M Ű E G Y E T E M 1 7 8 2

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

BIZTONSÁG MENEDZSMENT KUTATÓCSOPORT

VASVÁRI GYÖRGY CISM
Tiszteleti egyetemi docens

LENGYEL CSABA
biztonsági menedzser, KELER Rt

KISVÁLLALAT BIZTONSÁG KERETRENDSZERE

Vagyonbiztonság, informatikai biztonság

AJÁNLÁS

4.1 változat

2006

A KUTATÓ CSOPORT további tagjai, akik véleményükkel támogatták az ajánlás elkészítését:

Erdősi Péter CISA, PhD hallgató
Sántha Péter vezető szakértő

TARTALOMJEGYZÉK

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. Ezek 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 értelmezhetőek, hogy megadják, mit kell vizsgálni, melyek az elvárások, így ezek alapján a teendők is meghatározhatók.

„A Vállalati Biztonság Keret rendszere” 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 hozzáteszia kis energiafogyasztás)t 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, COBIT QUICKSTART ÉS COBIT SECURITY 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 kisvállatok informatikai ellenőrzési céljainak. 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 szabvány[1] pontjainak többségét lefedi, és ezt egy kimutatással támasztja alá.

[1] Megjelent magyar szabványként is: MSZ ISO/IEC 17799 Információtechnika. Az informatikai biztonság menedzselésének eljárás rendje.

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 felvételkor 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 kétségessé (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 humán politika hiánya, amely a megbízhatóság biztonsági követelményének érvényesítését kétségessé 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 eredményez, és nem teszi 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 szerződésekben 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 kockázatossá (V10, V11).

LOGIKAI HOZZÁFÉRÉS LEHETŐSÉGE

- A logikai hozzáférés korlátozatlansága, feltételekhez kötöttségének hiánya a kisvállalat számára az üzleti cél és követelmények teljesíthetőségét teszi kockázatossá (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 kockázatossá (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, kétségessé 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 exakt, matematikai eszközökkel nem értékelhetők, csak a vagyoni károk.

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

Ezeket a kockázati értékeket (a szürke 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 a 12. oldalon.

Ugyanakkor becsült értékekből kiindulva megadunk egy számszerűsített kockázat elemzési módszert is a következő oldalon.

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	3	2	3	4
	1	1	2	3	2	3	4	3	4	5
	2	2	3	4	3	4	5	4	5	6
	3	3	4	5	4	5	6	5	6	7
	4	4	5	6	5	6	7	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

Ebben az esetben a kockázati mátrix is számértékeket tartalmaz.

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 (papír alapú 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 napra kész meghatározása.
  - V2.) A felhasználók, munkatársak folyamatos biztonsági képzése, a biztonsági tudatosság naprakész biztosítása.
  - V3.) Gondoskodás megfelelő humán politika végrehajtásával, a felvételkor 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 napra készen 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 bevonásról, az SLA figyelembe vételével.
  - V11.) Az üzletmenet-folytonosság érdekében gondoskodás háttér, papíralapú, és elektronikus háttér megoldásokról, rendszerről más helyszínen, valamint 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.

    Az a vagyon és IT biztonsági alrendszereken 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 keret rendszere olyan jellemzőkkel kell, hogy rendelkezzen, amelyek a kisvállalat anyagi, létszám korlátainak megfelelnek, azaz megvalósíthatóak. Vizsgáljuk meg, hogy a fentiekben meghatározott keret rendszer 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 intézkedéseihez 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 tűrés határt.

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

- 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 tartalmaznak 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 exakt módszerekkel csak a vagyoni károkra határozható meg, a nem vagyoni károkra csak legjobb esetben is becsülhetők, így az azt 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 nagyobb*

- 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, habár röviden, de el kell végezni. Ezeket tartalmazza, az a Biztonsági Intézkedései 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) kör lehet. .

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 szempontnak megfelelő védelmi intézkedéseket nem tett meg, illetve ennek kockázatát a menedzsment felvállalta. Ezeket az audit kezdete előtt az auditorrral 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 megfelelőség igénylése. Az eddig írtak alapján belátható, hogy a kisvállalatok biztonsági rendszere erősségének értékelésére a CBS megfelelőség 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. A BIT
   - 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.
   - ✓ Védeni 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. Következetesen 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 szerződéseseket, 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, vírus védelem, 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?
13. Megtörténik-e az állomány biztonsági oktatása? Vannak-e biztonsági gyakorlatok? Dokumentáltak-e ezek?
14. 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.
15. Összevetik-e a teszteredményeket az üzleti céllal és biztonsági követelményekkel a végső biztonsági megoldás elfogadását megelőző értékeléskor? Bevonják-e az állományt az értékelésekbe?
16. Értékelik-e minden változtatáskor (patch-ek telepítésekor is) az érzékeny adatok integritását és az adatvesztés kockázatát?
17. Naplózzák-e változtatásokat a kritikus változásokat követően?

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

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