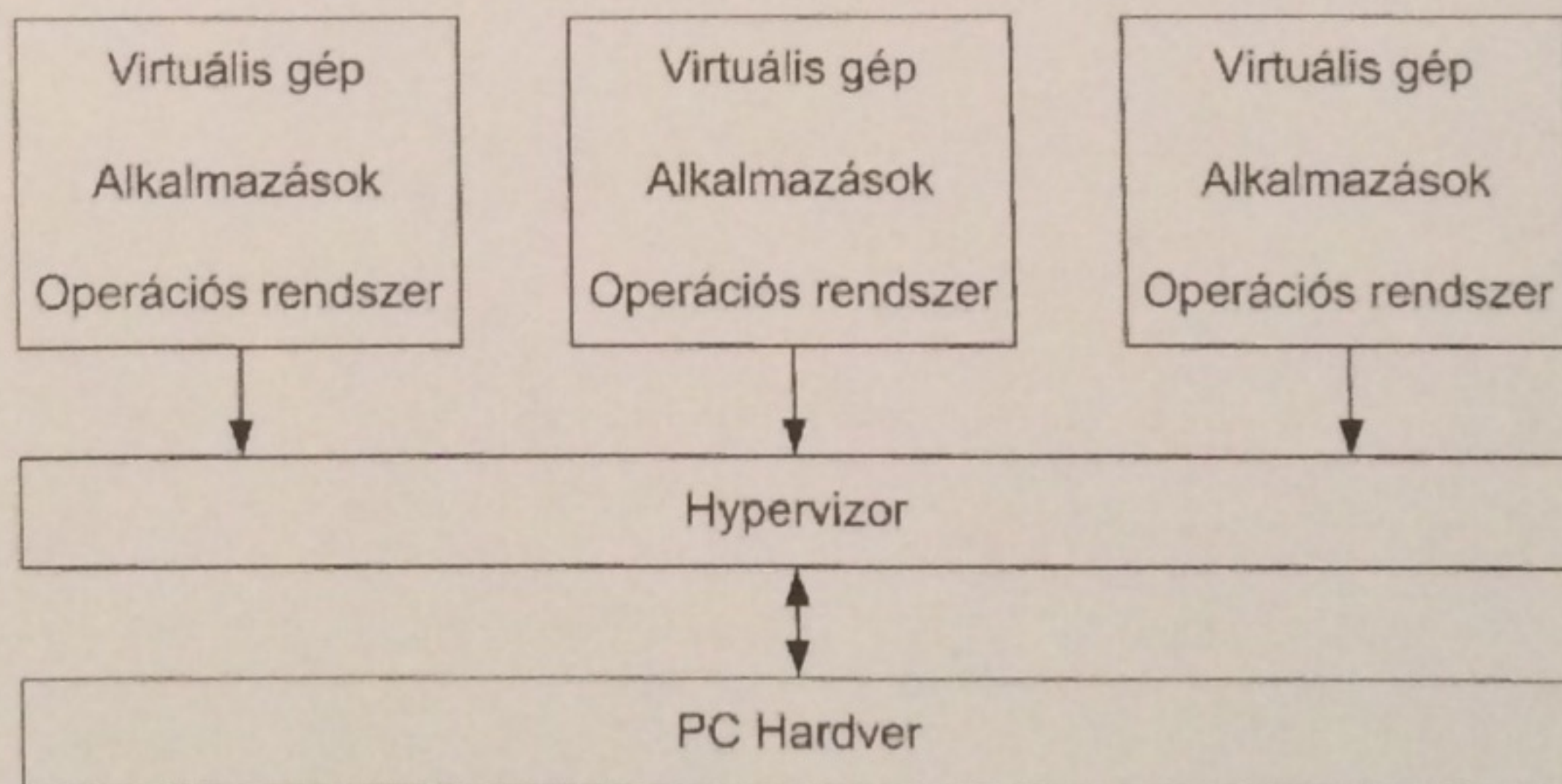
- Az erőforrások optimális kihasználása,
- Igény szerinti számítógépes kapacitás,
- Egyszerű életciklus-kezelés,
- Szolgáltatások minőségének automatizált, szabályokon alapuló karbantartása,
- Jelentősen alacsonyabb költségek.

7. Hardver virtualizáció

A hardver virtualizáció megfelel egy processzor áramköreinek, és a memóriavezérlőnek, amely lehetővé teszi több operációs rendszer futtatását (több VM).

8. A hypervisor

A hypervisor vagy Virtual Machine Manager (VMM) egy program, amely a virtuális gépek menedzsere, és a host hardver felosztásával teszi lehetővé, több VM és ezzel több (guest OS) operációs rendszer telepítését, futtatását, egy, egyedüli hardver-en. Mindegyik operációs rendszer rendelkezik processzorral, memóriával és más erőforrásokkal. A hypervisor vezérli a processzort és az erőforrásokat, allokálva minden operációs rendszerhez, amire szüksége van. Egy ilyen, lehetséges hypervisor architektúra az alábbi:



1. ábra: Egy lehetséges hypervisor architektúra

9. Operációs rendszer virtualizáció

Az operációs rendszer virtualizáció egy módszer, amikor a host operációs rendszeren több virtuális operációs rendszer fut. A host operációs rendszerek általában a szabványos operációs rendszerek (Windows, Linux). Az operációs rendszer virtualizálását az alábbi ábra mutatja be:

Alkalmazás 1.	Alkalmazás 2.	Alkalmazás 3.	Alkalmazás 4.
Vendég OS		Vendég OS	
Virtuális gép menedzser (VMM)			
Alap hardver			

2. ábra: Operációs rendszer virtualizáció

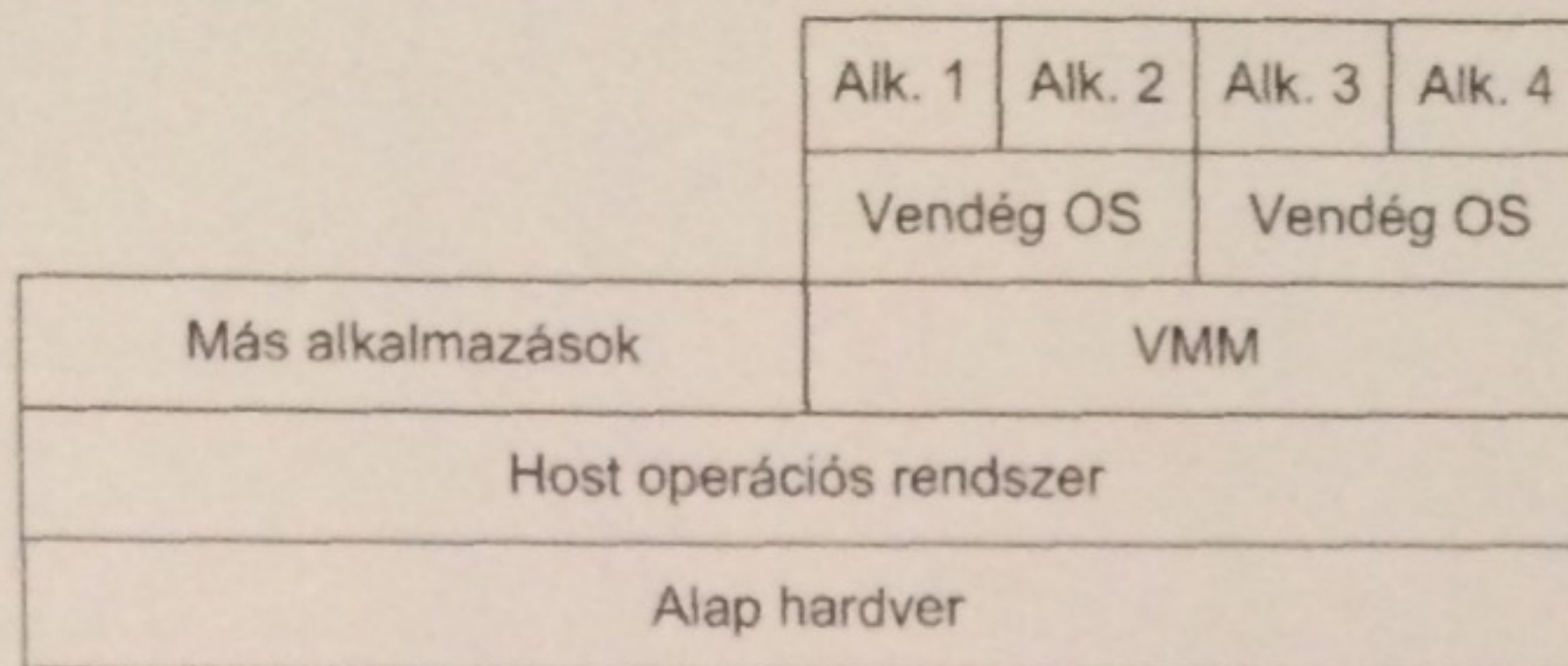
A VM-eken elhelyezett OS-ek, illetve alkalmazások újrainstallálás nélkül áthelyezhetők a virtuális környezetben, eltérő infrastruktúrában lévő VM-ekre, illetve a fizikai eszközre vagy onnan a VM-ekre. Virtual to Virtual (V2V), Virtual to Physical (V2P), Physical to Virtual (P2V) (lásd szakkifejezések).

10. Virtualizáció hypervisor nélkül

Egyes irodalmak azt állítják, hogy hypervisor nélkül is megoldható a virtualizáció. Ekkor nincs szükség, a driver emulációra. Ez nagyobb, gyorsabb teljesítményt eredményez, amelynek következtében több VM futhat egymástól elszigetelve, párhuzamosan. Ilyenkor a host OS virtualizáció történik, és az OS-en vannak elhelyezve a driverek. Azaz a host OS irányítja, teszi lehetővé a VM-ek működését, amelyeken telepítve vannak a driver emulációk.

11. Szerver virtualizáció

A szerver virtualizáció, a szerver erőforrásoknak az elfedése a szerver felhasználói előtt, beleértve az egyes fizikai szervereket, processzorokat, és az operációs rendszereket. A szerver adminisztrátor egy fizikai szerver több szigetelt virtuális környezetre való felosztására, egy szoftver alkalmazást használ. A virtuális környezeteket gyakran virtuális privát szervereknek hívják, de partícióknak, guestnek, konténernek vagy emulációnak is nevezik. Azaz a szerver virtualizáció sok szerver funkcionalitást átviszi kevesebb szerverre (konszolidáció).



3. ábra: Szerver virtualizáció

12. Szerver virtualizációs architektúrák

A gyártók, a szállítók versenye az architektúrák, széles változatát hozta létre. A [18] a szerver virtualizációs architektúrákat az alábbiak szerint csoportosítja:

- Host alapú virtualizáció, amely lehet
 - Teljes virtualizáció, amelynél a VM tartalmaz egy vendég OS-t, és az arra telepített erőforrásokat, meghajtókat használja a fizikai hostra telepített erőforrásokkal történő kommunikációra. A VM interfész a VMM-en (hypervizoron) át a hostjához.
 - Paravirtualizáció az API-k, és meghajtók a vendég OS magjába vannak telepítve.
 - Hardver támogatású virtualizáció, ahol a VM, és a hardver között egy pass through bus van telepítve (VM bus), és így a VM a hardver-en telepített erőforrásokat közvetlenül érheti el. A rendszer automatikusan őrzi a VM erőforrások címeit, így ez tényleges szigetelést valósít meg.
- OS virtualizáció (lásd 9. pont).

13. Tároló virtualizáció

A tároló virtualizáció a fizikai tároló egyesítése, több hálózati tároló eszközből egy tároló eszközzé, amelyet egy központi konzolról kezelnek. A tároló virtualizáció segíti a tároló adminisztrátort a háttér biztosításának a könnyebb megoldásban. A tároló virtualizáció lehetővé teszi sok felhasználónak vagy alkalmazásnak, hogy hozzáférjen a tárolóhoz anélkül, hogy érdekelt lenne, hogy hol és hogyan van a tároló fizikailag elhelyezve, menedzselve. A virtuális tárolás egy aggregált, logikai egyesítése az adatoknak, attól függetlenül, hogy az IT infrastruktúrán belül, hol van a fizikai tároló. A növekvő tárolási igényt, tehát dinamikusan lehet allokálni.

14. Alkalmazás virtualizáció

Az alkalmazás virtualizáció az, amikor a végfelhasználó rendelkezésére áll egy távoli, központi szerverről egy alkalmazás, illetve tárolók anélkül, hogy a felhasználó lokális rendszerén teljesen installálni kellene azt. Ekkor tehát a szerverek, alkalmazások, tárolók és az alkalmazási erőforrások dinamikusan el vannak választva.

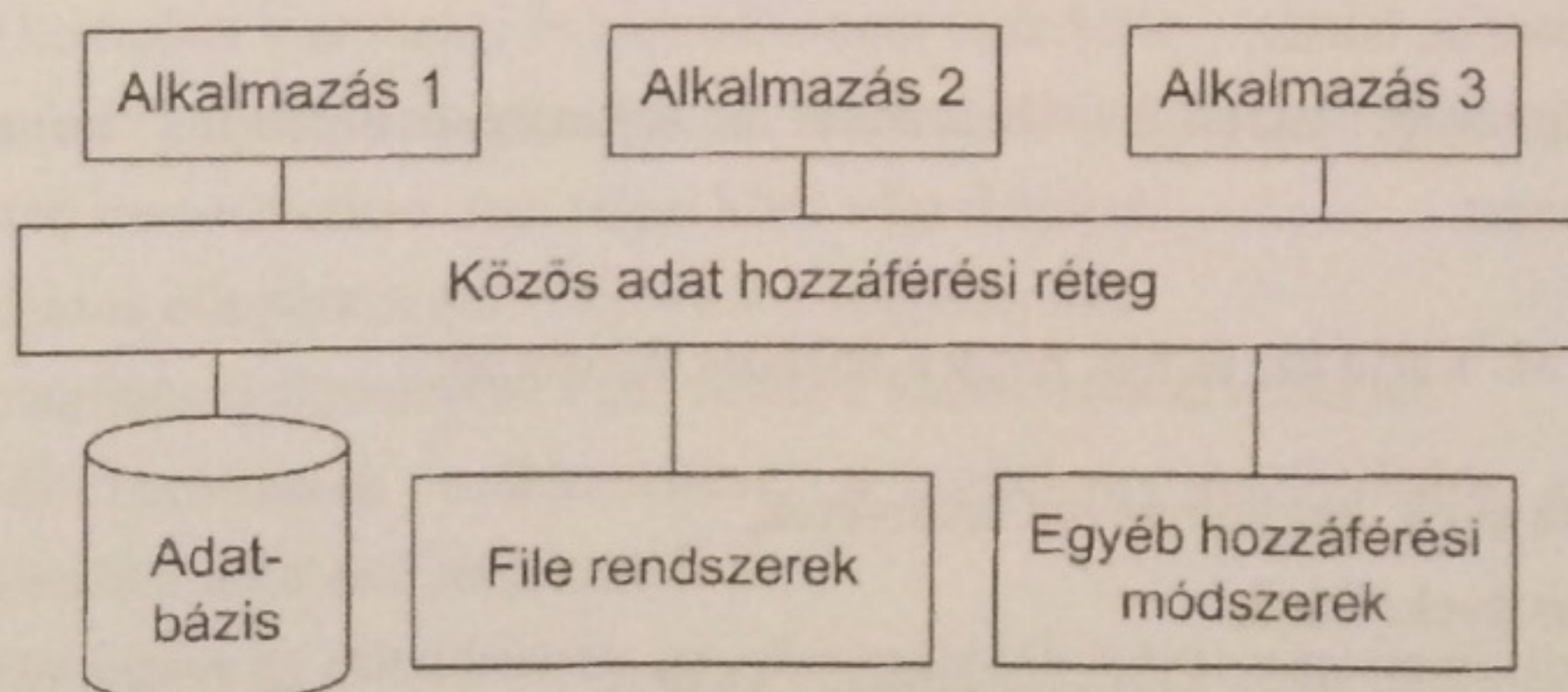
15. Desktop virtualizáció

A desktop virtualizáció a végfelhasználó számára lehetővé teszi, egy desktop környezetben a jogosult hozzáférést valamely alkalmazáshoz, attól függetlenül, hogy pillanatnyilag az alkalmazás hol van elhelyezve. Így a felhasználónak egy virtuális interfésze, virtuális eszköze (virtual appliance) van, amelyen indíthatja a hozzáférést a Web, lokális vagy szerver bázisú alkalmazáshoz, anélkül, hogy szüksége lenne Web oldalakra, Windows Start menüre vagy a terminálszolgáltatás interfészére. A virtuális desktop a központi szervertől távol van elhelyezve, lehetővé téve a felhasználónak a hozzáférést a távol, helyben elhelyezett alkalmazásokhoz.

Azaz a desktop computing virtualizálása lehetővé teszi a PC elhelyezkedési pontjának (ahol a számítógép ténylegesen van), illetve a felhasználó tényleges hozzáférési pontjának (ahonnan hozzá akar férni a számítógéphez) az elkülönítését. Ekkor az adatokat is a desktoptól távol tárolják, így a desktop kiépítettsége jelentősen csökkentve van a hagyományos számítógéphez képest.

16. Adat virtualizáció

Az adat virtualizáció, amikor az egyes adat tételeket a forrástól el vonatkoztatják, és a különböző adat hozzáférési módszereknek, egy közös adat hozzáférési rétege van. A hozzáféréshez, így egy protokoll szükséges, ami alkalmazás részéről, a támogatott hozzáférési módszerek hozzáférési kérését lefordítja egy speciális protokollra.



4. ábra: Adat virtualizáció

Az IBM két eljárást alkalmaz az adat virtualizációnál:

- in band eljárásokat,
- out band eljárásokat.

Az in band eljárásnál az adat, és a kontrol folyamat azonos útvonalon történik, míg az out band eljárásnál az adatok, és a meta adatok (adat az adatról) szét vannak választva, különböző helyekre. Az elkülönített szerveren (meta data controller) tárolják a mapping, és a looking táblázatokat.

17. Hálózat virtualizáció

A hálózat virtualizáció a rendelkezésre álló erőforrások összefogásának módszere, a rendelkezésre álló sávszélesség csatornákra osztására, amelyek függetlenek egymástól, és bármelyik hozzá, illetve visszarendelhető egy szerverhez vagy eszközhöz valós időben.

18. A virtuális eszköz

A VM-ekre telepített virtuális eszköz (virtual appliance) tartalmaz minden adatot, amely, egy távoli alkalmazás hozzáféréséhez szükséges. Tehát a virtuális eszköz egy alkalmazáshoz van kialakítva, és így a hálózati alkalmazások telepítési útját jelenti. Ez tulajdonképpen egy Software as a Service (SaaS), ahol az alkalmazás nyújtja szolgáltatásokat és a karbantartást is. A virtuális eszközök könnyen mozgathatóak, így könnyen követhetők a változások. Minden alkalmazást csatolva a saját virtuális eszközéhez, az alkalmazás igényeit pontosabban lehet szabályozni.

A virtuális eszköz a tradicionális eszköz minden előnyét nyújtja, valamint még a továbbiakat:

- könnyű értékelni, tesztelni,
- könnyű telepíteni,
- redundancia, háttér,
- skálázhatóság, mobilitás, beleértve a fejlesztési erőforrás tervezést, és az ellenőrzést.

Ezzel szemben M. Katin azt állítja, hogy a fejlődés fokozatai:

- 1990-es évek: hagyományos szoftverek,
- 2000-es évek: SaaS,
- Ma: appliance alapú szoftverszállítás (AbSD).

Ugyanis a gyakorlatban kiderült, hogy az SaaS problémái:

- A megbízhatóság kérdéses,
- A teljesítmény alakulása előre nem látható,
- Adatok elvesztése lehetséges,
- Az idő függvényében jelentős költség.

Ezzel szemben, az AbSD előnyei:

- Magas megbízhatóság,
- A redundáns komponensek redundanciát, és automatikus hiba áthidalást nyújtanak,
- Megbízható, skálázható a teljesítmény, egy erre a célra beépített megoldással,
- Könnyű védelem az önjavítás, és az automatikus karbantartás miatt.

19. Biztonság a virtualizációs környezetben

A tradicionális biztonsági rendszerek bíznak abban, hogy a hardver és a speciális operációs rendszerek védik a hagyományos környezetet, azonban azok a virtuális környezetben, ahol a cél a hardver igény csökkentése, nem lesznek használhatók. Továbbá a hagyományos legjobb gyakorlat, kérdésessé válik, mert a fizikai szegmentálást, és más módszereket csaknem lehetetlen implementálni virtuális környezetben. Végül a virtuális környezet, a hálózat komplexitása gyorsabban fejlődik, mint a hagyományos menedzsment és a monitoring rendszerek, így a fizikai és virtuális környezet átláthatósága rendkívül homályos.

Egyértelmű, hogy új védelmi módszerekre van szükség.

20. Néhány új kockázat

- A virtualizációs szoftver egy új réteget jelent a privilegizált szoftverben.
- A feladat szétválasztás elveszik.
- A VM-en belüli forgalom korlátozott látása.
- Nem komplett biztonsági és menedzsment eszközök.
- Az emberi tényező szerepének lebecsülése a virtualizáció szempontjából.
- A patch menedzsment nem teljes körű végrehajtása.
- A változás ellenőrzés nem teljes körű végrehajtása.
- A virtualizáció figyelembe nem vétele a katasztrófatervezésnél.
- Az új kockázatok csökkentésére, a védelem megújítására a virtualizáció megkezdése előtt kell intézkedni!
- A hagyományos ellenőrzések az alkalmazások körül nincsenek jelen a virtuális környezetben, így egy szervezetnek nincs képessége arra, hogy auditálja, mely információhoz fért hozzá, és mikor.

- A biztonsági eszközök tipikusan, a hagyományos környezetben a Web szerverek front end szintjén vannak elhelyezve, hogy a Web bázisú forgalmat ellenőrizzék. Mégis a behatolásoknak a 80%-a web bázisú protokollokon keresztül történik. A virtuális környezetben sok alkalmazás és szerver egy fizikai szerveren helyezkedik el, így a hacker ezen a rétegen behatolva, alkalmazások, adatbázisok tömegéhez juthat hozzá.
- A megfelelőség a legjobb gyakorlatnak a felosztást vagy osztályozást kulcsfontosságúnak tartja. Sok szervezet bizalmi zónákat képez. A virtuális környezetben a felosztás több fizikai hardvert futtat különböző virtuális környezetben, hogy csökkentse a hagyományos költségeket.
- Ha a hardver bázisú hálózati rendszer nem helyezkedik el a virtuális szerverek vagy az ezeken futó alkalmazások között, a menedzsment konzol nem képes a környezetben folyó aktivitások adatait gyűjteni, illetve láthatóvá tenni.

21. A virtualizációs környezet védelme

Elvileg nemzetközi megállapodás alakult ki, hogy az informatikai biztonságot a virtuális környezetben a fizikai szerverek biztonságával azonos módon kell biztosítani. Ennek alapján a virtualizáció megvalósításakor, például a következő védelmi intézkedéseket, kell tenni:

FUNKCIONÁLIS VÉDELMI INTÉZKEDÉSEK

- SZERVEZÉSI VÉDELMI INTÉZKEDÉSEK
 - Napra készre kell tenni az operációs rendszert és az alkalmazásokat, a VM-en és a hoston egyaránt. A host alkalmazásokat abszolút minimumon kell tartani csak, amit szükséges, szabad installálni.
 - A host operációs rendszert erősíteni kell, leállítani és lehetetlenné tenni a nem szükséges szolgáltatásokat. Biztosítani kell, hogy az operációs rendszer sovány legyen a támadási felület csökkentése céljából.
 - A nem használt VM-et ki kell kapcsolni, ha nem szükséges, ne fusson.
 - A VM-eket be kell építeni a Biztonsági Politikába.
- HUMÁN VÉDELEM
 - Elterjedt szemlélet, hogy az informatika csak technológiából áll. A humán tényezőt nem lehet figyelmen kívül hagyni. Rendkívül fontos a munkatársak képzése, gyakoroltatása, a rendeltetésszerű végrehajtás az ismeretek, a gyakorlat hiánya miatt elkövetett hibák csökkentése érdekében.

- Gondoskodni kell arról, hogy a virtualizáció annak negatív és pozitív következményei a szervezeti (biztonsági) kultúra pontosabban a belső ellenőrzési funkciók részévé váljanak.
- FIZIKAI VÉDELMI INTÉZKEDÉSEK:
 - A jövőben a hypervisor szoftver flash tárolására optikai médiát kell alkalmazni, a mágneses média nemcsak elavult, hanem biztonsági sebezhetőséget okoz, amely megakadályozza a flash technológia használatát.
 - A host gép egy egyedülálló hibapontot képez (single point of failure), a technológia (mint a duplázás és a folytonosság) segít csökkenteni ezt a kockázatot.
- LOGIKAI VÉDELMI INTÉZKEDÉSEK:
 - Minden VM-et tűzfalnak kell elszigetelni minden másik VM-től, és a hosttól úgy, hogy csak a megengedett protokollok kerülhessenek lebonyolításra, valamint minden lehetséges utat vizsgálni kell.
 - Antivírus szoftvert kell installálni és naprakésszé tenni a VM-eken, és a hoston. A VM-eket megfertőzhetik vírusok és férgek, mint a fizikai gépeket.
 - A host, és a VM-ek között Ipsecet vagy erős rejtjelezést kell alkalmazni, mivel a forgalom a VM-ek és a host között lehallgatható és kompromittálható. A szállítók kevésbé szívesen alkalmazzák a rejtjelezést, ez tehát reális fenyegetés. A legjobb gyakorlat szerint a gépek között a kommunikációnak rejtjelezve kell lennie.
 - A host számítógépről ne bolyongjanak az Interneten, mert a kém szoftverek, rosszindulatú szoftverek okozta fertőzés a hoston lehetséges, mivel a host gép irányítja a VM-eket, és azok a problémák, amelyek a VM-en lépnek fel, komoly zavarokhoz és potenciálisan leálláshoz vagy szolgáltatás elvesztéshez vezethetnek.
 - A host számítógépen az adminisztrátor és az adminisztratív belépési tárolók (accountok) bizalmasak. Egy jogosulatlan felhasználó hozzáférése a kiemelt belépési tárolókhoz, szignifikáns biztonsági eseményhez vezethet. A kutatások azt mutatják, hogy az adminisztrátor (root) belépési tárolója a hoston szignifikánsan kevésbé biztonságos, ha összehasonlítjuk a VM vagy a fizikai hálózati gép belépési tárolójával, és a jelszavakkal. Emlékezzenek, hogy a biztonság olyan erős, mint a leggyengébb belépési pont.

- Védeni kell a host számítógépet, és gondoskodni VM-ek lehallgatás elleni a védeleméről.
- A megoldásokat, amelyek szigetelik a hypervisor típusú implementációs folyamatokat, támogatni kell, ezek a rendszerek elősegítik a szigetelést, és jobban védik a környezetet.
- Gondoskodni kell, hogy a host meghajtók naprakészek legyenek: ez fogja biztosítani, hogy a hardverek optimális sebességgel fussanak, de a szoftver legkésőbbi változata fogja biztosítani, hogy az öreg hibákat a meghajtó szoftverekben csökkentsék, ne lehessen kihasználni, mert az potenciálisan szolgáltatás megtagadást eredményezhet.
- A hardver port technológiát ki kell kapcsolni minden VM-nél, ha a VM környezet nem használja például az olyan technológiákat, mint az USB.
- A hardver erőforrások megosztását korlátozni és csökkenteni kell. A biztonság és az erőforrás megosztás nem megy együtt. Adatszivárgás, és maradvány a probléma, amit okoz, okozhat, ha a változó VM-ek az erőforrásokat megosztják. Ezeket, az erőforrásokat (CPU, RAM, merevlemez, és mások) konzervatívan kell kezelni, és követni kell a legjobb gyakorlatot a szolgáltatások rendelkezésre állásának biztosítására.
- Ha lehetséges gondoskodni kell arról, hogy a hálózati interfész kártyák verziója meg legyen jelölve minden virtuális gép részére. Gondoskodni kell, hogy a VM-hez irányuló és onnan eredő forgalom szigetelve legyen.
- A particionálás diszk határokat képez, amelyet használhatunk minden VM részére kijelölt partíció elválasztására és védelmére. Ha egy VM a kijelölt partíció normál korlátján túl növekszik, más VM-ekre gyakorolt hatását korlátozni fogja.
- Gondoskodni kell arról, hogy a VM-ek ne tudjanak kapcsolódni egymáshoz, ha nincs szükség arra. A VM-ek közötti kommunikáció fontos, amint az előbbieken szó volt arról. A VM-ek közötti kommunikációra egy elkülönített hálózati kártyát alkalmazzunk, eltérő hálózati címekkel. Ez jóval biztonságosabb, mint a VM-ek közötti forgalmat a „védtelen” hálózaton átirányítani.
- A hálózati hozzáférés ellenőrzés (NAC, Network Access Control) hozzájön a VM hosthoz. Ez speciálisan igaz az eszköz bázisú VM szerverre, ha ez a jellegzetesség lehetővé tudja tenni a pontosan implementált NAC végig tudjon menni a kapcsolatokon.
- Szigorúan kell kezelni a VM-ekhez a távoli hozzáférést, és különösen a host géphez, mert ez nem kívánatos veszélyforrást képez.
- Kerülni kell az IP címek megosztását, mivel ez egy tipikus erőforrás megosztás és problémákat, valamint sebezhetőséget okoz.

- GARANCIÁLIS VÉDELMI INTÉZKEDÉS

- Szigorúan kell kezelni a VM-ekhez a távoli hozzáférést, és különösen a host Számonkérhetőség biztosítása.
- Figyelemmel kell követni az eseménynaplókat, mind a host gépen, mind a VM-en. A megfigyelés (monitoring) gyakran elkerüli a figyelmet a virtuális környezetben. Az ésszerű magatartás a virtuális szoftver által ajánlott host bázisú megfigyelés. Ezeket a naplókat páncélszekrényben szükséges tárolni a jobb védelem, és egy későbbi auditálás céljára (a számon kérhetőség biztosítása).

A továbbiakban 7 gyakorlati lépés a VMM-ek biztonságának megteremtésére. Ezek a következők:

1. Az állapot tudatos kialakítása, felmérése:

- Milyen informatikai szolgáltatásokat nyújt a virtualizáció?
- Kik vannak az üzleti és az IT egységekben?
- Melyek a releváns szabályozási és szerződéses követelmények, amelyeket a virtualizáció lehetővé tesz, illetve kell tennie az üzleti folyamatok számára?
- Melyek azok a technológiák és IT folyamatok, amelyeket alkalmaznak?
- Maradt-e a múltból magas szintű kockázat?

2. A kivételes hozzáférési jogosultságok számának csökkentése és monitorozása, amelyhez a következő kontrollok szükségesek:

- Dokumentálni kell a virtualizációs adminisztrátorokat, akiknek kivételezett hozzáférési jogosultságuk van a VM-ekhez, és gondoskodni kell ezeknek a jogosultsággal történő egyeztetéséről, a nem egyeztethetőket (ghost account) törölni kell.
- A virtualizációs menedzserekkel a munkát csökkenteni kell az adminisztrátorok mennyiségére, a minimumra.
- Személycsere esetén gondoskodni kell a hozzáférési jogosultságok visszavonásáról.
- Az accountokat rutinszerűen negyedévenként, évenként újra kell akkreditáltatni a fluktuáció függvényében.

3. Meg kell határozni, kikényszeríteni a virtualizációs konfiguráció szabályokat, a VM-ek konfigurációs és logikai beállításait.

4. Integrálni és segíteni kell a változás menedzsment folyamatok kikényszerítését. Ha már a VM-ek „ismert és biztonságos állapotban” vannak, minden változtatásnak a változás menedzsment által autorizáltnak, tervezettnek és igazoltnak kell lennie.

5. El kell készíteni a bizalmas, virtualizált szerverek kialakításának könyvtárát. A megfelelő ellenőrzés hiánya és a gyors virtualizáció biztonsági eseményekhez, és

megfelelőségi, valamint audit hiányosságokhoz vezet. A könyvtár egy virtuális képet nyújt, amelyet authorizált, biztonságos konfiguráció telepítésére használhatunk.

6. A változás menedzsmentbe integrálni kell a teszt és elfogadási folyamatokat.
7. Gondoskodni kell arról, hogy a virtualizációs tevékenységek a változás menedzsmenten keresztül történjenek.

22. Biztonság a virtualizációval

A virtualizációból eleve adódnak védelmi lehetőségek. Erre néhány példa:

- A DRP. A virtualizáció lehetővé teszi a visszaállítási műveletek időtartamának és költségének csökkentését. Ugyanis az első node a fizikai hardveren van elhelyezve, a második a VM-en készen arra, hogy hiba esetén átvegye a működést.
- Bűnügyi elemzés. Az elemzés céljára szükséges ismerni, hogy a bűnözők miként másolják le a merevlemez tartalmát. A megoldás lényegében automatizálva van a virtuáliskörnyezetben. A P2V a merevlemez tartalmát az adatok megváltoztatása nélkül pontosan másolja, és mivel a támadó nyomokat hagy a rendszer naplóban, ez elemzésre alkalmas.
- Honeypotting. Egy program a felhasználói környezetben a támadó számára csábító adatokkal és naplózó érzékelőkkel ellátva. Így a behatolás eszköze, módszere feltárható, és ennek megfelelően, a biztonság menedzsment számára lehetőség van az új védelmi intézkedésre.
- Sandboxing. A virtualizált rendszer erőforrásainak szigorúan ellenőrzött készlete. A támadó az elszigetelés következtében nem tud kommunikálni a host OS-szel, ahol a felhasználói adatokat tárolják, és ahonnan hozzáférhet a hálózathoz.
- Behatolás jelzés. A behatolás jelzésre olcsó megoldás.

23. A virtuális környezet és a biztonság

A hagyományos rendszereknél a védelmi eszközök tipikusan a web szerver front endjén helyezkednek el a forgalomszűrés végett, mégis a behatolások 80%-a a web bázisú protokollokkal történik. A virtuális környezetben, ahol sok alkalmazás és szerver egy szerveren fut, és erre behatolás történik az alkalmazások és adatbázisok sokaságához válik lehetővé a hozzáférés. A virtuális környezet védelmének lehetséges megoldása, a szoftver bázisú védelem.

24. A működésfolytonosság virtualizációs környezetben

A virtualizáció megszakítja az összeköttetést az OS és az alatta lévő hardver között. A fizikai elemek újra elő vannak állítva szoftverben. Ez lehetővé teszi, hogy egy hardveren több OS fusson. Így kevesebb fizikai hardverre van szükség. A standard szerver átlagosan a CPU-t 5-15%-ra köti le, míg ez a virtualizációs környezetben 60-70%. A szerver kiesése a virtualizációs környezetben futó összes VM-re hat, azaz több alkalmazás eshet ki.

Védelmet a redundancia, és főleg egy távoli számítóközpont (háttér) nyújthat, azonban nem mindegy, hogy a szervezet BCP-je hogyan állítja meg a működés folytonosság megszakadását (visszaállítás), és hogyan hárítja el a károkvetkezményeket (helyreállítás). Tehát a virtualizáció csökkentheti a működés folytonosság megszakadás hatásait, de a hogyan, mennyi idő alatt jó megtervezése meghatározó.

A működés megszakadás és következményei elleni védelem:

- A VM-et nyugalomba kell helyezni, a memória és a merevlemez írásának megállítása végett. A virtuális szerver egy interfésszel rendelkezik a VM hibernálásához.
- Rögzíteni kell a jelenlegi memória pillanatképét a VM számára. A VM ugyanakkor hibernálva van. A virtuális szerver írja a VM memória tartalmát egy átmeneti megőrző fájlba.
- A VM konfigurációs adatait rögzítse. Ezeket az adatokat tartalmazza egy VM konfigurációs fájl.
- Rögzítse a fizikai adatokat konzisztens módon. Minden meghajtó a VM-ben képviselve van egy vagy több virtuális merevlemez fájlban. Minden meghajtó konfigurálható az undo meghajtó tulajdonságában, amely megengedi az adatok visszajátszását a meghajtóra írni; ha ez a tulajdonság konfigurálva van, az undo meghajtó fájljait szintén rögzíteni kell. Sok VM alkalmaz rétegezett merevlemezeket; egy alap image fájl tartalmazza a közös OS fájlokat, megosztva több VM között. Minden VM-nek van egy addicionális különbség lemeze, amely VM-enként tartalmazza az információkat. Ez a megközelítés szignifikánsan képes csökkenteni a lemez területet, de az alap virtuális meghajtót védeni kell minden különbség meghajtóval.
- Amennyiben minden fájlnak van háttere, a VM-k hibernált vagy nyugalomba helyezett állapotát a kiadásával jelölni kell.

25. A virtualizációs környezet ellenőrzése

A virtuális környezetben az adatközpontok auditálásának három fő területe van:

- Adatközpont műveletek.
- Az adatközpont szolgáltatásai.
- A virtualizált adatközpont.

Az auditálás magas szintű ellenőrzési céljai:

- Az „ismert és bizalmas állapot” helyzete, a változás menedzsment.
- A megfelelőség a politikáknak, a SOX-nak, a Basel II.-nek és egyéb jogszabályoknak, szabályozásnak.
- A biztonság. A Biztonsági Politika, a szabványok, a legjobb gyakorlat követelményeinek a rendeltetésszerű megvalósítása, végrehajtása.
- Az IT műveletek a kritikus alkalmazásoknál az installáció (változás menedzsment), a konfiguráció és az IT műveletek rendeltetésszerű végrehajtása.

Néhány ellenőrzendő konkrét követelmény:

- Adatközpont követelmények:
 - A virtualizálás létrehoz egy kerülő utat képező réteget a futó OS és a fizikai gép között. Felmerül például a kérdés, hogy a VM a fizikai védett határok között van-e?
- Szerver követelmények:
 - A virtualizációs réteg állapota (a VMM és a menedzsment terület) az azonos folyamatok futtatását igényli ezeken, mint a kritikus szerverek. Például auditálni kell a folyamatot, amely a felfüggesztett gépeket naprakésszé teszi és újraindítja.
 - Ellenőrizni kell, hogy a kapacitás menedzsment elegendő kapacitást biztosított-e?
- Adatközponti szolgáltatások követelményei:
 - Biztonsági követelmény, hogy a konfigurációban megjelenő további kockázatok és a virtuális infrastruktúrában a potenciálisan lehetséges támadás kockázatának, valamint a biztonsági események helyes kezelésének az ellenőrzése.
 - A háttér követelmény.
 - A konfigurációnál az infrastruktúra leírása a fizikai és virtuális leképezés pontosságának az auditálása, a mozgás képesség miatt. A virtuális infrastruktúra használhat olyan virtuális erőforrásokat, mint a virtuális tárolás és a virtuális hálózat, amelyek rugalmasságot biztosítanak, és megosztják a fizikai erőforrásokat, elkülönített infrastruktúrán és belső

kommunikációs kényszerrel. A virtuális hálózatnak, pedig kezelnie kell, hogy melyik gép férhet hozzá, melyik virtuális erőforráshoz.

- Adatközpont műveletek:
 - Minden virtuális erőforrás legyen egy biztonságos fizikai határon belül.
- Szerverek:
 - Antivírus és változat kezelés (pl. a kritikus szerverek szigetelése korlátozott hálózati kapcsolattal).
 - Adattisztítás (data scrubbing). Virtuális tárolás használatánál az adatokat meg kell tisztítani, a különböző VMM-ek elhelyezése között. Azaz evidencia kell legyen, hogy az adat a VMM szolgáltatásokon keresztül nem szivárog.
 - Kapacitás menedzsment. A virtualizált lemezek, és hálózatok nagyobb lehetőséget nyújtanak a kapacitás menedzsmentnek.
- Adatközpont szolgáltatások:
 - A konfiguráció menedzsment adatbázisnak (CMDB) tartalmaznia kell, az összes virtuális erőforrás adatait a fizikai elhelyezkedésükről is.

26. A sikeres virtualizációt fenyegető kockázatok

- A patching, a virtuális hálózat, a VM alkalmazás elképzelések, az aláírások napra készre tételének nem adekvát ellenőrzése.
- A behatolás ellenőrző rendszerek erőltetett láthatósága, VM-ek közötti forgalomban.
- Hiányos megoldás (Biztonsági Politika, és biztonsági beállítások hiánya) a mobil VM-eknél.
- Mind a fizikai, mind a virtuális rendszerek nem megfelelő kezelése.
- A szabványok, és politikák nem megfelelő kezelése.
- Az eszközök, és folyamatok megkerülhetősége.

27. A virtualizáció előnyei

- A VM lehetővé teszi az erőforrások hatékonyabb alkalmazását, a több OS-t alkalmazó környezetet konszolidálva a nem megfelelően kihasznált szervereken kisebb számú virtuális szerverrel.
- A VM a menedzselhetőséget könnyebbé teszi. Például nincs szükség a szerver leállítására több memória hozzáadásához vagy a CPU naprakészre tételéhez.
- Az általános adminisztráció komplexitása csökken, mert minden VM szoftver környezete független az alapot képező fizikai szerver környezettől.
- A VM környezete teljesen szigetelt a host géptől, és más VM-ek környezetétől, így magas biztonságú környezetet alakíthat ki, például konfigurálni lehet a

VM-eket különböző biztonsági elrendezés szerint. Tehát bármely felhasználói kísérlet a rendszer akadályozására meg lesz hiúsítva, mert egy virtuális környezet nem tud a másikhoz hozzáférni a virtualizációs rendszer engedélye nélkül. Más szóval a hozzáférést letiltja teljesen.

- Az öreg OS áthelyezhető, mivel a fizikai gépen, amelyen fut, nehéz megfelelő hardverhez jutni. Így lehet futtatni az öreg szoftvert, amelyet nem tudott az újabb platformra áttenni.
- Szimultán lehet futtatni egy hardver részen több különböző OS-t, különböző szállítótól.
- Mivel a VM-ek fájlokban vannak, ezért könnyebben lehet őrizni, másolni egy VM-et, illetve gyorsan lehet mozgatni a teljes konfigurált rendszereket egyik fizikai szerverről a másikra.
- A virtualizáció megengedi, hogy szállítson egy előkonfigurált környezetet egy külső vagy belső telepítési forgatókönyv szerint.
- A VM-ek lehetővé teszik a hathatós hibaelhárítást, és a teljesítmény megfigyelést. Az OS-eknél a hibaelhárítás teljesítmény veszteség nélkül, és egy jóval komplikáltabb hibaelhárító környezet nélkül.
- A VM nyújt egy kompatibilis absztrakciót, így egy szoftver, amelyet számára írtak, futni fog rajta. Például egy hardver szintű VM-en futni fog minden szoftver, OS és alkalmazás, amelyet a hardverre írtak. Hasonlóan egy OS szintű VM-en futni fognak az alkalmazások, amelyre különleges OS és magas szintű VM-en programok futni fognak, amelyeket magas szintű nyelveken írtak.
- A VM-eket szigetelni lehet attól, amit futtatnak, és ezek hibamentes tartalmat nyújtanak. Be lehet vinni hibákat a szoftverbe megelőző jelleggel, a szoftver magatartásának a tanulmányozása céljára. Megőrizheti az állapotot, tanulmányozhatja, módosíthatja, visszatöltheti, stb. Továbbá a szigetelés e típusához a virtualizációs réteg végre tudja hajtani a teljesítményszigetelést úgy, hogy a VM által felhasznált erőforrások nem szükségszerűen hatnak más VM-ek teljesítményére.

A virtualizáció előnyei, összefoglalva:

- Energia és hardver megtakarítás,
- Logikai erőforrások konszolidációja,
- Szerver portabilitás,
- Az alkalmazások magas rendelkezésre állása.

28. Számítástechnikai tevékenység a felhőben, értelmezése

A felhő számítástechnikai tevékenység (cloud computing) egy módszer, amely szerint a tevékenységek, a kapcsolatok, a szoftver, a szolgáltatások egyesített elérése egy hálózaton keresztül történik. A szerverek és kapcsolatok e hálózatát hívják felhőnek, amely a felhasználók számára lehetővé teszi a hozzáférést, akár egy szuper számítógép szintű eszközhöz is. A felhasználó csak egy vékony kliens eszközt használ (iPhone, Blackberry, laptop, virtuális eszköz), amellyel elérheti mindazon erőforrást, amelyre az adott pillanatban szüksége van. Ezt a módszert nevezik „igény szerinti számítástechnikai tevékenységnek (on demand computing)” is, ahol a felhasználó igényei szerinti erőforrások rendelkezésre állását, karbantartását egy szolgáltatásnyújtó (service provider) biztosítja.

A virtuális szerverek, tehát az interneten át érhetőek el, amely azt jelenti, hogy azok a tűzfalon kívül helyezkednek el (pl. ez lehet kiszervezés). A cél a kapacitás növelése új infrastruktúra beruházása nélkül, a meglévő kapacitás kibővítése valós időben az interneten keresztül, azaz az interneten jelenlévő felhő bázisú szolgáltatásokkal.

29. Felhő bázisú szolgáltatások

A felhő bázisú szolgáltatások néhány típusa:

- A szoftver mint szolgáltatás (SaaS) a szoftvert az interneten át egy szállító vagy egy szolgáltatásnyújtó a kereső útján biztosítja több felhasználó részére, amely egy több társbérlős architektúra.
- Közszolgáltatási számítástechnikai tevékenység (utility computing), amely felhasználói igények szerinti tárolást és virtuális szervereket biztosít.
- Web szolgáltatások a felhőben (web services in the cloud) a felhő bázisú szolgáltatást nyújtók egy, a felhasználónál elhelyezett program interfésszel (API, application program interfész), amely lehet virtuális eszköz is, teszik lehetővé a hozzáférést, a felhasználó funkcionalitás felhasználás kérését.
- Platform mint szolgáltatás (Platform as a service) a kialakított saját alkalmazások, a szolgáltatásnyújtó infrastruktúráján futnak, amelyek a felhasználó számára az interneten keresztül elérhetőek.
- Menedzselt szolgáltatásnyújtó (service managed provider, MSP) az IT részére (inkább, mint a felhasználó részére) olyan szolgáltatásokat nyújt, mint az e-maileknél a víruskeresés vagy alkalmazás monitoring.
- Kereskedelmi szolgáltató platformok (service commerce platforms) egy hub, amellyel a felhasználók interaktív kapcsolatban lehetnek, és az kereskedelmi környezetet nyújt, mint utaztatás, titkári tevékenység.

30. Rács számítástechnikai tevékenység

A rács számítástechnikai tevékenység (Grid Computing) a hálózatban elhelyezett több számítógép erőforrásainak (erőforrás virtualizáció) azonos idejű használata (szolgáltatás megosztás) egy problémának a megoldására, vagy hozzáférés lehetőségének a nyújtása nagy tömegű adatokhoz. Egyesek szerint a rács számítástechnikai tevékenység a felhő számítástechnikai tevékenység szinonimája.

31. Szakkifejezések és értelmezésük

- **Adattisztítás** (data scrubbing): A nem korrekt, nem teljes, nem megfelelően formátált vagy duplikált adatok módosítása vagy visszavonása.
- **Adat virtualizáció** (data virtualization): Elvonatkoztatás az egyes adatok forrásától, és egy közös adathozzáférés réteg biztosítása a különböző adatok hozzáféréséhez.
- **Alkalmazások elszigetelése** (application isolation): A VM-ek el vannak szigetelve egymástól, nincs tudomásuk arról, hogy más VM is fut ugyanazon a gépen.
- **Alkalmazások konszolidációja** (application consolidation): A szállítók és a házi készítésű vagy licenszelt alkalmazások számának csökkentése, amely a rendszer komplexitását egyszerűsíti.
- **Alkalmazások virtualizációja** (application virtualization): A szoftver egy távoli szerveren fut, nem a felhasználó számítógépén (application portability vagy application service virtualization).
- **Egyedülálló ponthiba** (single point of failure): Egy eszközben egy komponens vagy egy pont a hálózatban, amely ha meghibásodik, a teljes eszköz vagy hálózat hibáját okozza, és ez redundanciával védhető.
- **Egységbe zárt** (encapsulated): A virtualizáció egy tulajdonsága, amely megfelel egy VM által tároltak útjának a tároló rendszerben egy egyedülálló fájlba.
- **Elszigetelt** (isolated): A virtualizáció egy védelmi módszere, amely biztosítja, hogy egy VM ne legyen képes hatást gyakorolni más VM-re, annak ellenére, hogy azonos hardveren futnak.
- **Élő háttér** (live back up): Egy VM másolása, miközben áram alatt van a VM-en kívülre, archiválás céljából.
- **Élő áthelyezés** (live migration): Egy VM mozgatása, miközben áram alatt van egy fizikai rendszerből a másikba, a szolgáltatásainak megszakadása nélkül.
- **Felhő számítástechnikai tevékenység** (cloud computing): Amikor a szoftver, a szolgáltatások elérése hálózaton keresztül történik.

- **Fizikaiból virtuálisba** (physical to virtual, P2V): Egy OS áthelyezési művelete a fizikai számítógépről egy VM-re vagy partícióra újrainstallálás nélkül. A migráció további változatai V2V, a konverziós folyamat különböző szerver virtualizáció között, és V2P a migráció a VM és a fizikai gép között.
- **Gazda gép** (host machine): A fizikai gép, amelyen fut a virtualizációs szoftver és más fizikai erőforrásokat tartalmaz (mint a memória, a merevlemez, a CPU), valamint más erőforrásokat használ, mint a hálózat, amelyet a VM is használ.
- **Gazda OS** (host OS): Ez az OS helyet ad egy vagy több VM-nek, és felosztja közöttük a fizikai erőforrásokat. A virtuális vagy particionáló termék itt van installálva.
- **Ghost account**: Egy speciális programmal másolt account.
- **Hardver virtualizáció** (hardver virtualization): Egy hardver komponensbe beágyazott VM menedzser.
- **Hálózat virtualizálás** (network virtualization): A rendelkezésre álló erőforrások összegyűjtésének módszere, a rendelkezésre álló sáv szélesség csatornákra történő felosztására.
- **Hypervisor** (hypervisor): Egy virtuális gép (VM) kezelő, irányító, amely egy program több operációs rendszerének egy hardveren történő működését teszi lehetővé.
- **Ismert és biztonságos állapot** (known and trusted state): Egy erőforrás ismert (feltárt) és megfelelő védelemmel ellátott állapota.
- **Konfiguráció Menedzsment Adatbázis** (CMDB, Configuration Management Database): Minden releváns adatot tartalmaz az IT által használt komponensekről és ezek összefüggéseiről.
- **Konszolidáció** (consolidation): A funkcionalitás átvitele sok szerverről kevés szerverre.
- **Közmű számítástechnikai tevékenység** (utility computing): Egy kiemelkedő üzleti modell, ahol a felhasználók nem vesznek hardvert, de a használatáért fizetnek. A szolgáltatást nyújtók a hardver számítási idejét igény szerint lízingelik, használják.
- **Menedzselt szolgáltatásnyújtó** (managed service provider, MSP): A menedzselt szolgáltatásnyújtó hálózatbázisú szolgáltatásokat, alkalmazásokat és készülékeket nyújt és menedzsel, vállalatoknak vagy más szolgáltatóknak.
- **Migráció, áthelyezés** (migration): 1.) A fizikai gépről a VM-re P2V, pl. egy OS áthelyezési művelete a fizikai számítógépről egy VM-re vagy partícióra, újrainstallálása nélkül. 2.) V2V, a konverziós folyamat, különböző szerver virtualizáció között, és 3.) V2P a migráció a VM és a fizikai gép között.

- **Operációs rendszer** (operating system, OS): Virtualizáció, egy számítógépen futtat több OS azonos időben, és a guest OS különbözhet a host OS-től. Disk felosztásnál (disc partitioning) a guest OS-nek azonosnak kell, lennie a host OS-sel.
- **Összegyűjtés** (clustering): Több számítógép, több tároló redundáns összekapcsolása, amely a felhasználó felé egyként áll rendelkezésre.
- **Paravirtualizálás** (paravirtualization): A virtualizációs technológia erősítése, amelyben a guest OS újra kompilálva van a VM-en belül.
- **Rács számítástechnikai tevékenység** (grid computing): Több számítógép erőforrásainak alkalmazása hálózatban, azonos időben egy probléma megoldására, amely több számítógépet igényel és hozzáférést nagy tömegű adathoz.
- **Skálázhatóság** (scalability): Egy alkalmazás vagy termék képessége (hardver, szoftver) jól folytatni a működését, ha annak (vagy tartalmának) a méretét, a térfogatát a felhasználó igénye szerint cserélik.
- **Szellem belépési tároló** (ghost account): Egy addicionális felhasználói tároló a Word Processing felhasználók részére.
- **Szerver virtualizáció** (server virtualization): Szerver erőforrások, mint a fizikai szerver, a processzor, és az OS eltakarása a felhasználó elől. A szerver adminisztrátor egy szoftvert alkalmaz egy fizikai szerver több virtuális környezetre történő felosztására.
- **Szerver konszolidáció** (server consolidation): Az ún. szerver terjeszkedés műveletének csökkentése az erőforrás felhasználás optimalizálásával, és a rendelkezésre álló számítógépek menedzsmentjének egyszerűsítésével.
- **Szoftver, mint szolgáltatás** (software as a service, SaaS): Egy szoftver elosztási modell, amelyben az alkalmazásokat egy szállítónál helyezik el, és a felhasználók egy hálózaton át érhetik azt el (pl. internet).
- **Szoftver szállítás** (software streaming): A szoftver komponenseknek (pl. alkalmazások, OS-ek, desktopok) utat biztosít a hálózaton, a központtól a végfelhasználóhoz.
- **Szigetelés** (isolation): Az operációs rendszeren futó VM-eknek nincs tudomásuk arról, hogy ugyanazon a gépen más VM-ek is futnak.
- **Tárolás virtualizáció** (storage virtualization): A fizikai tárolás összegyűjtése több hálózati tároló eszközből, amely egy tárolóként jelenik meg, és a központi konzolról kezelik.
- **Teljes virtualizáció** (full virtualization): Egy VM telepítése a fizikai gépen, amely lehetővé teszi, hogy a standard OS módosítás nélkül fusson a fizikai gépen.
- **Vendég OS** (guest OS): Egy operációs rendszer a VM-re installálva vagy egy disk partíció a host vagy a fő OS-hez adva. A vendég OS lehet különböző a host OS-től.

- **Vékony kliens** (thin client): Egy központilag kezelt számítógép, amelyen nincs CD/DVD-ROM, hajlékony lemezmeghajtó és bővítési helyek.
- **Virtuálisból fizikaiba** (V2P, virtual to physical): Egy OS és bármely alkalmazás áthelyezési művelete, egy VM-ről vagy partícióról egy vagy több fizikai számítógépre, újrainstallálás nélkül.
- **Virtuális Gép** (VM): A fizikai gép reprezentációja, amelyet a virtuális szoftver futtat, kezel.
- **Virtuális Gép Monitor** (VMM): Szoftver megoldás, amely host OS-en fut.
- **Virtuálisból virtuálisba** (V2V, virtual to virtual): Egy OS és bármely alkalmazás áthelyezési művelete, amelynek a VM vagy egy partíció ad helyet egy virtuális infrastruktúrában egy másik VM-re vagy partícióra, amely eltérő infrastruktúrán van anélkül, hogy újrainstallálnák.
- **Zöld számítástechnikai tevékenység** (green computing): A számítógép és a vele kapcsolatban lévő erőforrások használata, környezeti felelősséggel.

Irodalomjegyzék

- [1] S. Campbell, M. Jeronima: An introduction to Virtualization. INTEL Corp. 2006.
- [2] Virtualization. virtualization.info. Symantec.
- [3] Gartner Rush: Virtualization Can Weaken Security. Gartner Symposium. ITxpo. 2007.
- [4] iSCSI Superior Storage for Virtualization. searchstorage.com. Dell. 2007.
- [5] IT Agility through Automated Policy-based Virtual Infrastructure. Intel Information Technology.
- [6] Protecting Virtualized Environment with System Center Data Protection. Protection Manager. Microsoft Corp. 2007.
- [7] IBM: Why virtualization matters to the enterprise today. 2007.
- [8] A virtuális környezet biztonságossá tételének kihívásai. www.stonesoft.com. 2007.
- [9] G. Kim: Practical steps to mitigate virtualization security risks. Tripwire Inc. www.tripwire.com. 2008.
- [10] A. Baldwin, S. Shiu, Y. Beres: Auditing in shared distributed virtualized environments. HP. Labs. Uk. 2008.
- [11] Secure Virtualization Achieve and Maintain IT Security in Virtual Environment. Tripwire.Inc. 2008.

- [12] B. Botelho: VMware entering final phase of virtualization evolution Cloud computing. 2008.
- [13] R. Kvanagh: Virtual Appliances -The Evolution of a Gold Standard. ISACA. 2008.
- [14] G. Shields: Best practices in implementing virtualization. Realtimepublishers.com. 2008.
- [15] G. Gruman: What cloud computing really means. InfoWorld. 2008. 04.
- [16] Marti Katin: Got the Enterprise Software Blues? Appliance based Software Delivery. KACE 2006.
- [17] An introduction to the HP Virtual Server Environment. HP. 2007.
- [18] Chris Wolf: Let's get Virtual – A Look at Today's Server Virtualization Architectures. Burton Group. 2007.

Tévhitek az információról, a biztonságról „Errare humanum est”

Vasvári György CISM

Információs Társadalomért Alapítvány
1507 Budapest, Pf. 213
Telefon: +36-1-279-1510, Fax: +36-1-279-1511
e-mail: gvasvari@tiphaz.hu

Absztrakt

Az információval, informatikával és biztonsággal foglalkozó hazai ismeretterjesztő „szakirodalom” és sajtó széles palettája az elmúlt évtizedekben – tisztelet a kivételnek – nem segítette a pontos értelmezés beépülését a számítástechnikai eszközökkel egyre jobban telezsúfolt környezetünk használati kultúrájába. Jelen cikk a tévhitek kialakulását vizsgálja és egyes konkrét példákat igyekszik helyretenni.

Kulcsszavak: tévhit, adat, információ, információrendszer, biztonság

1. Bevezetés

Az elmúlt évtizedekben, az informatikai, az információval és az információ technológiával foglalkozó tudomány, és ipar, szolgáltatás folyamatos fejlődésen ment végbe és a folyamat nem állt meg. Kétségtelen, hogy az információs társadalomban ma már egyre többen rendelkeznek olyan ismeretekkel és tapasztalatokkal, amely elsősorban a személyes célra használt számítástechnikai oktatás, alkalmazás, eszközök, és az internet széles körű elterjedésének köszönhető. Így természetesen egyre nagyobb számban vannak olyanok, akik tanulva, önképzéssel, vagy a mindennapi munkájuk során megszerzett ismeretekkel rendelkeznek. Ha megvizsgáljuk a TÉVHIT következményeit, akkor az igazán komoly kockázatot az jelenti, ha a téves nézetek vagy vezetői döntés formájában jelentkezik vagy pedig az informatikát alkalmazók körében a minden napi munkájuk során.

A tévhit, a Columbia Encyclopaedia szerint, a valóság helytelen reprezentációja.

A tévhit tehát, irracionális. Különösen veszélyes a tévhit, ha a biztonság körében van jelen, mivel ez hibás védelmi intézkedést von maga után, és különösen káros, ha a védelmi

intézkedés elmaradását eredményezi. Szükségesnek tartom megemlíteni annak a vállalati vezetőnek az esetét, aki a Működés Folytonossági Terv készítése közben megkérdezte, hogy „Önök atomtámadásra akarnak felkészíteni minket?”.

Vitathatatlan, hogy a tévhitek elleni küzdelemben a megfelelő színvonalú, szervezeti kultúrát, biztonsági kultúrát a szervezet küldetése függvényében meghatározó tényezőnek kell tekinteni.

Szükséges azonban arra figyelmeztetni az olvasót, hogy az alábbi tévhit gyűjtemény és a valós válaszok, nem általánosan elterjedt tévhitekről szólnak, hanem okulásképpen a szerző által, munkája során összegyűjtött, egyes nézeteket mutatnak be, tehát a példák többsége nem általánosítható, és a cikkben a teljesség igénye nélkül szerepel.

2. A tévhitek keletkezéséről

Tévhitkeletkezésének okai között a következőket adhatjuk meg:

- Az objektív szemlélet hiánya;
- A megfelelő ismeretek hiánya;
- Az állásfoglalás, nézet kialakítása nem megfelelő elemzés, vizsgálat alapján történt, hibás következtetés;
- A veszélyérzet hiánya;
- A saját tevékenységem fontosságának igénye;
- Túlzott bizalom, bizonyos, már meglévő eljárásokban vagy az adott, már meglévő bizalom, indokolatlan értékelése;
- Nem egyezés a szervezet kultúrájával (biztonsági kultúrájával);

Felmerül az a kérdés is, hogy vajon az értelem (ismeret, tudás, gondolkodás stb.), és/vagy az érzelem (érzékenység, sértődés, ragaszkodás stb.) játszik-e szerepet a tévhitek kialakulásában.

A Magyar értelmező szótár szerint:

- Az értelem a megismerő tevékenység legmagasabb foka, a logikus gondolkodás képessége.
- Az érzelem az a lelki jelenség, amelyben a környező világ jelenségeihez, és önmagunkhoz való viszonyunk tükröződik.

A tanulmány szerzője szerint a válasz azonban már nem az ő szakmai kompetenciája.

3. A tévhitek

3.1. Az adatról, és az információról

T1: Az adat és az információ azonos fogalmak

Néhány évtizeddel ezelőtt azt vallották, hogy az információ a rögzített adat. Kb. tíz évvel ezelőtt még külföldi szabványban is megjelent, hogy valójában a jelentésük azonos. Ma az adat, és az információ meghatározása, az ISO/IEC 27002 szabvány, illetve a COBIT 4.1 felhasználásával:

- Jel, esemény, tény, utasítás, elképzelés: A jel tehát térben és/vagy időben érzékszerveinkkel, eszközeinkkel érzékelhető, felfogható, egyes esetekben mérhető jelenség, folyamat. A jelek így lehetnek:
 - Látható, szemünkkel érzékelhető, esetleg kezünkkel tapintható jelek (rajzok, képek, szimbólumok, tárgyak vagy virtuális tárgyak, mint a hologram),
 - Hallható jelek (beszéd, zene, zaj), amely a fülünkkel érzékelhető.

Az információelmélet a jeleket két osztályba sorolja:

1. Analóg jelek, amelyek valamilyen fizikai jelenséggént érzékelhetők, időben és térben folyamatosak.
2. Digitális jelek, amelyek számszerűek, diszkrét értékkel vannak reprezentálva.

Az analóg és digitális jelek egymásba átalakíthatóak.

- Az adat tények, elképzelések, utasítások vagy a legtágabb értelemben vett strukturált, nem strukturált jelek (rajzok, hangok stb.) emberi vagy technikai eszközökkel történő formalizált ábrázolása közlés, feldolgozás, illetve távközlés céljára.
- Információ az értelmezett adat, amelynek következtében új ismerethez jutunk, amely tehát ismerethiányt, bizonytalanságot szüntet meg. Továbbá a tudomány és a technika három alapelemének egyike (energia, anyag, információ).

A jel, az adat és az információ között tehát meghatározott kapcsolat áll fenn. Például az egy (1) lehet jel (kódolva jelsorozat), amely közlés, írás illetve technikai úton továbbítva adat, míg megértve, hozzárendelve jelentését információ (pl. 1 db INFOTA kiadvány).

- Tudás az adatok értelmezésének, a hatékony valamint eredményes felhasználásának képessége, amelynek létrejöttében nemcsak a képzés, hanem a tapasztalat is alapvető szerepet játszik.

T2: Az adatvédelem, és az információvédelem azonos

A személyes, és közérdekű adatok védelmével foglalkozó törvény egyértelműen kimondja, hogy az adatvédelem, és az adatbiztonság a személyes adatokra vonatkozik, azaz e két fogalmat lefoglalja, ezért nagyon megfontoltan kell kezelni, használni ezeket, a fogalmakat. Egyáltalán nem mindegy, hogy például adatvédelmi felelősnek, adatbiztonsági felelősnek, információ biztonsáért felelős munkatárnak, milyen feladatokkal foglalkozókat nevezünk ki. Az adatvédelmi, adatbiztonsági felelős a személyes adatok védelmével foglalkozik, foglalkozhat. Ugyanakkor az információvédelem, mivel az információ minden információra, adatra vonatkozik, beleértve a személyes adatokat is, nem azonos fogalom.

Egy vállalatot (szervezetet) alkotó rendszerek:

- Üzleti rendszer,
- Termelési, szolgáltatási rendszer (ha ilyen a vállalat küldetése),
- Információ rendszer, amelynek része az
 - informatikai, számítástechnikai rendszer,
- Biztonsági rendszer
 - Üzleti biztonsági alrendszer,
 - Üzembiztonsági alrendszer,
 - Információ biztonsági alrendszer.

T3: Információs rendszer és nem informatikai rendszer a helyes kifejezés.

Az információ rendszer, mivel az információ a vállalat, a szervezet minden pontján megtalálható, szükségszerűen átfogja az egész vállalatot. Ezzel szemben az informatikai rendszer fogalom a számítástechnikai rendszerre vonatkozik, amely a rendszerbe beadott adatokat, információkat feldolgozza, és azt elektronikusan vagy papír alapra kinyomtatva vagy emberi beszéd útján továbbítja. Az ISACA által kiadott COBIT Security Baseline 2. 2007 a következő definíciókat adja meg:

Az információbiztonság a menedzsment folyamatokat, a technológiát szolgálja, biztosítja, hogy az üzleti vezetés bízhatson az üzleti tranzakciókban.

A számítástechnikai (informatikai) biztonság a számítógép biztonsága, lehet függeni tőle, és a rajta futó, a feladatok végrehajtásához szükséges (általunk elfogadott) szoftvertől.

Meg kell említeni, hogy a Magyar értelmező szótár szerint

- az információ adat, értesülés, míg
- az információs, az információval kapcsolatos tájékoztatást jelenti.

Tehát, amit általában információs rendszernek hívnak, helyesen információ rendszer, míg az információs rendszer például a közlekedési vállalatoknál az utastájékoztató rendszer, azaz egy olyan információ rendszer, amely a tájékoztatás céljára szolgál.

3.2 Általános kérdésekről

T4: Ez csak nálunk, Magyarországon fordulhat elő.

Az információ biztonság olyan terület, ahol ma már a támadási célok, módszerek, eljárások igen gyorsan terjednek, és világszerte megjelennek, globalizálódnak. Ennek oka az internet, amely a különféle támadások globális terjedésében közvetlen szerepet játszik. Mégpedig vagy úgy, hogy saját maga teszi ezt lehetővé, mint a lehetőségek felkínálója vagy egyes esetekben a célok, módszerek, eljárások ismertetésével járul hozzá. Ez utóbbi az az eset, amikor a támadás a szervezeten belül történik meg. Továbbá, egy ilyen nézet kialakulásában a tények ismeretének hiánya is megmutatkozik.

T5: A mi vállaltunkat nem érte, és így nem is fogja támadás érni.

Gyakoriak az olyan példák, amikor biztonsági esemény a szervezet életében még nem fordult elő, vagy ha előfordult még soha nem jelentették. Ez nem jelenti azt, hogy nem is fog előfordulni. A biztonsági eseményeket motiváló alábbi tényezők, egyértelműen mutatják, hogy bekövetkezhetnek a szervezet és a potenciális támadók oldalán egyaránt olyan változások, amelyek a támadó számára indokoltá teszik annak végrehajtását. Ilyen motivációs tényezők lehetnek, például:

- A pénzügyi helyzet jelentős változásai,
- Egyes személyek személyes adatai,
- A tevékenységek során elkövetett hibák,
- A piaci verseny szempontjából érdekessé vált adatok,
- A védelem hiányosságai a támadási módszerek függvényében (ami ma még elriasztó volt, holnap motiváló lehet), a védelem alakításában szerepet játszó, a döntéshozók nem tartanak lépést a változásokkal, és hozzájárulnak a támadók információs előnyének, fölényének a védekezőkkel szembeni folyamatos fenntartásához, esetleges növekedéséhez.

Vajon minden embert, akit kirabolnak, már érte hasonló támadás korábban is?

T6: A vállalati biztonsági kockázat egyenlő az IT biztonsági kockázattal.

A vállalati biztonság a vállalat olyan kedvező állapota, amikor a vállalat fenyegetettsége minimális. A vállalatot a COSO ERM szerint egyaránt fenyegetik belső és külső kockázatok, amelyeket nem lehet nullára csökkenteni. A kockázatok soha nem szűnnek meg. A vállalat biztonsági rendszere az alaptevékenység, termelési és az információbiztonsági alrendszereiből épül fel. Ezekben a fenyegetettség soha nem egyenlő nullával. Tehát nem lehet egy vállalat biztonságát csak az egyik alrendszer biztonságával azonosítani, mivel akkor is maradnak még területek kockázatoknak kitéve (védelmi intézkedések megtétele esetén is). Továbbá a biztonsági rendszeren belül két (három) biztonsági alrendszer egymással kölcsönhatásban van, így a védelem hiánya egy biztonsági esemény bekövetkezésekor a másik rendszerre hatást gyakorolhat, amely lehet, hogy így nem találkozik védelmi intézkedéssel.

3.3. A humán erőforrásokról***T7: Az emberek alapvetően nem megbízhatóak.***

Véleményem szerint, ez egy félremagyarázása annak a biztonságtechnikában ismert tételnek, amely szerint a biztonság szempontjából az ember a leggyengébb láncszem. Ugyanis ez a tétel nem ezt jelenti. Az emberekben meg lehet bízni, és e szerint is kell kezelni őket. A tételből az következik, hogy egy munkatárs megbízhatatlanná válhat, például szenvedély beteg lesz. Ezért, komoly figyelmet kell fordítani a humán kockázatok csökkentésre tett védelmi intézkedések meghatározására, kiválasztására, és megvalósításuk, végrehajtásuk ellenőrzésére. A megbízhatóság a felvételkor döntendő el annak a figyelembe vétele mellett, hogy minden ember képességei különböznek egymástól. Egy szervezetnek lehet meghatározott képességekre vonatkozó igénye.

T8: Nálunk csak megbízható munkatársak vannak.

Ez a nézet az előző fordítottja. Optimális felvételi követelmények esetében is az egyes munkatársak képességek függvényében egy biztonsági eseményre történő válaszuk fenyegetést jelenthet a vállalat biztonságára nézve. A humán erőforrásoknál is fenn áll az a biztonsági tétel, hogy bármilyen erősségű védelmi intézkedéseknek a megtétele esetén is számolni kell maradék kockázatokkal. Például felvételkor nem derül ki, hogy döntési helyzetbe kerülve ki hogyan fog reagálni.

T9: A külső szakember nem megbízható, nem szabad kiszervezni.

A kiszervezés kétségtelen felvet biztonsági kockázatokat, ez azonban nem azt jelenti, hogy ha valóban érdek fűződik hozzá, nem szabad megtenni. Az ilyen kockázatok, a vállalatbiztonság érzékenysége függvényében csökkenthetőek, és ez a feladat, nem a tiltakozást jelenti ellene. Ma a vállalatok számára a kiszervezés a költségek csökkentésének módszere szerte a világon széles körben alkalmazott. Számtalan szabvány, ajánlás, gyakorlati tapasztalat, leírás áll rendelkezésre, amelyek alapján a kiszervezés kockázatait szakszerűen és eredményesen elfogadható szintre lehet csökkenteni.

T10: A biztonsági intézkedések nem sérthetik egyének érdekeit.

A biztonsági rendszerben megtett intézkedések ezzel szemben igen gyakran sérthetik az egyének érdekeit, ugyanis lehetséges, hogy egy feltárt kockázat, egy feltárt hiányosság, illetve egy biztonsági esemény következménye, a kockázat csökkentése érdekében megteendő intézkedés, amely feladatköröket, hatásköröket, jogokat, jogosultságokat változtathat meg. Az egyén természetes reakciója ilyen esetben nem az öröm, hanem akár a sértődés is. Ezért feltétlenül! szükséges az intézkedés meghozatalakor annak emberi hatásait is mérlegelni, majd kezelni.

T11: A szervezet, vállalat iránti hűség, elkötelezettség egy határon túl röghöz kötöttséget eredményez.

A vállalat iránti hűség, az ahhoz való ragaszkodás fontos alakítója, a biztonsági tudatosságnak. Az, hogy egy alkalmazott szereti a vállalatot, nemcsak jövedelem kérdése, hanem a főnökhöz való viszony, az előtte álló reális szakmai, emberi, jövedelmi, azaz megbecsülési lehetőségek, amiért úgy érzi, hogy érdemes tenni, és maradni. Ez tehát nem röghözkötöttség, mert mindenkinek saját elhatározásán múlik, hogy marad, vagy megy.

T12: A legjobb fejlesztő, szervező a legjobb rendszergazda, akinek a rendszerrel kapcsolatban bármilyen tevékenységről döntési joga van.

Természetesen egy rendszert, annak a fejlesztője ismeri a legjobban. Ezzel azonban élni, nem visszaélni kell. Ugyanis ha minden fejlesztőt elszippant az üzem, akkor felmerül a kérdés, hogy ki fogja ezeket a jó rendszereket fejleszteni. Az a megoldás, hogy fizessük meg és lássa el mind a két feladatot, biztonsági szempontból megengedhetetlen. Az, aki fejleszt, nem üzemeltethet és fordítva se. Azaz ez két olyan feladatkör, amelyet ugyanaz a személy nem tölthet be (segregation duty).

T13: A munkatársaink alapképzettsége biztosítja a jövőben is a megfelelő felkészültséget.

Az életet a folyamatos változás jellemzi. A támadók mindig előttünk járnak. Ezért az új helyzetek új védelmi intézkedéseket és azok elsajátítását igénylik. A biztonsági képzettség, mint maga a biztonság is a folyamatosság, a folyamatos képzés jegyében valósulhat csak meg.

3.4. A rejtjelezésről

T14: A rejtjelezéssel, teljes biztonságot lehet nyújtani.

Ez a nézet nem veszi figyelembe, hogy egyrészt nincs 100%-os biztonság, másrészt a rejtjelezett szöveg megfejthető, erre különböző módszerek vannak. Például sokáig az RSA-t megfejthetetlennek tartották, míg a magyar Dénes József matematikus kandidátus meg nem találta egy 19. század elején megjelent matematikai lapban azt az eljárást, amellyel a megfejtés lehetségesé vált. Másik példa: a szovjet diplomácia olyan erős rejtjelezési eljárást használt, hogy elvileg meg nem fejthetőnek tartották. Azután a Szovjetunió összeomlását követően, az amerikaiak közölték a szovjet diplomácia elmúlt évtizedekben küldött rejtjelezett anyagait, amelyeket egy szovjet rejtjelező elkövetett nem tudatos hibája alapján tudtak éveken keresztül megfejteni. Tehát nincs olyan eljárás, ami megfejthetetlen, ellenben van olyan erős rejtjelezési módszer, amelynek használható időn belül a számítástechnikai eszközök jelenlegi fejlettsége mellett a megfejtése nem lehetséges.

T15: A biztonságos rejtjelezés lehet szoftver, vagy hardvereszközzel.

A szoftverek a fejlesztők vagy a rendszert alkalmazók (pl. a rendszert jól ismerő rendszergazda) által manipulálhatók. Ugyanakkor a hardver eszközök következmények nélkül, nem tűnnek semmilyen manipulálást, ezért a csak szoftveres eljárások biztonsági erőssége gyenge. Elég gyakori, hogy két eszközt egyaránt alkalmaz.

T16: A hálózati rejtjelezés biztonságot nyújt.

Az állítás ellen szólnak a következők:

- A hálózatokról az azokon haladó információk leszívhatóak. Különösen belső hálózatokon, amikor még nem kerültek a hálózatra vagy már eljutottak a cél állomás hálózatára, nagy a kockázata.
- A hálózatra kerülés előtt, belső munkatársak is manipulálhatják, illetve nem tudatos hibát követhetnek el.

- A bérelt vonalak különösen kockázatosak, mert a szolgáltató a bérelt vonalak egyes szakaszait – a bérlő tudta nélkül – változtathatja.
- A rejtjelezés biztosítja a hitelességet.

Tekintettel arra, hogy egy rejtjelezett szöveg manipulálását nem lehet kizárni, így a rejtjelezett szöveget meg lehet változtatni vagy a küldőt az eredetet hamisan feltüntetni. A hitelességet az elektronikus aláírás alkalmazásával lehet biztosítani.

3.5. A kockázatokról

T17: A kockázatokat fel kell számolni.

Ez természetesen egy normális igény, azonban ha megtesznek egy kockázattal szemben egy védelmi intézkedést, akkor meg lehet, és meg is kell határozni, becsülni, a kockázat csökkenésének mértékét. Lehet, különböző erősségű védelmi intézkedéseket tenni, de olyan védelmi intézkedés nincs, amelynél nem marad maradék kockázat. Azaz, itt jön a biztonságtechnika alaptétele: 100%-os a biztonságtechnikában csak az, hogy semmi nem 100%-os. A vezetők jelentős része nem tudja elfogadni, hogy komoly költségek árán nem juthat teljes biztonsághoz, és ilyenkor a munkatársait vonja felelősségre.

T18: Erős védelemnél a kockázat nem következhet be.

Különösen vezetők részéről gyakran hangzik el az a kérdés, ha adok ehhez pénzt, akkor többet nem fog ez előfordulni? Erre, pedig csak az lehet a válasz, hogy az intézkedés eredménye a kockázat meghatározott mértékű csökkenése. Például, egy katasztrófahelyzet bekövetkezési valószínűségének kockázatának mondjuk 60%-os csökkentése olyan eredmény-e, amely a vállalat biztonság érzékenységének függvényében a beruházási igényt indokolja-e vagy sem. Ennek alapján lehet a megteendő intézkedésről dönteni.

T19: A kockázatot ki lehet, és kell számítani.

Divatos dolog, olyan programokat készíteni, reklámozni, amely szerint a programmal a kockázatok kiszámíthatóak. A valóság azonban az, hogy a jövőt nem lehet kiszámítani. A kockázat a bekövetkezési valószínűség bizonytalanságát fejezi ki. A Neumann János és Morgenstein által kidolgozott játékelmélet kellőképpen bizonyítja ezt. Ezek a programok valójában komoly segítséget jelenthetnek egy kockázat meghatározásához, de becsült elemet, elemeket sem nélkülöznek. Azaz figyelembe lehet venni, használni lehet őket, de az eredmény soha nem lesz tökéletes. Az ellentét valójában ott oldható fel, ha a kockázat becsült minősítéseihez (alacsony, kicsi, közepes magas, igen magas), például egy ötös skálán számértékeket, rendelünk. Alacsony=1, kicsi=2, közepes=3, magas=4, igen magas=5).

Ebben az esetben a kockázatokkal már lehet a számszerűsített minősítések alapján számításokat végezni. Ettől azonban a kiindulás becsült marad. Így az eredmény sem tekinthető egzakt értéknek.

T20: A kockázati étvágó a vállalat anyagi lehetőségeitől függ.

Kétségtelen, hogy egy vállalat, szervezet anyagi lehetőségei meghatározzák beruházási lehetőségeit. Azt viszont, hogy egy vállalat mennyi maradék kockázatot vállalhat fel, azt a vállalat biztonság érzékenysége függvényében kell meghatározni. Arra pedig van lehetőség, hogy ennek a szintnek az elérésére a vállalat költségviselő képességének megfelelően határidőket tűzzenek ki. Ebből azonban az következik, hogy a vállalat felvállal egy időszakot, amikor a kockázati étvágót meghaladó kockázatok lesznek jelen. Ez természetesen újabb kockázat létrejöttét jelentheti, amelyet a vezetésnek szintén fel kell vállalnia.

A kockázati étvágó a maradék kockázatok becsült értékeinek összege, amelyet a vállalat megenged. Azaz, ha az így kijött érték magasabb a megengedettnél, akkor egy vagy több maradék kockázatot csökkenteni kell.

T21: A kockázatos tevékenységet el kell kerülni, nem szabad alkalmazni, és a kockázatok ellen védekezni kell.

Ismeretesek olyan vállalkozások, amelyek bizonyos tevékenységeket nem végeznek, az azzal járó kockázat miatt. A legismertebb példa, amikor internet használatot egyáltalán nem engedélyeznek egy vállalatnál. Kétségtelen, hogy ekkor az internet alkalmazás következtében kockázat sem lép fel. Ugyanakkor számos hátrány jelentkezik, mind az ismertek szerzése, mind a vállalat marketing tevékenysége területén. A helyes álláspont nem a kockázatot hozó tevékenység elkerülése, hanem az indokolt alkalmazások, és előnyeik meghatározása, valamint a pontos szabályozás, az alkalmazások folyamatos ellenőrzése.

A másik igen jellemző példa az outsourcing, kiszervezés elkerülése. Nem ismételjük meg a fentieket, de hozzátesszük, hogy vajon, ha nem alkalmazok valamilyen, egyébként komoly előnyöket jelentő megoldást, az nem jelent a vállalkozás számára működési problémát, de adott esetben veszteséget is okozhat.

Itt kívánjuk rögzíteni, hogy a tévhitek nélkülözik a szakszerű vizsgálatokat, megfontolásokat, így maguk is kockázatot képeznek, és nem is vezethetnek előnyökhöz.

3.6. A jelszavakról

T22: A jelszó biztonságos.

A felhasználók egy jelentős része abban a hitben él, hogy a jelszavak minden esetben biztonságosak. Valójában azonban leggyakrabban nem használnak elég hosszú jelszót, mivel azt meg kell jegyezni. Azok, akiknek több jelszót kell használniuk, különösen hajlamosak arra, hogy feltörhető jelszavakat alkalmazzanak. A véletlen számsorozatból álló jelszó feltörhetetlen lenne, ha az előállítása, nem követelne meg olyan feltételeket, amelyeknek a megteremtésére általában nincsen lehetőség.

3.7. Védelmi intézkedésekről

T23: Egy munkakör ellátásához széleskörű, nem korlátozott hozzáférési jogosultság kell.

A munkavállalók általában, különösen az ügyek intézői, a rendszergazdák úgy gondolják, hogy eredményes munkát csak széleskörű információk birtokában tudnak végezni. Az ISO 27000-es biztonsági szabványok szerint ugyanakkor korlátozni kell a hozzáférési jogosultságokat, ahogy az amerikaiak mondják a „need to know”, a szükséges tudás elvét alkalmazva. Ezért a hozzáférési jogosultságok megállapításával a megbízottnak a dolga, hogy megismerve az adott szakterület vezetőjének a véleményét, csak azokat a hozzáférési jogosultságokat biztosítsa, amelyek az adott munkatárs munkájának ellátáshoz szükségesek.

T24: A védelmi intézkedéseket nem oktatni, hanem jó szabályzat alapján végrehajtani kell.

A jó szabályzat kevés a rendeltetésszerű végrehajtás biztosításához. Ugyanis egyrészt oktatással meg kell értetni, minden vonatkozásban egy védelmi intézkedést, másrészt u.n. ismételt, fegyelmezési gyakorlatokkal, el kell érni, hogy a rendeltetésszerű végrehajtás, véletlen hibák miatt ne sérüljön.

T25: A sikeresen működő védelmi intézkedést nem szabad megváltoztatni.

A sikeresen működő védelmi intézkedés egy biztonsági esemény közvetlen vagy közvetett hatása miatt módosítható, mivel a támadók folyamatosan a védelem módszereit megismerve élnek előnyükkel.

T25: Nálunk ez nem történhet meg

Elég gyakori annak a hangoztatása, elsősorban vezetők részéről, hogy biztonsági intézkedéseik, a munkatársak biztonsági kultúrája kellő mértékben biztosítja azt, hogy „nálunk ez nem történhet meg”, ezért egy meghatározott védelmi intézkedésre itt nincs szükség. A védelmi intézkedés azonban, nem az adott vállalat (szervezet) negatív minősítése, esetleg nem felesleges pénzkiadás, hanem annak a felismerése, hogy 100%-os biztonság nem létezik, azaz mindig van maradék kockázat. Egy biztonsági esemény bekövetkezési valószínűsége tehát soha nem lehet egyenlő nullával. Érdeemes idézni J. Essinger „Számítógépes biztonság a pénzügyi szervezetekben” című, 1996-ban megjelent könyvéből, amely szerint az angol bankok első kockázata a bankvezetők takarékosági mániája, amely a védelmi intézkedést vagy egy védelmi intézkedés erősségnövelésének elvetését indokolják.

3.8. Az ellenőrzésről

T27: A külső, audit felesleges, mert az auditor azt írja le, amit az auditált cég munkatársai mondanak.

A külső független audit ellenzőinek véleménye ez, amely azon alapul, hogy a helyzetfelmérés során az auditorok a munkatársakkal interjúkat készítenek, és az ezekből levont következtetéseket a helyzetfeltárási jelentésben foglalják össze. Ugyanakkor az említett ellenzők, amikor az auditor megállapításainak helytállóságáról elfogadó nyilatkozatot kell tenniük, már lényegesen más véleményt képviselnek. A munkatársak interjúi, a szemlékkel, dokumentumok feldolgozásával, és tesztekkel kiegészítve alakítják ki az auditor megállapításait.

T28: Az audit során feltárt veszélyforrások kompromittálják a vállalatot, elsősorban a vezetést.

Ez a nézet igen nagy kockázatot jelent, mert a támadási módszerek gyorsabban fejlődnek, mint a védelmi módszerek. A támadáskor a támadó mindig előnyben van. Ezért a rendszeres ellenőrzés, a veszélyforrások, az új kockázatok feltárása elengedhetetlen a hatékony védelem megteremtéséhez.

T29: A belső ellenőr szakmai kompetenciáját, az adja meg, hogy azt a szakterületen ellenőrzi, amelyen dolgozik, amelyhez ért.

Amennyiben az ellenőrzendő területen olyan szakkérdésekkel kell foglalkoznia a belső ellenőrnek, amelyekben nem kompetens, akkor szakértőt kell igénybe vennie. Azonban, mind a belső ellenőrnek, mind a szakértőnek függetlennek kell lennie a vizsgált területtől. A Belső Ellenőrök Világszervezete egyértelműen kimondja, hogy azt a területet, ahol a belső ellenőrt foglalkoztatják, azt ő maga nem ellenőrizheti. Ez egyébként megfelel a szabványokban is szereplő feladatszétválasztás elvének is. A SOX felveti, hogy az auditori, szakértői tevékenységet csak akkreditált szervezet által regisztrált szakemberek végezhetnek.

T30: Az auditor, a szakértő kötelessége minőségi munka végzése.

Vitathatatlan, hogy az auditortól el lehet várni a minőségi munkát (ISACA Etikai Kódex), ez azonban – mint a gazdasági élet minden más területén – nem zárja ki, sőt szükségessé teszi a minőségbiztosítást és a minőségbiztosító minőséget igazoló nyilatkozatát, azaz a Minőségbiztosítási Záradékot az audit jelentés végén. A minőségbiztosító kompetenciáját az adott munkára egy erre jogosult szervezet által kiállított Megbízólevéllel kell igazolni.

3.9. A vállalat, a szervezet üzleti érdekeiről

T31: Az üzleti érdek az elsődleges.

Az üzleti érdek természetesen egy üzleti tevékenységet folytató vállalatnál elsődleges, azonban ez nem mehet a biztonság rovására, ugyanis a biztonság is üzleti érdek. Meg kell azt állapítanunk, hogy jelentős kockázati tényező a biztonság szempontjából, a vezetők, vagy az anyavállalat takarékosági célkitűzéseinek helytelen arányú megválasztása. A takarékoság szükséges, de egyúttal kockázatot is jelent egy cég pénzügyi problémáinak megoldására. Ki kell mondani, hogy a védelmi intézkedések elhatározásakor a pénzügyi érdekek nem lehetnek kizáró tényezők, csak a megvalósítási prioritások meghatározóak.

T32: A biztonsági esemény üzleti titkot képez, ezért kerülni kell a cégen kívüliek tájékoztatását, a számonkéréshez a hatóságok bevonását.

Kétségtelen, hogy nem tesz jót a vállalatról alkotott képnek, ha egy biztonsági esemény kiszivárog, azonban ami büntett, az a rendőrségre tartozik, és nem lehet eltitkolni. Ennek a vezetői magatartásnak igen negatív hatása van a munkatársakra, nincs elrettentő vagy szebben mondvá visszatartó ereje, így egy azonos elkövetés motiváló tényezője lehet.

3.10. A rendszerekről

T33: A vállalat szervezése, folyamat szemlélettel történik.

A vállalatokat, amelyek rendszerek, rendszerszemlélettel kell megközelíteni. Ma már vállalati szintű biztonsági megoldásokat igényelnek a szakemberek, mint például: a vállalati szintű kockázatmenedzsment (enterprise wide risk management), vagy a vállalati szintű azonosság menedzsment (enterprise wide identity management). Ugyanakkor a vállalatot alkotó rendszerek (üzleti, termelési szolgáltatási, információ és biztonsági rendszer) folyamatokból épülnek fel, és az egyes folyamatokban a célt tevékenységekkel realizálják. Előfordul, hogy egyesek a vállalat rendszerei közé nem veszik be a biztonsági rendszert. A biztonsági rendszer a vállalatot (szervezetet) alkotó három (kettő) rendszert átfogja, azaz vállalati szintű. Elemei pedig azok a biztonsági alrendszerek, amelyek az egyes rendszerek biztonságáról gondoskodnak. A vállalati rendszeren belül azonban a szervezésnek már folyamat szemlélettel kell történnie.

T34: A vállalatot alkotó rendszerek függetlenek egymástól.

A vállalatot, szervezetet alkotó rendszerek nem függetlenek egymástól. Egyrészt egyaránt az adott vállalat küldetéseinek megvalósítását szolgálják, másrészt tevékenységeik egymásra épülnek, átfedik egymást. Legyen itt példaképpen az információrendszer, amely egyaránt feldolgozza a másik rendszerek adatait, és az eredményt szolgáltatja a másik rendszerek számára. Adatok a vállalat minden pontján keletkeznek, és igényelhetik őket.

T35: Az egyes rendszerek gazdáinak kell döntenie, minden, a rendszert érintő kérdésről.

Ez a vélemény ellentmond a feladat szétválasztás elvének, amely szerint (lásd COBIT 4.1), nem lehet ugyanaz a személy felelős üzemeltetésért és fejlesztésért vagy biztonságért és bármilyen más tevékenységért, stb. Ezt a sarokszabályt nevezhetjük a belső függetlenség biztosítását szolgáló szabálynak is.

3.11. A biztonságról

T36: A biztonságnak biztosítani kell a teljes védettséget.

Vitathatatlanul ez lenne az ideális minden vállalat, szervezet számára. Azonban a teljes védettség azt jelenteni, hogy az adott szervezet ellenálló képessége maximális, azaz sikeres támadás végrehajtásának a valószínűsége nulla. Ez azonban – miután a kockázatokat nem lehet nullára csökkenteni – a gyakorlatban egy indokolt, de nem megvalósítható igény. A

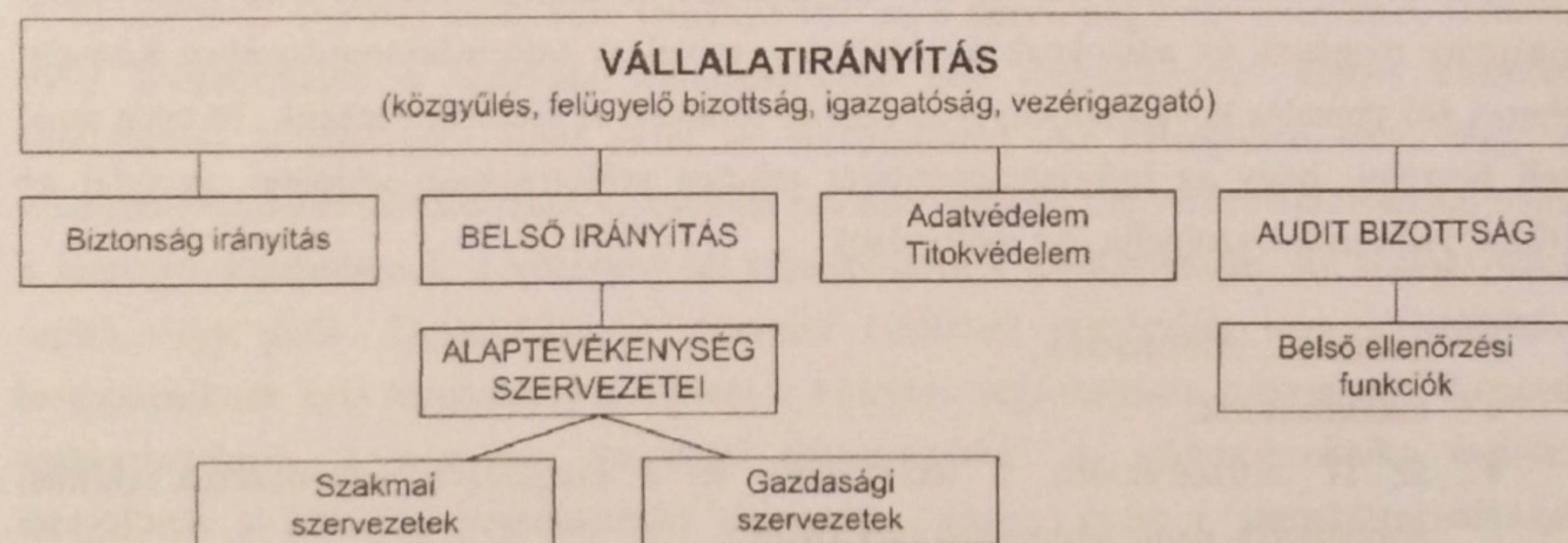
támadók és a védelem között egy véget nem érő verseny áll fenn, de az előny mindig a támadónál van, mert sem a támadás módszerét, sem az időpontját nem lehet előre megjósolni.

T37: A biztonságot, a vállalatot, szervezetet alkotó rendszerekben kell irányítani.

Az említett feladatszétválasztás elve alapján a biztonságot vállalati szinten az alkalmazásának területeitől elválasztva kell, szabad irányítani. Ez hasonlatos, a nemrég a Belső Ellenőrök Világszervezte által kialakított új szervezeti elemhez, a belső ellenőrzési funkciókhoz, amelyet a felső vezetéshez tartozó Audit Bizottságnak kell arányítani. A belső ellenőrzési funkciók: a belső ellenőrzés, a megfelelőség menedzsment, a kockázat menedzsment és mindezt még ki szokták egészíteni a vállalati kultúra menedzsmenttel.

T38: A vállalat információrendszerének biztonságával, magában az információrendszerben kell foglalkozni

Az információrendszerben kell lennie biztonsággal foglalkozó munkatársnak, hasonlóan a másik rendszer(ek)hez, de ennek a személynek a szakmai irányítását a biztonsági szervezetnek kell ellátnia, azaz a szervezet főnöke csak munkajogi szempontból irányíthatja őt. A ma elvárt szervezetet szemlélteti az alábbi ábra.



1. ábra: A ma elvárt szervezet

A ma elvárt szervezet vállalati szintű biztonságirányítást, belső ellenőrzési funkciókat (kockázatmenedzsment, megfelelőség menedzsment, szervezeti kultúra menedzsment, belső ellenőrzés menedzsment) követel meg, amelyek jelentősen átalakítják egy vállalat szervezetét. Ez az elvárás az irányítás, megfelelőség, kockázat menedzsment, belső ellenőrzés, és a kultúra menedzsment integrált, centralizált, és összehangolt rendszere. A COSO anyagok határozottan rámutatnak arra, hogy ezek a tevékenységek valójában ellenőrzést igényelnek. Ellenőrzést pedig az irányításnak kell integráltan kézben tartani úgy, hogy az ellenőrzést végzők függetlensége az ellenőrzött területektől, tevékenységektől

függetlenek legyenek. Ezek az anyagok egyértelműen kimondják, hogy valaki azt a területet, ahol egyébként dolgozik, nem ellenőrizheti.

Természetesen, a kis szervezeteknél, vállalatoknál e szervezeti felépítésben megfogalmazódott elveket be kell tartani, de funkciókat össze lehet és kell vonni. Kisvállalat az, amelyik korlátozott erőforrásokkal rendelkezik (Nemzetközi Munkaügyi Szervezet).

T39: A biztonsággal az adatbiztonsági felelős foglalkozik.

Az adatbiztonsági (és adatvédelmi) felelősnek a top menedzsmenthez kell, tartoznia. Feladatköre a személyes és közérdekű adatokra vonatkozik. A biztonságért felelőssel az előző pont foglalkozik, aki tehát külön személy. Az adatvédelem, adatbiztonság, és az információvédelem, számítástechnika védelem feladatait más jogszabályok, illetve szabványok határozzák meg. (adatvédelmi tv, illetve a például az MSZ-ISO/IEC 27001 és 27002 szabvány).

T40: A védelmi intézkedések célja az adatok védelme.

Kétségtelen tény, hogy az adatokat (minden adatot, nemcsak a személyes adatokat), az információrendszerben meg kell védeni. Ugyanakkor az adatok védelme nem vonatkozhat kizárólag magának az adatoknak a védelmére, mivel az információrendszerben bármely elemet érő támadás következményei az adatok sérülését is eredményezhetik. Itt tehát arról kell beszélni, hogy az információrendszer minden erőforrásának védelme, egyúttal az adatok védelmét is szolgálja. Az erőforrások:

- az adatok, információk,
- alkalmazások,
- az IT infrastruktúra: a technológia és a kiegészítő berendezések (klíma, áramellátás, papír feldolgozó eszközök)
- az ember.

Végül az adatvédelem a személyes és közérdekű adatok védeleméről szóló törvény által lefoglalt, és csak ezekre vonatkoztatott fogalom. Hasonlóképp az információrendszer védelmének célja nemcsak a vagyontárgyak védelme, mert az erőforrásokat megnézve a négyből az első három vagyon, illetve vagyontárgy, míg a védelem célja/tárgya az összes IT erőforrás. Ebből az következik, hogy a vagyontárgyak védelme, nem fogja át az összes erőforrások védelmét.

3.12. Az adatok biztonságérzékenység szerinti osztályozásáról

T41: Nálunk igazán nincs mit titkolni.

Egyes vállalatok küldetése olyan tevékenységeknek a végrehajtását teszi szükségessé az üzleti cél megvalósítása számára, amelyek többekben azt a hitet kelthetik, hogy nálunk igazán nincs mit titkolni. Ez a kérdés azonban csak kockázatelemzés végrehajtása és értékelése után válaszolható meg. Egy vállalatot fenyegetnek külső és belső kockázatok egyaránt. Ezek erőssége valóban függ a tevékenységek biztonság-érzékenységétől, hiszen minél biztonságérzékenyebb egy tevékenység, annál több a védendő adat, információ. Azt azonban az információs hadviselés korában, nem lehet végképp állítani, hogy minket nem fenyeget semmi, senki. Például minden vállalatnak a birtokában, van alaptevékenységével kapcsolatosan számtalan adat és az alkalmazottainak személyes adatai, amelyek természetesen védelmet igényelnek.

3.13. A számítástechnika szerepéről

T42: Az információrendszer szolgáltatásait a szakterületek számára az informatikusok határozzák meg.

A 70-es, 80-as években különösen jellemző volt az a nézet, hogy egy szervezet, vállalat, bank tevékenységét a számítás technikusoknak kell meghatározni. Sajnos azonban napjainkban is találkozni lehet ezzel az elképzeléssel. Az kétségtelen tény, hogy a számítástechnika alkalmazásának színvonala egy szervezetnél alapvetően befolyásolni tudja a szervezet küldetésének, a küldetési cél teljesítésének a hatékonyságát. Ez a hatás lehet segítő vagy gátló. Ugyanakkor a szervezet (vállalat) stratégiáját nem a számítástechnikusoknak kell meghatározni, hanem a küldetés végrehajtásán közvetlenül dolgozó szakembereknek, a szervezet Stratégiai Bizottságának. A számítástechnika eszköz, szolgáltatás a küldetés végrehajtásán dolgozók számára, ezért a számítástechnikával kapcsolatos igényeket, mindig a küldetési cél, és annak teljesítésére kidolgozott vagy a megvalósítás közben jelentkezett igények határozzák meg. Ez nem csökkenti, hanem növeli a számítástechnika jelentőségét, mivel annak szolgáltató képessége alapvetően segíti vagy korlátozhatja a küldetési célok meghatározását, teljesítését.

4. Mit lehet tenni a tévhitek csökkentésére

4.1. A biztonsági kultúra szerepe

A tévhitek a szerző tapasztalatai szerint mindig egyéneknél alakulnak ki. Az egyén sajátosságai, személyiség jegyei például az egyén biztonsági kultúrájának, ezen belül a biztonsági tudatosságának az alakítói, másrészt ezek is formálják az egyén sajátosságait. Nyilvánvaló az, hogy egy szervezetben a biztonsági kultúra a biztonsági tudatosság színvonala jelentős mértékben befolyásolhatja a tévhitek kialakulását. Ezért, amikor egy szervezet a biztonsági kultúrának az alakítására, szinten tartására programot készít, figyelmet kell fordítania arra is, hogy a tévhitek e program tárgyát képezzék. Nehezen vitatható, hogy ahol a biztonsági kultúra és a szervezet tevékenységeinek, küldetésének biztonság érzékenysége kölcsönhatása, a kultúrának az erősítésekor fontos szempont, nem fogunk gyakran tévhitekkel találkozni.

4.2. Az oktatás, nevelés lehetősége

A biztonsági kultúra erősítésének eszköze az oktatás, nevelés, és mondjuk ki, a közvetlen, és közvetett befolyásolás. Közvetlen befolyásolás, a képzéseken történhet, míg a közvetett befolyásolás vezetői döntésekkel, vezetői magatartásokkal, illetve az írásos propaganda eszközeivel végezhető. A szervezet, a vállalat érdekei, a biztonságérzettség alapján meghatározhatóak a szervezet számára kedvező személyiségjegyek, és a nevelésnek, képzésnek, propagandának ebbe az irányba kell haladnia, és a nem megfelelő személyiség jegyekkel rendelkezőket befolyásolni. Ennek az eredményessége nem kizárt, elérésének a valószínűsége nem zero.

5. Tíz axióma a biztonságról

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 üzleti, termelési (ha van), és informatikai rendszerből áll.
5. A vagyonbiztonság, termelési biztonság és informatikai biztonság egyaránt a bizalmasságtól, sértetlenségtől és rendelkezésre állástól függ.

6. A veszélyforrások, kockázatok nem állandóak, ezért rendszeresen vizsgálni kell őket.
7. Az üzletmenet folytonosság csak akkor biztosítható, ha az egész mikro gazdasági rendszerre kiterjed.
8. A biztonságsszervezés csak a Biztonsági Átvilágítástól indulva és szisztematikusan végezve lehet eredményes.
9. Az erőforrásokat védeni kell a biztonsági alrendszerekben.
10. A biztonság külön szakma, nem is egy.

6. Mellékletek

6.1. Rövidítések

COBIT: Control Objectives for Information and Related Technology

COSO: Committee of Sponsoring Organizations of the Treadway Commission

ISACA: Information System Audit and Control Association

OCEG: Open Compliance and Ethic Group

ERM: Enterprise Risk Management

SOX: Sarbanes Oxley Act. House of Representatives. USA

6.2. Néhány figyelembe veendő szabvány

1. MSZ-ISO/IEC 27001. az információbiztonság irányítási rendszerei. Követelmények.
2. ISO/IEC 27002. Code of practice of information security management.
3. ISO/IEC 27005. Information technology – Security techniques- Information risk management.
4. ISO 15408. Common Criteria. 2.1.
5. Information Security Forum. Good Practice Version 2007.
6. ISO/TR 13569. Banking and related financial devices - Information security guidelines.
7. ISO 19011. Guidelines for quality and, or environmental system auditing.

Irodalomjegyzék

- [1] Enterprise Risk Management. COSO. 2004.
- [2] COBIT 4.1 ITGI. 2007.
- [3] The Compliance function in banks. Basel Committee on Banking Supervision.
- [4] Integrating Risk Management, Compliance and Culture. OCEG. 2006.
- [5] A Felügyeleti Tanács 1162006. számú ajánlása a belső védelmi vonalakról. PSZÁF. 2006.
- [6] Vasvári György: Vállalati Biztonságirányítás. Informatikai biztonság Menedzsment. Time Clock Kft. 2007.
- [7] Vasvári György: Vállalti (szervezeti) kockázat menedzsment. Információs Társadalomért Alapítvány. 2008.

Informatikai biztonsági kockázat példatár

Vasvári György CISM

Információs Társadalomért Alapítvány
1507 Budapest, Pf. 213
Telefon: +36-1-279-1510, Fax: +36-1-279-1511
e-mail: gvasvari@tiphaz.hu

1.1. A veszélyérzet

A vállalatok jelentős részénél a biztonság nem szervezett, és a tényleges védelmi igényeket nem elégíti ki. Kérdés mindez minek tudható be. A biztonság megteremtése igen költségigényes. J. Essinger például azt írja, hogy az angol bankoknál az első veszélyforrás a menedzserek költségtakarékossági igénye. Kétségtelen, hogy a korszerű igényeket kielégítő biztonsági alrendszer kiépítése jelentős költségeket igényel. Egyes szerzők szerint ez a költség évente elérheti az informatikai erőforrások bekerülési értékének 10%-át. Ugyanakkor jelentős problémát okoz annak a felismertetése, hogy minden védelemben van maradék kockázat, a támadási módszerek fejlődése pedig a kedvező állapot megváltozásának valószínűségét folyamatosan növeli. Ezért a védelem folyamatos korszerűsítése alapvető igényként jelentkezik. Tehát egymással szemben áll a magas beruházási költség és a kockázat csökkentése. A kockázat tudatos felvállalásán alapulhat a menedzsment döntése, amelynek eredményeképpen a biztonsági rendszer nem lesz tökéletes, „csak” a döntésnek megfelelő mértékű védelmet fogja nyújtani. A menedzserek azonban igénylik annak kidolgozását, hogy a biztonsági rendszer kiépítése, fejlesztése milyen gazdasági eredményt hoz. Erre nincs egzakt, forintban kifejezhető válasz. Becslésre pedig akkor lenne lehetőség, ha hosszabb időtartamra rendelkezésre állna a bekövetkezett támadások statisztikája. Ez azonban két okból nem áll rendelkezésre, egyrészt a vállalatok „üzletpolitikai okokból” nem hozzák nyilvánosságra a biztonsági eseményeiket, másrészt maguk számára sem tartják nyilván azokat. J. Essinger fentiekben már idézett könyvében azt írja, hogy az angol bankok nem tárják fel a biztonsági események nagy részét, amit feltárnak annak nagy részét nem jelentik, amit jelentenek annak nagy részét nem követi védelmi intézkedés.

A probléma a veszélyérzet hiányára vezethető vissza, amely a fenyegetettség fel nem ismerésén alapul. Ezzel kapcsolatban rá kell mutatnunk a beosztottak viszonyára is a védelmi intézkedésekhez. Sok esetben a helyes védelmi intézkedések gyenge (szabálytalan) végrehajtással párosulnak. Tipikus példa erre hazánkban az a viszonylag jó jelszavas

hozzáférés-védelmi rendszer, amelynek üzemeltetésénél a gyakorlatban közismert, tehát mindenki által ismert, jelszavakat használnak (mert így egyszerűbb).

A veszélyérzet hiánya pedig a humán erőforrások biztonsági tudatosságának a gyengeségén, a támadások bekövetkezési valószínűségének a fel nem ismerésén, és ebből következően a védelmi intézkedéseket indokolatlannak tartó állásponton alapul.

1.2. A példák ismertetési módszere

A példákat a következő struktúrában ismertetjük: Pl. 1.

- A SZERVEZET: amelynél a Biztonsági Átvilágítás történt, de biztonsági okokból csak a típusát megadva. A könyv viszonylag sok pénzügyi szervezeti példát ismertet, mert a szerző a jelzett időszakban sok pénzügyi szervezetnél (bank, biztosító intézet, egyéb pénzügyi vállalkozások) végzett átvilágítást. Egyes veszélyforrásokat több vállalatnál találtunk, így ez esetekben ezt tüntettük fel.
- A FELTÁRT HELYZET: amely alapján a veszélyforrás megállapítása történt, ugyanis csak alátámasztott, igazolható tények alapján állapítható meg veszélyforrás.
- MIÉRT VESZÉLYFORRÁS: az indoklás.
- MIT FENYEGET: A veszélyforrások az erőforrások bizalmasságára és/vagy sértetlenségére és/vagy rendelkezésére állására jelentenek, jelenthetnek fenyegetést. Ezek közül az elsősorban jellemzőt adjuk meg, vagy kettőt, de ha hármat is egyaránt fenyeget, a biztonságot szerepeltetjük.
- MIT SZÜKSÉGES TENNI: a veszélyforrás képezte kockázat csökkentésére tehető védelmi intézkedés.

A kockázat azért nem szerepel az egyes veszélyforrásoknál, mert az, hogy a veszélyforrás milyen mértékű kockázatot jelent, mindig a vállalat, szervezet adottságaitól függ, tehát reálisan megbecsülni sem célszerű azt.

A Példatár a biztonságsszervezés ajánlott struktúrája szerint tárgyalja az egyes példákat.

2. Példák

2.1. Szervezési veszélyforrások

2.1.1. Biztonsági szervezet

Pl. 1.

- A SZERVEZET: Pénzügyi szervezet.
- A FELTÁRT HELYZET: Két informatikai főosztály, amelyeket elvileg a vezérigazgató fog össze.
- MIÉRT VESZÉLYFORRÁS: Az interjúk során egyértelműen kiderül, hogy a két főosztály között a gyakorlatban semmilyen együttműködés nincs. A veszélyforrás elemzés hatására a két főosztályvezető között pozícióharc indul. Az informatikai biztonsággal a két főosztályvezető alatt, szintén nem együtt működve, van biztonsági szervezet. Ez a megoldás kizárja az összehangolt együttműködésen alapuló informatikai biztonsági alrendszert, nincs egyenszilárdságú informatikai biztonság.
- MIT FENYEGET: Biztonságot.
- MIT SZÜKSÉGES TENNI: Az integrált információrendszer, az integrált informatikai, és külön integrált biztonsági szervezeti felépítés szükséges.

Pl. 2.

- A SZERVEZET: Iparvállalat.
- A FELTÁRT HELYZET: Egymástól független, nem együttműködő, sőt egymást leértékelő biztonsági szervezet külön az üzleti, a termelési és az információ rendszerben.
- MIÉRT VESZÉLYFORRÁS: Az egymással konkuráló biztonsági szervezetek, nem teremtenek az egész vállalatot átfogó, azonos erősségű biztonsági rendszert, azaz sok támadási lehetőséget kínálnak.
- MIT FENYEGET: Biztonságot.
- MIT SZÜKSÉGES TENNI: A biztonsági struktúra csak akkor hatékony, teremt egyenszilárdságú biztonságot, ha a vezérigazgató közvetlen felügyeletéve integrált biztonsági szervezet van, amely a vagyonbiztonsági, üzembiztonsági, és informatikai biztonsági felelősöket szakmailag irányítja.

2.1.2. Humánpolitika

Pl. 3.

- A SZERVEZET: Igazgatási szervezet.
- A FELTÁRT HELYZET: A biztonság érzékeny értékpapírokat úgy selejtezik, hogy kijelölt munkatársak a zsákokban összegyűjtött, és forgalomból kivont értékpapírok azonosítóit, a selejtezési helyiségben számítógépen rögzítik. Ezután a selejtezési bizottság megjelenik, és szűrőpróbával ellenőrzi, hogy megtörtént-e a selejtezendő értékpapírok azonosítóinak rögzítése. Ezt jegyzőkönyvezik, és ezután engedélyt adnak a selejtezésre.
- MIÉRT VESZÉLYFORRÁS: Ez a rendszer lehetővé teszi a már rögzített értékpapírok eltulajdonítását, és későbbi jogosulatlan felhasználását (mint ahogy erre kísérlet is történt).
- MIT FENYEGET: Biztonságot.
- MIT SZÜKSÉGES TENNI: A biztonság érzékeny papírok, adathordozók selejtezését egy bizottság előtt, először érvénytelenítéssel, majd egyenkénti azonosító rögzítés után, egyenkénti megsemmisítéssel kell végezni, végig a bizottság ellenőrzése mellett.

Pl. 4.

- A SZERVEZET: Iparvállalat.
- A FELTÁRT HELYZET: A Biztonsági Politika első pontjában azt írják, hogy a „biztonság megkívánja, hogy a munkatársakat, ne tekintsük megbízhatónak”.
- MIÉRT VESZÉLYFORRÁS: A bizalmatlanság visszahatása a munkatársakban azt a gondolatot ébresztheti, hogy ha már nem bíznak bennem, akkor úgyis mindegy, ez pedig minimálisan a védelmi intézkedések nem rendeltetésszerű végrehajtásához vezethet.
- MIT FENYEGET: Bizalmasságot.
- MIT SZÜKSÉGES TENNI: A munkatársakban meg kell bízni, és a megbízhatóságukról a felvételékkor kell meggyőződni, és a teljes foglalkoztatásuk alatt intézkedéseket kell tenni, a megbízhatóságuk fenntartása, a vállalathoz való hűségük erősítése érdekében.

Pl. 5.

- A SZERVEZET: Pénzügyi szervezet.
- A FELTÁRT HELYZET: Nincs külön informatikai biztonsági szervezet, a biztonsági feladatokat más informatikai feladatok mellett, ugyanazok a munkatársak látják el.
- MIÉRT VESZÉLYFORRÁS: A védelmi intézkedések rendeltetésszerű ellátása ütközhet az informatikai vagy egyéb vállalati érdekekkel, és ebben az esetben nem érhető el a biztonsági cél. A biztonsági feladatok más feladatok melletti ellátása, akadályozhatja a védelmi intézkedések megfelelő ellátását.
- MIT FENYEGET: Biztonságot.
- MIT SZÜKSÉGES TENNI: A magyar (MSZ ISO/IEC 17799,), a nemzetközi szabványok (ISO/IEC 17799) és ajánlások (COBIT 3) egyértelműen előírják, hogy a biztonsági és biztonságkritikus feladatokat más feladatok mellett nem lehet ellátni.

Pl. 6.

- A SZERVEZET: Pénzügyi szervezet.
- A FELTÁRT HELYZET: A biztonsági követelmények, például a titoktartás nem érvényesül a kívánatos mértékben a munkaviszony megszűnte után.
- MIÉRT VESZÉLYFORRÁS: A munkahelyváltoztatás jelentős százalékban azonos szakmai érdekeltségű vállalathoz történik, és ezek érdekeltek a korábbi munkahely titkainak ismeretében.
- MIT FENYEGET: Bizalmasságot.
- MIT SZÜKSÉGES TENNI: A szervezet Titokvédelmi Utasítása szerint osztályozott titkok bizalmas kezelésére a munkaviszony megszűnte utáni időre is kötelezettséget kell vállalni a munkatársaknak a munkaviszony létesítésekor.

Pl. 7.

- A SZERVEZET: Pénzügyi szervezet.
- A FELTÁRT HELYZET: A veszélyforrás elemzés véleményezésekor a Szervezet felső vezetése nevében felvetették, hogy miért írunk csak rosszat róluk.
- MIÉRT VESZÉLYFORRÁS: Nem értették, hogy a veszélyforrások feltárása az ő érdekeiket szolgálja, nem kezelték a biztonságot súlyának megfelelően.

- MIT FENYEGET: Biztonságot.
- MIT SZÜKSÉGES TENNI: Erősíteni kell folyamatosan a biztonsági tudatosságot, a veszélyforrások felismerését, a védelmi intézkedések indokoltságának elfogadását, csökkenteni kell a veszélyérzet hiányát. Mindezt az összes munkatársra kiterjedő szervezett oktatással lehet elérni.

Pl. 8.

- A SZERVEZET: Pénzügyi szervezet.
- A FELTÁRT HELYZET: A munkatársak között feltűnt néhány kábítószer fogyasztó. A humánpolitikai vezető segített azoknak, akik hagyták, hogy támogassa őket a szenvedélybetegségtől megszabadulni, a többiek kiléptek. Ezt felvetve az informatikai munkatársak közölték, hogy ilyen kérdéssel nem hajlandók foglalkozni.
- MIÉRT VESZÉLYFORRÁS: A szenvedélybetegségek a munkatársat megbízhatatlanná, zsarolhatóvá teszik. Az ilyen esetek feltárása, kezelése nélkül előbb vagy utóbb biztonsági eseményhez vezetnek.
- MIT FENYEGET: Biztonságot.
- MIT SZÜKSÉGES TENNI: A feltárásában, gyógyításában a humánpolitikai vezetőn kívül, a közvetlen munkatársaknak is részt kell venniük.

Pl. 9.

- A SZERVEZET: Tanácsadó vállalat.
- A FELTÁRT HELYZET: A vállalat öt rendszergazdát foglalkoztat, akik között a feladatok nincsenek felosztva, aki éppen kéznél van, az végzi el az adott feladatot.
- MIÉRT VESZÉLYFORRÁS: Az azonos feladatot ellátó öt munkatárs együtt felel a feladatok teljesítésért, aminek következtében a számon kérhetőség nincs biztosítva, amennyiben probléma merül fel nem állapítható meg a felelős.
- MIT FENYEGET: Biztonságot.
- MIT SZÜKSÉGES TENNI: A feladatokat, felelősségeket a munkatársak között egyértelműen fel kell osztani, és a munkaköri leírásukban azt rögzíteni kell.

2.1.3. Biztonsági dokumentumok

Pl. 10.

- A SZERVEZET: Több vállalat.
- A FELTÁRT HELYZET: Nincsenek meg hiánytalanul a biztonsági dokumentumok (Átvilágítási Jelentés, Biztonsági Politika (Szabályzat), Üzletmenet Folytonossági Terv).
- MIT FENYEGET: Biztonságot.
- MIÉRT VESZÉLYFORRÁS: A biztonsági dokumentumok hiányossága vagy hiánya azt jelzi, hogy nem folyik a biztonságtudatos munka szervezése, amely állandó feladat.
- MIT SZÜKSÉGES TENNI: A biztonságszervezés a biztonságirányításból indul ki, az irányítást végzők által elkészített és karbantartott Biztonsági Stratégiából. Ennek alapján kell elvégezni és dokumentálni az átvilágítást, a kockázat menedzsmentet, az üzletmenet folytonosság folyamatos biztosítását.

2.1.4. Iratkezelés

Pl. 11.

- A SZERVEZET: Több vállalat.
- A FELTÁRT HELYZET: Az Iratkezelési Utasítás nem tér ki az elektronikus iratok kezelésére, sem a papír alapú irodából az átmenetre az elektronikus irodába és vissza.
- MIÉRT VESZÉLYFORRÁS: Amennyiben nincs az elektronikus iratok kezelése szabályozva, az a bizalmasság, a rendelkezésre állás sérüléséhez vezethet.
- MIT FENYEGET: Biztonságot.
- MIT SZÜKSÉGES TENNI: Az elektronikus iratok kezelése, létrehozása, feldolgozása (módosítása), tárolása (archiválása), továbbítása, selejtezése is megkívánja a biztonsági szempontok figyelembe vételével a szabályozást. Tehát ki kell egészíteni az Iratkezelési Utasítást.

Pl. 12.

- A SZERVEZET: Pénzügyi szervezet.
- A FELTÁRT HELYZET: Számítástechnikai eszközöket kivontak a felhasználásból és értékesítették. Az egyik berendezés bizalmas adatokat is tartalmazott.
- MIÉRT VESZÉLYFORRÁS: A bizalmas adatok jogosulatlan kézbe kerülhetnek, felhasználásuk biztonsági eseményhez vezethet.
- MIT FENYEGET: Bizalmasságot.
- MIT SZÜKSÉGES TENNI: A számítástechnikai eszközöket először a felhasználásuk megszüntetése után megnyugtató módon törölni kell, és meg kell győződni arról, hogy a tárolók, adathordozók nem tartalmazzanak osztályozott adatokat, programokat.

Pl. 13.

- A SZERVEZET: Több vállalat.
- A FELTÁRT HELYZET: A dokumentációk kezelésére nincs szabályozás.
- MIÉRT VESZÉLYFORRÁS: Ez a helyzet ahhoz vezethet, hogy egy felmerült problémát a szakemberek vagy egyáltalán nem vagy csak hosszas munka után tudnak kezelni, megoldani.
- MIT FENYEGET: Rendelkezésre állást.
- MIT SZÜKSÉGES TENNI: A dokumentációk kezelését úgy kell szabályozni, hogy egyértelműen derüljön ki a felelős a készítésükért, kinek kell kapni belőle, hol kell legalább egy példányt megőrizni belőle, ki adhat engedélyt a módosításukra, végül a selejtezésükre.

2.1.5. Titokvédelem

Pl. 14.

- A SZERVEZET: Iparvállalat.
- A FELTÁRT HELYZET: Az informatikai biztonságért felelős személy az adatvédelmi felelős volt.

- **MIÉRT VESZÉLYFORRÁS:** Ez nem egyszerűen helytelen elnevezés használat, ugyanis ebben az esetben az eredmény, hogy sem az adatvédelemmel, sem az informatikai biztonsággal nem foglalkozik megfelelően. Egyébként ezek egymást kizáró feladatok egy személy számára.
- **MIT FENYEGET:** Biztonságot.
- **MIT SZÜKSÉGES TENNI:** Az adatvédelmi felelősnek a személyes adatok védelmével kell foglalkoznia a titkárság alárendeltségében, míg az informatikai biztonsági felelős a biztonsági szervezethez tartozik.

Pl. 15.

- **A SZERVEZET:** Több vállalat.
- **A FELTÁRT HELYZET:** Az adatvédelmi (adatbiztonsági) felelős munkakör nincs a vagyon, az üzem, illetve informatikai biztonsági munkakörtől elválasztva.
- **MIÉRT VESZÉLYFORRÁS:** Ennek eredménye, hogy nem valósul meg sem a személyes adatok védelme, sem a biztonsági alrendszerekben a védelmi intézkedések meghatározása, az adatok, alkalmazások, helyiségek és eszközök biztonság érzékenységük szerinti osztályozása alapján. Így a védendő erőforrások nem kapnak a biztonság érzékenységükkel arányos védelmet, sebezhetőségük nő.
- **MIT FENYEGET:** Bizalmasságot.
- **MIT SZÜKSÉGES TENNI:** A személyes adatokat a vonatkozó törvény szerint kell védeni, míg a vállalati erőforrásokat biztonság érzékenységük szerint a Titokvédelmi Utasításban kell osztályozni.

Pl. 16.

- **A SZERVEZET:** Tanácsadó vállalat.
- **A FELTÁRT HELYZET:** Nincs egyértelműen meghatározva, melyek a titkok, és azokat hogyan, mennyire kell védeni. Hivatkozásként az államtitokról szóló jogszabály szerepel, valamint a személyes adatok védelméről szóló tv., amely nem vonatkozik a vállalatra.
- **MIÉRT VESZÉLYFORRÁS:** A téves hivatkozás, valamint az osztályozás hiánya következtében az erőforrások nem kapnak bizalmasságukkal arányos védelmet.
- **MIT FENYEGET:** Biztonságot.

- MIT SZÜKSÉGES TENNI: A védelmi intézkedések erősségének meghatározása előtt, a Titokvédelmi Utasításban meghatározottak szerint, az MSZ ISO/IEC 17799 szabvány előírásának megfelelően osztályozni kell elsősorban az adatokat, helyiségeket és eszközöket (valamint az egyéb erőforrásokat), biztonság érzékenyséjük szerint az arányos védelem biztosítása érdekében.

Pl. 17.

- A SZERVEZET: Több vállalat.
- A FELTÁRT HELYZET: A szabályozások vagy nincsenek osztályozva (papír és elektronikus alapon egyaránt) vagy nyilvánosként kezelik.
- MIÉRT VESZÉLYFORRÁS: A nyilvános kezelés azt jelenti, hogy a vállalaton kívül, és nem azt, hogy a vállalaton belül bárki hozzáférhet. Így az egyébként valamilyen osztályozásra jogosult szabályozások, a nem osztályozott csoportba kerülnek, az egyébként legalább „belső használatra” korlátozott helyett, ami jogosulatlan kezekbe kerülő szabályozásokat eredményezhet.
- MIT FENYEGET: Bizalmasságot.
- MIT SZÜKSÉGES TENNI: Az osztályozásnál a nyilvános, azaz nem osztályozott besorolás a nem biztonság érzékeny szabályozásokra vonatkozik, míg a bizalmasan kezelendőket a belső használatra vagy bizalmas, titkos osztályokba kell besorolni. Pl. az Informatikai biztonsággal foglalkozó szabályzatok, utasítások, eljárás rendek általában a bizalmas osztályba sorolandók.

2.2. Technikai veszélyforrások

2.2.1. Fizikai hozzáférés

Pl. 18.

- A SZERVEZET: Iparvállalat.
- A FELTÁRT HELYZET: A számítóközpont az őrtornyokkal és azokban fegyveres előerős védelemmel, valamint betonfallal körülvett gyártelepen kívül, a közútra néző épület földszintjén, üvegfallal az épület belépő tere felé volt elhelyezve. Az épület egyébként a beton falon belül lévő vegyi anyag tartálytól kb. 25-30 méterre volt.

- **MIÉRT VESZÉLYFORRÁS:** Az elhelyezés a veszélyérzet hiányát tükrözte, mind a falon kívüli elhelyezés, mind az utcára nyíló üvegfa, mind a robbanásveszélyt jelentő tartály közelsége miatt. Ez egyrészt kétségesse teszi a hatékony hozzáférés védelmet, másrészt a robbanásveszély a rendelkezésre állás biztosíthatóságát.
- **MIT FENYEGET:** Rendelkezésre állás.
- **MIT SZÜKSÉGES TENNI:** A központi számítástechnikát jól védhető területen biztonságosan zárt falakkal, és közúttól, valamint robbanás veszélyes anyagokat tároló helyiségektől, berendezésektől távol kell elhelyezni.

Pl. 19.

- **A SZERVEZET:** Távközlési vállalat.
- **A FELTÁRT HELYZET:** A műszaki hibák munkaidőn kívüli javítása esetén gyakran vették igénybe az otthontartózkodó műszakiakat. Ekkor a távdiagnosztizálás, illetve javítás egy olyan távbeszélő vonalon történt, amelynek a hívószáma a használatos számmezőkön kívüli mezőből volt.
- **MIÉRT VESZÉLYFORRÁS:** Az a hiedelem, hogy a használaton kívüli számmező biztonsági veszélyforrás, ugyanis ha a támadó jól képzett, valamint a használati mód nem titkos, lehetősége van a hívott szám lehallgatására, és utána az azzal való visszaélésre.
- **MIT FENYEGET:** Biztonságot.
- **MIT SZÜKSÉGES TENNI:** Lehallgatás védett vonalat kell használni a távjavítás, távdiagnosztizáláshoz.

Pl. 20.

- **A SZERVEZET:** Pénzügyi szervezet.
- **A FELTÁRT HELYZET:** Az egyes biztonság érzékeny helyiségekbe csak a belépést korlátozzák egy nem rendszerre kötött kódkapcsolós elektronikus zárral, amely így nem rögzíti sem a belépés, sem a kilépés időpontját.
- **MIÉRT VESZÉLYFORRÁS:** Nem lehet megállapítani az egyes biztonság érzékeny helyiségekben ki, mikor, mennyit tartózkodott a helyiségben, így nincs lehetőség a számonkérésre, az utólagos vizsgálatokra.
- **MIT FENYEGET:** Bizalmasságot.
- **MIT SZÜKSÉGES TENNI:** Számítástechnika vezérelt, mind a kétirányú mozgást ellenőrző és rögzítő rendszert kell alkalmazni.

Pl. 21.

- A SZERVEZET: Pénzügyi szervezet.
- A FELTÁRT HELYZET: A biztonság érzékeny, zárt helyiségként osztályozott helyiségek falai gipszkartonból készültek.
- MIÉRT VESZÉLYFORRÁS: A gipszkarton egyszerű eszközökkel áttörhető, a helyiség nem védett a jogosulatlan behatolás ellen.
- MIT FENYEGET: Biztonságot.
- MIT SZÜKSÉGES TENNI: A zárt helyiségeket a MABISZ előírásainak megfelelően, behatolás védelmet biztosító falazattal kell ellátni.

Pl. 22.

- A SZERVEZET: Több vállalat.
- A FELTÁRT HELYZET: A mobil számítástechnikai eszközök munkahelyi és házon kívüli védelmi feladatai nem szabályozottak.
- MIÉRT VESZÉLYFORRÁS: Egyrészt így nagy a valószínűsége a házon belüli eltulajdonításnak, másrészt házon kívüli eltulajdonítás esetén jogosulatlanul juthatnak osztályozott, biztonság érzékeny információkhoz.
- MIT FENYEGET: Biztonságot.
- MIT SZÜKSÉGES TENNI: Szabályozni kell a mobil eszközöknek a házon belüli és házon kívüli kezelését, és engedélyhez kell kötni kivitelüket a tárolt adatok, alkalmazások függvényében.

Pl. 23.

- A SZERVEZET: Több vállalat.
- A FELTÁRT HELYZET: A munkaasztalok elhagyás esetén is tele vannak különböző papír és elektronikus adathordozókkal, valamint a magára hagyott számítástechnikai munkahely bejelentkezett állapotban marad.
- MIÉRT VESZÉLYFORRÁS: Jogosulatlan betekintés, eltulajdonítás, a bejelentkezett állapotban a munkahelyen dolgozó munkatárs jelszavával visszaélés lehetséges.
- MIT FENYEGET: Biztonságot.

- **MIT SZÜKSÉGES TENNI:** Az MSZ ISO/IEC 17799-es hazai szabvány előírja az üres íróasztal, sötét képernyő politika kötelező alkalmazását a munkahely elhagyásakor. Ez nem képernyővédő alkalmazást jelenti, hanem a bejelentkezést követően az információrendszerrel létrejött viszony meghatározott időn túli inaktivitás esetén történő automatikus megszakítását.

2.2.2. Fizikai rendelkezésre állás

Pl. 24.

- **A SZERVEZET:** Iparvállalat.
- **A FELTÁRT HELYZET:** A folyamatos áramellátás biztosítása érdekében a központi számítástechnika épületétől kb. harminc méterre lévő transzformátor háztól két elektromos tápkábelrel oldották meg a kettős betáplálást.
- **MIÉRT VESZÉLYFORRÁS:** A közeli transzformátorháztól, egymástól nem távol vezetett két kábel adott esetben egyszerre sérülhet meg, azaz szűnhet meg a betáplálás.
- **MIT FENYEGET:** Rendelkezésre állást.
- **MIT SZÜKSÉGES TENNI:** A kettős betáplálást az Elektromos Művek két egymástól lehetőleg legtávolabb lévő alállomásától kell vezetni.

Pl. 25.

- **A SZERVEZET:** Távközlési vállalat.
- **A FELTÁRT HELYZET:** A távközlési vállalat a központi számítástechnika elhelyezésére épületet kívánt felépíteni, és szakértői véleményt kért biztonsági szempontból a kijelölt, egyébként tulajdonát képező területen való elhelyezésről. A szomszédos telken éppen megkezdtek egy benzinkút építését. Álláspontunkkal szemben találtak egy szakértőt, aki azt nyilatkozta, hogy a benzinkút nem jelent veszélyforrást a tervezett épületre nézve.
- **MIÉRT VESZÉLYFORRÁS:** A benzinkút robbanásveszélyes, és szabványos úgynevezett robbanás biztos kivitelezés esetén is van maradék kockázat, amit egy új épület helyének kijelölésekor nem szabad felvállalni.
- **MIT FENYEGET:** Rendelkezésre állást.
- **MIT SZÜKSÉGES TENNI:** A nemzetközi ajánlások szerint a számítástechnika elhelyezése nem lehet robbanás veszélyes anyagok tárolási helye közelében.

Pl. 26.

- A SZERVEZET: Pénzügyi szervezet.
- A FELTÁRT HELYZET: Egy hosszabb ideje működő pénzügyi szervezetenél a biztonsági átvilágítás során megállapították, hogy nincs a számítástechnika elhelyezésére szolgáló épületben Faraday háló. Majd a vizsgálati jelentést olvasva a gondnok bemutatta az építészeti tervet, amely szerint az épület építésekor beépítették azt. Kiderült, hogy az eredetileg beépített Faraday háló földelése megsérült.
- MIÉRT VESZÉLYFORRÁS: A Faraday háló hiánya lehetővé teszi a számítástechnikai eszközök elektromágneses kisugárzását, a környezeti elektromos és elektromágneses zavarok besugárzását, amely egyrészt a bizalmasságot sérti, másrészt veszélyezteti a számítástechnikai eszközök működését, működőképességét. Itt azonban szó volt a rendszeres ellenőrzés, karbantartás elmaradásáról is.
- MIT FENYEGET: Bizalmasságot, sértetlenséget.
- MIT SZÜKSÉGES TENNI: Rendszeresen ellenőrizni, karbantartani kell a Faraday hálót is.

2.2.3. Logikai hozzáférés

Pl. 27.

- A SZERVEZET: Pénzügyi szervezet.
- A FELTÁRT HELYZET: A beosztott munkatársak a központban nem kívántak több jelszót megjegyezni, ezért megállapodtak, hogy lecserélik jelszavaikat azonos jelszóra. Így mindenki ugyanazzal a jelszóval és jogosultságokkal rendelkezett. (egyesekek az átvilágítást végzők közül ezt a megoldást közismert jelszónak nevezték el).
- MIÉRT VESZÉLYFORRÁS: Az azonos jelszó és jogosultságok gyakorlatilag megszüntették a hozzáférésvédelmet, aminek eredményeképpen megszűnt a biztonság is.
- MIT FENYEGET: Biztonságot.
- MIT SZÜKSÉGES TENNI: A jelszó csak egyedi lehet, és a hozzárendelt jogosultságok is, amelyet minden felhasználó köteles bizalmasan kezelni. Amennyiben az információrendszer több jelszót igényelne felhasználónként, akkor

a single sign on (egyszeres bejelentkezés) rendszerét kell alkalmazni, amikor is egy jelszava van mindenkinek, és a korlátozott hozzáférést egyéb adatokhoz, alkalmazásokhoz, a jogosultságok megadásával határozzák meg, így a belépés után, a továbblépési jogosultság automatikusan kerül eldöntésre.

Pl. 28.

- A SZERVEZET: Pénzügyi szervezet.
- A FELTÁRT HELYZET: A jogosultságok jelszóhoz rendelése nem a munkaköri leírason alapul.
- MIÉRT VESZÉLYFORRÁS: Ez lehetővé teszi, hogy szemben a kötelezően alkalmazandó, szükséges tudás elve alapján megadott jogosultságokkal a jelszó birtokos valójában jogosulatlan tevékenységeket végezzen.
- MIT FENYEGET: Biztonságot.
- MIT SZÜKSÉGES TENNI: Alkalmazni kell a „szükséges tudás, szükséges cselekvés” elvét, a szabványoknak megfelelően, és csak a munkaköri leírásban rögzített feladatok alapján szabad jogosultságot a jelszóhoz rendelni.

Pl. 29.

- A SZERVEZET: Pénzügyi szervezet.
- A FELTÁRT HELYZET: Az erőszakkal kikényszerített bejelentkezés esetén a munkatársak saját jelszavukkal lépnek be a rendszerbe.
- MIÉRT VESZÉLYFORRÁS: Ez azzal jár, hogy a kikényszerített bejelentkezést követő tevékenységek a munkatárs felelősségére kerülnek rögzítésre.
- MIT FENYEGET: Sértetlenséget.
- MIT SZÜKSÉGES TENNI: Az erőszakkal, például rablótámadás esetén jogosulatlan művelet végrehajtása céljából kikényszerített bejelentkezéshez külön jelszóval kell rendelkezni a munkatársaknak, amely jelszó egyúttal riasztást is ad.

Pl. 30.

- A SZERVEZET: Több vállalat.
- A FELTÁRT HELYZET: A többször használatos jelszavakat nem ellenőrzöttek és nem szabályozottan cserélik.
- MIÉRT VESZÉLYFORRÁS: A túl hosszú ideig használt jelszó felfedésének nagy a valószínűsége, így az komoly veszélyforrást lépez.

- MIT FENYEGET: Bizalmasságot, sértetlenséget.
- MIT SZÜKSÉGES TENNI: A többször használatos jelszavaknál a jelszócserét elő kell írni időszakonként, de a korszerű megoldás, ha a rendszer a cserét kikényszeríti.

2.2.4. Logikai rendelkezésre állás

Pl. 31.

- A SZERVEZET: Több vállalat.
- A FELTÁRT HELYZET: A mentések egy példányban történnek, és a mentési eljárás nem szabályozott.
- MIÉRT VESZÉLYFORRÁS: A mentések egy példányban és rendezetlen szabályok szerinti végzésük fenyegetést jelent a rendelkezésre állásra nézve.
- MIT FENYEGET: Rendelkezésre állást.
- MIT SZÜKSÉGES TENNI: A mentéseket szabályozott eljárás szerint kell végrehajtani, és legalább két példányt kell készíteni, valamint az egyik példányt biztonságos helyen, az épületen kívül kell tárolni.

Pl. 32.

- A SZERVEZET: Bankok.
- A FELTÁRT HELYZET: a bankok nagyszámú, nem bizalmas, azaz általuk nem uralt hálózattal állnak kapcsolatban. Ezek felé és felől általában nem maradéktalanul szabályozott, kialakított a védelem.
- MIÉRT VESZÉLYFORRÁS: A nem bizalmas hálózati kapcsolatok gyenge védelme lehetővé teszi a jogosulatlan behatolást, fenyegeti a rendelkezésre állást, de a bizalmasságot is.
- MIT FENYEGET: Biztonságot.
- MIT SZÜKSÉGES TENNI: A nem bizalmas hálózati kapcsolatok felőli védelemre a tűzfal önmagában nem nyújt elegendő védelmet, szükséges a rosszindulatú szoftverek (vírus, spyware, spam) elleni aktív védelem, valamint behatolás védelmi (IDS, vagy IPS) szoftver alkalmazása is.

Pl. 33.

- A SZERVEZET: Pénzügyi szervezet.
- A FELTÁRT HELYZET: Harmadik féltől megrendelt szoftverben több éves használat után egy új belépő jelentése nyomán kiderült, hogy rosszindulatú szoftver van, amely a beérkező pénzmennyiségek meghatározott részét jóváírja egy-két munkatárs számláján, akik azt időnként felveszik és szétosztják egymás között.
- MIÉRT VESZÉLYFORRÁS: Ez a szoftver a csalást valósította meg, és megkárosította a pénzügyi szervezetet. A szoftver készítői természetesen tagadták, hogy a fejlesztés során náluk került be a rosszindulatú szoftver.
- MIT FENYEGET: Biztonságot.
- MIT SZÜKSÉGES TENNI: Az átadás/átvételkor „fenyegetésmentességi nyilatkozatot” kell kérni a szállítótól, mert az ilyen szoftverek igen erősen fenyegethetik a rendszernek a sértetlenségét, rendelkezésre állását.

Pl. 34.

- A SZERVEZET: Több vállalat.
- A FELTÁRT HELYZET: Az alkalmazói rendszereket leállás esetén újra kell indítani, ehhez azonban nem áll mindig rendelkezésre az újraindítási eljárás rendje.
- MIÉRT VESZÉLYFORRÁS: A nem megfelelő, pontosabban jobb híján kigondolt újraindítás veszélyezteti az alkalmazásnak a rendelkezésre állását. Egy katasztrófa bekövetkezése után, a kárelhárításkor a visszaállítás nem történhet meg újraindítás nélkül.
- MIT FENYEGET: Rendelkezésre állást.
- MIT SZÜKSÉGES TENNI: A szoftverek átadás/átvételekor a szállítónak át kell adni az újraindítási eljárás rendet, amelynek egy másolatát zárt helyen kell folyamatosan őrizni biztosítva a napra készségét.

Pl. 35.

- A SZERVEZET: Több vállalat.
- A FELTÁRT HELYZET: Nincs Üzletmenet Folytonossági Terv, a katasztrófák esetére.

- **MIÉRT VESZÉLYFORRÁS:** Az üzletmenet folytonosságának megszakadásakor csak pillanatnyi ötletek alapján tudják a katasztrófa következményeit elhárítani. Nincsenek felkészülve, ami ez vissza- és helyreállítás helyett újabb problémákhoz vezethet.
- **MIT FENYEGET:** Rendelkezésre állást.
- **MIT SZÜKSÉGES TENNI:** El kell készíteni a vállalat Üzletmenet Folytonossági Tervét (ÜFT, BCP).

Pl. 36.

- **A SZERVEZET:** Több vállalat.
- **A FELTÁRT HELYZET:** A biztonsági események kezelésére nincs Eljárás Rendjük a bekövetkező nem várt biztonsági problémákra ötletszerűen adnak választ.
- **MIÉRT VESZÉLYFORRÁS:** Az ötletszerű, felkészülést nélkülöző válaszok nem adnak helyes megoldást a biztonsági eseményekre.
- **MIT FENYEGET:** Rendelkezésre állást.
- **MIT SZÜKSÉGES TENNI:** Ki kell dolgozni az Eljárás Rendet, napra készen kell tartani, a biztonsági eseményeket naplózni kell, mindezt a Biztonsági Események Kezelési Rendjében kell szabályozni.

Pl. 37.

- **A SZERVEZET:** Több vállalat.
- **A FELTÁRT HELYZET:** A vírusvédelem a hagyományos vírusokra tér ki, nincs aktív védelem, nem naplózzák a biztonsági eseményt!
- **MIÉRT VESZÉLYFORRÁS:** Mindez azt eredményezi, hogy a vírustámadások sikerességének folyamatosan nő a valószínűsége.
- **MIT FENYEGET:** A bizalmasságot, sértetlenséget, rendelkezésre állást.
- **MIT SZÜKSÉGES TENNI:** A vírustámadások helyett a rosszindulatú szoftverek ellen kell aktív rendszerekkel védekezni, ami például a kém szoftverek és a kényszerű reklámok elleni aktív védekezést is jelenti.

2.2.5. Hálózatok biztonsága

Pl. 38.

- A SZERVEZET: Iparvállalat.
- A FELTÁRT HELYZET: A jumbo disk egységet egy külföldi szállító, hazai képviselő híján maga szervizelte, ami azt jelenti, hogy az információrendszerrel távdiagnosztikai és távjavítási kapcsolatban volt.
- MIÉRT VESZÉLYFORRÁS: A gyakorlatban ez korlátlan tevékenységi lehetőséget nyújtott számára attól függetlenül, hogy így hozzáférhetett bizalmas információkhoz is.
- MIT FENYEGET: A bizalmasságot, sértetlenséget.
- MIT SZÜKSÉGES TENNI: Amennyiben elkerülhetetlen olyan szállítótól vásárolni, aki nem rendelkezik nálunk szervizzel, akkor a távkapcsolatot megfelelő védelemmel kell ellátni, és a végzett tevékenységeit naplózni kell.

Pl. 39.

- A SZERVEZET: Pénzügyi szervezet.
- A FELTÁRT HELYZET: A sok fiókos pénzügyi szervezet egyik fiókjánál a vezető év végén a megmaradt éves pénzügyi keretből, engedély nélkül internet csatlakozásokat vásárolt az egyes számítástechnikai munkahelyek számára.
- MIT FENYEGET: Biztonságot.
- MIÉRT VESZÉLYFORRÁS: A pénzügyi szervezet tűzfalakkal védekezett az Internet felé, ugyanakkor ez a fiók ezt a védelmi rendszert megkerülte, és miután az egyes munkahelyek a belső hálózathoz is csatlakoznak, ellenőrizetlen ajtót nyitott az internet felé.
- MIT SZÜKSÉGES TENNI: Egyrészt szabályozni kell a külső hálózatokhoz, nem bizalmas hálózatokhoz történő csatlakozás jogosultságát, valamint a betartást folyamatosan ellenőrizni kell. Másrészt a biztonsági tudatosságot, a veszélyérzetet a központon kívül is állandóan erősíteni kell. A biztonsági átvilágításnál az auditor számára kiemelt feladat a helyzetfeltárás során a külső hálózati csatlakozások maradéktalan feltárása.

2.2.6. Az információ rendszer életciklusa alatti biztonság

Pl. 40.

- A SZERVEZET: Több vállalat.
- A FELTÁRT HELYZET: A fejlesztés/beszerzés során nem érvényesítik megfelelően a biztonsági követelményeket.
- MIÉRT VESZÉLYFORRÁS: A nemzetközi, de a hazai tapasztalatok szerint is igen gyakran tudatosan kerül rosszindulatú szoftver vagy bármely, a biztonságot fenyegető megoldás a harmadik félnél folytatott fejlesztés során a számítástechnikai eszközbe.
- MIT FENYEGET: Bizalmasságot, sértetlenséget
- MIT SZÜKSÉGES TENNI: A megrendeléskor kell a fejlesztés körülményeivel, a fejlesztés tárgyával kapcsolatos biztonsági követelményeket meghatározni, nem utólag beépíteni például a biztonsági elemeket.

Pl. 41.

- A SZERVEZET: Több vállalat.
- A FELTÁRT HELYZET: Az átadás/átvételkor, illetve az azt megelőző szállításkor nem érvényesítik a biztonsági követelményeket.
- MIÉRT VESZÉLYFORRÁS: Ez lehetőséget teremt a fenyegetést jelentő megoldások bejuttatására a megrendelt eszközbe a szállítás alatt.
- MIT FENYEGET: Bizalmasságot, sértetlenséget.
- MIT SZÜKSÉGES TENNI: A megrendeléskor ki kell kötni a szállításra és az átadás/átvételre vonatkozó biztonsági követelményeket valamint az ellenőrzés jogát. A szállítónak az átadáskor fenyegetés mentességi nyilatkozatot kell tennie.

Pl. 42.

- A SZERVEZET: Több vállalat.
- A FELTÁRT HELYZET: Házi fejlesztés esetén nem korlátozzák a fejlesztő kapcsolatát a javításra átadott szoftverrel, mondván a legjobb rendszergazda a fejlesztőből lesz.
- MIÉRT VESZÉLYFORRÁS: A két biztonságkritikus munkakör egyidejű betöltése lehetővé teszi a szoftver manipulálását.

- MIT FENYEGET: Bizalmasságot, sértetlenséget.
- MIT SZÜKSÉGES TENNI: A fejlesztő és üzemeltető munkaköröket azonos személy nem töltheti be, írja a COBIT 3, mivel ezek biztonságkritikus feladatok (segregation duty).

Pl. 43.

- A SZERVEZET: Több vállalat.
- A FELTÁRT HELYZET: A különböző szoftverek (alkalmazói szoftver, rendszer szoftverek, stb.) új változatai szinte rendszeres tevékenységet, sőt elvárt tevékenységet várnak a fejlesztőtől. A változtatás jogosultsága és az egyéb ezzel járó kötelezettségek nem meghatározottak.
- MIÉRT VESZÉLYFORRÁS: Így előfordulhat jogosulatlan személy részéről történő módosítás, valamint elmaradhat az új változat bevezetése minden alkalmazónál, továbbá a dokumentáción átvezetése.
- MIT FENYEGET: A sértetlenséget.
- MIT SZÜKSÉGES TENNI: A programváltozás menedzsment, azaz a változtatáskezelés szabályozása a megoldás.

2.2.7. Számonkérhetőség

Pl. 44.

- A SZERVEZET: Több vállalat.
- A FELTÁRT HELYZET: A jelszavakhoz rendelt jogosultságok és a jogosulatlan tevékenységek (kísérletek) naplózása, illetve a naplók értékelése nem volt megoldva.
- MIT FENYEGET: Bizalmasságot, sértetlenséget.
- MIÉRT VESZÉLYFORRÁS: Az ellenőrzés hiánya motiváció a jogosulatlan tevékenységet elkövetni szándékozók (beleértve a saját munkatársakat is) számára.
- MIT SZÜKSÉGES TENNI: A biztonsági szervezetnek a naplókat (audit log, audit trail) folyamatosan ellenőrizni kell a jogosulatlan tevékenységek elkövetése vagy elkövetési kísérleteknek a felfedése szempontjából.

Pl. 45.

- A SZERVEZET: Több vállalat.
- A FELTÁRT HELYZET: Az informatikai erőforrások különösen a szoftverek leltára elhanyagolt, nem napra kész.
- MIT FENYEGET: Rendelkezésre állást.
- MIÉRT VESZÉLYFORRÁS: A vagyonleltár hiányosságai lehetővé teszik a jogosulatlan eltulajdonítást, amely az adatok, alkalmazások felfedéséhez, esetleg módosítás utáni visszatételéhez vezethet.
- MIT SZÜKSÉGES TENNI: Meg kell követelni az éves vagyonleltáron kívül, az évközi változások folyamatos követését.

3. Néhány tanulság

- A veszélyérzet hiánya a védelmi intézkedések megtételének elmaradáshoz, vagy be nem tartáshoz vezethet. „A nálunk ez nem történhet meg” elv súlyos fenyegetést képvisel. „ÉS HA MÉGIS”???
- Ha nem teszünk semmit, az a legnagyobb kockázat.
- A jó védelmi intézkedés megtétele nem azonos a rendeltetésszerű végrehajtással.
- A munkatársak megbízhatóságát teljes vállalati foglalkoztatásuk alatt, sőt azután is meg kell őrizni.
- Az elrettentés annak bizonyítása, hogy a menedzsment el van szánva a védelmi intézkedések rendeltetésszerű üzemeltetésének megkövetelésére, mely a biztonságirányítás elfogadott módszere.
- A biztonsági tudatosság folyamatos erősítése az előfeltétele annak, hogy a védelmi intézkedések hatékonyságát fenntartsák.

Végül célszerű figyelembe venni a NYOLC AXIÓMÁT A BIZTONSÁG MENEDZSMENTRŐL:

- Nincs 100%-os védelem, így mindig van maradék kockázat.
- Az adat (információ) védelme a személyes adatok védelmét jelenti. Az adatbiztonság vagy a személyes adatok biztonságát vagy minden adat (személyes adat, üzleti adat, stb.) biztonságát jelenti az informatikai biztonságban. Az adat az egyik informatikai erőforrás az öt közül, és az informatikai biztonság mind az öt védelmét igényli.

- Csak az integrált, egész vállalatot átfogó, egyenszilárdságú biztonsági rendszer nyújt hatékony védelmet.
- A veszélyforrások, kockázatok nem állandóak, ezért rendszeresen vizsgálni kell őket.
- A gazdasági szervezet mikrogazdasági rendszer, amely az üzleti, termelési (ha van), és az információ rendszerből áll.
- A vagyonbiztonság, termelési biztonság, és informatikai biztonság egyaránt a bizalmasságtól, sértetlenségtől, és rendelkezésre állástól függ, és ezek átfedik egymást.
- Az üzletmenet folytonosság csak akkor biztosítható, ha az egész mikrogazdasági rendszerre kiterjed.
- A biztonságtechnika, biztonságszervezés külön szakma, és nem is egy.