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

INFORMATIKAI BIZTONSÁGI SZAKÉRTŐ KÉPZÉS

VASVÁRI GYÖRGY CISM
Informatikai biztonsági szakértő

INFORMATIKAI BIZTONSÁGI KOCKÁZAT PÉLDATÁR

(A feltárás 1993-2005 között, biztonsági átvilágítások során történt)

2005

TARTALOMJEGYZÉK

1. BEVEZETÉS

1.1. A PÉLDATÁR CÉLJA

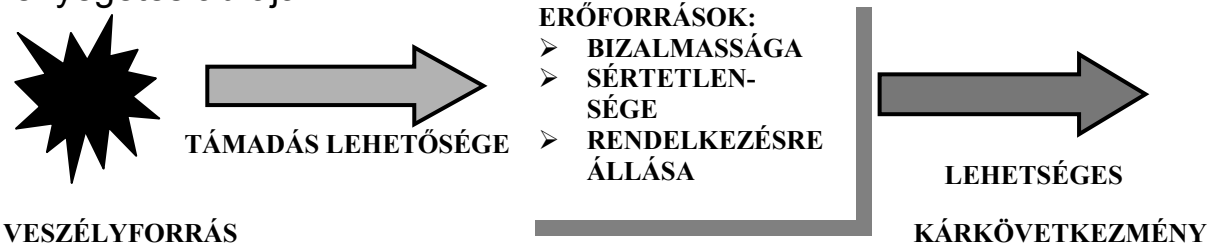
A Szerző az elmúlt több mint tíz évben nagy számú biztonsági átvilágítást végzett, illetve vett részt ilyen munkában. Arra a következtetésre jutott, hogy az informatikai szakértői, vezetői munka sikere jelentős mértékben azon múlik, hogy kellő időben feltárásra kerülnek-e az állandóan megújuló veszélyforrások, az új kockázatok. Ehhez természetesen a szándékon kívül, szükséges még a veszélyforrások felismerésének gyakorlata. Az először végzett biztonsági átvilágításoknál, a szakértő problémája, hogy hol keresse azokat.
A PÉLDATÁR célja, hogy a végzett átvilágítások tapasztalataiból kiemelve azokat a feltárt veszélyforrásokat, amelyeket különösen fontosnak ítél meg, pontosabban gyakrabban találkozott velük, bemutassa. Ezek ismeretében az átvilágítás első fázisaiban, a helyzetfeltárás, és az erre alapozott veszélyforrás elemzés során az átvilágítónak, van hol kezdenie. A tapasztalatok megszerzése közben, azonban, javasolt gyűjteni a magunk által feltárt veszélyforrásokat, és azokból célszerű egy saját veszélyforrás adatbázist felállítani a későbbi átvilágítási feladatokhoz.
Felhívom az olvasó figyelmét arra, hogy egy biztonságszervezéssel foglalkozó cég javaslatomra felállított ilyen adatbázist, amely néhány év után több mint ötszáz különböző veszélyforrást tartalmazott. A cég munkatársai az átvilágításhoz előkészítendő ellenőrzési listát ekkor már, figyelembe véve az átvilágítandó cég adottságait, ennek felhasználásával állították össze. Jó megoldás lenne, ha ez az adatbázis először a Példatárban megadott veszélyforrásokat tartalmazná.

Sikeres átvilágításokat kíván

A SZERZŐ

1.2. ALAPFOGALMAK

BEKÖVETKEZÉSI VALÓSZÍNŰSÉG:
Az esélye annak, hogy a veszélyforrás képezte fenyegetettség támadásként, bekövetkezzen, biztonsági esemény történjen.
BIZTONSÁG:
Olyan kedvező állapot, amelynek megváltozása nem valószínű, de nem is kizárt.
BIZTONSÁGI ESEMÉNY:
Minden olyan esemény, amely a biztonságra nézve fenyegetést jelent, vagy jelenthet.
FENYEGETÉS:
A fenyegetés a támadás lehetősége a támadás tárgyát képező erőforrás bizalmassága, vagy sértetlensége, vagy rendelkezésre állása ellen. A fenyegetés ábrája:



INFORMATIKAI ERŐFORRÁSOK:
Adat, ember, technológia, alkalmazások, támogatások (létesítmények, kisegítő berendezések).
KÁRKÖVETKEZMÉNY *(sebezhetőség):*
A veszélyforrás képezte támadás bekövetkezése esetén az erőforrások sérülése.
KOCKÁZAT:
Az erőforrások sérülésének, és a támadás bekövetkezésnek valószínűsége.
KOCKÁZAT MENEDZSMENT:
A feltárt veszélyforrások alapján a kockázat megállapítása , döntés a védelmi intézkedés megtételéről, vagy a kockázat felvállalásáról, a védelmi intézkedés kidolgozása, a maradék kockázat megállapítása.
MARADÉK KOCKÁZAT:
Az a kockázat, amely a védelmi intézkedés megtétele után marad fenn, és a csökkentésre nem tesznek védelmi intézkedést.
KOCKÁZATI MÁTRIX:
Egy mátrix amelyben a veszélyforrás, a bekövetkezési valószínűség, a kárkövetkezmény, a védelmi intézkedés, és a maradék kockázat szerepel.

VÉDELMI INTÉZKEDÉS:
A kockázat csökkentésére szervezési, vagy technikai eszközökkel tett intézkedés.
VESZÉLYFORRÁS:
A veszélyforrás mindaz, aminek támadás formájában történő bekövetkezésekor a rendszer működésében nem kívánt állapot jön létre, az erőforrások biztonsága sérül.

1.3. A KOCKÁZAT MENEDZSMENT

A kockázat menedzsment a helyzetfelmérés alapján megállapított veszélyforrásokhoz a becsült bekövetkezési valószínűség, és a becsült kárkövetkezmény alapján a becsült kockázatok megállapítása, majd annak eldöntése (mgm), hogy kell-e védelmi intézkedést tenni, és annak milyen legyen az erőssége. Ezután kell becsléssel a maradék kockázatokat megállapítani. A becslés oka, hogy sem a bekövetkezési valószínűség, sem a nem vagyoni kárkövetkezmény számítással nem állapítható meg. Azok a törekvések, amelyek számításokkal végzik ezt el, kivétel nélkül becsléssel meghatározott adatokból indulnak ki.

A kockázat becslése:

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

Ahol P=Probability, a bekövetkezési valószínűség, amely lehet VS7igen kicsi, S= kicsi, M7közepes, L=nagy, XL=igen nagy, és
V= Vulnerability sebezhetőség, kárkövetkezmény, amely lehet R=Részleges (és ez lehet S, M, L), valamint G=Globális (amely lehet S, M, L)
A kockázati mátrix:

Veszély for.neve	Fenyege-tettség	Beköv. valósz.	Sebez-hetőség	Kockázat	Védelmi intézkedés	Maradék Kockázat
Tűz	Rend.állás	M	GL	L	tűzvédelem	S

1.4. 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 költség igényes. 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 álláspontón alapul.

1.5. 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: (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 biztonságszervezés 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 egyen szilárdságú informatikai biztonság.
- MIT FENYEGET: Biztonságot
- MIT SZÜKSÉGES TENNI: Az integrált információ rendszer, az integrált informatikai, és külön integrált biztonsági szervezeti felépítés szükséges.

Pl. 2.

- A SZERVEZET: Iparvállalat
- A FELTÁRT HELYZET: Egymástó 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 egyen szilárdságú biztonságot, ha vezérigazgató közvetlen, integrált biztonsági szervezet van, amely a vagyonbiztonsági, üzembiztonsági, és informatikai biztonsági felelősöket szakmailag irányítja.

2.1.2. HUMÁN POLITIKA

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 szúrópróbával 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 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 végrehajtáshoz 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,), nemzetközi szabványok (ISO/IEC 17799), és ajánlások (COBIT 3) egyértelműen előírják, hogy a biztonsági, és biztonság kritikus 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 munkahely változtatás 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 humán politikai vezető, aki közülük hagyta, annak segítségére volt a szenvedélybetegségtől megszabadulni, a többiek kiléptek. Ezt felvetve az informatikai munkatársak közölték, hogy ilyen kérdéssel nem hajlandók foglalkozni.

- MIÉRT VESZÉLYFORRÁS: A szenvedély betegségek 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 humán politikai vezetőn kívül, a közvetlen munkatársak is részt kell, hogy vegyenek.

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 biztonság tudatos 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 üzletment folytonosság folyamatos biztosítását,

2.1.4. IRATKEZELÉS

Pl. 11.

- A SZERVEZET: Több vállalat
- A FELTÁRT HELYZET: Az Iratkezelési Utasítás nem tér ki az elektronikus íratok 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 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 tartalmaznak 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 kiderüljön 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 felelős a személyes adatok védelmével kell foglalkozzon a titkárság alárendeltségében, míg az informatikai biztonsági felelős a biztonsági szervezethez tartozik.

Pl. 15.

- A SZERVEZET: Több vállalat
- A FELTÁRT HELYZET: Az adatvédelemi (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 osztályozni kell.

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 érzékenységük 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 élőerős védelemmel, valamint beton fallal 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 üvegfala, mind a robbanás veszélyt jelentő tartály közelsége miatt. Ez egyrészt kétségessé teszi a hatékony hozzáférés védelmet, másrészt a robbanás veszély 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 helyiségek, berendezésektől távol kell elhelyezni.

PI. 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 biztonságos veszélyforrás, ugyanis a támadó jól képzett, valamint a módszer nem titkos, így 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.

PI. 20.

- A SZERVEZET: Pénzügyi szervezet
- A FELTÁRT HELYZET: Az egyes biztonság érzékeny helységekbe, 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.

PI. 21.

- A SZERVEZET: Pénzügyi szervezet
- A FELTÁRT HELYZET: A biztonság érzékeny, zárt helyiségként osztályozott helyiségek falai gipsz kartonból készültek.

- MIÉRT VESZÉLYFORRÁS: A gipsz karton 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.

PI. 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.

PI. 23.

- A SZERVEZET: Több vállalat
- A FELTÁRT HELYZET: A munkaasztalok elhagyása esetén 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 a képernyővédő alkalmazást jelenti, hanem a bejelentkezést követően az információ rendszerrel létrejött viszony meghatározott időn túli inaktivitás esetén történő automatikus megszakítását.

2.2.2. FIZIKAI RENDELKEZÉSRE ÁLLÁS

PI. 24.

- A SZERVEZET: Iparvállalat.
- A FELTÁRT HELYZET: A folyamatos áramellátás biztosítása érdekében a központi számítástechnika épületétől kb. harminc méterre lévő transzformátor háztól két elektromos tápkábellel volt a kettős betáplálás megoldva.

- MIÉRT VESZÉLYFORRÁS: A közeli transzformátor háztól, 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 mennél távolabb lévő alállomásától kell vezetni.

Pl. 25.

- A SZERVEZET: Távközlési vállalat.
- A FELTÁRT HELYZET: A távközlési vállalat a központi számítástechnika elhelyezésre épületet kívánt felépíteni, és szakértői véleményt kért biztonsági szempontból a kijelölt, egyébként tulajdonát képező területen való elhelyezésről. A szomszédos telken éppen megkezdték egy benzinkút építését. Álláspontunkkal szemben találtak egy szakértőt, aki azt nyilatkozta, hogy a benzinkút nem jelent veszélyforrást a tervezett épületre nézve.
- MIÉRT VESZÉLYFORRÁS: A benzin kút robbanás veszélyes, 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 szervezetnél a biztonsági átvilágítás során megállapították, hogy nincs a számítástechnika elhelyezésére szolgáló épületben Faradayháló, majd a vizsgálati jelentést olvasva a gondnok bemutatta az építészeti tervet, amely szerint az épület építésekor beépítették azt. Kiderült, hogy az eredetileg beépített Faradayháló földelése megsérült.
- MIÉRT VESZÉLYFORRÁS: A Faradayháló 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 Faradayhálót is.

2.2.3. LOGIKAI HOZZÁFÉRÉS

PI. 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. (egyesek az átvilágítást végzők közül ezt a megoldást közismert jelszónak nevezték el).
- MIÉRT VESZÉLYFORRÁS: Az azonos jelszó, és jogosultságok gyakorlatilag megszüntették a hozzáférés –védelmet, 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 információ rendszer 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 tovább lépési jogosultság automatikusan kerül eldöntésre.

PI. 28.

- A SZERVEZET: Pénzügyi szervezet
- A FELTÁRT HELYZET: A jogosultságok jelszóhoz rendelése nem a munkaköri leíráson 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 kikényszeríttet bejelentkezés esetén a munkatársak saját jelszavukkal lépnek be a rendszerbe.
- MIÉRT VESZÉLYFORRÁS: Ez azzal jár, hogy a kikényszeríttet bejelentkezést követő tevékenységek a munkatárs felelősségére, kerülnek rögzítésre.
- MIT FENYEGET: Sértetlenséget
- MIT SZÜKSÉGES TENNI: az erőszakkal, például rablótámadás esetén jogosulatlan művelet végrehajtása céljából kikényszeríttet 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 ellenőrzötten, 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 jelszó cserét 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 végzése 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 nagy számú 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: A biztonságot
- MIT SZÜKSÉGES TENNI: A nem bizalmas hálózati kapcsolatok felőli védelemre a tűzfal önmagában nem nyújt elegendő védelmet, szükséges a rosszindulatú sw-ek, (vírus, spyware, spam) elleni aktív védelem, valamint behatolás védelmi (IDS, vagy IPS) sw alkalmazása is.

Pl. 33.

- A SZERVEZET: Pénzügyi szervezet
- A FELTÁRT HELYZET: Harmadikféltől megrendelt sw-ben, több éves használat után, egy új belépő jelentése nyomán kiderült, hogy rosszindulatú sw van, amely a beérkező pénz mennyiségek meghatározott részét jóváírja egy-két munkatárs számláján, akik azt időnként felveszik, és szétosztják egymás között.
- MIÉRT VESZÉLYFORRÁS: Ez a sw a csalást valósította meg, és megkárosította a pénzügyi szervezetet. A sw készítői természetesen tagadták, hogy a fejlesztés során náluk került be a rosszindulatú sw.
- MIT FENYEGET: Biztonságot
- MIT SZÜKSÉGES TENNI: Az átadás/átvételkor „fenyegetésmentességi nyilatkozatot” kell kérni a szállítótól, mert az ilyen sw-ek 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 sw-ek 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, és 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, napra készen kell tartani, és a biztonsági eseményeket naplózni kell, amelyet 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 esemény!
- 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 sw-ek ellen kell aktív rendszerekkel védekezni, ami például a kém sw-ek, és a kéretlen 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 képviselet híján, maga szervizelte, ami azt jelenti, hogy az információ rendszerrel távdiagnosztikai, és távjavítási kapcsolatban volt.
- MIÉRT VESZÉLYFORRÁS: A gyakorlatban ez korlátlan tevékenységi lehetőséget nyújtott számára, attól függetlenül, hogy így hozzá férhetett 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 kerül rosszindulatú sw, vagy bármely a biztonságot fenyegető megoldás tudatosan 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, és az ellenőrzés jogát. A szállítónak az átadáskor fenyegetés mentességi nyilatkozatot kell tennie.

Pl. 42.

- A SZERVEZET: Több vállalat
- A FELTÁRT HELYZET: A házi fejlesztés esetén nem korlátozzák a javításra a fejlesztő kapcsolatát az átadott sw-rel, mondván a legjobb rendszergazda a fejlesztőből lesz.
- MIÉRT VESZÉLYFORRÁS: A két biztonság kritikus munkakör egyidejű betöltése lehetővé teszi a sw manipulálását.
- MIT FENYEGET: Bizalmasságot, sértetlenséget
- MIT SZÜKSÉGES TENNI: A fejlesztő és üzemeltető munkaköröket azonos személy nem töltheti be, írja a COBIT 3, mivel ezek biztonság kritikus feladatok (segregation duty)..

Pl. 43.

- A SZERVEZET: Több vállalat
- A FELTÁRT HELYZET: A különböző sw-ek (alkalmazói sw, rendszer sw-ek, stb.) új változatai szinte rendszeres tevékenységet, sőt elvárt tevékenységet képeznek a fejlesztőtől. A változtatás jogosultsága, és az egyéb ezzel járó kötelezettségek nem meghatározottak.
- MIÉRT VESZÉLYFORRÁS: Így előfordulhat a jogosulatlan személy részéről történő módosítás, valamint elmaradhat az új

változat bevezetése minden alkalmazónál, valamint a dokumentáción átvezetése.
- MIT FENYEGET: A sértetlenséget
- MIT SZÜKSÉGES TENNI: A programváltozás menedzsment, azaz a változtatás kezelés 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 naplókat (audit log, audit trail) folyamatosan a biztonsági szervezetnek jogosulatlan tevékenységek elkövetése, vagy elkövetési kísérleteknek a felfedése szempontjából, ellenőrizni kell.

Pl. 45.
- A SZERVEZET: Több vállalat
- A FELTÁRT HELYZET: Az informatikai erőforrások, különösen a sw-ek 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 vagyon leltáron 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 az után is meg kell őrizni.
- Az elrettentés, annak bizonyítása, hogy a menedzsment el van szánva a védelmi intézkedések rendeltetésszerű üzemeltetésének megkövetelésére a biztonságirányítás elfogadott módszere.
- A biztonsági tudatosság folyamatos erősítése az előfeltétele, a védelmi intézkedések hatékonysága fenntartásnak.
- Végül célszerű figyelembe venni a

NYOLC AXIÓMÁT A BIZTONSÁG MENEDZSMENTRŐL :

1. Nincs 100%-os védelem, így mindig van maradék kockázat.
2. 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.
3. Csak az integrált, egész vállalatot átfogó egyenszilárdságú biztonsági rendszer nyújt hatékony védelmet.
4. A veszélyforrások, kockázatok nem állandóak, ezért rendszeresen vizsgálni kell őket.
5. A gazdasági szervezet mikró gazdasági rendszer, amely az üzleti, termelési (ha van), és az információ rendszerből áll.
6. A vagyonbiztonság, termelési biztonság, és informatikai biztonság egyaránt a bizalmasság, sértetlenség, és rendelkezésre állástól függ, és ezek átfedik egymást.
7. Az üzletmenet folytonosság csak, ha az egész mikró gazdasági rendszerre kiterjed, biztosítható.
8. A biztonság technika, biztonságszervezés külön szakma, nem is egy.