Komplex biztonságmenedzsment

Zólyomi Zsolt

Témavezető

Prof. Em. Dr. Berek Lajos egyetemi tanár

Biztonságtudományi Doktori Iskola

Budapest, 2019
Szigorlati Bizottság:

Elnök:

Prof. Dr. Pokorádi László egyetemi tanár, ÖE

Tagok:

Dr. habil. Berek Tamás egyetemi docens, külső - NKE

Dr. Kiss Sándor ny. egyetemi docens - külső

Nyilvános védés bizottsága:

Elnök:

Prof. Dr. Rajnai Zoltán egyetemi tanár, ÖE

Titkár:

Dr. Pethő Richárd adjunktus, ÖE

Tagok:

Dr. habil. Berek Tamás egyetemi docens, külső – NKE

Dr. Őszi Arnold tanársegéd, ÖE

Dr. habil. Farkas Tibor egyetemi docens, külső – NKE

Bírálók:

Dr. habil. Kovács Tibor egyetemi docens, ÖE

Dr. Fialka György, külső

Nyilvános védés időpontja

..............................
TARTALOMJEGYZÉK

Bevezetés ........................................................................................................................................6
1 A biztonság és a biztonságmenedzsment ................................................................................9
   1.1 A biztonság és annak értelmezése ................................................................................9
1.2 A biztonságmenedzsment ................................................................................................13
   1.3 A kérdőív és annak kiértékelése ..................................................................................17
      1.3.1 A kérdőív kiértékelése .........................................................................................19
      1.3.2 Összefoglalás ....................................................................................................25
2 A komplex vállalati biztonságmenedzsment ........................................................................26
   2.1 Vállalati biztonságmenedzsment ..................................................................................26
   2.2 Elgondolásom: Komplex vállalatbiztonsági szabályzat tervezet ..................................27
   2.3 Összefoglaló ..............................................................................................................29
3 Biztonsági irányítási rendszer és ellenőrzés .......................................................................30
   3.1 A rendszer elemei: ......................................................................................................30
   3.2 A rendszer működése: ...............................................................................................32
   3.3 A biztonsági irányítási rendszer kulcsfontosságú területei ...........................................33
   3.4 Összefoglaló ..............................................................................................................33
   3.5 A biztonsági szervezet pénzügyi kontroll modellje ......................................................34
   3.6 Összefoglaló ..............................................................................................................37
4 A vállalatbiztonsági szabályzat kialakítása .........................................................................38
   4.1 Kockázatelemzés .........................................................................................................42
      4.1.1 Általános szabályok, vezetők felelőssége ................................................................43
      4.1.2 A biztonsági szervezet felelősségei, feladat meghatározás .................................43
   4.2 Fizikai biztonság .........................................................................................................51
      4.2.1 Külső biztonság ....................................................................................................51
      4.2.2 Az épület határai és az épületen belüli biztonság ...............................................54
      4.2.3 Zár- és kulcskezelési szabályok .........................................................................60
      4.2.4 A vállalatnál alkalmazott belépési ellenőrzés és a belépőkártyák formái ..........62
4.3 Biztonsági események kezelése, belső vizsgálatok ........................................... 70
  4.3.1 Biztonsági események ................................................................................. 70
  4.3.2 Belső vizsgálatok ...................................................................................... 73
4.4 Speciális biztonsági feladatok ......................................................................... 78
  4.4.1 Utazásbiztonság ......................................................................................... 78
  4.4.2 Oktatás ........................................................................................................ 81
4.5 Információbiztonság ......................................................................................... 82
  4.5.1 Általánosságban .......................................................................................... 85
  4.5.2 Tiszta asztal folyamat ................................................................................ 87
  4.5.3 Bizalmi iratok megsemmisítésénél szabályozása .......................................... 88
  4.5.4 Külső értekezletek ...................................................................................... 89
  4.5.5 Adatosztályozási szabályzat ....................................................................... 90
  4.5.6 Adatosztályozás .......................................................................................... 91
  4.5.7 Adatkezelési szabályok .............................................................................. 93
4.6 Krízismenedzsment ............................................................................................ 94
  4.6.1 Szerepek és felelősségek, áttekintés .......................................................... 106
  4.6.2 A krízismenedzsment szervezeti felépítése ............................................... 111
  4.6.3 A krízismenedzsment folyamata ................................................................. 111
  4.6.4 A krízismenedzsment terv ........................................................................ 115
4.7 A humánbiztonság ................................................................................................ 116
  4.7.1 A humánbiztonság lényegi elemei ............................................................... 117
  4.7.2 Összeférhetetlenség ................................................................................... 121

Összegzett következtetések ..................................................................................... 126
Új tudományos eredmények .................................................................................... 127
Ajánlások ................................................................................................................ 128
Hivatkozások .......................................................................................................... 129
Felhasznált irodalom ................................................................................................ 137
Ábrajegyzék .......................................................................................................... 146
A szerző publikációi ........................................................................................................................................... 147
Mellékletek.......................................................................................................................................................... 150
Köszönénetnyilvánítás ....................................................................................................................................... 173
Bevezetés

Értekezésem témájának tekintetében szükségesnek tartom megjegyezni, hogy a biztonság területén tevékenykedem mintegy harminc éve. Jelenleg a Flex, amerikai multinacionális vállalat Európa, Közel-Kelet, Afrika (EMEA) régiójának biztonsági vezetését vállaltam el, ahol ma is tevékenykedem. Így az utóbbi húsz év témám területén történő munkálkodással töltöttem el, ahol a kezdetektől fogva adott volt az alapvető indítatás afelé, hogy átfogóan és minden részletre kitertően egyre jobban megismerjük a biztonságmenedzsmentet, annak hazai és nemzetközi eredményeit, feltérképezzük jelenlegi fejlettségi szintjét és tevékenyen hozzájáruljuk annak emeléséhez.

A biztonságmenedzsment területén szakmai munkával és kutatással eltöltött időszak alatt meggyőződésemmé vált, hogy az általam vizsgált terület további tanulmányozására, fejlesztésére folynamatosan szükség van. Kutatómunkám továbbfejlesztése számomra és a biztonságmenedzsmentet foglalkozó kollégák részére is segítséget nyújthat a magas szintű, teljes lefedettségű vállalatbiztonság létrehozására és működtetésére, ezáltal a vállalat értékeinek hatékony megóvására.

A tudományos probléma megfogalmazása
Magyarországon a biztonságmenedzsment többnyire nincs a helyén. A biztonságmenedzsmentet, mint a biztonságot közvetlenül befolyásoló tényezőt veszik alapul.

A biztonságmenedzsment az adott szervezet rendeltetésszerű működését, így a biztonságot közvetlenül befolyásoló védelmi erőforrás, de ezt a biztonsági szféra sem fogta még igazából fel.

A téma kutatásának hipotézisei
1. A szervezeteknél/vállalatoknál egy bizonyos szint felett a biztonságmenedzsment az adott szervezet biztonságát közvetlenül, pozitívan befolyásoló védelmi erőforrás.

2. A vállalati biztonságmenedzsmentet komplex módon lefedő új elméleti és gyakorlati tartalommal rendelkező törzsanyag létrehozása szükséges, amelyre kellőképpen tudnak támaszkodni a biztonsági vezetők, biztonsági szakemberek és oktatók.

3. Magyarországon a vállalatoknál eltérő összetételű, feladatú biztonságmenedzsment szervezet működik, mely a vállalati hierarchiában leggyakrabban nem a megfelelő helyen van, valamint a biztonságmenedzsment nem minden területét átfogó biztonsági szabályzat-rendszer
működik. A legtöbb vállalat vezetősége a biztonságmenedzsmentet nem az indokolt fontossága szerint kezeli, ezért az nem lehet képes a maximális eredmények elérésére, a legmagasabb hatékonysággal védeni a vállalat értékeit.

4. Véleményem szerint a biztonságmenedzsment törzsanyagának alkalmazásával a biztonsági vezetők jobb eredményeket tudnak elérni, a kockázati tényezők nemkívánatos hatásait csökkenteni tudják a vállalati értékek megvédésének szempontjából, illetve szakmai elismertségük növekedhet a vállalat vezetőségén belül, így a biztonságmenedzsment jelentősége és érdekérvényesítő képessége is magasabbra kerülhet a vállalati hierarchiában.

Kutatási módszerek

Értekezésemben elsősorban empirikus és logikai kutatási módszereket terveztem alkalmazni. Az általam tanulmányozott, kutatott vállalati biztonságmenedzsment témát három irányvonal mentén terveztem kutatni és vizsgálni.

Az első irányvonal a hazai és a nemzetközi szakirodalom összegyűjtése és tanulmányozása volt. 1998-tól napjainkig folyamatosan vettem részt szakmai, tudományos konferenciákon, belföldön szervezői és előadói, külföldön előadói minőségben. Ezeken a konferenciákon lehetőségem volt szakterületemet érintően, szakemberekkel konzultálni, véleményeket megismerni, ütköztetni, és az általam elfogadott, feldolgozott eljárásokat, következtetéseket értekezésembe beépíteni. A tudományos konferenciák szüneteit is arra használtam fel, hogy kötetlen formában ismerkedhess meg más szakemberekkel, felelősségük és aktivitásuk területével. A beszélgetések során lehetőség nyílt az ismeretek elmélyítésére, illetve kiszélesítésére is, amelyek szintén hozzájárultak ahhoz, hogy szélesebb révalátásom alakulhasson ki a biztonságmenedzsment struktúrájára és eredményeire.

A második irányvonal értekezésem témájának vizsgálata kapcsán, terveztem empirikus úton információkhoz jutni. Elsősorban a biztonsági vezetőkhöz intézett kérdőív formájában, az általuk megadott visszajelzéseket megismerve és elemezve jutottam el ismételten (kiinduló álláspontomat megerősítve) ahhoz a felismeréshez, hogy a vállalati biztonságmenedzsment törzsanyag létrehozása indokolt és szükséges.

A harmadik irányvonal a vállalati biztonsági vezetők előtt álló biztonsági kihívások és biztonsági kockázatok tükrében kialakított alapvető biztonsági törzsanyag kidolgozása, amely eléggé általános ahhoz, hogy széleskörben használható legyen, de eléggé specifikus is, hogy megfelelő módon
szabályozzon, valamint egyszerűen áttekinthető, homogén rendszert alkosson. Kutatómunkám során végig szem előtt tartottam, az eredményeim hasznosságát, vagyis a kész értekezés, biztonsági vezetők és szakemberek általi felhasználhatóságát. Az eredményeimet szakmai életutam alatt folyamatosan megosztottam a biztonsági szakemberekkel, kollégákkal, publikációimban és konferenciákon tartott előadásaim során.

Az értekezésem alapjául szolgáló ismeretanyag gyűjtését, a kutatómunkát 2018. december 15-én fejeztem be.
1 A BIZTONSÁG ÉS A BIZTONSÁGMENEDZSMENT

1.1 A biztonság és annak értelmezése

Mi a biztonság, mit értünk alatta, amikor szóba hozzuk, megfogalmazzuk? A mai angol nyelvhasználatban a „security” a latin „securitas” (biztonság, gondtalanság, lelki nyugalom) szó többlépcsős módosulásával került be. Ez az átvétel és átalakulás az 1100-as évek elejétől az 1400-as évek végétől tartott (Sikernesse, Sikerhede, Sikerte, majd Security). A magyar nyelvben a biztonság szó „biztonlét” jelentéssel került be az 1862-ben kiadott Czuczor Gergely féle szótárba[101], ahol még új szóként jelölik: „Divatba nem régen jött szó, a régi és helyesebb biztosság értelmében.”[101, I. kötet, 680. o.] A jelenleg is használatos magyar értelmező szótár szerint a biztonság jelentése a következő: „A dolgoknak, életviszonyoknak olyan állapot, amelyben kellemetlen meglepetésnek, zavarnak, veszélynek nincs v. alig van lehetősége, amelyben illyentől nem kell félni.”[104]

A hazai szakirodalomban többféle, többrétegű és a biztonságot különbözőképpen értelmező meghatározásokkal találkozhatunk, ezek összefoglalása nem célja az értekezésnek, sokkal inkább annak az iránynak a felvázolása, ami a legközelebb áll a biztonságmenedzsmenthez.

Számomra a legjellemzőbb módon határozza meg a biztonság fogalmát: Dr. Berek Lajos, Dr. Berek Tamás, Berek László 2016-ban az Óbudai Egyetemen megjelent, Személy és vagyonbiztonság című kiadványuk, melynek az első fejezetében foglalkoznak a szerzők a biztonság fogalmának értelmezésével.

„A biztonság személyek és szervezetek azon állapota, melyet, a létüket, illetve rendeltetésszerű működésüket veszélyeztető szándékos jogellenes magatartások és az azokkal szemben alkalmazott védelmi erőforrások együtthatása határoz meg.”[105]

Ezzel a megfogalmazással tudok a leginkább egyetérteni, hiszen, ha nagyon leegyszerűsítiük a biztonság értelmezését, akkor az veszélymentességet, a veszély, vagy a fenyegetettség hiányát jelenti, amit tőkéletesen lefed a fenti definíció. Még a biztonság alapértelmezésén kívül szükségesnek tartom megemlíteni a biztonság fontosságát. A biztonságot, Maslow piramisa alapvető fontosságúnak tartja, mindjárt a második szinten említi a létszükségletek kielégítése után, vagyis a biztonságra igény van, a biztonság az ember alapvető szükséglete. (szükséglet: a bennünk támadt hiányérzet megnyilvánulása, saját megfogalmazás).
Összefoglalhatjuk, hogy a biztonság olyan személy, vagy szervezet állapota, amelynek léte és rendeltetése van. Ezt a létet, illetve rendeltetést veszélyezteteti valami, amely veszély kivédésére és elhárítására az ember létrehozza, elkészíti a védelmet. Pl: a személy, vagy szervezet értékeit, vagyonát veszélyeztetetti több tényező is, tűz, természeti-, vagy ember által okozott katasztrófa, támadás, lopás, stb. A lopás példájánál maradva ezt a veszélyeztetést, vagy más szóval kockázati tényezőt az ember úgy tudja elhárítani, ha védelmi berendezéseket telepít, űrséget szervez és működtet, kapcsolatban van a bűnüldőző hatóságokkal, stb.

A fentiekből jól nyomonkövethető, hogy értekezésemben nem a nagy egésszel, a mindenre kiterjedő általános biztonsági kérdésekkel, hanem annak egy szeletével a nagy multinacionális és/vagy nagyvállalatok, gazdálkodó szervezetek biztonságával kívánok foglalkozni.

„A biztonságot közvetlenül két tényező határozza meg. Az egyik a veszélyeztetés, azaz a szándékos jogellenes magatartások, melyek negatívan befolyásolják a biztonságot. A másik az alkalmazott védelmi erőforrások mennyisége és minősége. Minél több erőt és hatékonyabb őrzést és védelmet alkalmazunk, annál magasabb szintű lesz a biztonság. Ugyanis az alkalmazott védelmi erőforrások a szándékos jogellenes magatartásokkal szemben hatnak, azt akadályozzák, a legjobb esetben megakadályozzák.” [106]

A biztonság megszervezéséről született szakvélemények, akár egy objektum esetében, akár egy rendszer felépítéséről értekeznek a vagyonvédelmet egy piramis formával ábrázolják. Ezt a piramist általában három részre osztják fel, mechanikai-, elektronikus-, és élőerős védelemre.

![1. ábra A vagyonvédelem (saját szerkesztés)](image)

Ennek a háromszintű piramisnak a kibővített formáját használják sokan, hivatkozva Utassy Sándor: Komplex villamos rendszerek biztonságtechnikai kérdései, doktori (PhD) értekezése 2009. alapján.
Ebben a piramisban már megjelennek védelmi intézkedések, biztosítás és a kockázat is, de a biztonságmenedzsmentet senki sem említi. [111]

Ezzel szemben én egy átfogóbb megközelítést javaslok, ami véleményem szerint jobban lefedi a biztonsági rendszert. A piramis ábrázolást egyébként kedvelem, mert jól lehet vele ábrázolni a hierarchiát (alá-, fölé rendeltséget) és kimutatható a tényezők aránya is, de ebben az esetben elégtelenül ábrázolja a biztonsági redszert. A lenti grafikus ábrázolás alapján látható, hogy a három fő elem a mechanikai-, elektronikus-, és élőerős védelem van a centrumban, ahol azonos arányban szerepelnek, hiszen minden egyes szervezet/vállalat esetében annak sajátosságai, szükségletei alapján kerülnek meghatározásra az arányai. Pl.: egy hulladékgyűjtő állomás elektronikai védelmi rendszere nem hasonlítható egy IT vállalat szerverfarmjának elektronikai védelmi rendszeréhez, vagy egy multinacionális óriásvállalat beléptető-rendszerre sem említhető együtt egy kb. tízszemélyes iroda beléptetés rendszerével, stb. Mindezekre a fő védelmi elemekre hatnak a kockázati tényezők, amelyeket számításba kell venni, ezek előzetes elemzésének eredményei alapján szükséges kialakítani a fő védelmi rendszereket. Ezt az egész rendszert pedig körbefonja a biztonságmenedzsment. A biztonságmenedzsment a biztonsági rendszer vezető része/eleme, amely megtervezi, létrehozza, működteti, és folyamatosan tökéletesíti a teljes biztonsági, vagy védelmi rendszert, ami nélkül nem beszélhetünk megfelelő, hatékony védelemről.
A biztonságot befolyásolják közvetlen és közvetett tényezők, a közvetett tényezők, mint a jogi környezet, biztosítási intézményrendszer, gazdasági tényezők, közbiztonság, munkanélkülség, stb. [105] A közvetlen tényezőkről már volt szó a 6. oldalon, a kockázati tényezők és a védelmi erőforrások [105]. Ebbe én még beleértem a biztonságmenedzsmentet is, mert a biztonságmenedzsment a lehető legközvetlenebbül befolyásolja a biztonságot, mint védelmi erőforrás. Egy szint felett, ammi lehet árbevétel, vagy dolgozói létszám, vagy a termék, vagy tevékenység értékessége, bizalmassága, egyértelműen kötelezően kellene biztonságmenedzsmentet alkalmazni a biztonsági rendszer kialakítására és működtetésére. Sajnálatos módon elterjed az a nézet, hogy a biztonság egy improduktív szervezet, mert nem hoz létre bevételt. Ezt az álláspontot a felkészületlen vezetők vallják, akik nem képesek átfogó rendszerekben gondolkozni, ezért ezek a vezetők és az általuk vezetett szervezet/vállalat hosszú távon nem lehet sikeres, mert nem tudják a rájuk bízott szervezetet a leghatékonyabban működtetni. Ez a hozzáállás helytelen. A biztonsági szervezet egy felkészült és hatékony biztonságmenedzsmenttel a szervezet/vállalat veszteségeinek minimalizálásával, vagy megszüntetésével jelentős financiális bevételt tud teremteni (nem engedi, hogy a dolgozók, illetve külsősök ellopják a vállalat értékeit). Egy lehetséges másik útja a biztonságmenedzsment vállalati
értékteremtésének, amikor bevonják a leltárián yok feltárásába, illetve azok megszüntetése
érdekében bevezetendő leltárfolyamatok megtervezésébe, ellenőrzési pontok kialakításába.

Összefoglalva megállapíthatjuk, hogy egy felkészült biztonságmenedzsment a szervezet bevételeit
növelheti, hatékony tevékenységével produktív ágazatként növelheti a vállalat pénzügyi
hatékonyságát.

1.2 A biztonságmenedzsment

Mit érünk ma Magyarországon vállalati biztonságmenedzsment alatt, valamint milyen fejlettségi
szintre pozicionálhatjuk napjainkban a nemzetközi biztonságmenedzsment jelenlegi vezető
tudományos, szakmai iránymutatásaihoz viszonyítva?

A vállalati biztonságmenedzsment, hazai kialakulásának előzményei, gyökerei, lényegének
értelmezése, jelenlegi szintjének a gyakorlatban megvalósuló irányai különböző mértékben
eltérnek a nemzetközi vezető eljárásmódktól, vagy nem teljes egészében fedik le a vállalati
biztonságmenedzsment teljes spektrumát, ezért szükséges és kívánatos az átfogó komplex
biztonságmenedzsment eljárás mielőbbi általános gyakorlattá válása.

A rendszerváltás, vagy rendszerváltozásig hazánkban nem létezett vállalati
biztonságmenedzsment. Az akkori társadalmi és gazdasági rendszer vagyon-, és
személybiztonsági kérdésekben kizárólag az állami rendészeti, tűz-, katastrófa-, polgárvédelmi
(és titkosszolgálati) szervekre támaszkodott. Ezen kívül, helyenként, főleg veszélyes ipari
üzemekben létrehozott üzembiztonsági rendsztet tevékenykedett, mely inkább munkabiztonsági
feladatokat látott el, de foglalkozott vagyonvédelemmel is. Még megemlíthetjük a különböző őröket
a rendszerváltás előtti időszakból, mint akik szintén a biztonsággal foglalkoztak a huszadik
század nagyobbik részében Magyarországon, pl.: éjjeliőr, vadőr, mezőőr, halőr, stb. Az állami és
a társadalmi tulajdon, kollektív tulajdon volt, egyéni értelemben csak személyi tulajdonról
beszélhetünk. Ebben a korszakban magán tulajdon gyakorlatilag nem létezett, az össztulajdon 2
%-t sem érte el, így annak védelmével sem kellett foglalkozni.

Ilyen biztonsági háttér mellett ért el minket a szabad piacgazdaság minden biztonsági kockázati
tényezőjével együtt. Erre nem voltunk felkészüelve, mint ahogy az elbizonytalannitott rendészeti
szervek sem. Az alapfeladatuk ellátására igyekeztek erőket átcsoportosítani miközben régebbi
szerepükhoz képest kivonultak a gazdasági területről. Ekkor szembesültek az immár tulajdonossá
vált vezetők is azzal, hogy már maguknak kell gondoskodniuk az értekeik védelméről. Mivel vállalati
biztonságmenedzsment képzés egyáltalán nem létezett, illetve még ma sem nagyon létezik, ezért különböző vezetési irányok alakultak ki, amelyek még ma is tartják magukat, bár már a kívánatos komplex biztonságmenedzsment is kialakulóban van.

**Biztonságmenedzsment szemléleti irányai:**

1. rendőri-katonai,
2. őrzésvédelmi,
3. munkavédelmi,
4. biztonságtechnikai,
5. informatikusi,
6. komplex biztonságmenedzsment.

**A rendőri-katonai irány:** volt rendőri és katonai vezetők által bevezetett irányzat, mely az objektumok fizikai védelmére, illetve a nyomozásokra koncentrál. Ez a legdominánsabb biztonságvédelmi irányzat jelenleg hazánkban.

**Az őrzésvédelmi irány:** vagyonvédelmi szolgáltatók szemléletéből alakult ki, fő súlypont az emberi (őrök általi) őrzésre helyeződik, általában „külsős” szemszögől ítélik meg a szükséges védelmi szintet.

**A munkavédelmi irány:** munkavédelmi mérnökök által képviselt elgondolás, ahol a munka-, tűz-, és egészségvédelemre helyeződik a fókusz. A vészhelyzet-menedzsmenten belül a vészhelyzeti reagáláson van a fő hangsúly.

**A biztonságtechnikai irány:** biztonságtechnikai mérnökök által megközelítés, ami a biztonságtechnikai rendszeren és elemein alapul, kamerarendszer, beléptetőrendszer, riasztó rendszerek.

**Az informatikusi irány:** informatikus mérnökök által gyakorlott eljárásrend, jellemzője az informatikus, analitikus rendszerszemlélet, melyben majdnem kizárólagos prioritása a számítástechnikai rendszerek, elemeinek, illetve a hálózatvédelmi rendszereknek van.

Mind az öt előzőleg felsorolt biztonságmenedzsment irányzat a lehető legszűkebben értelmezi a biztonságmenedzsmentet, kizárólag a saját szakmai elméletének és gyakorlatának megvalósítását tartja feladatának, a biztonságmenedzsment egyéb feladatait igyekszik kizárni a felelősségi
területéből, illetve áthárítani más szervezeti egységekre, lemondva ezáltal az átfogó szintű kontroll kialakításáról.

Példaképpen a rendőri-katonai, illetve az őrzésvédelmi irányzat számára megfelelő megoldás az, ha nem kell részt venniük az információbiztonság megvalósításában (e-mail ellenőrzés, internet használat figyelés, vállalat kárára történő információáramlás, stb.), azt teljes mértékben ráhagyják az IT szervezetre. Ez egy kényelmes felállási mód véleményük szerint, de ezzel át is adják a teljes ellenőrzést az IT szervezetnek a terület felett, vagyis a szükséges adatok nem állnak azonnal a rendelkezésükre, majd egy jövőbeni visszaélés kivizsgálásához, vagy ezekhez az adatokhoz csak körülményesen és késedelemmel juthatnak hozzá [91].

A komplex biztonságmenedzsment: (security) nemzetközi, elsősorban angolszász alapú megközelítés, betelepült multinacionális vállalatok által magukkal hozott szigorú biztonsági kultúra és eljárásrend. A magántulajdon védelme megkövetelte és kialakította saját védelmi rendszerét, ami a XX. század utolsó harmadában indult lendületes fejlődésnek. Jellemzője, hogy átfogó módon áll a biztonságnak, hogy minden elemét igyekszik integrálni a rendszerébe.


Szövényi György: Biztonságszervezői menedzsment [66] című értekezésében még többségében megtalálható a rendőri-katonai szemlélet, nagyon erős jogi háttérrel, de már a komplex biztonságmenedzsment is megnyilvánul egyes elemeihez. Pl.: A biztonságszervező menedzser eszköztára (84-93.o), ahol a humánbiztonság nélkülözetetlen elemeit fejt ki a szerző.

Szintén figyelemre méltó, hogy a szerző már használja „A komplex biztonságvédelmi rendszer kialakítása” (98-107.o) fejezetében a komplex kifejezést, de még nem érti alatta az átfogó komplex
biztonságmenedzsmentet teljes egészében. Sajnos a témánkat teljes mértéken lefedő, magyar, összefoglaló mű még nem készült el, ezt pótolni kell.

Nem szabad elfeledkezni arról, hogy jelentős számban jelennek meg hazai publikációk a biztonsággal foglalkozó lapokban, mint a Detektor Plusz magazin, az Árgus, a Biztonság, stb. Több hazai egyesület, pl.: MBVE, MBF, vagy a Kamara igen aktívan tevékenykedik annak érdekében, hogy a biztonság a megfelelő szintre kerüljön. Még sok a teendő ebben az irányban, hogy amikor a biztonságmenedzsmentről beszélünk, akkor ugyanazt is értsük alatta mindannyian. Ezt akkor érhetjük el, ha van megfelelő oktatás, tananyag és rendszer. Ennek a célnak az eléréséért a jelenkori biztonsági szakemberek vagyunk a felelősök, nekünk kell tenni azért, hogy mindez megvalósulhasson.

A hazai viszonyokat közelebbről érezzük, de ha kitekintünk Európába, vagy még távolabb a világ bármelyik régiójába, akkor sem éppen megnyugtató érzéseink keletkeznek. Számos problémát, kriízhelyzetet, érdekkellentetést, konfliktust tapasztalhatunk. Elegendő azonban, a közelmúltbeli 2008-as gazdasági válságra, a 2011-gyel kezdődött „arab tavasz”-ra, a mostanában is pengeélen táncoló, Európai Unió adósságválság megoldásának kísérleteire, a migrációs nyomásra és a globális felmelegedés hatásaira, a világ népességének növekedési ütemére, valamint az atomhatalmak szembenálló politikai és gazdasági érdekeire gondolni. Ezek a tendenciák, mind azt mutatják, hogy pillanatok alatt romolhat az általános biztonság, pl.: több lesz az anyagi javak elleni támadás, lopás, betörés, szállítmányok eltulajdonítása, fosztogatása, stb. Vagyis jóval több feladatunk lesz és sokkal mostohább körülmények között kell mindezeket elvégeznünk. Mindezekre fel kell készülnünk, mert csak akkor leszünk képesek megvédeni a ránk bízott értékeket, ha egy hatékonyan működő, a biztonság teljes spektrumát átfogó, komplex biztonsági rendszert tudunk működtetni. A szerencséssebbeknek közülünk ehhez rendelkezésre is fognak állni a szükséges anyagi alapok, a kevésbé szerencsésseknél, pedig még sokkal hatékonyabban kell majd felhasználniuk szellemi kapacitásaikat.

Összegezve megállapítható, hogy a rendszerváltozástól eltelt majdnem három évtized alatt a hazai biztonságmenedzsment több irányban is jelentős eredményeket tud felmutatni, határozott fejlődésen ment keresztül, de az összefogó, rendszerező, standardizáló feladatok még előttünk vannak. Kivánatossá vált egy egységes, komplex biztonságmenedzsment rendszer kialakítása, amely a nemzetközi eljárások mentén a hazai viszonyok figyelembevételével képes átfogó, hatékony, jól működő rendszerként üzemelni.
Egy középkori latin szólás szeretnék idézni, amit úgy szólok, hogy: "Extra Hungariam non est vita, si est vita, non est ita." Ami magyarul így szólok: Magyarországon kívül nincs élet, ha van élet, nem ilyen. [67] Ezt én úgy értelmezem, hogy minden általános szabályt valamilyen mértékben az adott hely/ország szokásai szerint módosítani kell, vagyis a helyi sajátosságokat figyelembe kell venni, hogy a szabály megfelelően tudjon megvalósulni.

**Célkitűzés, a komplex vállalati biztonságmenedzsment felvázolása**

Értekezésemben a komplex biztonságmenedzsment egyik értékes, követendő, amerikai megközelítésén keresztül vázlatosan ismertetem, majd az általam elgondolt komplex vállalati biztonságmenedzsment lényegét részletesebben bemutatom, felsorolom a legszükségesebb elemeit, melyek kidolgozásával megvalósítható a megfelelő szintű, korszerű és hatékony vállalati biztonságmenedzsment.

**A komplex biztonságmenedzsment:** (security) nemzetközi, elsősorban angolszász alapú megközelítés, betelepült multinacionális vállalatok által magukkal hozott szigorú biztonsági kultúra és eljárásrend. A magántulajdon védelme megkönnyítette és kialakította saját védelmi rendszerét, ami a XX. század utolsó harmadában indult lendületes fejlődésnek. Jellemzője, hogy átfogó módon áll a biztonsághoz, annak minden elemét igyekszik integrálni a rendszerébe. [68]

### 1.3 A kérdőív és annak kiértékelése

A magyarországi biztonsági menedzsmentet megcélozva egy kérdőíves felmérést végeztem el. A kérdőív felhasználása annak érdekében történt, hogy mielőtt rátérnék a komplex vállalati biztonsági menedzsment kifejtésére, annak megalapozásaként a kérdőívben visszajelzett eredmények feldolgozásával azok kiértékelésével kívánom mintegy szakmailag bevezetni és megalapozni a vállalati komplex biztonságmenedzsment témakörét.

A Magyarországi Biztonsági Vezetők Egyesületének (MBVE) 1998-tól vagyok a tagja.

Az egyesület elsődlegesen a magyarországi pénzügyi és ipari tevékenységű multinacionális társaságok biztonsági vezetőinek és a meghatározó hazai cégek és intézmények biztonsági szakembereinek együttműködési formáit igyekszik kialakítani. A szervezet tagjai cégeiknél magas szintű biztonsági rendszereket igyelkeznek alkalmazni és azonos szakmai elvek szerint dolgozni.

Az egyesület szoros kapcsolatot tart fenn a szaktárcával, véleményezi és ajánlásokkal segíti a jogalkotási és jogalkalmazási munkát. Emellett folyamatosan együttműködik szakmai szervezetekkel, köztületnek és oktatási intézményekkel is.

Az egyesület közvetlen politikai tevékenységet nem folytat, szervezete pártoktól független és azoknak anyagi támogatást nem nyújt.

Kutatáson során azt tartottam a legcélszeletesebbnek, ha az egyesület tagjaihoz fordulok egy kérdéssorral 2014. októberben. Ebben a kérdőívben feltett kérdéseimmel arra kerestem a választ, hogy a vállalati biztonsági vezetők milyen feladatkörrel rendelkeznek, hol helyezkednek el a vállalati hierarchiában, és mennyire átfogó szabályzati rendszer szerint tudják ellátni.

1.3.1 A kérdőív kiértékelése

Tevékenység szerinti megoszlás

<table>
<thead>
<tr>
<th>Tevékenység</th>
<th>Válaszadók száma</th>
<th>Válaszadók aránya</th>
</tr>
</thead>
<tbody>
<tr>
<td>Gyártó cég</td>
<td>13</td>
<td>62%</td>
</tr>
<tr>
<td>Bank</td>
<td>4</td>
<td>19%</td>
</tr>
<tr>
<td>Infrastruktúra</td>
<td>4</td>
<td>19%</td>
</tr>
<tr>
<td>Összesen</td>
<td>21</td>
<td>100%</td>
</tr>
</tbody>
</table>

Az 4. ábrán a válaszadók vállalatainak biztonsági szempontból lényeges tevékenység szerinti megoszlása látható. A válaszadók vállalatainak több mint a fele, 13 vállalat, 62 % valamilyen terméket előállító vállalatok közé sorolható. A válaszadók kevesebb, mint egynegyede, 4 vállalat, 19 %-a bank, míg a megmaradt 4 vállalat, 19 % az infrastruktúra, közlekedés, hírközlés, egészségügyi ellátás területén tevékenykedik. Meglehetős széles körét ölelik fel a gazdasági élet meghatározó szereplőinek.
Az 5. ábrán a válaszadók vállalatainak biztonsági szempontból lényeges, a vállalati hierarchia alapján, alárendeltségi szint szerinti megoszlása látható. A válaszadók vállalataiknál, több mint a felénél 12 fő 57 % a vállalat első számú vezetőjéhez van beosztva, neki jelent, míg a vállalatok kevesebb, mint a felénél 9 fő 43 % nem közvetlenül az első számú vezetőnek, hanem egy második szintű vezetőnek van alárendelve. A válaszadók közül egy sincs harmadik szintű, vagy annál alacsonyabb szintű vezető alá rendelve. Ez mindenképpen pozitívum. A vállalati biztonságmenedzsment hatékonysága és érdekérővé váltja a képessége tekintetében údvizzöltött lenne, ha a biztonsági vezetők minden vállalatnál az első számú vezetőnek tartoznának beszámolással a tevékenység bizalmassága és a legmagasabb szintű hatékonyság elérése szempontjából. Amennyiben a biztonsági vezető nem az első számú vezető alá van közvetlenül rendelve, abban az esetben hatékonysága, minden a közé és az első számú vezető közé beépített szinttel elméletileg a felére redukálódhat. Véleményem szerint azok a biztonsági vezetők, akik egy második szintű vezető alá vannak rendelve, hatékonyságuknak 50 %-át elveszíthetik.
Felelősségi terület szerinti megoszlás

<table>
<thead>
<tr>
<th></th>
<th>Válaszadók száma</th>
<th>Válaszadók aránya</th>
</tr>
</thead>
<tbody>
<tr>
<td>Helyi v. országos</td>
<td>16</td>
<td>76%</td>
</tr>
<tr>
<td>Regionális</td>
<td>5</td>
<td>24%</td>
</tr>
<tr>
<td>Összesen</td>
<td>21</td>
<td>100%</td>
</tr>
</tbody>
</table>

A 6. ábrán a válaszadók felelősségi területük szerinti megoszlása látható. A válaszadók több, mint háromnegyede, 16 fő, 76% felelősségi területe az országhatár keretein belülre korlátozódik, helyi, vagy országos lefedettséggel. A válaszadók majdnem negyede, 5 fő, 24% viszont már regionális, több országra kiterjedő felelősségi területtel rendelkezik a vállalatán belül, ami azt mutatja, hogy a magyar biztonsági szakemberek, vezetők sikereket érnek el nemzetközi szinten is. A multinacionális vállalatok vezetői építenek a magyar biztonsági vezetőkre, képzettségüknek és szakértemüknek értéke van multinacionális gazdasági környezetben is.
A 7. ábra megmutatja, hogy a válaszadók kétharmada, 13 fő, 62% lineáris szervezeti felépítésben tevékenykedik, ami, véleményem szerint követendő, mert egy tiszta, egyenes utasítási rendszer szerint működik, egyértelmű a hierarchikus alá-, és fölérendeltség, ki adhat utasítást kinek, a felelősség minden esetben személyhez köthető. A válaszadók közül 8 fő, 38% végzi feladatait mátrix rendszerű szervezeti felépítésben. Ehhez hozzátenném, hogy a 6. ábrán bemutatott 5 fő már regionális felelősségi körben végzi munkáját, ami a 7. ábra alapján, ha a régiós felelősséggel rendelkező válaszadók számát levonjuk, úgy, hogy a mátrix rendszerű szervezeti felépítésben tevékenykedik, ami 38%. Az első vonal a biztonsági szervezeti felettes feladatokat való közvetlen kapcsolati alárendeltség szerint, a második vonal, általában egy lazább, pontozott vonal a kapcsolati rendszer szerint működik, amiken az alá-, és fölérendeltésen kívül az oldalirányú, mellérendelési munkakapcsolatok is feltűnnek, vagyis azonos szintű vezetőkkel kell együtt tevékenykedni. A kérdőív 7. ábra alapján, ha a régiós felügyelettel rendelkező válaszadók számát levonjuk, így mindösszesen 3 fő, 14 % marad, aki helyi, vagy országos szinten, mátrix struktúrában végzi munkáját. Elismerem, hogy a mátrix rendszerben vannak előnyei, különösen projekt feladatok esetén, de én mégis azon a véleményen vagyok, hogy a lineáris rendszerben való tevékenység hatékonyabb, gyorsabb és tisztább felelősségi és hatáskörökkel rendelkezik.
A regionális biztonsági vezetők esetében a fővonal mindenképpen a biztonsági szervezetben belüli egyértelmű hierarchikus szervezeti felépítés, míg a többi (nem a biztonsági szervezethez tartozó osztályok, pl.: gyártás, HR, IT, létesítménygazdálkodás, stb.) mátrix típusú szervezeti struktúrában tevékenykedőkkel egy lényegesen lazább munka-kapcsolati rendszer működik.

### Szabályzati lefedettség szerint

<table>
<thead>
<tr>
<th>Válaszadók száma</th>
<th>Válaszadók aránya</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Teljeskörű</strong></td>
<td>11</td>
</tr>
<tr>
<td><strong>Nem teljes körü</strong></td>
<td>10</td>
</tr>
<tr>
<td><strong>Összesen</strong></td>
<td>21</td>
</tr>
</tbody>
</table>

Az 8. ábrán már a főkérdés a szabályzati lefedettség kerül bemutatásra a válaszadók visszajelzései alapján. A vállalati biztonságmenedzsment öt fő kérdéskörére, plusz a biztonsági oktatásra kérdezem rá, eszerint a hat tágan értelmező témakör lefedi a teljes vállalati biztonságmenedzsmentet, így egy átlátható képet kapunk a szabályzati lefedettségről. Az összkép várakozásaimat igazolta, mivel a válaszadók fele, 11 fő, 52 % rendelkezik csak teljeskörű biztonsági szabályzattal, míg a válaszadók felénél, 10 fő, 48 % csak részleges szabályzati lefedettséggel találkozunk. Ez az a konkrét pont, amiben alap feltételezésem visszaigazolódik, és amiért úgy gondolom, hogy szükséges és hasznos az a tevékenység(em), amivel egy használható alap biztonsági szabályzat, segédlet került kidolgozásra a vállalati biztonsági vezetők számára ebben az értekezésben.

8. ábra Szabályzati lefedettség szerint (saját szerkesztés)
### Szabályzati hiányosságok megoszlása

<table>
<thead>
<tr>
<th>Témakör</th>
<th>Válaszok száma</th>
<th>Hiányzó szabályok</th>
<th>Meglévő szabályok</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Fizikai biztonság</strong></td>
<td>1</td>
<td>5%</td>
<td>95%</td>
</tr>
<tr>
<td><strong>Információ biztonság</strong></td>
<td>5</td>
<td>24%</td>
<td>76%</td>
</tr>
<tr>
<td><strong>Humán biztonság</strong></td>
<td>6</td>
<td>29%</td>
<td>71%</td>
</tr>
<tr>
<td><strong>Kriszis mgmt.</strong></td>
<td>8</td>
<td>38%</td>
<td>62%</td>
</tr>
<tr>
<td><strong>Vizsgálatok</strong></td>
<td>6</td>
<td>29%</td>
<td>71%</td>
</tr>
<tr>
<td><strong>Biztonsági oktatás</strong></td>
<td>3</td>
<td>14%</td>
<td>86%</td>
</tr>
<tr>
<td><strong>Összesen</strong></td>
<td>21</td>
<td>100%</td>
<td></td>
</tr>
</tbody>
</table>

#### 9. ábra ábra Szabályzati hiányosságok megoszlása (saját szerkesztés)

A 9. ábrán jól látható a szabályzati lefedettségek és hiányosságok megoszlása a főbb témakörök szerint. A legjobb eredmény a fizikai biztonság témakörében született, ami biztató, hiszen ez a biztonságmenedzsment legfajsúlyosabb területe, ebben a témában 95 %-os a lefedettség 20 fő, és csak 5 % a hiányosság, 1 fő visszajelzése alapján. Biztonsági oktatás lefedettsége 18 fő, 86 % alapján rendben lévő, csak 3 fő, 14 % esetében hiányzik. Az információ biztonság 16 fő, 76 % esetében lefedett, azonban hiányzik 5 fő, 24 % tekintetében. A humán biztonság és a vizsgálatok témaköreinek esetében már csak 15 fő, 71 % foglalkozik az említett területekkel és 6 fő, 29 % esetében ezek a területek már hiányoznak. A legrosszabb a helyzet a kriszismenedzsment szabályozottságát illetően, ez a terület a válaszadók csak kb. kétharmadánál van szabályozva, 13 fő, 62 %, és ez a terület 8 fő, 38 % esetében nincs lefedve.
Szabályzati lefedettség átlaga

<table>
<thead>
<tr>
<th>Szabályzati lefedettség átlag</th>
<th>77%</th>
</tr>
</thead>
<tbody>
<tr>
<td>Szabályzati hiányok átlaga</td>
<td>23%</td>
</tr>
</tbody>
</table>

A 10. ábra megmutatja, hogy a válaszadók esetében átlagosan a vállalati biztonság menedzsment 77 %-a van biztonsági szabályzattal lefedve és átlagosan a biztonságmenedzsment 23 %-ka még nincs szabályzattal megfelelően alátámasztva.

1.3.2 Összefoglalás

A kérdőív kérdéseire adott válaszok elemzése után megállapítható, hogy a magyarországi vállalatbiztonsággal foglalkozó biztonsági vezetők több, mint fele 12 fő, 57 % nem az elsőszámú vezetőnek jelent, ezért nem tud a legjobb hatékonysággal működni. Szabályzati lefedettség tekintetében a válaszadók majdnem a fele 10 fő, 48 % nem rendelkezik teljes szabályzati lefedettséggel. Átlagosan a válaszadók 77 %-kos szabályzati lefedettséggel rendelkeznek, a legrosszabb az arány a krízismenedzsment estében, ahol 8 főnél, 38 % sajnálatosan nincs lefedve a téma. Indokolt a vállatbiztonság törzsanyagának létrehozása.
2 A KOMPLEX VÁLLALATI BIZTONSÁGMENEDZSMENT

Értekezésemem elkészítése során az a gondolat vezérelt, hogy munkámmal hozzá tudjak járulni, mintegy követhető elképzelésként, hogy a kívánatossá vált és egységes komplex vállalati biztonságmenedzsment rendszer kialakítathatásra kerülhessen. Remélem, hogy értekezésem megírásával hasznos támogatást, iránymutatást tudok nyújtani a biztonsági szakmán belül a vállalati biztonságmenedzsment szakemberei számára, hogy egyre több vállalatnál, intézménynél bevezetésére kerülhessen a megfelelő szintű, korszerű és hatékony komplex vállalati biztonságmenedzsment.

2.1 Vállalati biztonságmenedzsment

Mivel a hazai szakirodalom nem fedi le teljes egészében a vállalati biztonságmenedzsmentet, ezért szeretném egy amerikai példával vázolni azt a követendő, kívánatos szintet [42], ami elméleti alapul szolgálva, megindíthatná szakembereink gondolatait mind elméleti, mind gyakorlati síkon a komplex biztonságmenedzsment megvalósításának irányába.


Az első fejezetben az általános biztonságmenedzsmenttel foglalkozik. Az általános szervezeti irányelvekkel kezdi művét, hogyan nézzen ki a biztonsági szervezet szervezete, hogyan illeszkedik a vállalati struktúrába, milyen szerepe lehet a biztonsági szervezetnek (óvó, védelmező, oktató, támogató, stb.), mi a szerepe a biztonsági igazgatónak, a menedzsereknek, középvezetőknek, illetve a biztonsági beosztottnak.

A második fejezetben a biztonsági személyzet menedzselésével foglalkozik. Hogyan válasszuk ki a leendő kollégákat, mit tartalmazzon a munkaköri leírásuk, milyen kiképzésben, oktatásokban részesítsük őket, hogyan kommunikáljunk a kollégákkal, milyen morált és fegyelmet tartsunk, hogyan motiváljuk és léptessük elő az alkalmazottainkat, illetve milyen módszerekkel tudjuk motiválni az alvállalkozóinkat.

A harmadik fejezetben az operációs feladatokkal foglalkozik. Hogyan alakítsuk ki a szabályzati rendszert, mi legyen a biztonsági szabályzatban, hogyan tervezzük a következő évet pénzügyi szempontból, költségvetési tervezés, hogyan tervezzünk beruházásokat, milyen kockázatokkal kell
számolnunk, hogyan szervezzük meg saját szervezetünk adminisztrációját, hogyan alakítsuk ki és írjuk le munkafolyamatainkat, hogyan szervezzük meg az információ és adatvédelmet, hogyan használjuk a statisztikai eredményeinket céljaink elérése érdekében.

A negyedik fejezetben a biztonsági szervezetek kívüli kapcsolatokkal foglalkozik. Hogyan adjuk el a biztonságot szervezetünkön kívül, milyen kapcsolatot célszerű kialakítani a hatóságokkal és más szervekkel, intézményekkel?

Az ötödik fejezetben azokat a hibákat írja le, amelyeket nem szabad elkövetni a biztonság menedzselése során, illetve, ha mégis megtörtént, akkor hogyan lehetséges a károk minimalizálása.

Sennewald alapján kijelenthetjük, hogy szükséges lenne egy hasonló, szinte tankönyvszerű elméleti alapra a magyar nyelvű szakirodalomnak is, amelyet a biztonsági vezetők közvetlenül a gyakorlatban tudnának alkalmazni. Mindamellett, hogy ezzel nagymértékben meg lehetne könnyíteni a munkájukat, nagyon hasznos eszközként szolgálhatna egy ilyen közös elméleti alap ahhoz, hogy standardizált, egységes biztonságméleti és gyakorlati tudás alakulhasson ki.

2.2 Elgondolásom: Komplex vállalatbiztonsági szabályzat tervezet

A komplex biztonságmenedzsmenten belül a szabályzatnak meghatározó szerepe van, itt található meg mindazon szabályok összefoglalása, amelyek alapján a biztonsági tevékenység végezhető. Kezdésként meg kell határozni azt, hogy mi a szabályzat célja, majd a szabályzat hatályának és a felelősségek megfogalmazásának kell következnie [73]. Rögzíteni kell, hogy kikre és milyen szervezetekre terjed ki a szabályzat, és ki a felelős a szabályzat elkészítéséért és karbantartásáért.

A felelősségek meghatározásánál kiemelt fontossága annak a lefektetése, hogy mi a vezetőség feladata a szabályzat bevezetésével és a betartatásával kapcsolatban, valamint meg kell határozni a biztonsági szervezet és a biztonsági szolgálat feladatát is, annak érdekében, hogy a feladatok és felelősségi körök pontosan definiáltak és szeparáltak legyenek. Törekedni kell arra, hogy ne alakulhasson ki olyan tisztázatlan helyzet, amikor senki sem felelős egy feladat végrehajtásáért, illetve többen is felelősök ugyanazért, ezért a feladatnak valódi felelőse nincsen.

A szabályzat fő részének ki kell térni a fizikai biztonság követelményeinek a meghatározására. A kockázatelemzéssel célszerű kezdeni, amiben le kell írni az általános sajátosságait, és magát a kockázatelemzési folyamatot. Meg kell határozni, hogy mennyire fontos az a telephely, amelyet éppen vizsgálunk a vállalat, vállalkozás szempontjából. Majd sorra kell venni a kockázati kategóriákat, terrorizmus, katasztrófa kitettség, munkahelyi erőszak és bűnügyi fertőzöttség.
tekintetében. A következő terület a külső biztonsági kontrollok meghatározása, mint a vállalat tulajdonhatárának jelzése, a telekhatár kivilágítása, a gépjármű parkolók, tárolók biztonsági követelményeinek a leírása, a tulajdonhatárok szükséges védelmi eljárások, fizikai akadályok, egyéb, nem egyértelmű bejutási pontok, illetve a rejtőzködésre alkalmas helyek és a kritikus közművek biztonsági követelményeinek a megfogalmazása.[43] A fizikai biztonságon belül az épületek határainak és az épületeken belüli biztonságnak kell következnie. Itt kell kitérni az ablakok, üvegfalak, ajtók biztonságának követelményeire. Meg kell határozni a vállalat belső tereinek, korlátozott hozzáférésű területeinek, illetve más cégekkel közös helyiségeinek a biztonsági követelményeit. Ki kell térni a nyilvános területekre, rakodóterekre, és a bérlokk által használt területekre is. Ide tartozhatnak még az egészségügyi létesítmények, bankfiókok, vagy pénzkiadó automaták és a felvonók is. A postaszolgálat, a postabontó fizikai biztonságának meg- határozása is elengedhetetlenül fontos. Az ajtózárakra, kulcsokra és a kulcsahasználatra vonatkozó szabályokat is létre kell hozni. A következő terület a vállalatnál alkalmazott beléptetési ellenőrzés és az azonosító kértékkal kapcsolatos beléptetési ellenőrzés és az azonosító kértékkal kapcsolatos felállítása. Meg kell határozni a beléptető rendszer eljárásait, folyamatait, a területi vezetők engedélyezési kötelezeteit, a rendszer kezelőjének jogosultságait és engedélyeit. Fel kell állítani a belépőkértékkal rendszerét, a kértékk formai követelményeit, mint az állandó, vagyis fényképes, mint az ideiglenes kértékk tekintetében is. K i kell dolgozni a jogosultság kérelem és engedélyezés auditálható és zökkenőmentes eljárásait. A biztonságtéchnikával kapcsolatosan létre kell hozni egy standard rendszert, amely meghatározza azt a technikai követelményszintet, amit a biztonsági központok, a kamera-, riasztó-, és beléptető rendszerekhez vonul ki. Ezáltal tudjuk biztosítani az egészséges biztonságtéchnikai háttért. Létre kell hozni a személy-, és gépjármű átvizsgálás szabályozott rendjét. A humánbiztonság területén meg kell határozni az összeférhetetlenségi szabályokat, majd meg kell valósítani a teljes folyamatot, a kitöltendő formanyomtatványoktól a vizsgálatok lezárásáig. A szabályzatban szükséges kitérni a válsághelyzetek kezelésére. Meg kell határozni a vészszakasz és válságkezelési program követelményeit, meg kell fogalmazni a válságkezelési vezetőség feladatait, a tervek és gyakorlatok kapcsán. Elő kell írni az oktatási, gyakorlati követelményeket, mind tartalom, mind időintervallum tekintetében. Szabályozni kell a vizsgálatokkal kapcsolatos tevékenységet, mit és hogyan lehet tenni, mikor kell hatósághoz fordulni, milyen legyen a hatósági kapcsolattartás szintje és mélysége? Mi minősül biztonsági eseménynek, annak milyen jelentési kötelezettsége van, mit kell azonnal és hogyan, milyen úton jelenteni? A következő fontos terület az információbiztonság, meg kell határozni itt is a felelősségeket, úgyminthegy a feladata a vezetőknek és a beosztottaknak, hogyan kezeljük a bizalmas hulladékot, hogyan óvjuk a bizalmas adatokat, és mi az eljárás munkahelyen kívül tartott megbeszéléseken? Utazásbiztonsági
szabályok megalkotásával segíthetjük és kontrollálhatjuk a munkatársak utazásait. Nagymértékben segíti a biztonsági folyamatok betartását, ha folyamatos képzésekkel oktatásokkal tartjuk frissen a biztonsági tudatosságot a kollégáink és a biztonsági szervezeten kívül tevékenykedő munkatársak esetében is.

2.3 Összefoglaló

Összegezve megállapítható, hogy a hazai biztonságmenedzsment előzmények, alapok nélkül, több irányban is jelentős eredményeket tud felmutatni a magánszférában, határozott fejlődésen ment keresztül, de az összefogó, rendszerező, standardizáló feladatok még előttünk vannak. Ehhez nyújt iránymutatást ez a értekezés, melynek célját egy külföldi példán keresztül a saját elgondoláson felvázolva, mintegy követhető elképzelésként, annak érdekében, hogy a kívánatossá vált és egységes, komplex vállalati biztonságmenedzsment rendszer kialakításra kerülhessen. Remélem, hogy értekezésem megírásával hozzá tudok járulni ahhoz, hogy a biztonsági szakmán belül kialakulhasson a hazai kompleks biztonságmenedzsment szemlélet és ehhez egy követhető irányvonalat sikerült felvázolnom. A jövőbeli célom alapvetően erre az értekezésre támaszkodva, ehhez kapcsolódva a komplex vállalati biztonságmenedzsment további területeinek a lefedéséhez szükséges eljárások felvázolása, pl.: a biztonsági folyamatok dokumentálása, a folyamatleírások, folyamatábrák és végrehajtási utasítások mintaszerű kialakításával, a biztonsági szolgáltatók egyszerű és hatékony minőségi ellenőrző rendszerének bemutatásával. A rendszer nem zárt, ahhoz mindig hozzá lehet építeni további szükséges modulokat, illetve ki lehet hagyni az adott vállalat tevékenységének és biztonsági szükségeleteinek megfelelően [92].
3 Biztonsági irányítási rendszer és ellenőrzés

A biztonsági irányítási rendszer általános leírásával, a rendszer elemeivel, működésével, a belső folyamatokkal és az önellenőrzéssel szeretnék foglalkozni a továbbiakban. Egy lehetséges modell felvázolásával mutatnám be, hogy milyen rendszer kialakításával tudjuk elérni, hogy a biztonsági szervezet szakszerűen, folyamatosan megújulva és ellenőrzés alatt működjön.

Egy biztonsági szervezet működtetése nem egyszerű feladat, ezért fontos, hogy kialakítsuk saját irányítási, vezetési rendszerünket, hogy erre tudjunk kézbe venni és viszonylag automatikussá tenni a működését, amelyre csak a rendszer által kidobott javítandó részekkel kelljük foglalkoznunk. A lényeg szerintem a következő, hogy egy objektív, mérhető, ellenőrző pontokkal és visszacsatoló funkcióval rendelkező szisztéma működjön, és ne kelljen mindig kézi irányításra kapcsolva, feltalálni mindennap a „spanyolviaszt”.


3.1 A rendszer elemei:

- **szabályzatok**: egységes szabályzati rendszert szükséges kialakítani, amelyben minimálisan elválík a helyi és a vállalati (régiós, vagy globális) szint. A vállalati szinten kell meghatározni azokat a kereteket, irányelveket, amelyek alapján létre kell hozni a helyi szabályzatokat.

- **belső folyamatok**: a biztonsági tevékenységet folyamatosítani kell! Be kell azonosítani a folyamatokat, majd kategorizálni minden munkafolyamatot és kialakítani a teljes folyamatszemléletet. Amikor felveszünk egy folyamatot, akkor el kell készíteni az egységes rendszer szerinti **folyamatleírást**, ahol összefoglaljuk a folyamat összes lényeges elemét, mint a folyamat neve, azonosítója, kiadója, kiadás dátuma, a folyamat rövid leírása, a bejövő és kimenő adatokat, illetve a folyamatba betöltött és a folyamat eredményét használó szervezeteket. Itt kell szerepeltetni a mérési pontokat, amelyek segítségével tudjuk mérni, meghatározni a folyamat működését. a folyamatleírás mellé szükséges elkészíteni a **folyamatábrát**, mellyen grafikusan is jól
látható az egész folyamat. A munkafolyamat megértésének és elvégzésének megkönnyítése és egyértelművé tétele érdekében ajánlott egy részletes végrehajtási utasítás elkészítése, ami pontról pontra felsorolja a munkafolyamat során a szükséges teendőket.

- **munkaköri leírások**: célszerű, ha elkészítjük minden munkatársunk részletes munkaköri leírását, ami jóval bővebb, mint egy HR-es munkaköri leírás, hisz ez nem csak vázlatosan tartalmazza a munkafeladatokat, hanem teljes részletességgel igyekszik lefedni azt, minden egyes munkafolyamatával egyetemben.

- **teljesítmény kontroll**: célokat kell kitűzni a biztonsági szervezet szintjén, majd ezen belül meg kell határozni a biztonsági szervezet kisebb egységeinek a céljait is és ezeket le kell bontani az egyén szintjére is. Mindenkinek rendelkeznie kell éves egyéni célokkal, amelyek illeszkednek a biztonsági szervezet egészének a célkitűzéseibe. Ezen teljesítményeket legalább negyedévente, objektív módon szükséges mérni és értékelni.

A rendszert úgy lehet elképzelni, mint egy piramis (8. ábra) négy oldalát, egyik oldal a szabályzati oldal, a következő a folyamat oldal, majd a munkaköri leírások oldala és végül a teljesítmény kontroll oldala következik. A piramis talapzatán, az alsó szinten az egyéni és a lokális folyamatok/szabályzatok helyezkednek el, míg ahogy főjebb haladunk a piramison, úgy haladunk főjebb a hierarchiában is.

![Diagram](https://example.com/diagram.png)

11. ábra A biztonságirányítási rendszer hierarchiája (saját szerkesztés)
3.2 A rendszer működése:

Három szinten tudjuk ábrázolni a rendszert a működés szempontjából (12. ábra), a biztonsági vezetés a főfolyamatokra tud közvetlenül támaszkodni, de a támogató folyamatokkal (melyeket képletesen A, B, C, D betűkkel jelöltem) együtt lesz képes a rendszer működni.

Még szemléletesebben lehet ábrázolni a rendszert (13. ábra), ha folyamszemlélet irányából vizsgáljuk, mert ebben az esetben a főfolyamatok és a támogató folyamatok szintje mellett harmadikként megjelennek a rendszerfolyamatok is. A rendszerfolyamatok, mint a dokumentumok kezelése, az intézkedések és a reklamációk kezelésével együtt válik valódi egésszé, hisz ezek a rendszerfolyamatok biztosítják számunkra az egész rendszer működését, nélkülük a munkafolyamatok nem lennének egységesen összekapcsolva.
3.3 A biztonsági irányítási rendszer kulcsfontosságú területei:

- biztonsági szabályzatok egységesítése a legmagasabb (globális, regionális, országos) szinten,
- biztonsági folyamatok pontos definiálása,
- egységes folyamatok alapján pontos egyéni feladat meghatározás,
- feladatok teljesítésének rendszeres ellenőrzése-értékelése,
- oktatási program – biztonsági tudatosság fejlesztés,
- folyamatos ellenőrzés-értékelés,
- tervszerű felülvizsgálat,
- folyamatos fejlesztés.

A kulcsfontosságú területek közül a legtöbbet érintettem, illetve nem szorulnak további magyarázatra, de a tervszerű felülvizsgálatot szeretném kiemelni. A tervszerű felülvizsgálat szorosan kapcsolódik az egyéni és csoportos célok teljesítésének ellenőrzéséhez és a szabályzatokhoz való megfelelősség, valamint a folyamatok időszakos felülvizsgálatához is. Az elnevezés a biztonsági szervezet önellenőrzését, belső auditját jelenti. Célszerű kialakítani a munkatársak közül egy bizottságot, aminek lehetnek állandó tagjai is, pl. a folyamatgazda, vagy olyan vezető, aki több terület felett gyakorolja menedzseri feladatait, illetve lehetnek ad hoc tagjai is, akiket más területekről irányíthatunk az épp aktuális felülvizsgálatra. Rendkívül hasznos lehet ez a fajta felülvizsgálati folyamat, hisz meggyőződhetünk egy adott terület tevékenységéről és mindemellett egyfajta továbbképzési lehetőség a kollégáknak is, hiszen több helyszínt megismernek, az ott tapasztaltakkat tudják majd saját területükön kamatoztatni, illetve a szabályzatainkba és eljárásainkban is nagyobb magabiztosságot szerezhetnek, mert tudni kell, hogy mi alapján ellenőriz bármit is, biztosnak kell lenniük a szabályzati hátterüket illetően.

3.4 Összefoglaló

Összefoglalva, megállapíthatjuk, hogy egy biztonsági irányítási rendszer segítségével biztosíthatjuk a biztonsági szervezet hatékony és szakszerű működését. Támaszkodni lehet a világosan megfogalmazott szabályzati rendszerre, a feladatok, az elvárások egyértelmű meghatározására, és a tevékenység visszaellenőrzését biztosító önellenőrzési rendszerre. Így a folyamatos korrekt munkavégzés működtetése párosul a munkafolyamatok állandó ellenőrzésével és ezáltal azok folyamatos tökéletesítésével. Mindezek által a biztonsági szervezet állandó képességévé válik a folyamatos megújulás és a teljesítményjavulás [93].
3.5 A biztonsági szervezet pénzügyi kontroll modellje

A biztonsági szervezet feladatainak egy olyan területét szeretném bemutatni, amelyik nincs annyira a fókuszban, leginkább a háttérben fejti ki elengedhetetlenül fontos tevékenységét. Ez a folyamat a biztonsági szervezet pénzügyi kontroll modellje. Minél nagyobb egy vállalat, vagy cégcsoport annál inkább szertéga gazzóbó a tevékenysége, szervezeti felépítése, és ebből következve a költséggazdálkodása és beruházásai is. A biztonsági szervezet feladata, hogy biztosítsa azt, hogy uniformizált és standardok szerinti biztonsági rendszer működjön mindenhol, a követelményrendszeről ne lehessen eltérni. Ezt a célt elérhetjük a szabályzati rendszer kialakításával, vagyis szabályzati úton minden biztonsági kölést, költséget hozzárendelünk a biztonsági szervezethez. Nem meglepő módon, általában ez még nem elegendő, hiszen bizonyára szemtanúi lehetünk már olyan helyzeteknek, amikor a szabályzatot nem tartották be megfelelőképpen. Tehát érvényt kell szereznünk a szabályzat betartásának, illetve ellenőriznünk kell, hogy az valóban úgy történik-e ahogy az meg van határozva [100].

A modell lényege

A biztonsági szervezet a ténylegesen felmerült biztonsági jellegű költségek nyomon követése és optimalizálása érdekében, a szakmai és technikai felelősség mellett az ehhez tartozó elszámolási felelősséget is kézben kell, hogy tartsa [70] [71]. A pénzügyi kontrollal szembeni elvárás a biztonsági (vagyovvédelmi) költségekkel való hatékony gazdálkodás, valamint, hogy bármikor követhető legyen mekkora összeget fordít a cég ténylegesen a biztonságra. [20]

A modell működés kialakításáért, szabályszerű működtetéséért és kiterjesztéséért a biztonsági szervezet vezetője felel, aki az egyes funkcionális feladatköröket szervezeten belül szakértői felé delegálja (pénzügyi tervezési biztonsági szakértő, mint feladatgazda, költségbiztonsági szakértő, beszerzési biztonsági szakértő, stb.). A beosztott biztonsági vezetők hatáskörükben teljes körűen támogatják a modell megvalósítását. A cég, vagy cégcsoporton belüli kiterjesztés tárgyi és időbeli hatályáról a biztonsági szervezet vezetője dönt.

A modellműködtetés alapelemei

A biztonsági eszközöket speciális kóddal szükséges megjelölni és az eszköznyilvántartásban elkülönítésre kell, hogy kerüljenek. A termelési, logisztikai, kereskedelmi, stb. szakterületek biztonsági eszközeinek tulajdonosa, költségviselője, üzembe helyezője, felelős megőrzője továbbra is az illetékes más szervezeti egység, további esetekben pedig a biztonsági szervezet.
A biztonsági anyagcsoport kóddal megkülönböztetett biztonsági szolgáltatások adatainak könyvelése egyúttal statisztikai rendelés számra is történik, a funkcionális elkülönítés, lekérdezhetőség és kontroll miatt. A felelős költséghelyenek a biztonsági szervezetnek kell lennie.

Költségviselő költséghelytől függenlenül, a biztonsági szervezet kizárólagos feladata és felelőssége a biztonsági eszközökkel, szolgáltatásokkal kapcsolatos mindennemű:

- szakmai, pénzügyi elszámolási és elszámoltatási, irányítási, illetve operációs tevékenység (működtetés, karbantartás), szakmai döntés, fejlesztés (biztonsági projekt, illetve üzleti projekt biztonsági része), kontroll, beruházási és operációs jellegű költség, stratégiai és más szervezeti egység költséghelyi tervezése, nyilvántartása és az integrált pénzügyi erőforrás felhasználás folyamatos értékelése
- közreműködés a beszerzési folyamatban, szerződéskezelés, igények bevitele a pénzügyi rendszerekbe, jóváhagyása, teljesítésigazolása, kapcsolattartás a beszállítókkel, beszállítói tevékenység felügyelete
- kapcsolattartás a tervezési, kontrolling és pénzügyi társszakterületekkel.

A modell működtetés szabályozásának lényegi elemei, a modell működtetés kialakítása

A modellműködtetés kialakítása megvalósítási ütemterv alapján történik, melynek célja a biztonsági jellegű tervezési, elszámolási, beszerzési folyamatok, feladatok, eszközgazdálkodási felelősségkörök, a modellműködtetés szerepeinek szabályozása.

A biztonsági szervezet instrukciói alapján a biztonsági eszközállomány felülvizsgálatra kerül, megtörténik a statisztikai rendelésszám struktúra és a tervezési, igénylési, beszerzési folyamatok kialakítása. A biztonsági szolgáltatások és karbantartások kezelésének és az adathozzáférés kizárólagosságának biztosítása a pénzügyi elszámolási rendszerekben. A biztonsági vezető illetékessége eljárni a szabályozásban és a döntéshozatali rendszerekben történő szükséges változtatások, módosítások érdekében. A szabályozásban meghatározó jelleggel a biztonság szervezet bír, természetesen, folyamatos együttműködésben és párbeszédet biztosítva az érintett más szervezeti egységekkel.
A modell működtetés folyamatosságának biztosítása

A biztonsági szervezet dönt az adott időszak integrált szakmai és pénzügyi biztonsági tervéről, folyamatosan nyomon követi és elemzi az integrált biztonsági jellegű beruházási és operációs költség felhasználás alakulását, menedzseli a biztonsági szerződésállományt, felméri más szervezeti egységek biztonsági igényeit, javaslatot tesz a biztonsági folyamatok fejlesztésére.

Adatszolgáltatások, egyeztetések, kommunikáció

A hatékony modellműködtetés és döntés előkészítés elengedhetetlen feltétele a folyamatos tájékoztatás, a jelentési, egyeztetési és adatszolgáltatási előírások, egyeztetések biztosítása, a működőképes kommunikáció. Meg kell határozni:

- az adatszolgáltatók körét,
- az adatszolgáltatás rendszerességét, illetve határidejét,
- az adatszolgáltatás formáját, stb.

Jelentések

Az integrált költségrőportok a felső vezetés, a biztonsági főigazgató, a beosztott biztonsági vezetők és igény szerint más szervezeti egységek felé a biztonsági költségek alakulásának bemutatását, amelyek döntés előkészítő javaslatok megvalósítását szolgálhatják.

Kontroll

A kontroll célja a valóságos modell működés ellenőrzése az optimális biztonsági eszköz és költséghatékonyság biztosítása érdekében.

A felügyeleti kontroll a következőket vizsgálja:

- a modell alapelemek érvényesítését az integrált működésben: operáció, erőforrás, kapacitás, szerződések, beszámolás, költség, (terv, tény, várható),
- a biztonsági eszköz, szolgáltatás nyilvántartás, elszámolás elvi és gyakorlati szabályairól, folyamatos érvényesítését,
- a tervezett biztonsági költségek betartása, az esetleges eltérések okainak és kockázati tényezők feltárása.
A modell továbbfejlesztése és kiterjesztése

A modell fejlesztése a szabályszerűség és költséghatékonyság szellemében, a kontrollálhatóság fokozása érdekében történhet. Az integrált adatszolgáltatás megbízhatósága miatt az igénylési, jóváhagyási, teljesítésgazolási, berögzítési, stb. feladatok biztonsági munkakörhöz rendelését, a folyamat zártságát biztosíthatja kell. A modell kiterjesztését leányvállalatokra (ha vannak) az érintett cégek működési struktúrájának, a helyi sajátosságainak és jogi szabályozásának, számítógépes vállalatirányítási és elszámolási rendszerének figyelembevételével kell elvégezni. A bevont leányvállalatok csatlakozási szerződéseket kapcsolódnak az anyavállalati szolgáltatási szerződéseikhez, projekteikhez.

3.6 Összefoglaló

Az eredeti szándék szerint bemutatásra került a biztonsági szervezet feladatainak egy olyan területe, amely a háttérben tevékenykedik és nem is tartozik a hagyományos biztonsági szakterületek közé. Elmondotjuk, hogy a biztonsági szervezet pénzügyi kontroll modellje hatékonyan képes biztosítani a folyamatos költségfigyelést, ezáltal a mindenki költségtérvekhöz is pontos adatokat szolgáltatni, valamint a legfontosabb funkcióját biztosítani, a biztonsági költségek felett kizárólagosan biztosítható a biztonsági szervezet örködését. Ezáltal biztosítható a biztonsági szolgáltatás nem kerülhet beszerzésre, illetve semmilyen biztonsági szolgáltatás nem kerülhet beszerzésre. Ezáltal biztosítható a biztonsági szolgáltatás beszerzésére, és mint tudjuk: „A jó gazda szeme hizlalja a jószágot!”.
4  A vállalatbiztonsági szabályzat kialakítása

Szükségessé vált egy vállalatbiztonsági iránumutató szabályzat kialakítása, erre szeretnénk egy használható példát bemutatni. Természetesen mindenkor a hatályos helyi, országos és európai uniós törvények, szabályzatok, pl.: GDPR (General Data Protection Regulation/általános adatvédelmi szabályok) követelmények teljes betartása mellett.

Főbb témakörei: hatály és felelősség meghatározása, kockázatelemzés, fizikai biztonság, biztonsági események kezelése, belső vizsgálatok, információbiztonság, krízismenedzsment, humánbiztonság, biztonsági szervezet pénzügyi kontroll modellje, speciális biztonsági feladatok.

A szabályzat célja

A biztonsági szabályzat meghatározza egy nemzetközi vállalat biztonsági folyamatait és követelményeit. [35]

Hatály és felelősség meghatározása

A biztonság mindenki kötelessége és feladata. A vállalati tulajdon védelme alapvető kötelezettsége minden vezetőnek és munkavállalónak.

A szabályzat hatálya

A szabályzat hatálya kiterjed a vállalat összes tagvállalatára. Azon tagvállalatok esetén, ahol nincs helyi biztonsági vezető, vagy biztonsági szervezet, ott a Biztonsági Alapszabályoknak kell megfelelni.

A szabályzat bevezetésének és használatának minden tagvállalatnál és minden országban, összhangban kell lennie a helyi jogszabályokkal. A szabályzattal kapcsolatos bármilyen nem megfelelősség esetén, legyen az jogi, vagy egyéb más okból, minden helyi biztonsági vezetőnek kockázat elfogadási nyilatkozatot kell előterjeszteni a biztonsági főigazgatóhoz.

Biztonsági alapszabályok

A látogatók, a külső vállalkozók, a beszállítók, a bérlők, a terület tulajdonosai, a munkavállalók által elvégzett minden tevékenységet a vonatkozó biztonsági szabályok betartásával kell végrehajtani. A helyi vezérligazgató / ügyvezető igazgató felelős a biztonsági alapszabályok teljes körű bevezetéséért és alkalmazásáért.
Épületek és irodák fizikai biztonsága

A bejáratokat biztonsági zárral kell ellátni. Az épületekben, irodaházakban távvezérlő riasztórendszer (pl.: mozgásérzékelés, tűzjelző) kell létrehozni. Földszintes irodák esetén kötelező az ablaküvegre biztonsági rácsokat, vagy fóliát helyezni a betöréseket megakadályozására.

Beléptetési szabályok

A vállalat telephelyein, létesítményeiben csak jogosult személyek léphetnek be. Az alkalmazottak, beszállítók, alvállalkozók és látogatók esetében is szabályozni kell. A vállalat munkavállalóinak belépését belépőkártyával és kulcsokkal lehet szabályozni. A külső partnerek belépését az alvállalkozók, illetve a látogatók beléptetését meghatározó szabályok szerint kell alkalmazni és adataikat regisztrálni.

A látogatók nem tartózkodhatnak vállalati személy kísérete (felügyelete) nélkül a vállalat telephelyein.

Kulcsokra vonatkozó szabályok

A vállalat minden alkalmazottja, szükség esetén rendelkezhet számára kiadott irodakulccsal. Ennek a kulcsnak a kezelése az irodai felhasználók felelőssége. Ha a munkaviszonya megszűnik, az alkalmazottaknak el kell számlonniuk a kulcsaikkal. Tilos a kulcsok másolása és harmadik fél részére történő átadás. (Mesterkulcs-rendszer alkalmazásánál a másolás lehetetlen.)

A szervezet vezetőjének (a vezérigazgató / ügyvezető igazgató), vagy az általa kijelölt személynek nyilvántartást (kulcs leltárt) kell vezetnie a kulcsokról (kinek, milyen számú kulcsot adott ki, stb.).

Tennivaló, kulcs elvésztése esetén

Ha egy kulcs elveszik, azt haladéktalanul jelenteni kell a szervezet vezetőjének. A szervezet vezetője intézkedéseket tesz a zárak megváltoztatására.

Tisza asztal irányelv (Clean desk policy)

Ennek a folyamatnak az a célja, hogy meghatározza a vállalat titkos vagy bizalmas információinak védel

Irányelv

1. A számítógépes munkaállomásokat zárolni kell, ha a munkavállaló nem tartózkodik ott.
2. A számítógépes munkaállomásokat a munkanap végén teljesen le kell állítani.
3. Munkaidő végén minden vállalati bizalmas információt el kell távolítani az asztalról, és zárható helyre elzární, íróasztalfiók, stb.
4. A vállalati bizalmas információkat tartalmazó iratszereknyeket zárt helyen kell tartani és zárt állapotban kell tartani, ha éppen nem használják.
5. A vállalati bizalmas információkhoz való hozzáféréshez használt kulcsokat nem szabad a felügyelet nélküli hagyni.
6. A fiókos íróasztal, munkaasztal, szekrény-széfek, széfek és szekrények kulcsait nem szabad a zárákban hagyni.
7. A laptopokat vagy Kensington vagy azzal egyenértékű biztonsági kábellel kell zárt fiókban kell tárolni.
8. A jelszavakat tilos a munkaállomáson tárolni, azok leírt, vagy kinyomtatott formában csak biztonságosan elzárva tárolhatóak, ahol más személy nem férhet hozzá.
9. A vállalati bizalmas információkat tartalmazó iratokat azonnal el kell távolítani a nyomtatóból.
10. A vállalati bizalmas dokumentumok megsemmisítésére egy iratmegsemmisítő darálót kell használni.

Összefoglaló

- A vállalati bizalmas dokumentumokat és számítógépes adathordozókat zárt fiókokban vagy iratszereknyekben kell tárolni.
- A laptopokat biztonsági kábel használatalval kell rögzíteni és védeni.
- A munkahely elhagyása előtt minden dolgozó köteles a munkaállomását (számítógépet) kikapcsolni és elzárnő a dokumentumait.

Bizalmas dokumentumok nem maradhatnak nyilvános, vagy nyitott helyen felügyelet/őrizet nélkül. Ha bizalmas dokumentumok mások által is hozzáférhető nyomtatóra letteek kinyomtatva, akkor ezeket a dokumentumokat haladéktalanul ki kell venni a nyomtatóból.

Az alábbi elemek példák arra, hogy mi nem maradhat felügyelet nélkül: jelszó, a vállalat bizalmas dokumentumai, IP címek, szerződések vagy szerződéstervizek, számlaszámk, szellemi tulajdon, munkavállalói nyilvántartások személyes adatokkal, társadalombiztosítási számk, egészségügyi adatok, pénzügyi adatok.

Fegyelmi intézkedések

E szabály megsértése felelősségre vonást és jogi lépéseket vonhat maga után, polgári, valamint egyes esetekben büntetőeljárás lefolytatását.
A vállalati tulajdon, értékek, eszközéinek kivitelére vonatkozó szabályok

A vállalat tulajdonában lévő eszközök csak a megfelelő engedély megszerzésével vihetőek ki a vállalat területéről. Az engedélyek nem vonatkoznak a saját tulajdonú eszközök (pl. Notebook, mobiltelefon, PDA) kivitelére, ezen eszközök behozatalát és használatát szükséges engedélyeztetni. Az engedélyeket a szervezetek vezetője adja ki.

Biztonsági események jelentése

A biztonsággal kapcsolatos összes incidensről jelentést kell tenni a vállalat biztonsági szervezetének, valamint meg kell tenni a szükséges intézkedéseket.

Bejelentendő események

Az alábbi incidenseket kell jelenteni a vállalat biztonsági szervezetének, vezetőjének: személyek fizikai sérülését, a vállalat eszközeinek 100.000,- HUF (példa szerinti összeghatár, kiskereskedelmi érték) mértékű veszteségét, a megmagyarázhatatlan leltárhiányokat, mindennemű fenyegetést, vállalati bizalmnasnak minősített adatok elveszítését, minden visszaélést a vállalat információtechnológiai rendszerei ellen, információtechnológiai rendszerekhez való jogosulatlan hozzáférése, illetve azok megszavarása, megsemmisítése esetén, a vállalat területén történt jogsértéseket, biztonsági incidensek, jogsértések vagy üzleti magatartás megsértését, amely a vállalat dolgozójának elbocsátását vagy büntetőeljárást vonhat maga után, olyan eseményeket, amelyek a médiában megjelenhetnek.

Azonnali jelentéstétel

A következő típusú eseményeket azonnal jelenteni kell a vállalat biztonsági szervezetének: súlyos természetű személyes fenyegetéseket, természeti katasztrófákat, robbantással, robbanóanyaggal, bombával kapcsolatos eseményeket, fenyegetéseket, emberölést, fegyveres támadásokat, tűzhelyzetet, szabotázst, nem ember által okozott robbanások és jelentős kémiai szennyeződésekkel járó incidenseket, súlyos adatvesztés, beleértve a kémkedés, a lehallgatás és a titkosított információk megszerzésének egyéb illegális eszközét, sikeres információtechnológiai rendszerbe történő behatolást, hackelést vagy zavarokat, jelentős lopásokat, rablásokat, olyan eseményeket, amelyek nemzetközi médiavisszhangot is kiválthatnak.

Minden biztonsági eseményt haladéktalanul jelenteni kell a vállalat biztonsági szervezetének telefonon és amint lehetséges elektronikus levél formájában is. Az incidensről szóló jelentést legalább az eseményt követő következő munkanapon el kell küldeni a biztonsági szervezetnek.
A közvetlenül jelenteni kívánt eseményeket (a fentiek szerint) haladéktalanul jelenteni kell a vállalat Biztonsági Központjának. (telefonon 7/24 biztonsági ügyelet, stb.).

A biztonsági szervezet pénzügyi kontroll modellje

A vállalat biztonsági szervezetét minden esetben be kell vonni a műszaki és pénzügyi tervezésbe a biztonsági berendezések, beruházások és szolgáltatások biztonsága és védelme érdekében. Professzionális támogatást nyújtanak a megfelelő minőségű szolgáltatások és eszközök kiválasztásához.

Utazásbiztonság

A helyi vezérigazgató / ügyvezető igazgató kötelessége betartani és betartatni az utazásbiztonság szabályait. A „piros” minősítésű országokban tervezett összes üzleti utazást jelenteni kell, és a biztonsági főigazgatónak előzetesen jóvá kell hagynia.

A vállalatbiztonsági szabályzat kialakítása, felelősségek

A helyi biztonsági vezetők felelősek a szabályzat bevezetéséért.

Hozzáférési korlátozások

A szabályzatnak a vállalaton belül korlátlanul hozzáférhetőnek kell lennie. A szabályzat külső felhasználása nem engedélyezett. Ettől eltérni, kizárólag a biztonsági főigazgató előzetes írásbeli engedélye alapján lehetséges.

Felülvizsgálati folyamat

A biztonsági szervezetnek létre kell hoznia egy ellenőrző folyamatot, a szabályzatban megfogalmazott követelmények ellenőrzésére. A követelményekkel kapcsolatban felmerülő kérdések megválaszolása, tisztázása a biztonsági szervezet hatáskörébe tartozik. A biztonsági szervezet folyamatosan auditálja a szabályzatnak való megfelelést.

4.1 Kockázatelemzés

A kockázatelemzés a kezdőpontja a vállalatbiztonság megszervezésének. A kockázatelemzéssel tudjuk meghatározni a vállalat létesítményeinek fenyegetettségi szintjét, kockázati tényezőit. Ez alapján mérhetjük, majd rendelhetjük hozzá a kockázatokhoz a megfelelő védelmi szintet. Így alakíthatja ki a biztonsági szervezet kockázati megközelítéssel a megfelelő védelmi strukturát, ami optimális esetben sem nem több, sem nem kevesebb mint, ami indokolt a kockázati tényezők alapján [95].
4.1.1 Általános szabályok, vezetők felelőssége

A vállalat vagyonának, fizikai-, humán-, és intellektuális értékeinek a védelme a vezetőség feladata. Ezen értékek közé tartoznak a vállalat vezetői, munkavállalói, technológiai, tárgyi eszközök, valamint az üzletmenettel kapcsolatos adatok, eljárások. A biztonsági szervezet vezetői és szakértői folyamatosan támogatják a vállalat vezetőségét ebben a tekintetben.

Vezetők kötelemei:

Elszámolható legyen az irányítása alá tartozó területen található vállalati vagyonnal és a szükséges biztonsági intézkedések bevezetésével biztosítja azok védelmét. Sajátítsa el a rá bízott értékek védelmével kapcsolatos összes biztonsági folyamatot, biztonsági követelmények és intézkedések hatékony alkalmazását. Jerlens a biztonsági szervezetek minden olyan tevékenységet, esetleges veszélyt vagy biztonsági eseményt, amelyek a vállalat tulajdonának, adatainak, eljárásainak, vagy egyéb vagyoni értékeinek károsodásával vagy veszteségével, illetve a vállalat alkalmazottainak sérülésével jártak vagy járhatnak. Kezdeményezzen azonnali helyesbítő intézkedéseket, ha a biztonságot veszélyeztető helyzet áll elő, és tájékoztassa a biztonsági szervezetet minden súlyos, a biztonságot veszélyeztető helyzetről. Az alkalmazottak számára tudatosítsa a biztonságot veszélyeztető helyzeteket és hívyja fel a figyelmüket biztonsági felelősségiükre. Tegye meg a megfelelő helyreállító intézkedéseket, amikor vagyonbiztonságot érintő jogszabálytól. Felelősségi körébe tartozóan, biztosítja az összes rá bízott vállalati adat és eljárás megfelelő minősítését és ellenőrzését. Biztosítja az adatvédelmi és a biztonsági követelmények a betartását.

4.1.2 A biztonsági szervezet felelősségei, feladat meghatározás

A biztonsági szabályzat meghatározza egy nemzetközi vállalat biztonsági folyamatait és követelményeit. A vállalat biztonsági szervezete a vállalat operatív egységei számára nyújt tanácsot, útmutatást, támogatást és segítséget a következő területeken:

- Minimalizálni a sérülés kockázatait a vállalat alkalmazottaira, vállalkozóira, ügyfeleire és másokra, a vállalat telephelyein.
- Minimalizálni a visszaélés kockázatát a vállalat pénzügyi, tárgyi vagy szellemi tulajdonával szemben.
- Minimalizálni a vállalat tárgyi eszkozeit éró károsodás vagy pusztulás kockázatát.
- Minimalizálni a kockázatát a vállalat szellemi tulajdonához való jogosultlan hozzáférés vagy jogosultlan nyilvánosságra hozatala tekintetében.
• Támogatást nyújt természeti katasztrófa vagy krízishelyzet esetén az emberek, a tulajdon és a hírmény védelme érdekében.
• A vezetőségtől vagy az illetékes hatóságoktól kapott utasítások alapján vizsgálatok lefolytatásával kapcsolatban.
• Az érintett operációs egységeknél biztonsági lokális, operatív szabályzatok (házi rend) elkészítése és bevezetése.

Bevezetés és megfelelés

Bevezetés

Az operatív egységek vezetői biztosítják, hogy a megfelelő biztonsági szabályok kidolgozására, bevezetésére és fenntartására kerüljön sor, amelyek megfelelnek az összes vonatkozó jogszabályi rendelkezésnek, szabályozásnak és kötelezettségnek minden helyszínén, és ezen kívül a vállalat-irányítási követelményeknek is.

Ezek közé a szabályok közé tartozik a vállalat összes biztonsági folyamata: a fizikai biztonság, krizismenedzsment, a biztonsági események kezelése, belső vizsgálatok, humánbiztonság, összeférhetetlenségi vizsgálat, pénzügyi ellenőrzés, és az információ biztonság.

Megfelelősség

A szabályzat meghatározza az összes telephelyre vonatkozó biztonsági alapkövetelményeket és választható biztonsági intézkedéseket kínál, amelyeket az adott helyszín kockázatelemzési eredményének függvényében kell bevezetni. Ezek a biztonsági alapkövetelmények és választható biztonsági intézkedések a rendszeres felülvizsgálat tárgyát képezik. A biztonsági előírások auditálása a biztonsági szervezet felelőssége.

A követelményeknek való megfelelés:

A vállalat tulajdonában álló vagy általa üzemeltetett telephelyeken be kell tartani a szabályzatban meghatározott és a személyek, tárgyi eszközök, valamint szellemi tulajdonú adatok védelmére szolgáló követelményeket. A vállalat által bérelt és üzemeltetett telephelyeken be kell tartani a szabályzatban meghatározott követelményeket. Nem a vállalat tulajdonában álló (bérelt, vagy nem a vállalat által üzemeltetett) telephelyen történő vállalati tevékenység esetén, minimum követelményként legalább a következő programoknak kell megfelelniük: kockázatelemzés, vészszakos tervezés, biztonsági események kezelése, biztonsági oktatás, fizikai biztonság és a vállalati beléptető rendszer használata a bérelményben a vállalat által használt helyiségek
vonatkozásában. Bármilyen nem megfelelést a vállalat biztonsági szabályzataiban foglaltaktól való eltérést, a vállalat biztonsági főigazgatója (vagy az általa kijelölt, a biztonsági szabályzatokért felelős személy) által jóváhagyott “Kockázat elfogadási” nyilatkozat alapján kell engedélyezni.

**Kockázatelemzés általános szabályai**

A vállalat alkalmazottait, szellemi tulajdonát és tárgyi eszközeit fenyegető veszélyek telephelyenként, országoként, működési területenként, környezettől és időponttól függően eltérőek lehetnek. A biztonsági szervezetnek ezért legalább évente felül kell vizsgálnia az egyes helyszíneken fennálló kockázatokat és ennek megfelelően kell meghatároznia a megfelelő biztonsági intézkedések szintjét.

**A kockázatelemzési folyamat**

A kockázatelemzés segít meghatározni, azonosítani azokat a kockázatokat, amelyek a vállalat telephelyeire vonatkozóan jelentősebb kihatással lehetnek az ott dolgozóknak, az üzletmenetre vagy a környezeti hatásokra. A biztonsági szervezet az elemzés eredményét annak eldöntésére használja fel, hogy van-e szükség még további kiegészítő biztonsági intézkedések bevezetésére az adott helyszín vagyvondédelmének megerősítése érdekében.

Az értékelés elkészítése két lépésből áll:

1. Az első feladat a telephely vagy helyszín besorolása annak fontossága alapján valamely fő kategóriába.
2. A második feladat során pedig a helyszínt az alkategóriák szerint kell értékelni. Az értékelés eredménye a korábban meghatározott fő kategóriát csak felfelé módosíthatja.

**Fő kategóriák: A telephely fontossága**

A vállalat helyszínei egymáshoz képest meglehetősen változó, egyenlétlen képet mutathatnak. Lehetnek hatalmas vagy apró irodák, gyártóüzemek, telephelyek, elosztó állomások, raktárak, stb. Méretüket tekintve jelentősen eltérhetnek egymástól, akár csak típusukban, illetve feladataikat illetően is. A biztonsági szervezet feladata, hogy megvizsgálja a telephelyeket és az alábbi kategóriák valamelyikébe besorolja azokat.

4-es kategória: (fekete) Ez a legmagasabb biztonsági kategória és szint. Ez a kategória csak egy 3-as kategóriájú helyszínen belül határolható el. Ennek a területnek vagy helyiségnek a megállapítása és biztonsági előírások meghatározása, a vállalat biztonsági főigazgatójának felelőssége.
3-es kategória: (piros) Ezek a legfontosabb telephelyek, ilyenek például a székházak, a nagyobb üzemek, vagy egyéb fontos helyszínek. Védelmi rendszereik a következők: biztonsági őrség, vagy fegyveres biztonsági őrség, szilárd kerítés, zárt láncú televízió rendszer (CCTV), riasztó rendszer, beléptető rendszer, kockázat elemzés, vészshelyzeti terv.

2-es kategória: (sárga) Ebbe a kategóriába tartoznak a működő alapvető üzemek, telepek és üzemeken kívüli telephelyek vagy egyéb, hasonló jelentős besorolású létesítmények. Ezek a helyszínek rendszerint kisebbek, mint a 3-as kategóriába tartozók.

Védelmi rendszereik a következők: biztonsági őrség, szilárd kerítés, zárt láncú televízió rendszer (CCTV), riasztó rendszer, beléptető rendszer, kockázat elemzés, vészshelyzeti terv.

1-as kategória: (zöld) Ebbe a kategóriába tartoznak a családi ház nagyságú létesítmények, kisebb üzemek, vagy más, mérsékelt fontosságú létesítmények. Védelmi rendszereik a következők: biztonsági őrség vagy véletlenszerű biztonsági őrjárat, szilárd vagy drótkerítés, zárt láncú televízió rendszer (CCTV), riasztó rendszer, beléptető rendszer vagy más belépési ellenőrzés, kiürítési terv.


A helyszínek védelmének a kategóriákkal mértékarányosnak kell lennie, de nem kötelező kizárólagos jelleggel, de minden új beruházásnál és felújításnál a biztonsági szervezet iránymutatása szerint kell eljárnii. Bár a legfontosabb cél, hogy minden kategória a neki megfelelő szintű védelmet kapja, elképzelhető, hogy egy alacsonyabb besorolású helyszín a követelményeknél magasabb szintű védelemben részesül. Minden eltérést a vállalat biztonsági főigazgatójának kell jóváhagynia. Minden alkategóriában négyféle lehetőség/mérés létezik, amelyek értéke pontokban adja az értékelést:

- nincs (fehér) - 0 pont
- alacsony (zöld) - 1 pont
- közepes (sárga) - 2 pont
- magas (piros) - 3 pont

Az összes alkategóriát a megfelelő követelmények szerint kell felmérni és értékelni, és a négy szint közül egyet kiválasztani (nincs, alacsony, közepes, magas). Ezt követően lehet elvégezni a pontozással történő értékelést (0, 1, 2, 3) valamelyik alkategóriára.
<table>
<thead>
<tr>
<th>Alkategória</th>
<th>nincs</th>
<th>alacsony</th>
<th>közepes</th>
<th>magas</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. Terrorizmus</td>
<td>0</td>
<td>1</td>
<td>2</td>
<td>3</td>
</tr>
<tr>
<td>2. Munkahelyi erőszak</td>
<td>0</td>
<td>1</td>
<td>2</td>
<td>3</td>
</tr>
<tr>
<td>3. Közveszélyes bűncselekmény, belső</td>
<td>0</td>
<td>1</td>
<td>2</td>
<td>3</td>
</tr>
<tr>
<td>4. Közveszélyes bűncselekmény, külső</td>
<td>0</td>
<td>1</td>
<td>2</td>
<td>3</td>
</tr>
<tr>
<td>5. Természeti és emberi eredetű katasztrófa</td>
<td>0</td>
<td>5</td>
<td>10</td>
<td>15</td>
</tr>
<tr>
<td>Összesen</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Pont</th>
<th>alacsony</th>
<th>közepes</th>
<th>magas</th>
</tr>
</thead>
<tbody>
<tr>
<td>ZÖLD</td>
<td>SÁRGA</td>
<td>PIROS</td>
<td></td>
</tr>
<tr>
<td>0-5</td>
<td>6-10</td>
<td>11-15</td>
<td></td>
</tr>
</tbody>
</table>

Amikor az összes alkategóriában elvégeztük az értékelést, ezeket a pontokat össze kell adni. Vagyis megkapjuk az alkategóriák felmérésének eredményét pontszámban. Az összesített pontszám pedig az adott helyszín kockázati kategóriáját fogja megmutatni az alábbiak szerint.

**Ponthatárok:**

<table>
<thead>
<tr>
<th>Pont</th>
<th>alacsony</th>
<th>közepes</th>
<th>magas</th>
</tr>
</thead>
<tbody>
<tr>
<td>ZÖLD</td>
<td>SÁRGA</td>
<td>PIROS</td>
<td></td>
</tr>
<tr>
<td>0-5</td>
<td>6-10</td>
<td>11-15</td>
<td></td>
</tr>
</tbody>
</table>

Ezután kétféle értékelést kaphatunk:

1. Az alkategóriák értékelésének eredménye **azonos vagy alacsonyabb** szintet mutat, mint a fő kategória. **Nincs további intézkedésre** szükség, mert a kockázat elemzés eredménye egyértelműen a fő kategória alapján kerül meghatározásra. Vagyis, az alkategória felmérésének eredménye nem lesz módosító hatással a fő kategória eredményére.

2. Az alkategóriák értékelésének eredménye **magasabb** szintet mutat, mint a fő kategória. **Intézkedésre** van szükség. Az alkategória felmérés módosítani fogja a fő kategória eredményét, vagyis az alkategória felmérés eredménye megemeli a fő kategória besorolását.

Az alábbiakban meghatározott minden kockázati kategóriára el kell végezni az adott helyszín kockázati felmérést, és azt évente, illetve a kockázati szint változásakor felül kell vizsgálni, és újra folyamodni az értékelés jóváhagyásért. Minden helyszínen, telep helyen dokumentálni kell a

A kategorizálás a kockázati szint alapján történik

1. alkategória: Terrorizmus

A vállalat könnyen válhat a világ bárhol terrorista tevékenység célpontjává. A cél a terrorista cselekmények vagy robbantások kockázatának csökkentése, a robbanószerkezetek azonosítására való képességünk növelése és a biztonsági esemény tényleges bekövetkezése esetén keletkező károk enyhítése.

nincs - Ez a feltétel akkor teljesül, ha az összes következő körülmény fennáll:

- Az elmúlt öt év során nem fordult elő terrorista merénylet.
- Nem tettek jelentést terrorista tevékenységről vagy terrorizmussal gyanúsított személyek letartóztatásáról.
- A helyi hatóságok a területet úgy tekintik, mint ahol nincs kockázata az esetleges terrortámadásnak.

alacsony - Ez a feltétel akkor teljesül, ha az összes következő körülmény fennáll:

- Az elmúlt három év során nem fordult elő terrorista merénylet.
- Nem tettek jelentést terrorista tevékenységről vagy terrorizmussal gyanúsított személyek letartóztatásáról.
- A helyi hatóságok a területet úgy tekintik, mint ahol alacsony a kockázata az esetleges terrortámadásnak.

közepes - Ez a feltétel akkor teljesül, ha a következő körülmények közül bármelyik fennáll:

- Az elmúlt három év során egy terrortámadás/merénylet fordult elő.
- Tettek jelentést terrorista tevékenységről vagy terrorizmussal gyanúsított személyek letartóztatásáról.
- A helyi hatóságok a területet úgy tekintik, mint ahol általában van kockázata az esetleges terrortámadásnak.

**magas** - Ez a feltétel akkor teljesül, ha a következő körülmények közül bármelyik fennáll:
- Az elmúlt három év során több esetben is előfordult terrorista merénylet.
- Többször is tettek jelentést terrorista tevékenységről.
- A helyi hatóságok a területet úgy tekintik, mint ahol magas a kockázata az esetleges terrortámadásnak.

### 2. alkategória: Munkahelyi erőszak

A munkahelyi erőszak fenyegetése eltérő lehet az egyes országokban. A biztonsági szervezet feladata, hogy a vállalat munkavállalói és tárgyi eszközeivel szemben elkövetett erőszakos cselekményeket megelőzzük, vagy csökkentsük.

**nincs** – ilyen esemény nem fordult elő az elmúlt három év során.

**alacsony** - ilyen esemény nem fordult elő az elmúlt egy év során.

**közepes** – egy esemény fordult elő.

**magas** – több mint egy esemény történt.

### 3. alkategória: Közveszélyes bűncselekmények/belső – amely a vállalat területén történt.

A biztonsági szervezetnek meg kell határoznia a bűncselekményekkel szembeni sebezhetőségének fokát a helyi bűnügyi statisztikák, a hatóságtól begyűjtött adatok, valamint a vállalat helyi létesítményinek általános üzleti környezete alapján. A termelő-gyártó vállalatok eszközei és termékei nagy kísértést jelentenek a bűnözők számára. A szervezett bűnözés szintén célpontként tekint a termékek előállításával foglalkozó vállalatokra. A biztonsági szervezet célja a bűncselekmények veszélyének elhárítása, illetve csökkentése a vállalat telephelyein és megakadályozni vagy elrettenteni a vállalat alkalmazottai, dolgozói elleni fenyegetéseket vagy bűncselekményeket.

**nincs** – az adott helyszínen nem fordult elő magas prioritású esemény az elmúlt három évben.

**alacsony** – az adott helyszínen egy magas prioritású esemény történt az elmúlt egy évben.

1 A magas prioritású események a 69. oldalon vannak feltüntetve
közepes – kisszámú, 2-3 eseményjelentés készült az adott helyszínen.

magas – több mint 3 eseményjelentés készült az adott helyszínen.

4. alkategória: Közveszélyes bűncselekmények/külső – amely a vállalat területén kívül történt:

nincs – az elmúlt három év során nem figyeltek meg bűncselekményt.

alacsony - az elmúlt egy év során nem figyeltek meg bűncselekményt.

közepes – kisebb számú bűncselekmény előfordul, de ennek nincs közvetlen hatása a vállalat tevékenységére.

magas – több bűncselekmény történt, hasonló vállalatok sérelmére.

5. alkategória: Természeti és ember által okozott katasztrófák

nincs – az elmúlt három év során nem figyeltek meg ilyen jellegű eseményt.

alacsony - az elmúlt egy év során nem figyeltek meg, vagy alacsony intenzitású esemény történt.

közepes – az elmúlt egy évben történt esemény, de ez nem volt közvetlen hatással a vállalat tevékenységére.

magas – az elmúlt egy évben történt esemény, és ez közvetlen hatással volt a vállalat tevékenységére.
4.2 Fizikai biztonság

4.2.1 Külső biztonság

Általános szabály: minden biztonsági berendezésnek működőképesnek kell lennie [48], és tesztelni szükséges legalább háromhavonta.

A vállalat tulajdonhatárának jelzése

A vállalat tulajdonában álló létesítmények határait jelezni kell és azt, hogy csak az arra felhatalmazott személyek léphetnek be. A kiírásoknak a helyi jogszabályokkal, törvényekkel összhangban kell lennie. A vezetőség felelőssége, hogy a vállalat tulajdonát megfelelően jelézzék a telekhatáron és belépési korlátozásokat vezessenek be. A több bérlővel rendelkező létesítmények, a városi közterületeken található létesítmények, bérelt területek és azok a helyszínek, ahol az ilyen feliratok a bérleti szerződés előírásaiba ütköznek, mentesek a követelmény alól.

Kritikus közművek

A helyszín első számú vezetőjének felelőssége, hogy azonosítsa a kritikus közműveket. A kritikus közmű olyan infrastruktúra, amelynek károsodása vagy pusztulása negatív hatással van a vállalat bevételére, kimaradása veszélyezteti az üzemészerű működést. Kritikus közművek lehetnek például az alábbiak: villamos, vagy más energia bekötőállomásai, gázfogadók, szerverszobák, tartálypark, vízhűtő, közműalagút, műholdas földi állomás, mikrohullámú parabola antennák, kommunikációs tornyok és állványok, hulladékkezelő központok, valamint víznyerő kutak, stb.

A kritikus közműveket évente kell azonosítani, felülvizsgálni és az eredményt dokumentálni.

A kritikus közműveknél az elvárások a következők:

- Kerítés, ha a kritikus közmű külterületen van és nincs egy helyiségben elzártan, vagy olyan különálló szerkezetben elhelyezve, amely az adott közmű közvetlen elérését lehetetlenné teszi.
- A belépés beléptető rendszeren keresztül, illetve a biztonsági szervezet által engedélyezett zárkészlet, vagy ezekkel egyenértékű egyéb belépés ellenőriző lehetőséggel.
- Folyamatos éjszakai kiválóítás.

Kiegészítő biztonsági intézkedések:

- Kamerarendszer és/vagy riasztórendszer.
Telekhatár világítás

Általában a létesítmény felügyelet, üzemeltetési szervezet (Facility) feladata, hogy a dolgozók munkabiztonsága, baleset megelőzési célból gondoskodjanak a helyszínek környezetében a megfelelő világításról. A világítás feleljen meg a vállalati, illetve a helyi munkavédelmi és önkormányzati előírásoknak [75].

Járművek beléptetése

Minden, a vállalathoz tartozó helyszínen gondoskodni kell róla, hogy csak az engedélyezett járművek léphessenek be. [39] Vészszubjekt esetén minden, a vállalathoz tartozó helyszínen biztosítani kell annak lehetőségét, hogy megakadályozzuk a belépést az engedélytel rendelkező alkalmazottak és járművek számára is.

Választható biztonsági intézkedések

Ajánlott minden helyszínen a gépjárművek ellenőrzése belépéskor, illetve átvizsgálásuk, amikor elhagyják a területet.

Campus (egyetem jellegű) helyszínek

A Campus jellegű helyszínekhez vezető főbejárat útja mentén ajánlott egy kapuőrház felállítása sorompóval, amelyet vészszubjektben a biztonsági személyzet tud működtetni.

A kapuőrházban található összes berendezésnek működőképesnek kell lennie és ezt legalább háromhavonta ellenőrizni kell.

A berendezéseknek a következő képességekkel kell rendelkezniük:
Másodlagos gépjármű behajtóknak zárhatónak kell lenniük, legyenek bezárt állapotban, így biztosítható, hogy a területre való bejutás csak az elsődleges bejáraton keresztül legyen lehetséges.
Másodlagos bejáratnak a következő felszerelésekkel és képességekkel kell rendelkeznie:
Az összes bejárat sorompóját folyamatosan zárva kell tartani, a behajtást csak érvényes belépőkártya használatával és/vagy ellenőrzött távvezérléssel lehet megvalósítni. A bejárati útszakaszokat kamerarendszerrel kell megfigyelni, amelyet a biztonsági szolgálat ellenőriz.

**Szabadtéri parkolók**

**Választható biztonsági intézkedések**


**Garázsok**

**Alapvető biztonsági követelmények**

A garázsban és/vagy parkolóhából az épületekbe történő belépés a vállalat által ellenőrzött beléptető rendszeren keresztül történhet a munkavédelmi szabályoknak megfelelően biztonságos és jól megvilágítottnak kell lennie. [9]

Ha a vállalat az egyetlen bérő:

A közvetlenül a vállalat által elfoglalt (bérelt vagy tulajdonában álló) terület alatt elhelyezkedő garázsokba a bejutás csak olyan járművek vagy gépjármű vezetők számára lehetséges, akik érvényes belépési engedélytel rendelkeznek.

Ha a vállalat nem az egyetlen bérő:

A közvetlenül a vállalat által elfoglalt terület alatt elhelyezkedő garázsokba a bejutást korlátozni indokolt, hogy csak olyan járművek vagy gépjármű vezetők számára legyen engedélyezve, akik érvényes belépési engedélytel rendelkeznek, amennyiben ez lehetséges.

**Választható biztonsági intézkedések**

Fizikai akadályok

A külső bejáratokat úgy kell megtervezni és megépíteni, hogy az előtereket és az üvegezett tereket járművel ne lehessen nagy sebességgel megközelíteni. [15] A forgalomterelő oszlopokat, térburkolati technikákat és egyéb tervezett akadályokat úgy kell beépíteni, hogy megakadályozzák a gépjárművek behajtását az olyan előterekbe és üvegezett terekbe és minden olyan területre, ahol nagyobb számban tartózkodhatnak személyek (tehát előterekben, konferenciatermekben, kavézókban, stb.), és ugyanakkor hozzáférhető a gépjárművek számára is [79].

Egyéb bejutási pontok

A telephelyek üzemeltetőinek tisztában kell lenniük azzal, hogy hol találhatóak az épületekbe történő behatolásra alkalmas védtelen, kevésbé nyilvánvaló pontjai, például szellőzőrácsock, lefolyók, aknafedők, közműalagutak, napfénytetők, tétőablakok vagy szellőzők. A biztonsági szervezet javaslatára alapján gondoskodni kell az ilyen jellegű bejutási pontok megfelelő védelméről. Az intézkedéseket dokumentálni kell és a dokumentumokat meg kell őrizni.

Rejtőzködésre alkalmas helyek

A helyszín környékén telepített kertészeti elemeknek legalább egy méteres távolságra kell lenniük az épületek külső falsíkjától, illetve a kerítéstől kívül-belül tartani kell az egy méteres távolságot. Ezáltal biztosítható az akadálytalán belátást, illetve azt, hogy ne tudjon senki elrejtőződni, illetve valamilyen tárgyat elrejtani.

Telekhatár védelem

Választható biztonsági intézkedések

Riasztó-rendszer telepítése, amely jelzi a területre történő illetékeltelen behatolást: Kerítésre épített riasztó. Infravörös behatolásjelző védelem. Mikrohullámú behatolásjelző védelem. Kamerarendszer riasztási funkcióval. [16] [27]

4.2.2 Az épület határai és az épületen belüli biztonság

Külső bejáratok

Az épületek külső bejáratait úgy kell megtervezni, hogy meg lehessen akadályozni az illetékeltelen behatolást, riasztással vagy megfigyelő lehetőséggel legyenek ellátva, amelyek garantálják biztonságosságukat és úgy legyenek megtervezve, hogy az erőszakos behatolásnak ellenálljanak.
A vészkijáratokat riasztóval kell felszerelni, és úgy kell megtervezni, hogy az erőszakos behatolásnak ellenálljanak. A távvezérelhető bejáratú ajtókat kaputelefonnal (intercom, kamerarendszer) és távnyitó berendezéssel kell felszerelni, ellenőrzésüket pedig a biztonsági szolgálat végezheti.

**Riasztók tesztelése és karbantartása**

A biztonsági riasztó rendszer minden elemét tesztelni kell, a teszteléseket dokumentálni szükséges annak érdekében, hogy rendeltetésszerű használata biztosítható legyen. A riasztókat legalább háromhavonta kell ellenőrizni és tesztelni. Minden tesztelés során felmerülő hiba esetén azonnal intézkedni kell a javítást illetően és a javítási munkákhoz és a megismételt tesztekhez is dokumentáltak kell lennie.

**Ablakok és külső üvegfalak**

A földszinten elhelyezkedő ablakok nyitása csak belülről legyen lehetséges és 25 centiméternél jobban ne lehessen kinyitni azokat.

Ahol nagy a terrortámadás veszélye, ott a helyszínek meg kellett vizsgálni arra nézve, mennyire lehetséges gépjárműbe rejtett bomba vagy egyéb robbanó eszköz használata.

A vizsgálat során figyelembe kell venni többek között az alábbi megfontolásokat:

Meg lehet-e közeli tani a vállalat területét közvetlenül? Lehet-e az épület közvetlen közelében parkolni? Van-e tömegközlekedési megálló (autóbusz, vonat, villamos, stb.) és/vagy taxiállomás, illetve le és felszálló hely a közelben? Milyen utak vezetnek a létesítmény mellett?

Ha annak megállapítására kerül sor, hogy nagy a veszélye gépjárműbe rejtett bomba vagy egyéb robbanó eszköz használatának a létesítmény területén vagy a létesítmény területének közvetlen közelében, erről értesíteni kell a helyszíni üzleti vezetőt, valamint a vállalat biztonsági főigazgatóját, írásos formában.

Ahol fennáll a robbantás kockázata, a helyszínek külső térre néző üvegfelületeit szilánkmentes biztonsági fóliával (Anti-Shatter Security Film, ASF) kell védeni. Az ASF-t a veszélynek kitett helyekre néző és a külső fal felületen elhelyezkedő ablakokra kell alkalmazni.

A biztonsági főigazgató felelős az AFS telepítésének felméréseért, a telepítés engedélyezéséért és a telepítés fontossági sorrendjének kialakításáért. A fontossági sorrendet és az értékelést dokumentálni kell.
Nyilvános területek

A nyilvános területeket a vállalat általános megközelítésre szánja, vagyis ilyen helyeken semmilyen ellenőrzést nem alkalmaz.

Minden nyilvános helyen, amilyen például egy előtér, szükséges felszerelni beléptető rendszert, hogy a vállalat belső területei felé, csak azokon keresztül lehessen bejutni érvényes belépőkártya használatával, beleértve a liftetek is. Rejtett helyre, helyekre szükséges vészszabályozást, ami a személyzettel ellátott előterekben helyeznek el, amelyeket a személyzet feltűnés nélkül használhatja tud hozni, így értesítve a vészszabályozót a biztonsági központ személyzetét, akik meg tudják tenni a szükséges intézkedéseket. Vészszabályozati terveket nyomtatott formában kell a helyszíneken tartani, amelyek utasításokat tartalmaznak a biztonsági és egyéb illetékes személyzet számára. Az eljárásokat minden évben tesztelni kell. A személyzet nélküli előterekben vagy létesítményi bejáratoknál, amelyek távolról és/vagy kézzel nyithatók, hang és képi (audiovizuális) rendszerek (például kaputelefon/videó, intercom, kamerarendszer, stb.) tegyék lehetővé a belépők azonosítását még mielőtt azok az épület belsőjeibe léphetnének.

Választható biztonsági intézkedések

A személyzettel ellátott előtérből nyíló külső és belső ajtók távvezérlési lehetősége azok zárására és nyitására. Egyirányú audiovizuális rendszerek, amelyek önműködően üzemelnek, amikor a riasztás megtörténik. A külső és belső kártyaleolvasók automatikusan leállnak, amikor a riasztás megtörténik. Megjegyzés: A fenti ellenőrző rendszerek egyetlen működtető szerkezetbe is lehet integrálni. A recepciós vészriasztása esetén automatikusan lezárnak az épület belső tereibe és az előtérbe nyíló ajtók (például a forgóajtók, a beléptető rendszer kártyaleolvasó ajtók, stb.). Az ajtóknak ugyanakkor mindig lehetővé kell lenniük a belülről kifelé történő vészkijárati funkciót, de meg kell akadályozniuk az előtérbe való bejutást. Riasztás érkezhet egy folyamatos felügyelet alatt álló ellenőrzési központba, és aktiválódhat egy kamera, valamint egy egyirányú hangosbeszélő az előtérben. Az előterek, illemhelyek, és egyéb hasonló nyilvános helyek nincsenek a behatolást érzékenyi lehessen. A kisüzemű berendezésekhez szükség esetén megfelelően rögzített vagy zárt behatolás védő lemecket kell alkalmazni, vagy mozgásérzékelőket szükséges elhelyezni az álmennyezet felett. A több bérő által használt épületekben a vállalat által használt emeleteken, a nyilvános területeken és a nyilvános felvonók előtereiben található illemhelyeknek zárva kell lenniük. Kulcsakkal csak a vállalat alkalmazottai rendelkezhetnek. A személyzettel ellátott előterekben az előtér és a recepciós pult elhelyezkedésének olyannak kell lennie, hogy a recepciós
ülı helyzetében a lehető legtöbbet lásson és ugyanerről a helyről ellenőrzése alatt tarthassa a területet és annak összes megközelítési lehetőségét.

A vállalat belső terei


A vállalat korlátozott hozzáférésű területei (beléptető rendszer)

A korlátozott hozzáférésű terület egy létesítményen belül található és egy bizonyos csoport rendelkezik felette, amelynek a vállalat, a létesítmény, vagy a termék szempontjából kritikusnak tekintett, meghatározott üzleti igénye vagy funkciója van.

A korlátozott hozzáférésű terület meghatározása a terület vezetőjének vagy az általa kijelölt személynek a feladata. A védett terület funkcióját és szintjét biztonsági szervezet évente felülvizsgálja.

A korlátozott hozzáférésű területekkel szembeni követelmények: Felügyelettel ellátott beléptető rendszer vagy elektronikus kódzáras készülék, ellenőrző funkcióval. A korlátozott hozzáférésű területek beléptető rendszerében nem szereplő személyek belépését és kilépését naplózni kell. A terület vezetőjének, vagy az általa kijelölt személynek legalább háromhavonta ellenőriznie kell a látogatók regisztrációs naplóját. Ezt a felülvizsgálatot aláirással és dátummal kell ellátani. Minden olyan személynek, aki nem rendelkezik a beléptető rendszerben engedélyvel vagy számkódos kombinációval a korlátozott hozzáférésű területre belépéshez, alá kell írnia a látogatók

A vállalat más vállalatokkal közös területei

A vállalat más vállalatokkal közös területei olyan területek, amelyeket a vállalaton kívül más vállalatok is használhatnának, ott saját termelő, vagy üzleti tevékenységüket folytathatják

A vállalat más vállalatokkal megosztott területeit úgy kell kialakítani, elhatárolni, hogy azokról a vállalat belső területeire csak érvényes jogosultság esetén lehessen bejutni. Amennyiben a gyártási, üzletmeneti okok miatt a fizikai elválasztás nem lehetséges, akkor más biztonsági intézkedések bevezetésére van szükség a belső területekre való behatolás megakadályozására, amelyek nem tartoznak sem az előtérhez, közlekedőkhöz, szociális terekhez, kávézókhöz vagy mosdókhoz. Intézkedésekhez lehetnek: Belépési ellenőrzés. A vállalat alkalmazottai által használt irodákat és/vagy saját tulajdonú adatokat biztonságba kell helyezni, amikor nem tartózkodik ott senki. A vállalat által nyújtott szolgáltatások: ha a szolgáltatásokat a vállalat nyújtja (pl. kávézó, iratmásolás, postázás, stb.), a hozzáférési lehetőségeket a bérleti megállapodás feltételeiben vagy szerződésben szükséges szabályozni.

Bérlők területei

A bérlők területei azok az irodák, emeletek vagy épületek, amelyeket a vállalat adott bérbe nem a vállalathoz tartozó külső vállalatnak.

Ha a vállalat nyújtja a szolgáltatásokat, a helyiséget, emeletet, épületet egy bérlő használja. A bérleti szerződésben világosan meg kell határozni, hogy milyen feltételek mellett léphet be a
vállalat ezekre a helyekre vészhelyzetben. A belépési ellenőrzések és a biztonsági intézkedések, amelyeket a vállalat határoz meg, a bérlőkre is vonatkoznak a közös használatú területeken. Intézkedések lehetnek: Belépési ellenőrzés. A bérlők nem juthatnak be olyan területekre, ahol bizalmassága nek találkozhatnak, illetve olyan berendezések működnek, amelyek bizalmassága dolgoznak (például terminállok, távoli nyomtatók, stb.). A vállalat által nyújtott szolgáltatások. Amennyiben az összes szolgáltatást a vállalat nyújtja (pl., beléptetőrendszer, riasztások felügyelete, vészhelyzeti reakció, stb.), nincs semmilyen különleges intézkedésre szükség, kivéve az alábbi eseteket: Minden biztonsági eseményt azonnal jelenteni kell, ami a létesítményen tartózkodó személy egészségét, vagy biztonságát veszélyezteti (például fenyegetés vagy erőszakos cselekedet). Minden biztonsági eseményt azonnal jelenteni kell, ami a létesítményre vagy az ott található vagyontárgyakra káros hatást gyakorolna.

**Pénzkiadó automaták (ATM) vagy bankok**

Alapvetően a vállalat biztonsági szervezetének nem feladata az eladási pénztárműveletek, hitelszövetkezetek, pénzkiadó automaták (ATM-ek) vagy bankok felügyelete. Az értékesístést végző szolgáltatónak kell harmadik fél által történő felügyeletet megszerveznie a betörés vagy rabság elleni védekezés érdekében. A riasztásokra adott válaszokat a vállalat biztonsági szervezetének jelenteni kell. Ahol van biztonsági központ, párhuzamos riasztást vagy olyan eljárást kell alkalmazni, amely lehetővé teszi, a biztonsági események korai észlelését, automatikus riasztási értesítése biztosítsa a biztonsági személyzet részére, hogy segítségére lehessen a bűnüldöző hatóságoknak, amennyiben azok megérkeznek a létesítménybe.

**Egészségügyi létesítmények**

Az egészségügyi létesítmény olyan helyiség, vagy helyiségek, ahol egészségügyi személyzet, orvosok, apolók személyesen vannak jelen annak érdekében, hogy foglalkozás egészségügyi szolgáltatásokat nyújtsanak, egészségügyi kérdésekben tanácsot, útmutatást adjanak, és orvosi kezelésben részesítsenek betegeket illetve orvosi vizsgálatokat végezzenek.

**Választható biztonsági intézkedések:** A külső ablakokat úgy kell kialakítani, hogy a terület közvetlen megfigyelését ne tegyék lehetővé. Pánikriasztó beszerelése javasolt, használatával közvetlenül tud jelezni az egészségügyi dolgozó a biztonsági központba olyan esetekben, amikor a biztonsági személyzet segítsége szükséges lehet, pl.: mentő hívása, agresszív személy megfékezése esetén, stb.
Felvonók

Közös használatú épületekben a nyilvános területekről közvetlenül a vállalat belső területeire érkező lifteket kártyaleolvasó szerkezettel, vagy más biztonsági eszközzel kell ellátni, amely megakadályozza illetéktelen személyek bejutását a vállalat belső területeire.

A postabontó biztonsága

A vállalat, vagy szerződéses postai szolgáltató postai szolgáltatására egyaránt alkalmazandó és rendezése a postabontó vezetőjének a feladata.


4.2.3 Zár- és kulcskezelési szabályok

Ajtózárakra és kulcsokra vonatkozó biztonsági intézkedések

Lehetőség szerint mesterkulcs rendszert kell telepíteni. [10] [51] [78]


A mesterkulcs a legmagasabb szintű kulcs, minden más kulcs a kulcsrendszer felépítése szerint alatta helyezkedik el, amely azonos kulcs sorozat minden elemével zárható zárat nyit. Az al-mesterkulcs a mesterkulcs alatti szinten helyezkedik el, amely azonos kulcs sorozat minden elemével zárható zárat nyit például egy egész épületben vagy emeleten. A maghúzó kulcs olyan kulcs, amely el tudja távolítani a zárbetétet.
A kulcsok következő szintjét csoportkulcsoknak nevezzük, az al-mesterkulcs alatti szinten helyezkednek el, melyek meghatározott helyiségekhez vezető összes zárat tudják nyitni, például villamos szekrények, karbantartáshoz használt helyiségek vagy házgondnoki, házmesteri szekrények kulcsai. A csoportkulcsok nem tekintendők mesterkulcsnak vagy al-mesterkulcsnak.


A kulcsrendszer beszállító szolgáltató működése

A kulcskezelési követelményeket alkalmaznia kell a vállalatnak és/vagy a szerződéses partnernek is. A kulcsrendszer gyártójának garanciája kell, a kulcskódot, cilinderek és a kulcsrendszer összes elemének átalakítását, vagy a sérülésmentes szállítását a beszállító akadályoztatása esetén is. A kulcsrendszer beszállítójának havonta biztonsági másolatot kell készíteni a kódokról, a kulcs mátrixról és a legyártott kulcsok cilinderek adatbázisáról. A kulcsrendszer beszállítójának banki kötelezettség vállalással vagy biztosítással, garanciával kell rendelkeznie. A kulcsrendszer beszállító követelményeit hathavonta felül kell vizsgálni. A kódok és csapok kombinációjának biztonságban kell lenniük és csak az arra feljogosított személy számára lehet elérhető. Minden másolt és ki nem adott kulcsnak leltározva és biztonságosan elzárva kell lenniük. A másoló berendezésnek és programnak, nyerskulcsoknak és csapoknak és más kulcsrendszer elemeknek elzárva kell lenniük, amikor nincsenek használatban, illetve felügyelet alatt.
4.2.4 A vállalatnál alkalmazott belépési ellenőrzés és a belépőkártyák formái

A vállalattól létesítményeibe való belépés ellenőrzése alapvető feladata a biztonsági szervezetnek, amit meg kell valósítani ahhoz, hogy a többi biztonsági intézkedés hatékonyan tudjon működni. A vállalat összes helyszínén kell, hogy legyen olyan folyamat, amely megakadályozza a jogosulatlan személyek belépését a vállalat létesítményeibe [76].

Belépés ellenőrzése

Elektronikus beléptető rendszert [94] kell alkalmazni összhangban a biztonsági standardokkal. Ettől eltérő beléptető rendszerkialakítása csak a vállalat biztonsági főigazgatójának engedélyével lehetséges.

A vállalati belépőkártyát a vállalat területén jól látható helyen, nyakban szalagon, vagy kitűzve, állandóan viselni kell.

Minden személy, az alkalmazottak és a nem a vállalathoz tartozó személyek is csak egy kártyát kaphatnak. A rendszeresített beléptető kártyán kívül kiadható olyan, a biometrikus jellemzőkön alapuló azonosítást lehetővé tévő vagy személyi azonosítóval nem rendelkező közelség-érzékelő kártyák is, amelyeket biometrikus beléptető rendszerek használnak.

A vállalat alkalmazottai számára:

- Az összes, a vállalat alkalmazásában álló személy részére egy rendszeresített vállalati belépőkártya kerül kiadásra (fehér színű),
- Azok az alkalmazottak, akiknek ideiglenes kártyára van szükségük, zöld csíkos belépőkártyát kapnak.

Nem a vállalathoz tartozó személy – kísérő nélkül (sárga csíkos):

- Azok a személyek, aki nem a vállalat alkalmazottai, de munkavégzés céljából lépnek a vállalat területére, jogosultak kísérő nélkül belépni a vállalat létesítményeibe, egy sárga színű csíkos belépőkártyát kapnak. Ilyenek lehetnek például a szerződött partnerek, alvállalkozók, üzleti partnerek, tanulók, stb.
- Azok a személyek, aki nem a vállalat alkalmazottai, de munkavégzés céljából lépnek a vállalat területére, de érkezésüket nem lehetett előre jelezni (pl. vízcsőtörés esetén a hiba elhárítására érkező személy) és csak rövid időtartamú itt tartózkodásra van szükségük, egy teljesen sárga színű ideiglenes belépőkártyát kapnak. Abban az esetben jogosultak kísérő nélküli munkavégzésre és belépésre, ha ezt a vállalat arra jogosult alkalmazottja aláírásával igazolja. Ezt a belépőkártyát távozáskor a biztonsági személyzet visszavonja.
Látogatók - kísérővel

Azon személyek, akik nem a vállalat alkalmazottai, és nem munkavégzés céljából érkeznek a létesítménybe, például külső cég képviselői tárgyalni érkeznek, ebben az esetben piros csíkos, ideiglenes belépőkártyát kapnak, valamint kísérésük a látogatás teljes időtartama alatt kötelező.

Fényképes (állandó) belépőkártyák

A vállalat minden helyszínén a szabványos belépőkártyákat kell alkalmazni. A belépőkártyák az alábbi színek követik és mutatják, hogy viselőjének van-e szüksége kíséretre:

- Fehér és zöld jelzésű (pl.: csíkos) = nincs szükség kísérőre
- Sárga jelzésű (csíkos) = nincs szükség kísérőre
- Piros jelzésű (csíkos) = kísérő szükséges

A fényképes belépőkártyákon az alábbiaknak kell felkerülniük:

- A vállalat logója
- A vállalat neve
- Színes fénykép legalább 24mm x 32mm (300 pixel x 400 pixel) és a minimum arcmeret fejtőtől álcúcig 18mm-25mm között kell lennie, és a szemmegasságnak 20-25 mm-en belül kell elhelyezkednie a fotó aljától.
- Csak fehér háttér lehet a fényképen
- Név
- Azonosító és a kártya száma
- A hátsó oldalon: visszaküldési cím

Megjegyzés: További adatok nem lehetnek a kártya elülső oldalán. Semmilyen más jelet, jelzést, színt vagy különleges megjelölést nem szabad a kártyák elülső felén alkalmazni.

Fehér alapszinű belépőkártya (alkalmazottak számára)

Mindent a vállalatnál alkalmazott személy ezt a fehér alapszinű, állandó belépőkártyát kapja.

Sárga (csíkos) belépőkártya (nem a vállalat alkalmazásában álló személy, munkavégzés céljából és kísérő nélkül tevékenykedhet, sárga csíkos állandó belépőkártyát kap)

Ebbe a kategóriába a következő személyek soroljuk: üzleti partnerek (A telephely vezetőjének a megítélése alapján a vállalat biztonsági szervezetének jóváhagyásával), alvállalkozók, tanulók.
Az ilyen típusú belépőkártyán egyedül a vállalat logója és a sárga csík az egyetlen jelzés. Nincs különbség a kártyán a fent nevezett típusok között. A fényképes belépőkártyánál említett tételeken kívül (lásd: fényképes belépőkártyák formái) a sárga csíkos azonosítóknak csak a következő adatokat kell tartalmazniuk:

- vállalat logója
- Színes fénykép legalább 24mm x 32mm (300 x 400 pixel) és a minimum arcméret fejtetől álcscúcsig 18mm-25mm között kell lennie, és a szemmagasságnak 20-25 mm-en belül kell elhelyezkednie a fotó aljától.
- Fehér hátterű fotó
- Sárga csík
- Név
- Kártyaszám
- A cég vagy hivatal neve
- A vállalkozó sorszáma

Más megjelölést, terület megjelölést, jelzést, színeket, speciális megjelölést, stb. nem lehet elhelyezni a kártya elején.

Fénykép nélküli (ideiglenes) belépőkártyák

Az ideiglenes belépőkártyák számára számos formai megoldás lehet használatban. A formától függetlenül azonban meg kell tartani a következő színkódot.

- Zöld (csíkos) belépőkártya - vállalat alkalmazottak részére, (új dolgozó és még nem készült el a fényképes, az állandó, fehér belépőkártyája, illetve otthon felejtette az állandó belépőkártyáját)
- Sárga (csíkos) belépőkártya – nem a vállalt alkalmazásban álló személy, munkavégzés céljából érkezett (kísérő nélkül)
- Piros (csíkos) belépőkártya – nem a vállalat alkalmazásában álló személy, nem munkavégzés céljából érkezett (kíséret szükséges)

A belépőkártyák időbeni érvényességei

Minden belépőkártyának érvényességi idővel kell rendelkeznie a beléptetőrendszer adatbázisában.

- fehér, állandó, alkalmazott belépőkártya tiz évig lehet érvényes.
• sárga, állandó, alvállalkozói belépőkártya a szerződés lejárataig, de maximum egy évig lehet érvényes.
• A belépőkártya érvényességének lejáratakor új fényképet és új kártyát kell készíteni.
• Azokat a belépőkártyákat, amelyeket több, mint 90 napja nem használtak, inaktiválni kell.

Biztonsági kategória
A beléptetőrendszerrel védett összes területre engedélyezi a belépést, vagyis minden kártyaleolvasóhoz való jogosultsággal rendelkezik. A biztonsági kategória jogosultságot a vállalat biztonsági főigazgatója engedélyezheti.

Az ideiglenes belépőkártyáakkal kapcsolatos belépési eljárások és a belépés engedélyezése
A receptión vagy a biztonsági területen kívül tartott ideiglenes beléptetőkártyákról napi nyilvántartást kell vezetni. Minden olyan belépőkártyát, amelyet időre nem adtak le, inaktiválni kell. A napi nyilvántartási folyamatot a biztonsági szervezet köteles legalább hathavonta ellenőrizni. Az ideiglenes kártyákat csak a látogatás időtartamára szabad érvényesíteni.

A vállalat azon alkalmazottait, akiket egy másik vállalati helyszínre rendeltek vagy ott látogatást tesznek, de nincs velük az azonosító kártyájuk, előbb azonosítani és ellenőrizni kell, hogy tényleg vállalati dolgozók-e. Az ellenőrzést követően a zöld csíkos belépőkártyát csak a látogatás időtartamára szabad kiadni, és azt a dolgozónak viselnie kell. Az ideiglenes beléptető kártyák helyett egyszer használatos kártyák is használhatók.

Belépés engedélyezése
Nem a vállalat alkalmazásában álló személynek hatóság által kiállított okmánnyal kell igazolnia magát (fényképes személyazonosító okmány, személyi igazolvány, útlevél, jogosítvány). A kártya kiadását egy a vállalat alkalmazásában lévő, arra jogosult vezetőnek vagy a kijelölt kapcsolattartó személynek engedélyeznie kell. Minden belépőkártyát a biztonsági szervezet vagy a biztonsági szervezet által felhatalmazott recepcionál kell kiadnia.

A nem a vállalat alkalmazásában álló személyek, akikhez kísérő kell (látogatók)
A beléptetést végző biztonsági öröke, vagy a recepciósnak kötelessége, hogy: érintkezésbe lépjen a látogatót fogadó vállalati dolgozóval, meg kell győződni a látogató személyazonosságáról, kiadni a megfelelő belépőkártyát, a látogatónak kötelessége regisztrálni magát, és jól látható
helyn viselnie a kártyát, a látogatást engedélyező személynek biztosítania kell a vendég folyamatos kíséretét, felügyeletét.

A beléptető rendszer eljárásai és folyamatai


A beléptetőrendszer területi vezetőjének feladatai: Amennyiben a beléptetőrendszer területi vezető személyében változás történik, a beállított változásokról értesítenie kell a biztonsági szervezetet. Azok a vezetők, akik nem a vállalat alkalmazásában állnak, indokolt esetben szintén kijelöhetők a beléptetőrendszer területi vezetőjének feladatára, amennyiben a vállalat helyiségeiben meghatározott területért felelnek. A beléptetőrendszer területi vezetőinek jelentését (az általános kategóriák kivételével) a területi vezetőknek vagy kijelölt megbízottjaiknak
háromhavonta felül kell vizsgálniuk. A beléptetőrendszer területi vezetők kötelesek minden szükséges változtatást elvégezni a rendszeren, amely a mindenkor állapotnak megfelelően a teljes működőképességet biztosítja, illetve minden változás esetén értesíteni kell a biztonsági szervezetet. Az általános belépési kategóriák, mint amilyen a főbejárat, a külső bejáratok, kapuk, stb. nem tartoznak a beléptetőrendszer területi vezetők felelősségi körébe, érvényesítésük a következő módon történik: A személyzeti adatbázist a beléptető rendszer adatbázisával háromhavonta egybe kell vetni. Ha az adatbázisok egybevetésének módszere nem alkalmazható, akkor is kell egy olyan folyamatot fenntartani, amelynek révén a beléptető rendszer adatbázisa háromhavonta ellenőrizhető. (pl. a személyzeti osztály/HR havonta megküldi a dolgozók névsorát a biztonsági szervezetnek)

A beléptetőrendszer kezelőjének jogosultsága vagy engedélyei

A felhasználó azonosító kiadására alkalmas összes rendszeren minden olyan személynek egyedi azonosítót kell kiadni, akiknek hozzá kell férniük a rendszerhez. A kezelőszemélyzet engedélyét vagy jogosultságát hathavonta ellenőrizni és dokumentálni kell. A felülvizsgálatot nem végezheti ugyanaz a személy, mint aki a beléptető rendszer kezelésének jogosultságait kiadja.

Fegyverek

Amennyiben a helyi törvények megengedik az arra jogosultak fegyverviselését a biztonságos munkakörnyezet megteremtéséhez való elkötelezettség alapján javasolt, hogy a vállalat tiltja meg a fegyverek viselését a vállalat területén. Ez a tiltás terjedjen ki a vállalat parkolói, bérelt épületeire, területeire is. A kivételek következők: a katonai vagy rendfenntartó erők tagjai szolgálateljesítés közben. Fegyveres kocsikísérők, a szállítás és kézbesítés során (a kísérőknek a fegyvereiket rejtve kell hordaniuk a vállalat területén) biztonsági központok építésére vagy felújításra vonatkozó javaslatokat a biztonsági főigazgatója engedélyezte a tűzfegyverek viselését. Olyan személyek, akiknek a biztonsági főigazgató engedélyezte.

Biztonsági központok

A vállalat területén biztonsági központ építésére vagy felújítására vonatkozó javaslatokat a biztonsági főigazgatónak kell véleményeznie és engedélyeznie. A napi tevékenységgel összefüggő és a vészhelyzetben alkalmazott eljárások kezelésére írásos utasításoknak kell elérhetőnek lenniük a biztonsági személyzet részére a biztonsági központokban. A biztonsági központokban szakképzett személyzetet kell alkalmazni. A biztonsági központokat legalább egy olyan telefons mellékvonallal el kell látni, amely nem a telephely saját központján keresztül működik. Erre a céla
mobiltelefon is alkalmazható. Amennyiben video és/vagy hangrögzítő berendezés van használatban, úgy minden rögzítő berendezést 24 óránként ellenőrizni kell, hogy valóban rögzíti-e a felvételeket. Az önellenőrzési funkcióval ellátott digitális hangrögzítő berendezések kielégítik ezt a követelményt. A felvételek rögzítését kizárólag a helyi jogszabályoknak megfelelően lehet alkalmazni.

A vállalat átvizsgálási eljárásai, szabályai

A vállalat alkalmazottainak és tárgyi eszközeinek védelme érdekében a vállalat fenntartja magának a jogot, hogy átvizsgálja bárki, személyes és egyéb vagyontárgyait, csomagjait, amelyet a vállalat telephelyeire bevisznek, vagy onnan ki akarnak vinni [94]. A vállalat területére behajtó gépjárművek szintén tárgyát képezik az átvizsgálásnak. Az ellenőrzésre való felszólítást követően a szerződésben foglalt megállapodások szerint minden személytől elvárt, hogy együtt működjön az átvizsgálás során [77].

Személyesnek tekintett adatokat, üzeneteket, tárgyakat, adatokat nem lehet vállalati eszközökön, rendszerekben, a vállalat munkahelyeiin tárolni vagy tartani, tehát a telefonrendszeren, irodai rendszereken, elektronikus állományokban, íróasztalon, fiókokban, szekrényekben vagy irodákban sem. A vállalat biztonsági szervezetének jogában áll belépni ezekre a területekre és minden egyéb, a vállalat által birtokolt létesítménybe. Ezen túlmenően alkalmazottainak és tárgyi eszközeinek védelme érdekében a vállalat megkérheti alkalmazottait, hogy átvizsgálhassa alkalmazottak személyes tárgyait, beleértve azok aktatáskáját és csomagjait, amelyek a vállalat helyszínein találhatók vagy onnan ki akarják vinni azokat. Az átvizsgálás alá vont alkalmazottnak együtt kell működnie az ellenőrzés során. A vállalat alkalmazottja a biztonsági főigazgató vagy a helyi biztonsági vezető előzetes engedélye nélkül nem léphet be egy másik alkalmazott munkaterületére, beleértve annak elektronikus adatállományait is.

 Követelmények:
 Figyelmeztetés:

Beszállítók, alkalmazottak és bármely belépő számára helyszíni figyelmezetető feliratokat kell elhelyezni. A figyelmezetető táblákat a személyzettel ellátott előterekben és ott, ahol a beszállítók megkapják belépőkártyáikat, jól látható módon kell elhelyezni. A feliratnak az alábbiakat, vagy azzal egyenértékű információkat kell tartalmaznia:

FIGYELMEZTETÉS MINDEN SZEMÉLYNEK, AKI BELÉP ERRE A TERÜLETRE:
MINDEN A VÁLLALAT TERÜLETÉRE BE-KILÉPŐ SZEMÉLY, JáRMŰ, ESZKÖZ, ALANYA ÉS TÁRGYA A BIZTONSÁGI ELLENŐRZÉSNEK!

Ezen kívül a beszállítók dolgozói és a látogatók által aláírt nyomtatványnak is ezt a figyelmeztetést kell tartalmaznia, megfelelő nyelven.

Titoktartás

Minden olyan személy, aki részt vesz az ellenőrzés végrehajtásában, köteles minden talált tárgyat, eredményt és gyanús dolgot, valamint egyéb információt, amely az ellenőrzés eredményeképpen felszínre kerül, bizalmasan kezelní, mint a vállalat bizalmas információját és csak azoknak hozhatja a tudomására, akik erre illetékesek.

Fizikai átvizsgálás

A személyes tárgyaknak a dolgozó tudomása nélkül végzett átvizsgálását a biztonsági főigazgatónak kell engedélyeznie. Az átvizsgálási folyamatot a helyi törvényekkel összhangban a helyi biztonsági szabályzatnak kell tartalmaznia. Bármely, a vállalat helyiségeibe bevitt vagy onnan kihozott személyes, vagy egyéb tárgy, illetve a vállalat területére behajtó gépjármű tárgya az átvizsgálásnak. Ruházat átvizsgálás nem végezhető (vetkőztetés, tapogatás). Erre az eljárásra csak bizonyos hatósági szervek jogosultak.

Véletlenszerű átvizsgálás


Elektronikus átvizsgálás

Elektronikus átvizsgáló eszközöket (fémdetektorkaput, röntgensugaras csomagátvizsgáló berendezést, vagy kézi fémkeresőt) lehet telepíteni ellenőrző pont létesítése érdekében, a vállalat épületének vagy meghatározott területének elhagyásakor az átmenő személyek és csomagjaik ellenőrzése céljából. Az ellenőrzési pontokon mindenkinék át kell haladnia, ha azok üzemben vannak. Ezen kívül, az ilyen épületekben vagy különleges kijelölt területeken jól látható módon
minden kijáratnál és ellenőrzési pontnál el kell helyezni azokat a feliratokat, amelyek a „Figyelmeztetés” részben ismertetett azonos tartalmú szöveget tartalmaznak. [59]

Az átvizsgáló berendezésekkel rendelkező összes telephelyen be kell vezetni egy tartalék eljárást is, amelyet a berendezés meghibásodása esetén lehet igénybe venni. A készülékek elhelyezése előtt használatukat, a biztonsági főigazgatónak kell engedélyeznie. Minden vonatkozó jogszabályt be kell tartani.

A vállalat tulajdonát képező, felelős személy megőrzésében lévő tárgyi eszközök

Azoknak a személyeknek, akiknek a birtokában a vállalat tulajdonát képező tárgyi eszköz van, meghatározott engedéllyel kell rendelkeznünk. Ezt az engedélyt maguknál kell tartani a vállalat területén kívül, illetve a kilépési ellenőrzésen áthaladás közben és az engedélyt a biztonsági személyzetnek bemutatni. Az illető személyt fel kell kérni, hogy igazolja magát és mutassa be a tárgyi eszköz elvitelére vagy birtoklására kapott engedélyt. Ha nincs engedély, fel kell kérni az illetőt, hogy a tárgyi eszközt hagyja a vállalat területén vagy menjen vissza az elvitelt lehetővé tévő megfelelő engedélyért. A személyt addig nem szabad feltartóztatni, hogy bűncselekményt készül elkövetni. A vállalat biztonsági személyzetével kapcsolatba kell lépni.

Az együttműködés elutasítása

Amennyiben az illető személy megtagadja az együttműködést a vizsgálat során, az együttműködésének hiányából fakadó következményekre fel kell hívni a figyelmét és meg kell ismételten kérni, hogy járuljon hozzá a vizsgálathoz. Ezen kívül tájékoztatni kell arról, hogy munkaadóját értesítsék az együttműködés megtagadásáról.

Amennyiben az illető továbbra sem hajlandó a vizsgálati folyamatban való együttműködésre, akkor: az illető személyt azonosítani kell, a helyzet körülményeit jelezni kell a biztonsági felettes vezetőnek, tájékoztatni kell a vállalat biztonsági szervezetének illetékesét, a személyt addig nem szabad feltartóztatni, amíg nincs alapos gyanú arra, hogy bűncselekményt készül elkövetni.

4.3 Biztonsági események kezelése, belső vizsgálatok

4.3.1 Biztonsági események

A biztonsági szervezet belső vizsgálatokat végez, annak érdekében, hogy megakadályozza, vagy feltárja azokat a cselekményeket, törvényértések és saját biztonsági eseményeket okoztak, az eseményekkel kapcsolatos fenyegetéseket, erőszakos cselekményeket,
a vállalat értékeinek megkárosítását, vagy azokra potenciális veszélyt jelentő tevékenységeket.

Jogkövetkezményekkel járóható vizsgálatok esetén a jogi osztályal együttműködve kell lefolytatni
az eljárást. Minden biztonsági eseményt és vizsgálatot jelenteni kell a biztonsági főigazgatónak,
különös tekintettel azokra az ügyekre, amelyekbe a hatóságok is be lettek vonva. [6] [55] [72]

Események jelentése

Minden biztonsági eseményt jelenteni kell a biztonsági főigazgatónak. Minden biztonsági eseményt
haladéktalanul azonosítani, jelenti kell, illetve a szükséges intézkedéseket meg kell tenni.

Jelentés:

A következő típusú biztonsági események magas prioritásúak, ezért azonnal jelenteni kell a biz-
tonsági főigazgatóság biztonsági központjába mely állandóan (24/7) működik. Telefonszám: XY

• személyes fenyegetettség,
• természeti katasztrófa,
• terrorista támadás, bomba fenyegetés,
• emberölés, emberrablás, tűszhelyzet, fegyveres elkövetés, szabotázs, robbanás, nagyobb
  vegyszer, vegyianyag kiömlés, szennyeződés,
• bizalmas adatvesztés, kémkedés, lehallgatás, vagy bármilyen más illegális módon elkövetett
  információ, vagy adatvesztés,
• betörés az információ-technológiai hálózatba, hekkertevékenség,
• Jelentősebb lopás, rablás, sikkasztás,
• Biztonsági esemény, mely várhatóan felkelti a media érdeklődését.

Folyamatos státusz jelentésekben kell tájékoztatni a biztonsági főigazgatót.

Biztonsági események meghatározása

A következő biztonsági eseményekről kell tájékoztatni a biztonsági főigazgatót:

• személyi sérülés,
• a vállalat vagyontárgyaiban keletkezett kár, vagy sérülés esetén, amely meghaladja az 100.000
  HUF-t (javasolt összeghatár, kiskereskedelmi érték),
• minden megmagyarázhatatlan leltáreltérést, illetve veszteséget,
• minden fenyegetést,
- bizalmas adatok elvesztését,
- adatokkal illetve adatkezeléssel kapcsolatos visszaélést,
- jogosulatlan hozzáférést a vállalat információs hálózatához, adataihoz, illetve bármilyen zavarkeltés, vagy adatmegsemmisítés a vállalat információ technológiai rendszereiben,
- törvénysértést,
- biztonsági eseményt, törvénysértést, vagy üzleti magatartás megsértését, amely munkavállaló elbocsátását vagy ellene vádemelést eredményezhet,
- biztonsági eseményt, mely várhatóan felkelti a média érdeklődését.

A vizsgálat végrehajtása

A vizsgálat ideje alatt az adatokat bizalmasan kell kezelni. Az adatokhoz való hozzáférésük, csak azoknak a személyeknek lehet, akik részt vesznek a vizsgálatban.

Hatóságok bevonása

A hatóságok haladéktalan bevonása szükséges, azokban az esetekben, amikor a biztonsági esemény olyan jellegű, hogy gyors hatósági intézkedés szükséges személy, vagy tulajdonvédelmi célból. Ilyen események lehetnek például: súlyos fizikai erőszak, illetve az azzal történő fenyegetés, (pl.: támadás, gyűjtőgatás, rablás, stb.). Betörés, betöréses lopás. Olyan biztonsági események esetében, ahol fennállannak a veszélye, hogy más bűncselekmény is megvalósulhat, amennyiben a hatóság nem kerülne értesítésre.

A helyi biztonsági igazgatónak minden esetben jelenteni kell a hatóságok bevonását a biztonsági főigazgatónak. Amennyiben erre lehetősége van, és a késedelem nem jár veszéllyel, úgy a hatóságok értesítése előtt kell tájékoztatni a biztonsági főigazgatót.

Belső jelentés

Minden a fentiekben felsorolt biztonsági eseményt jelenteni kell a biztonsági főigazgatónak. Amennyiben valamilyen változás történik az ügyben, úgy státusz jelentést kell készíteni és a tájékoztatást megadni. Minden biztonsági eseményről készült anyagot, az ügyet formálisan is le kell zárni. A biztonsági esemény ügygazdája folyamatosan értesíti a biztonsági és az üzleti vezetést a fejleményekről.
Külső jelentés

Lehetőség szerint kerülni kell a biztonsági folyamatok, biztonsági operációval kapcsolatos információk, adatok megosztását külső felekkel. Amennyiben ezen információk, adatok közzétételle kötelező (pl.: jogi eljárás során, hivatalos vizsgálat keretében), a biztonsági főigazgatót előzetesen értesíteni kell.

A vállalat alkalmazottainak speciális védelme

Amikor kiegészítő biztonsági intézkedések válnak szükségessé (fegyveres őr, otthoni riasztórendszer, vagy más a család védelmével kapcsolatos intézkedés, stb.) a vállalat területén kívül, akkor azt az addicionális biztonsági intézkedést a biztonsági főigazgatónak minden esetben jóvá kell hagynia.

Heti jelentés

A helyi biztonsági igazgatóknak minden héten jelentést kell készíteni a területükön történt biztonsági eseményekről és biztonsági aktivitásukról a biztonsági főigazgató számára. A heti jelentéseknél (javaslat) hétfőn 12 óráig kell beérkezniük a biztonsági főigazgatóhoz.

Amennyiben a határidőt valamilyen jelentős okból kifolyólag nem sikerül tartani, úgy arról a biztonsági főigazgatót a határidő lejárta előtt értesíteni kell.

4.3.2 Belső vizsgálatok

Általános rendelkezések

A biztonsági szervezetnek ki kell vizsgálnia azokat az eseteket, amelyek a hatáskörébe tartoznak szervezetileg, belső szabályok megsértését, illetve törvényt mérésére utaló eseteket [87]. Ezen ügyek keletkezhetnek különböző helyekről származó információk alapján, vagy a vállalat vezetőségének utasítása alapján, vagy a vállalat vezetőségének utasítása alapján. Különös hangsúlyt kell fektetni a korrupció, a csalás, pályázati folyamatok, összeférhetetlenségi esetek, kereskedelmi, pénzügyi visszaélésekre, fenyegetésekre, vállalati tulajdonok, illetve annak használatával való visszaélésekre illetve a termékek, vállalati eszközök, vállalati adatok és alkalmazottak védelmével, a vállalat hírnevének védelmével kapcsolatos feladatokra. [13] [45] [58] [62]

A biztonsági szervezet szakmai támogatást nyújt a vezetők és alkalmazottak számára az összeférhetetlenségi folyamat során, vizsgálja azokat a körülményeket, amelyek összeférhetetlenséget okozhatnak, valamint ellenőrzi a nyilatkozatokban foglaltak helyességét. Mindezek keretében a biztonsági szervezet információgyűjtéssel és elemzéssel foglalkozó egységei értékkelk a
beérkezett és megszerzett adatokat, amelyek alapján tájékoztatják a vezetőséget, így hozzájárulva támogatják a vezetőket üzleti döntéseik meghozatalában.

A biztonsági szervezet kizárólagos felelőssége a bűnüldöző hatóságokkal történő kapcsolattartás, információcsere, kommunikáció a büntetőeljárások során. A bűnüldöző hatóságoktól érkezett kérelem, információ kérés megválaszolása és együttműködés a biztonsági szervezet feladata. Amennyiben a vállalaton belüli más szervezeti egységhez érkezik ilyen jellegű felkérés, azt haladéklanul továbbítani kell a biztonsági szervezet részére, hogy időben és szakszerűen el tudjon járni a hatósági megkereséssel kapcsolatban. Amennyiben a vizsgálatnak lehetnek jogi következményei, abban az esetben a jogi szervezetet is tájékoztatni kell.

**Vizsgálati eljárások lefolytatása**

Minden vizsgálati eljárás elindítása előtt értesíteni kell a biztonsági főigazgatót. A vizsgálat csak az engedélyezése után indítható.

A biztonsági főigazgató a következő esetekben közvetlenül rendeli el a vizsgálat végrehajtását: saját hatáskörében bármikor, ha a hozzá eljutott információk, vagy jelentések alapján szükségessé válik, más szervezeti egység vezetőjének kérésére, a felsővezetés indítványozására.

Amennyiben a vizsgálatot nem a felsővezetés rendelte el, a biztonsági főigazgató jogosult eldönteni, hogy szükséges-e vizsgálat indítása, avagy nem. Döntéséről és annak körülményeiről a felsővezetést tájékoztatnia szükséges.

**A biztonsági főigazgató felelőssége a vizsgálati folyamatban:**

Koordináció és felügyelet, vizsgálati standardok, eljárások, vizsgálati végrehajtási módszerek meghatározása, abban az esetben, amennyiben fenyegetés, terrorizmus, vagy nagyértékű (pl.: 10 M HUF-t meghaladó) korrupciós ügyről van szó a vizsgálat levezetése az ő kompetenciájába tartozik, eljár minden olyan ügyben, ami komplexitása, érzékenysége, vagy egyéb más okból kifolyólag az ő hatáskörébe kerül, helyi biztonsági szervezet szakmai felügyelete, helyi biztonsági szervezetek ellenőrzése és szakmai támogatás nyújtása számukra, vizsgálati nyilvántartó rendszer kialakítása és fenntartása, minőségbiztosítási intézkedések kialakítása és működtetése.

**A helyi biztonsági szervezetek felelőssége a vizsgálati folyamatban:**

Vizsgálati eljárások végrehajtása a szabályzatokkal összhangban, vizsgálati jelentések küldése a biztonsági főigazgatónak, naprakész információk és jelentések bevitelé a vizsgálati adatbázisokba, folyamatos konzultáció, információcsere a biztonsági főigazgatóval, illetve az általa kijelölt
személyel, minden vizsgálat koordinálása a felelősségi területén, országhatárokon átnyúló vizsgálatok esetében az ügygazda minden esetben az a biztonsági vezető, ahol keletkezett az ügy és együttműködés keretében a másik ország biztonsági vezetője végzi el a saját területén a kért vizsgálatot, majd az eredményeket megosztja a vizsgálatot kérő biztonsági vezetővel.

A biztonsági főigazgató meghatározza a vizsgálati tevékenység ellenőrzési és értékelési rendszerét. Ennek égisze alatt meghatározásra kerülnek a teljesítménymutatók. Mindezen adatokat a helyi biztonsági szervezeteknek naprakészen kell feltölteni egy központi nyilvántartó rendszerbe, meghatározott formátumban, kötelező jelleggel.

Az elsődleges vizsgálati jelentést a helyi biztonsági szervezeti szintnek kell feltölteni a központi adatbázisba, azonosító számmal ellátva, ami lehetővé teszi a könnyű visszakeresését. A vizsgálat lezárásakor a vizsgálat főbb eredményeiről kell egy összefoglaló jelentést készíteni. A jelentést fel kell vinni az adatbázisba, ami garantálja, hogy eljut a biztonsági főigazgatóhoz. Minden jelentésnek, legyen elsődleges, azonnali verziója, ami a vizsgálat indításakor keletkezik és végleges változata, ami már a kész összefoglaló jelentés. Mindkét verziót elkészültek fel kell tölteni az adatbázisba. A vizsgálati adatbázisba feltöltött jelentések tartalmának összehangban kell lennie az ezen kívül készült dokumentumokkal, jelentésekkel, ez minden esetben a készítő szervezet felelőssége.

A vizsgálatot végző érdeke, hogy a lehető legpontosabban és legteljesebben sikerüljön feltárnia minden körülményt, ezért jogosultnak kell lennie hozzáférni minden olyan adathoz, adatbázishoz, amelyek segítséget tudnak nyújtani neki abban, hogy minden egyes a vizsgálattal kapcsolatos rendelkezésre álló információt le tudjon ellenőrizni. [18]

Annak érdekében, hogy a vizsgáló objektív értékelést tudjon adni a vizsgálat tárgyával kapcsolatban, követnie kell a jogszabályi előírásokat és belső utasításokat és kötelez az alábbiak szerint eljárni: teljes mértékben meg kell felelnie a jogszabályi előírásoknak és a belső szabályozásoknak és követelményeknek, különösen az adatvédelmi törvényben foglaltak és a személyiségi jogok tekintetében, megfelelő bizalmassággal kell kezelnie a tudomására jutott információkat, be kell tartania a belső adatosztályozási szabályzatban előírt az adat tartalmának megfelelő adatkezelési előírásokat, követnie kell a biztonsági főigazgató által előírt protokollt és jelentési rendszert, minden esetben egyeztetnie kell vezetőjével, ha más külső szervezetekből, személyektől szükségessé válik adatok bekérése, vagy meghallgatása, dokumentálnia kell a vizsgálati tevékenységét az előírtak szerint.

A vizsgáló a vizsgálati eljárás során hatással lehet az üzletmenetre, ezért azt úgy kell végrehajtania, hogy az üzleti tevékenységet csak olyan mértékben befolyásolja, ami elengedhetetlenül
szükséges a vizsgálati eljárás lefolytatásához és a várható eredmény tükörében arányosan terheli le a vizsgált szervezetet.

A vizsgálat dokumentálása

Minden dokumentum, ami a vizsgálat során keletkezik bizalmasnak minősül és annak megfelelő adatkezelési eljárást igényel. Az adatosztályozási szabályzat előírásai szerint kell eljáarni. A keletkezett bizalmas dokumentumok továbbításánál is be kell tartani az adatosztályozási szabályzatban foglaltakat.

Az elvégzett vizsgálatokat úgy kell dokumentálni, hogy az érthető legyen az olvasására felhatalmazott személyek számára, visszakereshető, könnyen kezelhető legyen, illetve az eredményeket alátámasztó dokumentumok legyenek mellékelve [88]. Amennyiben nemzetközi vállalatról van szó, úgy természetesen az összefoglaló jelentést angolul, vagy ha a vállalat hivatalos nyelve ettől eltérő, akkor azon a nyelven kell elkészíteni.

A dokumentumokat meg kell őrizni, mind a nyomtatott, mind a digitalis formátumban lévőket, az adatosztályozási szabályok szerint.

A vizsgálati jelentésnek a következő részletes adatokat kell tartalmaznia és a következőképpen kell felépülnie: a vizsgálat típusát (a biztonsági főigazgató által meghatározottak alapján), részletes magyarázata azoknak az információknak, amelyek a vizsgálatot indukáltak, az információforrás, helyszíne, időpontja, a vonatkozó jogszabályok és belső szabályzatok megjelenítése, amelyek meghatározzák a kereteket, körülményeket és azt a folyamatot, ami a vizsgálat tárgyát képezi, leíró magyarázatát a kapott információknak a vizsgálat tárgyával kapcsolatban, leíró magyarázatát azoknak az elemeknek, amelyek megsértik a szabályzatokat, folyamatokat, az érintett személyek és felelősségi szintjük beazonosítása a vizsgált folyamatra vonatkozóan, a vizsgált személyek, körülmények és gazdasági társasági kapcsolatok feltüntetése, minden más vonatkozó körülményt, ami a vizsgálati eljárás során lett feltárt, összefoglaló megállapítások (összefoglaló a feltárt hiányosságokról, szabálytalanságokról, ténylegről, amelyek biztonsági szempontból kimutathatóak), javaslatoat (a szabálytalanságok, hiányok megszüntetésére és intézkedéseket, ajánlásokat, amelyek megakadályozhatják a szabálytalanságok újbóli bekövetkezését).

Indokolt esetben, az ügy jellegétől függően, elsősorban vezetői utasításra el lehet térni a fent vázolt vizsgálati jelentési követelményektől, de a jelentésnek tartalmaznia kell a pontos, teljeskörű és érthető formában az esemény leírását a vizsgálat tárgyát és az eredmények részletes megállapításait.
Bizalmasság a vizsgálat során

A biztonsági szervezet vizsgálatot végző tagja bármilyen adatot és információt kérhet minden szervezeti egységtől a vizsgálat területével, témájával kapcsolatban. Minden vezetőnek és alkalmazottnak támogatni kell a vizsgálatban eljáró személyt azzal, hogy minden kért adatot és információt a vizsgáló rendelkezésére bocsájtanak.

A következő feltételekről tájékoztatni kell a vizsgálat kezdetekor a vizsgálat alá vont vezetőket és alkalmazottakat: az a személy, aki a vizsgálatattal kapcsolatosan adatkérést kapott a vizsgálótól arról másnak, kollégájának, vezetőjének, harmadik személynek tájékoztatást csak a vizsgáló előzetes engedélyével adhat. Ennek a kitételnek szerepelnie kell a titoktartási nyilatkozatban. Minden személy, aki valamilyen formában részt vesz a vizsgálatban, csak annyi tájékoztatást kaphat a vizsgálat tárgyáról, ami a tőle elvárt feladatának teljesítéséhez elengedhetetlenül szükséges.

A vizsgálat eredményeinek átadása

A vizsgálat eredményeit a biztonsági főigazgatónak kell benyújtani, amennyiben felülvizsgálta és nem kér kiegészítéseket, intézkedik arról, hogy a vizsgálat eredményeinek megismerésére jogosult vezetők a tájékoztatást megkapják. Amennyiben a feltárt hiányosságok alapján további átfogó, vagy széleskörű vizsgálat is szükségessé válik, abban az esetben az a vizsgálat eredményeinek megismerésére jogosult vezetők a tájékoztatást megkapják.

A bűnüldöző hatóságok bevonása és a hatósági megkeresések kezelése

A bűnüldöző hatóságok megkereséseire olyan folyamatot kell kialakítani, amely keretei biztosítják, hogy az adatszolgáltatás kizárólagosan a biztonsági szervezeten keresztül történhessen. Ezáltal biztonsági a következő feltételek: a vizsgálat eredményeinek megismerésére jogosult vezetők a tájékoztatást megkapják. Amennyiben a feltárt hiányosságok alapján további átfogó, vagy széleskörű vizsgálat is szükségessé válik, abban az esetben a vizsgálat eredményeinek megismerésére jogosult vezetők a tájékoztatást megkapják.

A helyi biztonsági szervezetek rendőrségi feljelentést a biztonsági főigazgató jóváhagyásával tehetnek. Ha a vizsgálat korlátozott hatásfokú, akkor a vállalat jogi, vagy más szervezeti egysége is tájékoztatásra kerülnek. A helyi biztonsági szervezetek a felelősek a bűnüldöző rendvén deltarehatás szükségesére. Az a helyi biztonsági szervezetek megkereséseikben foglaltak teljesítéséért. A szakmai felügyeletet a biztonsági főigazgató gyakorolja.
4.4 Speciális biztonsági feladatok

4.4.1 Utazásbiztonság

A vállalat dolgozóinak biztonsága és védelme érdekében a biztonsági szervezet előzetes tájékoztatást és tanácsokat ad az üzleti utazónak, belföldi és külföldi utazásokkal kapcsolatban. A vállalat dolgozói, üzleti utazásaik során számos biztonsági problémával találkozhatnak. A leggyakrabban tapasztalt problémák: utazás megszakítása, utcai zavargás, természeti katasztrófa, járvány, idegengyűlölet, stb. Az említett okok miatt szükséges a dolgozók figyelmét felhívni ezekre a veszélyes helyzetekre vagy átmeneti korlátozásokra bizonyos országokba történő utazásokkal kapcsolatban. [33] [47] [61]

A biztonsági osztály kérésre átfogó utazásbiztonsági konzultációt tart az utazó részére, hogy felhívja a figyelmet külföldre történő utazáshoz kapcsolódó biztonsági előírásokra.

A biztonság közös ügyünk. Az utazóknak ébernek, elővigyázatosnak kell lenniük, be kell tartaniuk a biztonsági előírásokat az utazásuk során.

Országok kockázatértékelésének rendszere

A biztonsági főigazgató megbízásából a biztonsági szervezet felelős tagja folyamatosan adminisztrálja és frissíti az országok kockázati adatbázisát. Az alkalmazottaknak ajánlott, hogy üzleti utazásaik előtt tájékozódjanak a célország biztonsági helyzetéről. A szükséges kockázati információkat az országokról a vállalat belső intranet oldalán célszerű elhelyezni, hogy minden dolgozó hozzáférhessen.

Utazási elővigyázatosság – sárga jelzés

Ha az adott ország, régió, vagy terület biztonsági helyzete hatással lehet az utazó fizikai, személyes biztonságára, utazási elővigyázatosságra van szükség. Minden földrajzi területen működő biztonsági szervezet felelős a helyi üzleti utazások felügyeletében.

Utazási korlátozás – piros jelzés

“Veszélyes” a besorolás, ha az adott területen, régióban vagy országban fokozott védelmi készültség indokolt a helyi biztonsági helyzet következményeként, ez további korlátozást jelent az üzleti utazóra. Minden földrajzi területen működő biztonsági szervezet felelős a helyi üzleti utazások felügyeletében.
Mikor egy ország besorolása megtörtént, a régió biztonsági igazgató és a vezérigazgató jóváhagyása szükséges az utazáshoz. Ez a szabály érvényes a vállalat alkalmazottaira, esetlegesen velük utazó hozzátartozókra és a vállalat érdekében utazó személyekre.

Az illetékes helyi biztonsági szervezetek regisztrálása kell minden „piros” országból történő utazást. Minden utazási igényt és jóváhagyást fontos dokumentálni és esetleges vizsgálatok miatt ezeket meg kell őrizni.

Ha „piros” országban működik biztonsági szervezet, akkor a helyi biztonsági osztálynak speciálisan az országra és telephelyre lebontott, az országból történő belépés előtti ismertetőt, összefoglalót kell biztosítani a más országból érkező tartós munkavállalók, látogatók, stb. részére. Ezt a dokumentumot folyamatosan frissíteni kell, de évente egyszer minimum felül kell vizsgálni.

A „piros” ország helyi biztonsági szervezetének kötelező az országból érkező tartós munkavállalókat elektronikus formában regisztrálni és a listát naponta frissíteni kell.

A biztonsági főigazgatónak vétójoga van a „piros” országból történő utazásokkal kapcsolatban.

**Szükséges előkészületek**

Ha a fent említett szükséges jöváhagyások már adottak: Annak érdekében, hogy a megfelelő szállást kapja az utazó munkavállaló, a kijelölt utazási szolgáltatóval kell felvennie a kapcsolatot. Az utazó munkavállalónak fel kell vennie a kapcsolatot a fogadó szervezettel az aktuális utazási tanácsokkal kapcsolatban. Az utazó munkavállalónak szükséges a fogadó szervezet számára elköldeni az utazás részleteit (a foglalt járatok menetrendjét, a hotel adatait és kapcsolattartáshoz telefonszámot). A fogadó szervezetnek intézkednie kell, hogy az utazó munkavállaló vagy egy munkatársuk, vagy egy megbízott külsős biztonsági vállalkozó várja a repülőtől. Ha az utazó munkavállaló nem fogja el a repülőt, a fogadó szervezetnek kell biztosítania, hogy az utazó munkavállaló a látogatás alatt megkapja a szükséges biztonsági útmutatást. Az utazó munkavállalónak nem ajánlott, hogy illetékes személy nélkül elhagyja a biztonságos épületet vagy helyszínt.

Ha biztonsági szervezet működik a fogadó országban, az utazó munkavállalónak ajánlott felvennie a kapcsolatot az országos biztonsági vezetővel esetleges biztonsági események esetére. Cél szerű kialakítani egy olyan biztonsági központot, ami a többi biztonsági központ felett áll és folyamatosan hívható 24/7, amit az utazók is tudnak használni információ kérésre-adásra.

Ha a „piros” országból történő üzleti utazást törlik, vagy bármilyen más okból nem valósul meg, esetleg meg kell szakítani vagy az utazási menetrend módosul a biztonsági szervezet jóváhagyása
után: Ha egy „piros” országba történő utazást közvetlenül az indulás előtt törölnek vagy bármilyen más okból meghiúsul, az utazónak haladéktalanul értesítenie kell a vállalat fogadó ország biztonsági vezetőjét (ha létezik ott ilyen pozíció) és az ügyvezetőt/vezérigazgatót. Ha egy várhatlanul felmerülő biztonsági helyzet az oka bármely országban, egy már jóváhagyott üzleti út törlésének, akkor a vállalat a fogadó országban működő biztonsági szervezetét (ha létezik) és az ügyvezetőt/vezérigazgatót az út elhalasztásáról az utazónak haladéktalanul értesítenie kell.

Utazásbiztonság - Alapszabályok

más adathordozón tárolva viszi magával, akkor ugyanazokat az elővigyázatossági előírásokat kell betartania, mint a laptop esetén. Ha az utazó eszközeit ellopják vagy eltünnek az utazás során, az utazónak a vállalat biztonsági szervezetének és a felettesének is jelenteni kell.

**Speciális utazásbiztonsági szabályok a vállalat felsővezetői részére**

A lenti szabályokat a vezetők utazásakor abban az esetben is kötelező betartani, ha más feltételekkel jelentősen kedvezőbb érhető el. Az utazásbiztonsági szabályzat belföldi és külföldi utazásokra is alkalmazandó és érvényes minden utazási formára is (repülőgép, helikopter, teherautó, busz, távolsági busz, autó, hajó stb.). [19]

a) A kivétel az általános szabály alól, ha az utazás vonattal vagy folyami hajóval történik. Ebben az esetben a csoportszintű biztonsági igazgató egyedi elbírálása szükséges, hogy az adott jármű életmentő berendezéssel való felszereltsége és biztonságossága megfelelő az előzetes felmérés alapján.

b) Az elnök és vezérigazgató és a vezérigazgató nem tartózkodhat ugyanazon jármű fedélzetén utazás közben, kivéve az a) pontban említett eseteket.

c) Első szintű vezető maximum két tagja utazhat ugyanabban a járműben, ugyanabban az időben, figyelembe véve az a) és b) pontban foglalt rendelkezéseket.

d) A második szintű vezetés csak két tagja utazhat együtt, és csak egy közülük utazhat együtt egy első szintű vezetővel, vagy az a) pontban említett személyekkel.


f) A tervezett utazást az indulás előtti 72 órával a biztonsági főigazgatónak, vagy az általa kijelölt személynek be kell jelenteni a vonat vagy a folyami hajózás, valamint a bérelt légi járművek bérlese esetén, vagy ha a b) -c) -d) nem lehet betartani.

### 4.4.2 Oktatás

**Oktatás és tudatosság**

A biztonsági főigazgatónak meg kell határoznia a biztonsági oktatás megfelelő menetét és rendszerességét, megalapítását, fejlesztését, illeszkedve az alkalmazandó törvényekhez, szabályokhoz, kötelezettséghoz a működési országokban és megfelel a helyi vezetésnek is. A lenti szempontokat szintén figyelemhez kell venni [21] [26]: minimálisra csökkentsék a vállalat dolgozóinak vagy a vállalat területén tartózkodó személyek fizikai sérülésének kockázatát,
minimálisra csökkentsék a pénzügyi, fizikai vagy szellemi vagyon hűtlen kezelésének kockázatát,
minimálisra csökkentsék a vagyontárgyak károsításának, megsemmisítésének kockázatát,
minimálisra csökkentsék a jogosulatlan belépést, közzétételel vagy megváltoztatását a vállalat
szellemi tulajdonának, katasztrófa esetén gondoskodni az emberek és a tulajdon biztonságáról.

Kötelező Biztonsági tanfolyamok és vizsgák új belépő dolgozók számára

A helyi biztonsági vezető/igazgató felelőssége, hogy az alkalmazottai megkапják a szükséges
oktatásokat és sikeres vizsgát tegyenek a lenti gyakorisággal: általános biztonsági oktatás (2
évente): új belépők, minden munkavállaló, fenyegető telefonok és gyanús csomagok kezelése
(évente): új belépők, minden munkavállaló, biztonsági összeférhetetlenségi oktatás (2 évente): új
belépők, minden munkavállaló, biztonsági vizsgálatok oktatás (2 évente): új belépők, minden
munkavállaló, vállalati kiűrítési tanfolyam és gyakorlat (évente): minden munkavállaló.

4.5 Információbiztonság

Az információbiztonság a biztonság egyik meghatározó eleme, hiszen ma már nem lehet
biztonságról értekezni az információbiztonság mellőzésével. Azok az idők már elmúltak, amikor
még csak a papír alapú dokumentumok, stencilezett példányok, illetve az indigók védelmével, azok
megsemmisítésével foglalkozott a TÜK, vagyis a titkos ügyirat kezelés. Az információbiztonság
ennél ma már jóval többet jelent. A másik végletnek tekinthetjük az úgynevezett „paperless” azaz
papírmentes folyamatokkal működő tevékenységeket, ahol már egyáltalán nem keletkezik papír
alapú dokumentum, már minden számítógépen, a virtuális térben történik. Ezek valóban a
végletek, a legtöbb szervezetnél, vállalatnál mind a papír alapú, mind a digitális információ
megtalálható, és ezek védelméről gondoskodni kell.

Az információbiztonság több, mint az IT biztonság, mert a teljes folyamatok és a papír alapú
dokumentumok védelmével is foglalkozik. Az információbiztonság az IT security-val szemben, ami
főleg a rendszer üzembiztonságát, folyamatos üzemelését biztosítja, a rendszer védelmére
koncentrál. Napjainkban sajnos sok tehetőség hacker, vagy hacker szervezet létezik, de ők sem
mindentudóak. A hackertevékenység általában a nem megfelelően védett rendszerek ellen irányul,
ahol nincs minden teljesen lefedve, megvédve. A rendszerben található hibákat, lyukakat, réseket
támadják, és azokon keresztül szerezhetnek meg jogosulatlanul információkat, adatokat. A
tapasztalatom azt mutatja, hogy egy gondosan megtervezett, megvalósított és üzemeltetett
rendszerbe nem tudnak bejutni jogosulatlanul. Természetesen ehhez hozzáartozik, hogy az
üzemeltetésnek ki kell terjedni a folyamatos felülvizsgálatokra, fejlesztésekre is, és szakadatlanul
figyelni kell a rendszert, itt főleg nem emberi tevékenységre gondolok, hanem speciális IT rendszerekre, amelyek minden a hálózatba érkezett kérést rögzítenek, naplóznak (logolnak), és elemeznek, ha valamit gyanúsnak tartanak, akkor automatikusan, késedelem nélkül riasztanak, igényelve az emberi beavatkozást.


Példaképpen vizsgáljunk meg egy háromszintű adatosztályozási rendszert. A három szint legyen alulról kezdve a következő: első szint a nyílt, azaz publikus információkat tartalmazó szint lenne, a másodikat nevezzük belső használatú dokumentumoknak, és a harmadik, a legszigorúbb szint legyen a bizalmas minősítésű adatok köre. Ezennel beazonosítottuk, vagyis felmérünk az adataink körét, most ezekhez szükséges kialakítani a védelmi szintet. Elő kell írunk, hogy mi a teendő ilyen
dokumentumok védelmével kapcsolatban. Értelemszerűen a nyílt, publikus adatok számára nem írunk elő semmilyen védelmet, hiszen, ezeket az információkat minden korlátozás nélkül meg lehet osztani külsősökkel, harmadik féllel, stb. A második szintű dokumentumok esetében már elő kell írnunk, hogy ezekhez a dokumentumokhoz csak vállalatunk dolgozói férhetnek hozzá. Ezeket külső személyek részére átadni, kiküldeni, stb. nem lehet. Ezeket a dokumentumokat kizárólag a vállalat szerveinek, számitógépeinek lehet tárolni, kinyomtatott példányait nem lehet a vállalat területéről kivinni. A harmadik, a bizalmas dokumentumok szintje, vagyis ezek a dokumentumok a cégen belüli sem elérhetőek mindenki számára, csak egy meghatározott, bizalmas információkhoz való hozzáférésre jogosult körnek, akiknek az információ szól. Értelemszerűen ez a kör mindig más, attól függően, hogy kihez szól, illetve kire tartozik az a bizalmas adat, vagy információ. Ebben a példában említett esetben ezekhez a harmadik szintű dokumentumokhoz kell létrehozni a legmagasabb szintű védelmi rendszert, amely garantálja, hogy csak az arra jogosultak férhetnek hozzá az adatokhoz. Előírhatjuk, hogy ezen dokumentumok csak egy adicionalis védelemmel ellátott szerveren tárolhatóak (erre többféle technikai megoldás is elérhető), kinyomtatott példányaikat csak mások által hozzá nem férhető helyen, elzárva kell tartani.

A következő fontos terület a vállalati levelezés, az e-mailek biztonsága. Bizalmas adatok küldése védelem nélküli elektronikus levélben indokolatlanul nagy kockázatot jelent. Elérhetőek olyan IT megoldások, rendszerek, amelyek az elektronikus levelezés biztonságát tudják szavatolni, mint például a PKI (Public Key Infrastructure, publikus kulcsú technológia). Ez már olyan titkosítási algoritmusokat tartalmazó azonosítási eljárás, ami a mai eszközökkel nem törhető fel. A rendszer által biztosított, hogy csak a címzett tudja elolvasni a levelet, mások számára hozzáférhetetlen marad az információ.

A technikai megoldások mellett szükséges olyan folyamatokat kialakítani, amelyek segítik a bizalmas információk megőrzést, vagyis hozzájárulnak a megvédésükhoz.

A „Clean Desk Policy”-t, a tiszta asztal folyamatot nem győzőm eléggé hangsúlyozni, hogy mennyire fontos a betartása, illetve a betartatása. Lényege, hogy mindenkinek gondoskodni kell arról, hogy amikor elhagyja a munkahelyét, akár csak egy percre is, akkor is, és mindenkor zárja le a számitógépét, a jelszó ismeretének hiánya miatt más ne tudjon hozzáférni a gépén tárolt adatokhoz, illetve mások által hozzá nem férhető helyre zárja el a bizalmas dokumentumait. Ezeket minden esetben meg kell tennie minden dolgozónak. A folyamat betartását a biztonsági szervezetnek ellenőrizni kell munkaidő után és az ellenőrzés tapasztalataira értesíteni kell a munkahelyi vezetőt, illetve a vezetőséget, akiknek el kell járni a vétkesekkel szemben a vállalati bizalmas információk védelmében. Ki kell térni arra is, hogy mi a teendő, ha központi nyomtatót
használ a vállalat, hogyan lehet biztonságosan kinyomtatni a bizalmas dokumentumokat, pl. elküldi a nyomtatóra a dolgozó az anyagot, de csak úgy tudja kinyomtatni, ha már fizikailag is a nyomtatónál tartózkodik, belépőkártyája, vagy más azonosító protokoll szerint azonosítja magát és jelen van a nyomtatásnál.

Hogyan történik a bizalmas dokumentumok megsemmisítése? Alapvetően két módszer lehetséges, melyeket biztonságosan lehet működtetni, egyénileg a dolgozó semmisíti meg a dokumentumokat egy irodai papírdarálón keresztül, vagy központilag történik a megsemmisítés egy ipari méretű daráló használatával. Gazdasági megfontolások alapján a központi megsemmisítő (daráló) használatát látom megfelelőnek. Ezt akkor lehet biztonságosan üzemeltetni, ha az egész folyamat, az egész lánc biztonságossá van téve és nincs benne sehol sem biztonsági rés. Például a vállalatnál el kell helyezni gyűjtőkonténereket, amelyekbe a dolgozók be tudják helyezni a megsemmisítésre szánt dokumentumokat. Ezeknek a konténereknek zárhatóaknak kell lenniük, a kulcsoknak másolhatatlanoknak kell lenniük és a biztonsági szervezet kontrollja alatt kell őket tartani. A konténereknek olyan rendszerűeknek kell lenniük, hogy abból illetékellenek ne tudjanak semmit sem kivenni. A központi helyen lévő iratmegsemmisítőt kamera kontroll alá kell helyezni, illetve, amikor a takarító személyzet, az általa eladott konténernek lévő megsemmisítését szeretné elkezdeni, akkor értesítenie kell a biztonsági személyzetet ügyeletesését, aki a helyszínről irányítja a kulccsal rendelkező kollégát, vagy kollégákat, általuk a konténerek kinyomtatását, és jelenléttükkel végig biztosíthatják a folyamatot, és jelentést készítenek az esetről.

Említem már a fizikai biztonsági folyamatokat, de szeretném felhívni a figyelmet arra, hogy elengedhetetlenül fontos a takarítás, a karbantartás, illetve hasonló folyamatok biztonsági szabályzása, mert felügyelet nélkül elég sok minden megtörténhet [96].

### 4.5.1 Általánosságban

A vállalat különféle információs eszközökkel, értékekkel rendelkezik. Ezek közé tartoznak a különösen értékes védett adatok, mint például az intelligenciás tulajdonság és a bizalmas információk. Ezen értékekvédelme kritikus, mert az adatok elvesztése, ellopása, vagy jogosulatlan használata veszélyeztetheti a vállalat jövőjét. [11] [12] [46] [54] [60]

A sikeres alapvető információbiztonság magában foglalja a vállalat munkavállalói és vezetői által létrehozott, elsajátított és betartott biztonsági eljárásokat [80]. Például egy még be nem jelentett vállalati termék leírásának jogosulatlanan jogosulatlan közjelentése kárt okoz a vállalatnak és jogosulatlan előnyhöz juttatja a vállalat versenytársaikat.
A biztonsági szervezet segíti a vállalat vezetőségét és támogatja a vállalat alkalmazottait a vállalatti adatok és információk védelmében. [2] [17]

A vállalat vezetőinek felelőssége

A vállalat minden vezetőjének kötelessége ismerni és betartani azokat a szabályokat, amelyek szükségessé teszik a vállalat információs értékeinek a megvédéséhez. A vezetők felelősek azért, hogy beosztottaik ismerjék, megértsék és betartsák azokat az információbiztonsági szabályokat, amelyek rájuk vonatkoznak. [1] [22]

A vezetők biztonsági felelőssége többek között, de nem csak kizárólag a következők: Beazonosítja és elszámol a saját területén lévő vállalati értékekkel és biztosítja azok védelmét a megfelelő biztonsági intézkedések bevezetésével. Biztosítja a megfelelő titkosítását és felügyeletét a vállalat tulajdonát képező információknak. Jelent a biztonsági szervezetnek minden olyan cselekményt, visszaélési kockázatot, vélt vagy valós veszteséget vagy olyan hasonló eseményt, ami veszteséget, kárt okozhat a vállalat tulajdonában (információ, vagyoni vagy vállalati alkalmazott sérülése). Ha egy alkalmazott jelenti, hogy egy jelszó biztonsága veszélyeztetve van, kitudódnak véletlen, hanyag vagy szándékos esemény hatására, az érintett információkat tartalmazó rendszer felelősét a lehető legrövidebb időn belül értesíteni kell a kockázat mielőbbi megszüntetése érdekében. Lefolytat átfogó vagyonvédelmi vizsgálatokat a saját felelősségi területén, meghatározott időnként és szükség szerint azonnali vizsgálatokat, ahol biztonsági visszaélés lehetősége felmerült. A biztonsági szervezetet értesíti a jelentős találatokról. Gondoskodik az alkalmazottak biztonság-tudatosságáról és biztonsági felelősségeik megértéséről rendszeres oktatások segítségével, biztonsági kérdések megvitatásával, tanácsadási lehetőséggel és megfelelő biztonsági megoldásokkal, ahol egyszer már visszaélés történt. Tájékoztatja az alkalmazottakat, hogy alapvető követelmény a vállalat egész területén a belépőkártya jól látható helyen való viselése. Megteszi a megfelelő, szükséges lépéseket és jelenti a biztonsági szervezetnek, amennyiben biztonsági szabályokkal való visszaélést tapasztal vagy akár feltételez látogatók, vállalkozók vagy vállalat partnerei részéről. Megbízonyosodik arról, hogy az alkalmazottak tudják, hogyan ismerhethetik fel, jelenhetik és kerülhetik el a káros kódok terjedését, például a számítógépes vírusokat, hálózati férgeket, amik léteznek a vállalaton kívül, de a munkaállomás vagy hálózati rendszerek mégis találkozhatnak ezekkel, hordozható média használatával vagy külső hálózatra csatlakozással. Az oktatások segítségével legyünk biztosak abban, hogy a dolgozók fel tudják ismerni az ilyen jellegű, ártó számítástechnikai vírusokat, férgeket, jelentik az eseteket és megakadályozzák azok terjedését olyan módon, hogy nem használnak magántulajdonú adathordozókat a vállalat tulajdonát képező munkaállomásukon és a

Munkavállalók felelősségeinek összefoglalása

A vállalat minden dolgozója felelős a rabszolgált értékeket megvédéséért, az információt is beleértve. Az alkalmazottak biztonsági felelőssége többek között, de nem kizárólag a következők:

Megérti és betartja a vállalat biztonsági szabályait: információ osztályozása, szabályozása, információs rendszerek biztonsága és használata (jelszó és internetes használat), helyi sajátos biztonsági szabályzatok, szabályok házirendek. A vállalat belépőkártyáját mindig látható helyen viseli a munkavégzés helyén. Felismer minden olyan helyzetet és eseményt, ami a vállalat tulajdonánában kár okozhat, visszaéléshez, lopásához vezethet. Jelent a biztonsági szervezetnek minden olyan cselekményt, visszaélési kockázatot, vélt vagy valós veszteséget vagy olyan hasonló eseményt, ami veszteséget, kárt okozhat a vállalat tulajdonában (információ, vagyoni vagy vállalati alkalmazott sérülése).

4.5.2 Tiszta asztal folyamat

Az intézkedés célja, hogy meghatározza, hogyan maradjanak biztonságban a vállalat titkos és bizalmas információi a munkavállaló távollétében is.

Irányelv:

A vállalati titkos és bizalmas információt tartalmazó dokumentumokat nyomtatáskor haladéktalanul el kell hozni a nyomtatóból. A már nem szükséges vállalati titkos és bizalmas információt tartalmazó dokumentumoknál a megsemmisítőt kell használni.

Összefoglalás

Minden vállalati titkos és bizalmas információt, iratot, számítógépes adathordozót zárható szekrényben kell tartani. Laptopokat biztonsági kábellel megfelelően rögzíteni kell. Irodát, szekrényeket és a fiókokat be kell zárni távozáskor. A mobiltelefonokat, táblagépeket jelszóval le kell zárni.

Néhány példa arra, hogy mit nem lehet felügyelet nélkül hagyni: jelszó, titkos iratok, bizalmas iratok, belső céges dokumentumok, IP címek, szerződéseknél és szerződéseknél vázlata, számlaszám, szellemi tulajdon, alkalmazottak személyes adatai, társadalombiztosítási szám, iskolai végzettség, egészségügyi információk, pénzügyi adatok.

Fegyelmi intézkedés:

Az előírás megsértése figyelmeztetést vagy jogi lépésekkel vonhat maga után. Továbbá a munkavállalók elveszíthetik a vállalati belépési jogosultságait vagy bizonyos esetekben polgári vagy büntetőjogi per indulhat ellenük.

4.5.3 Bizalmas iratok megsemmisítésének szabályozása

A vezetőknek meg kell határozni az ellenőrzés követelményeit, ami biztosítja, hogy jogosulatlan személy ne tudjon beleolvasni, vagy ne tudja eltávolítani megsemmisítés előtt a vállalat bizalmas dokumentumait. A biztonsági szervezet szükség szerint tanácsokat és segítséget ad.

Három módja létezik a bizalmas dokumentumok megsemmisítésének:

- A vállalat területén a dokumentumok tulajdonosa végzi a megsemmisítést.
- A vállalat területén, egy központi helyen történik a megsemmisítés.
- Külső helyszínen történő megsemmisítés beszállító által.

A vállalat területén keletkezett bizalmas, megsemmisítésre ítélte iratok összegyűjtését, szállítását, megsemmisítését, végezhetik szerződött partnerek a következő feltételekkel: Érvényben lévő szolgáltatási szerződést, megfelelő titoktartási záradékkal történő kiegészítése és aláírata a közvetlen partnerrel. A szerződött cégek rendelkeznie kell bizalmaságát és titoktartási szerződésnek, amit minden munkatársával aláírat, akik titkos dokumentumok megsemmisítését végzik. Felügyelete, vizsgálata és ellenőrzése a bizalmas iratokat tároló konténereknek és területeinek.
Minden bizalmas iratokat tároló konténernek védelme illetéktelen hozzáféréssel szemben. Konténeres vagy bálázott papírhulladék szállítása külső helyszínre megsemmisítés céljából, kizárólag zárható járművel történhet. A szállított mennyiséget induláskor és érkezéskor is ellenőrizni kell.


4.5.4 Külső értekezletek

Ha a vállalat vezetősége úgy dönt, hogy egy értekezlet külső helyszínen legyen megtartva, a biztonsági szervezetnek segítséget, ajánlásokat, tanácsokat kell adni a megbeszélés biztonságos lefolytatásához: [25]

Ha a megbeszélésen bizalmas információ is elhangozhat, a megbeszélés szervezését elrendelő vezető felelőssége a biztonsági szervezet előzetes értesítése, hogy végre lehessen hajtani a következő intézkedéseket: A biztonsági szervezet felméri a helyszín biztonsági kockázatát és a szükséges mértékben biztonsági intézkedéseket, ellenőrzéseket javasol, hogy az esemény lefolyása biztonságos legyen. Meghatározza a megfelelő intézkedéseket annak érdekében, hogy az adat- és információcsere a vállalat szabályzatának megfeleljen. Ha szükséges, öröket biztosít a helyszínre. Szükség esetén egyéb biztonsági intézkedéseket ajánl. Vezeték nélküli mikrofon és hang, vagy videó rögzítésre alkalmas készülékek használata nem támogatott olyan külső helyszínen tartott megbeszélésnél, ahol bizalmas információik is elhangozhatnak. Ha kép és hang rögzítése szerepel a szerződésben, a beszerzési osztálynak ki kell azt egészítene titoktartási megállapodással. Bizonyos esetekben a biztonsági szervezet a külső helyszín tárgyalóinak elektromos átvizsgálására kérhetik fel. Ez kivételes eljárás és csak a rendszeres átvizsgálás.
eredményes. Az ilyen vizsgálatok szükségességét alaposan fel kell mérni. A fentieken kívül, a biztonsági szervezet szükség esetén értesítheti az EMK (Egészségvédelem, Munkavédelem és Környezetvédelem) szervezetet is, hogy szintén vizsgálhatják a megbeszéléls körülményeit.

4.5.5 Adatosztályozási szabályzat

Általános szabályok

A bizalmas információk, adatok és a felhalmozott tudásvagyonya a vállalat tulajdona. A vállalat minden munkavállalója felelős a bizalmas információk megtartásáért, séreltlenségéért és a vállalatnál keletkező, hozzáférő, módosított, tárolt adatokért, függetlenül attól, hogy az adat milyen közegben és milyen formátumban található (elektronikus, papíralapú vagy egyéb formátum). [30] [38]

A szabályzat megsértése fegyelmi eljárást vonhat maga után, akár elbocsátást és/vagy jogi lépéseket. Megszegés esetén a biztonsági szervezet, információbiztonsági részlegét értesíteni kell. Ha az adott helyszínén a helyi biztonsági szervezetnél nem található külön információbiztonsági osztály, ilyen esetben a vállalati biztonság következő, magasabb szintje felé kell jelezni a visszaélést.

Adatfelhasználó

Adatfelhasználó az adatokkal kapcsolatban lévő, azokat munkavégzés céljából felhasználnó személy, szervezet, entitás. Az adatfelhasználó felelőssége, hogy az adatokat a szabályzatnak megfelelő módon kezelje.

Adatfelelős

Az adatfelelős általánosságban az a személy, aki felelős az információs értékekkel kapcsolatosan az üzleti folyamatokért. Az adatfelelős tudja, hogyan keletkezik az adat, jól ismeri átadásának, tárolásának, törlésének és egyéb feldolgozásának folyamatát. Az adatgazda felelős az információ kiértékelésért osztályozásért, besorolásáért. Az osztályozás során, ha szükséges, időszakos osztályozás is alkalmazható, megadja a lehetőséget, hogy később más besorolást kapjon az információ. A besorolási jelzés mellett ezt fel kell tüntetni. Mielőtt külső felhasználásra kerülne bármilyen vállalatot érintő adat, információ, az adatfelelősnek a besorolást illetően egyeztetni kell.

Az adatfelelőst értesíteni kell, ha az információ hozzáférését meghosszabíttották vagy módosították.
Bármilyen titkos információ hozzáférési jogosultságát érintő változást megfelelő módon dokumentálni kell, amiért az adatgazda a felelős. Az adatgazda szintén felelős az adatleltár létrehozásáért, karbantartásáért és frissítéséért.

**Adatleltár**

Az adatleltár olyan lista, amely tartalmazza a dokumentumok típusait egy adott szervezetben. A leltár meghatározza a fő tulajdonságokat, az osztályozást és az üzleti adminisztrátorokat. A leltározást frissíteni kell, ha bármilyen változás történt, de minimum évente egyszer.

**Folyamatos védelem**

Az információt védeni kell elévüléséig, a keletkezésétől a megsemmisítéséig. A védelmi szint az információ érzékenységének megfelelően nő, függetlenül attól, hogy milyen formában, hol található, mi a célja, hogy kezelik [81].

4.5.6 **Adatosztályozás**

A vállalaton belül (a javasolt példa szerint) az adatok négy osztályba sorolhatóak. A négy osztály (információs szint) az információ jelentőségével, értékével függ össze. Az információ besorolása az “élettartama” alatt változhat. Ezekben az esetekben a besorolási változások dátumát jelezni kell.

(Például az éves pénzügyi jelentés a publikálás előtt bizalmas információ, de utána nyilvános. A dokumentumon ezt fel kell tüntetni.)

A jelölésnek meg kell felelnie a definícióban szereplő feltételeknek. A jelölés használata kötelező, de az információ típusának legjobban megfelelő formában.

Az elektronikus dokumentumokon úgy kell jelezni a besorolást, hogy az a nyomtatáskor is látható legyen. (Például elektronikus levelezésnél a fejlécben vagy a tárgyban.)

Papíralapú dokumentumok érkezésekor bélyegzővel lehet biztosítani a címzettnel, hogy oda írja be a jelzést.

Ha az adatosztályozási jel nem helyezhető el a dokumentumon nyomtatás előtt (például rendszerből való nyomtatáskor), a nyomtatás után azonnal pótolni kell. Az adatosztályozásnál a legnagyobb körültkintéssel kell eljárni.

**Publikus / Nem titkosított adat – zöld jelölés** (a jelölés lehet egy csik, egy ábra, pl. kör, háromszög, stb.)

Ehhez az információs osztályhoz tartozhat például: éves gazdasági jelentés, Elikai Kódex vagy a vállalat honlapján található információk, adatok.

**Vállalati belső adatok – sárga jelölés**


Bármilyen adatot egyértelmű jelölés nélkül, belső adatként kell kezelni.

**Vállalati bizalmas adat – narancs jelölés**

Bizalmas adat az az információ, ami személyes, bizalmas, valamilyen szempontból védeni kell illetéktelen betekintéstől, módosítástól, továbbítástól és felhasználástól.

A vállalati bizalmas adatokba csak a jogosult személyek nyerhetnek betekintést. Abban az esetben, ha külső partner bevonása feltételezve szükséges, akkor a titoktartási megállapodás aláírhatása elengedhetetlen.

Azok az információk, amelyek felfedése, sérülése negatív hatást gyakorolna a vállalat üzleti eredményeire vagy kockázatná egy üzlet sikerét, bizalmas információként kell kezelni. Személyes adatokat tartalmazó dokumentumok szintén bizalmasak.

Példa a bizalmas adatokra: HR adatok, befektetési tervek / ajánlatok, ügyfelek adatai, projekt tervezetek, kutatás / fejlesztés adatok, termelési adatok, stb.

**Fenntartott információs osztály**
A következő osztály tagja az adatosztályozási rendszernek, de csak az alkalmazottak szűk csoportja találkozik ezel a legbízalmassabb adatvédelmi osztálytal. Csak jogosult adatgazdák használhatják ezt az osztályt.

Vállalati titkos adatok – piros jelölés

A „piros” információs osztályozást csak a vállalat felsővezetői használhatják. A titkos adatok információkezelési szabályzatát külön dokumentumban kell meghatározni.

Egyéb szabályok

Alapvetően a vállalatot érintő minden adatot meg kell védeni. Minden adat adatosztályozását rendszeres időközönként ellenőrizni kell, a használatától, adat érzékenységétől és fontosságától függően. Az adatosztályok biztonsági szintjét meg kell határoznia. Információs forrásokat kategorizálni és védeni kell a követelményeknek és az adatosztályozási kategóriának megfelelően. Az adatosztályozási besorolás és az osztályhoz tartozó biztonsági szint másoláskor vagy áthelyezéskor nem változtatható. [7]

4.5.7 Adatkezelési szabályok

A fent említett kategóriákba sorolt dokumentumok az adatosztályozási besorolásuk szerint különböző kezelést igényelnek. A fő szabályok a következők:

Publikus adat (zöld)

Nincs speciális követelmény. Külső kommunikációs szabályok vonatkoznak rá.

Vállalati belső adat (sárga)

Fő adatkezelési szabályok: Elektronikus dokumentumok bármilyen IT rendszerben és a vállalathoz tartozó bármelyik számítógépen tárolhatóak. Ésszerű elővigyázatosság elvárt az információk gondatlan felfedése védelmében.

Vállalati bizalmas adat (narancs)


Vállalati titkos adat

A vállalati titkos adatok kezelését külön dokumentumban kell szabályozni. Az adatosztályozással kapcsolatos kérdéseket a biztonsági szervezet felé kell jelezni.

4.6 Krízismenedzsment

Egyre többet hallani mostanában a katasztrófa elhárításról, vész helyzeti tervezésről, üzletfolytonossági tervekről, amelyek elengedhetetlenek egy vállalat működtetéséhez, de ugyanakkor azt is tapasztaltam, hogy nem mindig egységesen értelmezik, még a biztonsági kollégák sem ezeket a fogalmakat, nem pontosan ugyanazt gondolja mindenki egy folyamat, vagy elnevezés mögé, illetve időnként nem a helyes meghatározás kerül használatba egy folyamat kapcsolatban. Az üzletfolytonossági folyamat (ang.: Business Continuity Management, röv.: BCM) mindenki tart, talán fél is, mint „ördög a tömjénfüsttől”, de szerintem nem kellene. A távolságtartás abból eredhet, hogy nem teljesen ismert a folyamat, illetve, ha hallottunk róla, akkor leginkább IT BCM-ről, üzletfolytonosságról hallottunk, ami az üzletfolytonosságnak csak egy része. Az üzletfolytonosság magában foglalja a krízishelyzetet (ang.: Crisis Management, röv.: CM), válságkezelést és a vész helyzeti folyamatot (Emergency Management, röv.: EM), készenlétet, válaszlépésekét. Ez a három terület szorosan összekapcsolódik és egymásra épül.
Az üzletfolytonossági folyamatban meg kell szólítani a különböző üzleti területeket, és megkérni őket, hogy azonosítsák be a krízisfolyamatokat, illetve azokhoz tartozó munkaköröket, majd ezek alapján dolgozzák ki a vállalat üzletfolytonossági terveinek összevonásával a vállalat üzletfolytonossági terve is.

16. ábra Válságkezelés helyzete az üzletmenet-folytonosságban (saját szerkesztés)

17. ábra A válságkezelés bizonyított eredménye (saját szerkesztés)
Nézzünk egy példát, tételezzük fel, hogy egy termelő üzemről beszélünk, ahol létfontosságú az alapanyagok, segédanyagok, stb. időben történő beérkezése és rendelkezésre állása. Tehát az alapanyag ellátás egy krízisfolyamat a vállalat és az üzletfolytonosság szempontjából. Ha nincs alapanyag, mert például valamilyen okból kifolyólag a beszállító nem tud szállítani, akkor nem lehet termelni, nem lesz bevétel. Két megoldás lehet, az egyik, hogy biztonságos szintre hozzuk fel az alapanyag készletet, illetve alternatív beszállítók után néz a vállalat, hogy biztosítsa tudja a termelés zavartalanságát. Nagyon fontos, hogy az üzletfolytonossági terveknek előre el kell készülniük és folyamatosan felül kell azokat vizsgálni, illetve módosítani, amennyiben szükséges.
Ha nem vagyunk ezen tervek birtokában, akkor egy vész-vagy krízishelyzet esetén sokkal több időbe és pénzbe fog kerülni a termelés normál szintű visszaállítása.

Vegyünk egy másik példát a biztonsági szervezetek életéből, van egy kolléga a biztonságtechnikai csapatban, aki mondjuk a kamera-, vagy a beléptető-rendszer felelőse, ismeri csínját-bíjút, valószágosan márga a rendszernek. Ez nagyon örvendetes a szervezet szempontjából, de ugyanakkor nagyon kockázatos is, mert mi történik, ha ez a kolléga kiesik a munkából egy időre, egy baleset, betegség, vagy családi események miatt? Igaz, szokták azt mondani, hogy pótolhatatlan ember nincs, de egy jó szakembert nyilvánvalóan nem lehet egy pillanat alatt „a szögről leakasztani”. Ebben az esetben úgy tudjuk kizárni ezt a kockázati tényezőt és biztosítsa a saját szervezetünkön belül az üzleti folytonosságot, ha legalább egy másik kollégával is betanulhatjuk a rendszert és biztosítsuk, hogy folyamatosan figyelemmel tudja kísérni azt a területet is, amit ugyan nem ő működtet, de alkalom adtá neki kell majd belépnie és ideiglenesen, de megfelelően vinnie azokat a feladatokat.

A vészhatályozat folyamatnak domináns részét képezik a vészhatályozat tervek, amelyek biztosítanak egy vészhatályozat készenléletét, és meghatározzák, hogy különböző vészhatályozatok esetén milyen válaszlépéseket kell megtenni, illetve ezeket a válaszlépések megvalósítását szervezetünknek kell végrehajtani, kik a felelősök. Egy egyszerű példával elve: tűz esetén mi a teendő és az kinek a feladata, pl.: tűzjelzés, tűzoltóság értesítése, tűzoltás, stb. Sajnálatosan, nem minden vészhatályozat lehetséges elhárítani, megoldani, előfordulhat, hogy egy vészhatályozat kritikus okokból folyamatosan figyelemmel tudja kísérni azt a területet is, amit ugyan nem ő működtet, de alkalom adtá neki kell majd belépnie és ideiglenesen, de megfelelően vinnie azokat a feladatokat.

A vészhatályozat folyamatnak domináns részét képezik a vészhatályozat tervek, amelyek biztosítanak egy vészhatályozat készenléletét, és meghatározzák, hogy különböző vészhatályozatok esetén milyen válaszlépéseket kell megtenni, illetve ezeket a válaszlépések megvalósítását szervezetünknek kell végrehajtani, kik a felelősök. Egy egyszerű példával elve: tűz esetén mi a teendő és az kinek a feladata, pl.: tűzjelzés, tűzoltóság értesítése, tűzoltás, stb. Sajnálatosan, nem minden vészhatályozat lehetséges elhárítani, megoldani, előfordulhat, hogy egy vészhatályozat kritikus okokból folyamatosan figyelemmel tudja kísérni azt a területet is, amit ugyan nem ő működtet, de alkalom adtá neki kell majd belépnie és ideiglenesen, de megfelelően vinnie azokat a feladatokat.
ahol a vállalat működtetése és a krizishelyzetek elhárítása szempontjából minden kulcsfontosságú terület a legmagasabb szinten képviselve legyen. Minden vezetőnek kell, hogy legyen legalább egy helyettese, aki az ő távollétében tudja helyettesíteni. A krízismenedzsment vezetőségét ki kell oktatni a krízishelyzetbeli feladatára. A krízismenedzsment vezetőségét legalább évente egyszer össze kell hívni, ahol frissítő jellegű oktatást kell számukra biztosítani. Át kell tekinteni a krízismenedzsment folyamatát, időszerű módosításokat tehetnek, illetve célszerű egy szimulációs gyakorlatot is tartani, hogy biztosítani tudjuk a lehető legmagasabb szintű készenlétet, ezáltal biztosítva a leghelyesebb döntések meghozatalát egy valós krízishelyzet bekövetkezésekor.

Elengedhetetlenül szükséges a kiürítések begyakorlása ismétlen gyakorlatok által. Vészthelyzetben csak a begyakorolt tevékenységek működnek, ha ilyenek nincsenek, akkor jobb esetben nem biztos, hogy célvezető rögtönzőségeken, illetve legrosszabb esetben óriási pánikkal és zűrzavarral számolhatunk. Nem értek egyet azzal a véleménymel, hogy magunk ellen hangoljuk a dolgozókat. Szerintem a legtöbb kollégánk tisztában van a gyakorlatok szükségességével. Természetesen manapság „divatos, menő” dolog zúgolódnia, „hogy már megint ki kellett jóni az irodából, mert meleg van, vagy éppen hideg, de különben is milyen fontos munkát kellett félbehagyni, stb”.

Valójában belül mindenki vágyik a biztonságra, még a hőbőrgök is, sőt, ha látnak ilyenkor a gyakorlatok során például egy tűzoltót munka közben, akkor azt képesek önfeledten figyelni és csodálni is. A kiürítéshi gyakorlatoknál biztosítanunk kell, hogy a lehető legrövidebb időn belül legyenek képesek a dolgozók elhagyni a veszélyeztetett zónát, zónákat.

Ennek érdekében jól láthatóan ki kell jelölni a menekülési útvonalakat, a vészkijáratokat, illetve gyűlekezési pontokat kell kialakítani. Nagyon fontos, hogy mindenhol jól hallható kihangsúlyozó rendszerrel szereljük fől a létesítményeinket. Az összes technikai rendszert folyamatosan, lehetőleg hetente, de legfeljebb havonta tesztelejük le, hogy megfelelően működnek-e, illetve, ha bármilyen problémát észlelünk, azt haladéktalanul orvosoljuk, javítassuk ki. A dolgozókat ki kell oktatni, hogy mi a teendő vészthelyzet esetén, a hangjelzés esetén azonnal, a lehető legközelebbi vészkijáraton keresztül hagyja el az épületet és menjén a kijelölt gyűlekezési pontra és ott tartózkodjon, míg más utasítást nem kap. A biztonsági szervezet feladata egy kiürítés során, hogy leellenőrizze, hogy minden helyiséget elhagyat-e a dolgozók, illetve megakadályozza, hogy a már kiürített épületekbe bármik visszatérjen. Ha valaki nem hajlandó részt venni a kiürítésben, arról a személyről jelentést kell készíteni, és a vezetőjénél kezdeményezni a fegyelmi eljárást. A vészthelyzeti gyakorlatot, kiürítést a megfelelő fontossággal kell kezelni.
Nagyon sok múlik azon, hogy a krízismedenyszment egy működő folyamat legyen a vállalatoknál, mert csak így lehet biztosítani a vállalat értékeinek a megfelelő védelmét egy krízishelyzet folytán [97].

**Általános szabályok**

A vállalatnál létrehozott krízismedenyszment rendszer célja, hogy egy krízishelyzet esetén csökkentse annak hatásait a vállalat működésére, az alkalmazottak jólétére, egészségére, biztonságára, illetve a környezetre vonatkozólag. A rendszer létrehozza a krízis készültségi szintet, a reagálási modellt és a kidolgozott stratégiát és eljárásokat egy bekövetkezéndő krízishelyzet esetén. [3] [56] [86]

A vállalat krízismedenyszment rendszere meghatározza a vállalat krízismedenyszment készültségét és a reagálási modellt, íránymutatást ad a krízismedenyszment tervek elkészítéséhez, meghatározza a vezetőség és az alkalmazottak szerepét és felelősségét a krízismedenyszment folyamatban.

A krízismedenyszment rendszereinek kapcsolódni kell az általában a vállalat munkavédelmi szervezetéhez tartozó vészhelyzeti folyamathoz. A vészhelyzeti folyamat az azonnali taktikai válaszok megvalósításával foglalkozik egy egészségügyi-, munkavédelmi-, és környezetvédelmi vészhelyzet esetén, amíg a krízismedenyszment rendszer a magasabbszintű stratégiai kérdésekkel, illetve az azokra adandó válaszokkal foglalkozik mindenféle krízis esemény esetén. [5]

![18. ábra A vállalat krízismedenyszment rendszere (saját szerkesztés)](image)
Krizishelyzet reagálási modell

A vállalat krizishelyzet reagálási modellje biztosítja a vezetők részére azokat az irányelveket, amelyek mentén megfelelő válaszlépéseket lehet kidolgozni a felmerült kérdések megoldására. Ezen iránymutatások az egészség-, munka-, és környezetvédelmi incidensek súlyosságának szintjét veszik alapul. [28] [29]

A szintek a következők:

- **1-es szint – enyhe** jellegű egészség-, munka-, környezetvédelmi incident, kontrollált, vállalat általi reagálás, vész helyzeti válaszlépés.
- **2-es szint – közepes** jellegű incident, kontrollált, kooperatív válasz szükséges, esetleges média visszhang– vész helyzeti válaszlépés/krizismenedzsment.
- **3-as szint – súlyos** incident, nem lehet kontroll alatt tartani – krizismenedzsment.

Ez az események súlyosságán alapuló háromsíntú rendszer határozza meg a válasz módzatait. A szintek minősítés rendszere a vész helyzetek súlyossága és az azokra adandó szükséges válaszlépések szerint épül fel.

**1-es szintű válaszlépés:** a helyi esemény a következő jellemzőkkel rendelkezik: enyhe jellegű egészség-, munka-, környezetvédelmi esemény, vész helyzet, ami lokális kontrol alatt tartható, olyan vész helyzet, ami a vállalat területén történt, helyi erők hatékonyan tudják kezelni a vész helyzetet mind emberi, mind technikai erőforrások tekintetében, a vész helyzeti válaszlépések a helyi vész helyzeti vezetőség által vannak kezelve, szükség esetén az önkormányzati tűzoltóság, vagy más külső vész helyzeti reagáló szervezet bevonásával, a helyi média követi figyelemmel a vész helyzet kezelését.

** Példa:** egy helyszíni baleset, valamilyen környezetszennyező anyag kiömlése, mely a legrövidebb idő alatt megszüntetésre került.

**2-es szintű válaszlépés:** kooperatív válasz szükséges, a következő jellemzőkkel rendelkezik: közepes jellegű egészség-, munka-, környezetvédelmi esemény, vész helyzet, ami kooperatív együttműködést igényel, helyi erők nem képesek a vész helyzetet önmaguk kezelni, nem elegendő az emberi és/vagy technikai erőforrásai, országos média követi figyelemmel a vész helyzet kezelését.

** Példa:** környezetszennyező anyag kiömlése és személyi sérülés.

**3-as szintű válaszlépés:** Krizismenedzsment bevonása szükséges, a következő jellemzőkkel rendelkezik: súlyos jellegű egészség-, munka-, környezetvédelmi esemény, vész helyzet, ami
kooperatív együttműködést és a krízismenedzsment bevonását igényli, jelentős kormányzati figyelem és jelenlét, súlyos következményekkel járó emberi és környezeti hatások, a vállalat helyi, országos, vagy nemzetközi működésében zavarok, leállások keletkeznek, országos és nemzetközi média követi figyelemmel a krízishelyzet kezelését.

**Példa:** környezetszennyező anyag hosszantartó kiömlése, robbanás, több személyi sérülés.

**Krízishelyzetekre való felkészülés és válaszadási stratégia**

A vállalat krízismenedzsment rendszere létrehozza a strukturált és szisztematikus folyamatát az eseményekre adott válaszoknak olyan helyzetekben, amelyek veszélyt jelentenek a vállalat tevékenységére egészség-, munka-, és környezetvédelmi szempontból.

A krízismenedzsment rendszer olyan menedzsment és kommunikációs kérdésekkel foglalkozik amelyek segítségével a hatékony válaszlépések kialakíthatóak. Nem célja, hogy iránymutatást adjon az egészség-, munka-, és környezetvédelmi incidensek helyi kezelésére, ezeket a kérdéseket a vészhelyzeti folyamat fedi le.

**A vállalat háromszintű krízis készültségi és reagálási stratégiája tartalmazza:**

- **Incidens menedzsment** vagy taktikai válaszlépések bevezetése helyi szinteken. A helyi vészhelyzeti folyamat támogatása a helyi krízismenedzsment által.

- **Probléma menedzsment** vagy stratégiai válasz bevezetése a megfelelő országos szinten, vagy nemzetközi szinten.

- **Probléma menedzsment fő kategóriái:**
  - **emberek:** emberi élet, egészség és jólét védelme, környezet:
  - **környezet:** környezet védelme, **értékek/vagyón**, felmérni a krízis hatásait a jelenlegi és a jövőbeni üzletmenetre, kommunikálni a pénzügyi osztályokkal, a szükséges pénzeszközöket biztosítani, megfelelő információ és költségvédelmi szerepet tölteni.

  - **Hírénv:** elismerni a felelősséget, közvélemény tájékoztatása, kommunikálni az alkalmazottakkal, a kormányzattal, médiával, résszvényesekkel, felsővezetők mozgósítása.

  - **Kommunikáció** világos és következetes bejelentésben szükséges.

Ebben ki kell emelné, hogy a vállalat teljes mértékben elkötelezett a helyzet megoldásában és létfontosságának tekinti a sikeres válaszlépések bevezetését. A bejelentés/tájékoztatás nem csak a média számára szól, ugyanezt a tájékoztatást kell alkalmazni az alkalmazottak, ügyfelek, partnerek, kormányzati szervek és nem kormányzati szervezetek esetében is [83].
Ez a tájékoztatás négy fő elemből áll: elkötelezettség, együttműködés a kormányzattal, felkészültség, végrehajtás.

Alapvetés, cél és kapcsolat a tervek között

Annak a vállalati egységnek van elsődleges felelőssége a válaszlépések bevezetésében, amely felelősségi területén történt az esemény, kivéve, ha a vállalat vezetősége másképpen nem határozott. Az incidensek kezelését általában a lehető legalacsonyabb, helyi szinten szükséges megoldani. [4] A vállalat legmagasabb szintű krízismenedzsmentje határozza meg a válaszlépések folyamatát, struktúrját, azonosítja és meghatározza a stratégiai kérdéseket és támogatja a lokális krízismenedzsment folyamatait. A folyamat rugalmas, lehetővé teszi, hogy a vállalat vezetősége által kialakított legmagasabb szintű krízismenedzsment megfelelő személyi összetételének kialakítására, hogy az megfeleljen a mindenkor hely

A legmagasabb szintű krízismenedzsment feladata: kapcsolat létrehozása a helyi krízismenedzsmenttel, támogatni a helyi krízismenedzsment tevékenységét, az üzletmeneti igények szerint, beazonosítani a stratégiai kérdéseket, felmérni és elemezni az incidens lehetséges hatásait, az események kezelésének biztosítása a lehető legalacsonyabb szinten.

A következő ábra mutatja be, hogy hogyan kapcsolódnak egymáshoz a különböző szintű tervek a helyi vészhelyzeti tervektől a legmagasabb szintű krízismenedzsment tervekhez, összhangban a krízishelyzetekre való felkészültséggel, illetve az ezekre adott válaszlépésekkel:
Az országos szintű krízismenedzsment folyamat fedi le a kormányzati szervek, szabályozó hatóságok, országos média részéről felmerült kérdéseket, megkereséseket, amelyekben elvárják az országos vezetőség válaszát. A helyi krízismenedzsment kezeli a stratégiai kérdéseket és lehetővé teszi, hogy a helyi vészhelyzeti menedzsment kezelni tudja a taktikai kérdéseket a helyi vészhelyzetekre való reagálás során.

Milyen esetekben szükséges összehívni a krízismenedzsmentet? [14] Nagyobb folyamat hibák esetén: robbanás, tüzhelyzet, veszélyes anyag kiáramlás, támadás esetén (terrorizmus, bűncselekmény), közüzemi betáplálások zavara esetén, amelyek jelentős hatással vannak az üzletmenetre, természeti katasztrófák (árvíz, földrengés, stb.).
A tervek aktiválásának feltételei:

Válság kérdések

A vezetőknek és krízismenedzsment tagoknak tisztában kell lenniük azzal, hogy az alábbi kérdésekre adott válaszok befolyásolhatják a válaszlépések kialakítását.

- A vállalat felelős az incidens kialakulásáért?
- Fel lettek mérve az incidens következményei?
- A megfelelő tájékoztatások/bejelentések megtörténtek?
- A vállalat érte a szabályozó hatóságok igényeit és beavatkozásuk szükségességét?
- Tudják helyi szinten kezelni a helyzetet?
- Minden dokumentációs folyamat működik a vállalat érdekeinek védelmében?
- Szükséges egy magasszintű vezető helyszíni jelenléte?

Kommunikációs kérdések: [49]

A vezetőknek és krízismenedzsment tagoknak a következő pontokat is szükséges számításba venni:

- Melyek a vállalat kommunikációs stratégiái?
- A vállalat tudja kezelni az incidens hosszútávú hatásait?
- A vállalat nyomon követi a közvéleményt az incidenszel kapcsolatban?
- Tájékoztatja a vállalat az incidensről a részvényeseket?
- Milyen hivatalok és köztisztviselők érdeklődhetnek az incidensről?
- Megtett mindent a vállalat a gyors és tényszerű tájékoztatás biztosításában?

Súlyossági hatásvizsgálatok iránymutatásai

Az egészség-, munka- és környezetvédelmi incidensek súlyosságának értékelése megállapítja a bejelentési követelményeket és gyorsan kommunikál az incidens súlyosságának megfelelően a vállalat menedzsmentjével. Egy vészhelyzet gyorsan változhat, ezért rendkívül fontos az incidensek pontos értékelése. Az esemény megítélésében figyelembe kell venni az objektív tényeket és a szubjektív véleményeket is az incidens természetének megfelelően.
Az incidens helyes felmérése általában javítja a súlyossági értékelést, amint egyre több és több információ áll rendelkezésre. A korai információ lehet félrevezető, vagy téves, ezért fontos, hogy ne becsüljük alá az eset súlyosságát.

Az értékelési folyamat megkönnyezheti az eset mindenkor tényszerű ismeretét. Következetes és pontos értékelésre van szükség a vészhelyzeti folyamat megfelelő működéséhez.

A vállalatnak olyan értékelési metódust kell kialakítani az esetek súlyosságának megállapításához, amely elsődlegesen négy expozíciós tényezőt vesz figyelembe: emberek (egészség/sérülés, környezet, vállalati értékek, hírnév).

A súlyossági szint 1, 2, 3, 4, 5 szinteket úgy kell hozzárendelni minden egyes elsődleges expozíciós tényezőhöz, hogy az 1-es a legenyhébb, az 5-ös a legsúlyosabb eset.

Az incidens súlyosságának felbecsülése olyan döntési folyamat, ami a rendelkezésre álló tények, információk alapján történhet. A következő irányelvek nyújtanak segítséget az eset súlyosságának felbecsüléséhez.

A súlyosság felbecsülésének tényszerű adatokon, információkon kell alapulnia. Mivel sok kisebb incidens pontciálisan nagyobbat lehet, ezért fontos, hogy folyamatosan szigorúan a tényeken alapuljon a beértékelés. Egy terület van, a hírnév, ahol a potenciális kitettséget mindig a legsúlyosabb szintre kell meghatározni, mert ezen a területen a média gyorsan tud reagálni és riportokat készíti a látható eseményekről, vállalati válaszlépésekéről.

A súlyossági szintje változhat az incidensnek, ahogy változik a helyzet, vagy újabb információk állnak rendelkezésre. Így periodikusan felül kell vizsgálni a súlyossági szintet és módosítani, ahogy szükségessé válik.

A súlyosság felbecsülésének az célja, hogy előre lehessen jelezni az incidens lehetséges hatásait a vállalat tevékenységére nézve.

Értesítések és jelentések

A pontos, időbeni kommunikáció a vállalat szervezetei között, és ahol szükséges a külső hatóságokkal, szervezetekkel elengedhetetlen a hatékony incidens kezeléséhez. A kommunikáció kiterjed számos tájékoztatási igény kielégítésére a vészhelyzet menedzselése során. [31]

Tartalmazza a következőket: a vészhelyzet technikai szempontjait, szükséges információk a vállalat menedzment számára, kapcsolattartás, információ csere, együttműködés külső hatóságokkal, kormányzati szervekkel, nem kormányzati szervekkel és a nyilvánossággal.
Ezen információk felépítése egy strukturált, többszintű rendszerben történik. Az incidens súlyossága határozza meg a vállalat válaszlépéseit, illetve azt, hogy milyen szintű vezetők kerülnek bevonásra a folyamatba.

**Mikor kell értesíteni?**

Vészhelyzetek, vagy incidensek bekövetkezése esetén. Biztonsági, egészség-, munka-, környezetvédelmi eseteknél, ahol a vállalat érintett, személyileg, területileg, vagy termelési, kereskedelmi viszonylatban. Vagy olyan külső vészhelyzet történt, amely a vállalatra is hatással lehet, például: terrorista támadás, tűzhelyzet, bombafényegetés, robbanás, tűzeset, szabotázs, vandalizmus, közművek ellátási zavarai, árvíz, vagy más természeti katasztrófa, ember által okozott katasztrófa.

**Kit kell értesíteni?**

Többcsatornás értesítési vonal országos szintekről a vállalati szintre:

- Vészhelyzeti kommunikáció céljából az országos szintű üzletág vezető értesíti a vállalat üzletág vezetőjét.
- Országos szintű kommunikáció értesíti a vállalati kommunikációt.
- Országos szintű egészség-, munka-, környezetvédelmi vezető értesíti a vállalati egészség-, munka-, környezetvédelmi vezetőt.
- Országos biztonsági vezető értesíti a vállalati biztonsági vezetőt.

**Krizismenedzsment szabályok az incidensekre adott válaszlépések során**

Annak érdekében, hogy a lehető legkisebb hatással legyen egy vészhelyzet a vállalat tevékenységére, a következőképpen kell eljarni: ha a vállalat felelős az incidensért, akkor gyors és hatékony lépésekkel kell csökkenteni az incidens hatásait, ha nem egyértelmű, vagy nem tisztázott a vállalat felelőssége az incidens kialakulása miatt, ebben az esetben a krízismenedzsment folyamatot működtetni kell, készén állva a beavatkozásra, ha nem a vállalat felelős az incidens kialakulásáért, akkor segítséget (technikai és tanácsadói) nyújthat a válaszlépések megadásához, a vonatkozó jogi keretek között.

A vállalat krízismenedzsment készültségi és reagálási erőforrások mozgósítását eredményezheti, ha a következő körülmények fennállnak és gyors válaszlépéseket kell adni egy felmerült vészhelyzeteben. Az országos vezetőségnek menedzselni kell a vészhelyzetet. Biztosítani a vállalati
létesítmények védelmét és működőképességét, kormányzati felkérés, vagy jogi kötelezettség esetén, felkérés esetén, ha a vállalat tagja olyan egyesületnek/szövetségnek, ahol a kölcsönös segítségnyújtás és együttműködés működik.

A vállalat vezetőségének előzetes engedélyével lehet a következő esetekben részt venni a válaszlépésekben: kormányzati felkérés esetén, felkérés esetén, ha a vállalat tagja olyan egyesületnek/szövetségnek, ahol a kölcsönös segítségnyújtás és együttműködés működik, önkéntes részvétel a helyi önkormányzati katasztrófaelhárításban.

**Megjegyzés:** Minden olyan helyzetben másodlagos a vállalat vezetőség engedélyének megszerzése, amikor életveszély áll fenn, ezekben az esetekben az elsődleges intézkedés az életveszély elhárítása minden esetben.

4.6.1 Szerepek és felelősségek, áttekintés

Vészhelyzet bekövetkezése esetén az érintett helyszín vezetősége elsődleges feladata a válaszlépések végrehajtása. Ez magában foglalja az azonnali, közvetlen, helyszíni válaszlépéseket, a külső együttműködéseket annak érdekében, hogy csökkentsen az incidens üzletmenetre gyakorolt negatív hatásait, és az átfogó, minden irányra (külső-belsı) kiterjedő kommunikációt a vészhelyzettel kapcsolatban. Ez a feladattétlét mindaddig érvényben marad, amíg a vállalat vezetősége kifejezetten másként nem határozik.

**A helyi krízismenedzsment összehívása**

Miután megállapításra került, hogy az esemény, ami megtörtént magában hordozza egy vészhelyzet kialakulásának a lehetőségét, az érintett üzletág vezető összehívhatja a helyi krízismenedzsmentet, amit ő fog irányítani.

**A helyi krízismenedzsment, amikor összehívásra kerül a következő feladatokat látja el:**

Értesíti a vállalat megfelelő szintű üzleti vezetőjét, biztonsági vezetőt, kommunikációs vezetőt, egészség-, munka-, környezetvédelmi vezetőt. Fenntartja a kommunikációt a vállalat vezetőségével, tájékoztatja őket a vészhelyzeti válaszlépések státuszáról. Döntéseket hoz a helyzet mielőbbi megoldásának, illetve a hatásainak minimalizálásának érdekében. Értékel-elemzi a válaszlépéseket, azok hatásait az üzletmenetre. Biztosíta, hogy az erőforrások (anyagi-személyi) rendelkezésre álljanak és folyamatos felülvizsgálattal erősíti hatékony működésüket, ezáltal biztosítva a helyzet megfelelő kezelését. Együttműködik a helyi és a vállalat szintű pénzügyi szervezetekkel, hogy a szükséges pénzügyi keret rendelkezésre álljon és fedezze a válaszlépések

A tagok

Ha a helyi krízismenedzsment egy vészszöveg bekövetkezésével összehívásra került, akkor a kulcs pozíciókba az érintett helyszín vezetői kerülnek [84].

A helyi krízismenedzsment a következő szervezetek vezetői tartalmazza: kommunikáció, személyzeti (HR), biztonsági, jogi, pénzügyi, egészség-, munka-, környezetvédelmi. Ezen túlmenően a krízismenedzsment bevonhat más szakértő személyeket, erőforrásokat, ha a krízishelyzet kezeli azt megkívája és ezáltal hatékonyabbá válhatnak a válaszlépések.

A krízismenedzsment feladata

Meghatározní a vészszöveg lehetséges hatásait a vállalatra és az üzletmenetre nézve, a következőkre való tekintettel: személyek biztonsága és a környezet védelme, felelősség, a vállalat arculatának, hírnevének védelme, működőképesség és üzletfolytonosság biztosítása, információ gyűjtés és elemzés és ezek alapján a válaszlépések kidolgozása és bevezetése belső és külső területen egyaránt, támogatni a helyi szervezetek tevékenységét a válaszlépések kapcsán, folyamatosan felülvizsgált tájékoztató anyag készítése a vállalat menedzsmentjének, összehangoja és elősegíti más szervezetek, támogatók tevékenységét, biztosítja, hogy az eseménnyből és annak kezeléséből levont tanulságok megfelelően dokumentálva legyenek, a kidolgozott fejlesztési lehetőségekkel együtt.

Kvízizenedzsment tagok feladatai

KRÍZISMENEDZSMENT VEZETŐ

Képviseli az érintett üzletágat, összehívja a krízismenedzsmentet és átveszi a vezetői pozíciót, meghatározza a prioritásokat és előírányozza a stratégiai lépéseket, eligazítja a krízismenedzsmentet, frissen tartja a tagok tájékozottságát, teljes felelősséggel bír a krízismenedzsment tevékenységével kapcsolatban, beazonosít más lehetséges hatásokat és bekér olyan szakértőket, akik képesek a beazonosított hatások elleni válaszlépések kialakítására és kezelésére.
KRÍZISMENEDZSMENT VEZETŐ HELYETTÉS

Támogatja a döntéshozzalat a szükséges tagokkal kapcsolatosan, vezeti a krízimenedzsment központ napi tevékenységét, átveszi a krízimenedzsment vezető pozícióját a krízimenedzsment vezető távollétében, együttműködik a krízimenedzsment vezetőjével és a krízimenedzsment folyamat vezetőjével a következőkben: a teendők, fontos kérdések beazonosításában, a helyi válaszlépések támogatásában, tájékoztató anyagot készítésében a vállalati vezetőség számára.

ÉRINTETT ÜZLETÁGI TANÁCSADÓ

Tanácsaival segíti a krízimenedzsment vezetőt, abban, hogy a vezető tisztában legyen a vészszitázió határait, tanácsaival segíti a stratégiai kérdések kidolgozását.

KRÍZISMENEDZSMENT FOLYAMAT VEZETŐ

Összehívja és támogatja a kriszmenedzsmentet a kriszmenedzsment vezető utasítására, felelős a kriszmenedzsment központ működéséért, biztosítja, hogy a döntéshozzá folyamat és útmutatás ne térjen el a lényeges kérdésektől a tanácskozás során, valamint azonosítja a kritikus stratégiai kérdéseket, koordinálja a kriszmenedzsment menetrendjét és tájékoztatóit, támogatja a kriszmenedzsmentet a felmerülő kérdések megválaszolásában, a válaszlépések előkészítésében és a vállalat vezetősége számára készített tájékoztatók készítésében, stb.

HELYI KAPCSOLATTARTÓ

Támogatja a kriszmenedzsmentet: a vészszitázió utasításait közvetlenül és közvetetten érintett hatásaival szembeni válaszlépések bevezetésében, koordinálja a stratégiai döntések bevezetését, amelyek befolyásolják a vészszitázióban érintett helyszín tevékenységét, kapcsolatot épít ki és tart fenn az érintett helyszín vezetőivel, hogy biztosítsan tudja ezáltal a kriszmenedzsment részére a tényszerű tájékoztatást (például: időszakos tudósítás a mindenkori helyzetről a helyszínről).

Megjegyzés: a pozíció betöltésének elengedhetetlen feltétele az üzleti tevékenység alapos ismerete.

ORSZÁGOS SZINTŰ ÜZLETI VEZETŐ

Koordinálja a külső kapcsolatokat (média, kormányzati szervek, közvélemény), figyelemben tartja a törvényi kötelezettségeket és azok szerint cselekszik, felelős a belső kommunikációért az alkalmazottak irányába, konzultál a kriszmenedzsment vezetőjével, a kommunikáció vezetőjével a megfelelő külső kommunikáció kialakításában a média, kormányzati szervek és a közvélemény
felé, konzultál a jogi osztálytal a vállalat jogszabályi kötelezettségeiről a vész helyzet szempontjából, biztosítja, hogy az alkalmazottak folyamatosan tájékoztatva legyenek a krízishelyzet státuszáról és hatásairól, elősegíti a különböző osztályok üzleti erőforrásainak hasznosítását az optimális válaszlépések bevezetéseinek érdekében.

KOMMUNIKÁCIÓS VEZETŐ

Tájékoztatások előkészítése és végrehajtása a vész helyzet jelenlegi és várható hatásairól a vállalat hírnevének megőrzése mellett a részvényesek, kormányzati szervek és a nyilvánosság részére, hatékony külső kommunikáció minden érintett külső fél számára, konzisztens belső kommunikáció, átfogó tájékoztató készítése, begyűjtés és konszolidálja a külső információ kérő igényeket, előkészíti a lehetséges kommunikációs válaszokat, közleményeket, engedélyezetet a közlemények, tájékoztatók kiadását, figyeli a külső reakciókat, a közvéleményt, médiát, terjeszt az engedélyezett tájékoztatókat, támogatja tanácsai a krízismenedzsment vezetőjét a vész helyzet lehetséges jogi következményeiről, illetve a válaszlépések jogi következményeiről, konzultál a szükséges jogi személyzettel, összegyűjtí a lényeges adatokat az incidensről jogi szempontból.

JOGI VEZETŐ

Jogi szempontból felülvizsgálja a kibocsájtandó jelentéseket/tájékoztatásokat, kiemeli a legfontosabb jogi vonatkozásokat a krízismenedzsment vezető részére, naplózza az eseményeket, kidolgozza a jogi válaszlépéseket.

BIZTONSÁGI VEZETŐ

Kapcsolatot tart az országos bűnüldöző szervekkel és biztonsági tisztviselőkkel, tanácsokat és ajánlásokat ad az alkalmazottak biztonságának, az értekei védelmének érdekében és vizsgálati esetekben, a helyzet függvényében biztonsági intézkedési tervet dolgoz ki, javasolja, amennyiben szükséges további biztonsági erőforrások igénybevételét, ellenőrzi és tisztázza az incidenssel kapcsolatos információkat, működteti a beléptetőrendszt, konszolidálja a biztonsági alvállalkozóktól beérkező információkat, kifejlesz védelmi és vizsgálati stratégiákat, koordinálja a védelmi és vizsgálati stratégiákat a bűnüldöző szervekkel.

SZEMÉLYZETI VEZETŐ (HR)

Támogatja a krízismenedzsment munkáját tanácsaival, eljár soronkívüli engedélyezések ügyében, ha szükséges, együttműködik a válaszlépésekben a többi résztvevővel és képviseli a személyzeti szempontokat (például: munkaügyi kapcsolódások, munkajogi megfelelősség, stb.), koordinálja a
kommunikációval az alkalmazottak, alvállalkozók, stb. számára nyújtott tájékoztatásokat, kezeli a személyügyi nyilvántartásokat.

PÉNZÜGYI VEZETŐ

Kialakítja, koordinálja és felügyeli és vizsgálja az igényeket, kezeli a követeléseket, a különböző szükségessé válnak szolgáltatásokkal kapcsolatban, felméri a kártérítési igényeket, a pénzügyi irányelvek betartásával, felügyeli a követelések kiegyenlítését, tanácsot ad a krízismenedzsment vezetőjének a biztosítási fedezetről, feltételeiről, státuszáról, gondoskodik a megfelelő biztosítók, vagy más szükséges jogi személyek értesítéséről, jótállási és garanciális feltételekről.

TECHNIKAI TÁMOGATÁS

Technikai támogatási igények attól függenek, hogy milyen jellegű a vész helyzet. Minden incidens egyedi, ezért az elhárításához szükséges technikai támogatás is egyedi jellegű. A krízismenedzsment vezetője dönti el, hogy milyen jellegű technikai támogatás szükséges. Ezek lehetnek például: mérnökségi, vagy termelési, információ technológiai, vagy más technikai szakértők.

EGÉSZSÉG-, MUNKA-, KÖRNYEZETVÉDELEM


ÜZLETÁGI FUNKCIÓK KÉPVISELET

Általában ott szükséges, ahol a vész helyzet hatásai több üzletági tagot érintenek, illetve, ahol csak korlátozott létszámú személyzet áll rendelkezésre az adott üzletágban: tanácsadás az érintett üzletág képviseletében, krízismenedzsment vezető támogatása, hogy tisztában legyen az adott üzletág tevékenységével, tanácsadás a krízismenedzsment vezető részére az incidens üzletági hatásairól, koordinálja az érintett üzletágra vonatkozó stratégiai döntések végrehajtását.

Megjegyzés: a pozíció betöltésének elengedhetetlen feltétele az üzletág tevékenységének alapos ismerete.
4.6.2 A krízismenedzsment szervezeti felépítése

![Krízismenedzsment szervezeti felépítése](image)

20. ábra A krízismenedzsment szervezeti felépítése (saját szerkesztés)

4.6.3 A krízismenedzsment folyamata

A következő eljárás a krízismenedzsment tanácskozására vonatkozik. Ezen tevékenység célja, hogy biztosítsa az értekezlet struktúráját a krízismenedzsment céljainak eléréséhez.

Kezdeti tevékenységek

A következő tevékenységek kerülnek végrehajtásra a krízismenedzsment összehívásakor: tájékoztatás adása az incidens státuszáról, beazonosítása az incidensnek, hogy kihez, milyen szervezethez tartozik az incidens, meghatározni a krízismenedzsment tagjait és vezetőjét, felülvizsgálni a válaszlépések kezelésének folyamatát, biztosítani a tagok számára feladatuk megértését, meghatározni a krízismenedzsment célkitűzéseit, dokumentálni a főbb kérdéseket.
A krízismenedzsment kezdeti eljárásai

A következő lépések végrehajtása szükséges a krízismenedzsment összehívásakor:

1. krízismenedzsment összehívása a krízismenedzsment központba,
2. krízismenedzsment vezető tájékoztatja a krízismenedzsment tagjait,
3. a célok kitűzése (ez a legfontosabb),
4. krízismenedzsment tanácskozás,
5. a célok eléréséhez szükséges feladatok beazonosítása,
6. feladatok prioritálása, lépések megtervezése,
7. begyűjteni és feldolgozni az információkat, teendőket összeállítani,
8. meghatározni a legrosszabb forgatókönyvet,
9. újrafoglalnizi és frissíteni a stratégiát folyamatosan (pl.: naponta, ha hosszabb a krízis).

Krízismenedzsment központ

A pontos kommunikáció a helyi krízismenedzsment és a vállalat vezetősége között elengedhetetlen a hatékony kríziskezeléshez. Ahhoz, hogy a személyzet végre tudja hajtani a krízismenedzsment tervben vázolt feladatait szükség van egy kijelölt helységre.

A vállalatnak létre kell hoznia erre a célra egy dedikált krízismendezsment központot, amelyet a biztonsági szervezet tart fenn. Ahol krízismenedzsment megalapításra került, ott mindenhol létre kell hozni egy működő krízismenedzsment központot. Ezen központokat kell használni a krízishelyzet fennállásakor, itt tevékenykedik a krízismenedzsment.

A biztonsági szervezet felelős a krízismenedzsment helyiségének a kialakításáért, felszereléséért és fenntartásáért. A helyiséget fel kell szerelni vész helyzet esetén is működő elektromos be-táplálással.

A krízismenedzsment központot a következő eszközökkel kell felszerelni: konferenciabeszélgetésre alkalmas telefon, áramkimaradás esetén is működő elektromos hálózat, elektronikus (hálózattól függetlenül, külső adathordozón tárolt) és nyomtatott vész helyzeti terv, AM/FM vételére alkalmas rádió (elemmel működő), TV készülék megfelelő vevő egységgel, hálózat, LAN és internet, alaprajzok, térképek (hálózattól függetlenül, külső adathordozón tárolt) és nyomtatott példányok, dolgozói listák, otthoni címekkel, telefonszámokkal, vész helyzeti kontakt személyek elérhetőségeivel (hálózattól függetlenül, külső adathordozón tárolt) és nyomtatott példányok, külső telefonkönyv (hálózattól függetlenül, külső adathordozón tárolt) és nyomtatott példányok, belső
Alternatív krízismenedzsment központ

A biztonsági szervezetnek létre kell hoznia egy alternatív krízismenedzsment központot, ami a telephelyen kívül helyezkedik el, attól biztonságos távolságban arra az esetre, amikor nem lehet megközelíteni az állandó krízismenedzsment központot, vagy az használhatatlan állapotba került. A biztonsági szervezetnek kell fenntartani az alternatív központot. A felszerelési és dokumentálási követelmények ugyanazok, mint az elsődleges központ esetében. Hordozható felszerelés és dokumentáció is megfelelő lehet.

Krízismenedzsment kiképzés

Az alkalmazottaknak, vezetőknek oktatásban kell részesülniük. A krízismenedzsment folyamat során a biztonságot és a környezetvédelmet is figyelembe tartó tevékenységet folytathatnak, óvva saját és mások életét, testi épességét, egészségét, valamint minden idevonatkozó törvénynek és előírásnak meg kell felelniük. A hatékony krízismenedzsment képzésben résztvevő alkalmazottak biztosítják a krizishelyzetekre való megfelelő szintű felkészülést. Ez igaz azokra is akik közvetlenül az incidens helyszínén tevékenykednek, illetve azokra is, akik valamelyik magasabb szintű krízismenedzsment vezetőségében látják el feladatokat.

A képzésnek a következő elemeket kell minimum tartalmazni:

Az első képzést követnie kell minden évben az emlékeztető-felfrissítő képzésnek ezáltal, a tagok ismeretének szintentartásával biztosítva a megfelelő szintű kríziskészenlétet. Amennyiben a körülmények indokolják, úgy lehet az ismétlő képzéseket sűrűbben is féléves, negyedéves periódusokban is tartani, de minimum évente indulhatnak. Ha ennél hosszabb időkig maradnak, akkor a tagok ismeretének elhalványulnak, magabiztoságguk csökken, ezáltal döntéseik sebessége és határozottsága nem támogatja megfelelő képen a krízishelyzet hatékony kezelését.

Minden krízismenedzsment tagnak részt kell vennie az évenkénti emlékeztető képzésen.

A képzésnek a következő elemeket mindenléppen tartalmaznia kell: kiürítés, kezdeti tűzoltás, bombakeresés (ahol a helyi jogszabályok ezt megengedik), elsősegélynyújtás.

A képzés elemei helyettesíthetőek olyan okok szerint a kiürítést [50], amely biztosítja a haladéktalan reagálást, pl.: tűzoltóság, mentők, rendőrség az értesítésüket követően 5 percen belül képesek a helyszínen megjelenni és a mentést-elhárítást megkezdeni.
A krízismenedzsmentnek legalább évente ülést kell tartani, mint krízismedezsment vezetőség és felülvizsgálni a krízismenedzsment folyamatot. Ha valamelyik tag nem tud résztvenni a találkozón, akkor őt külön, személyesen ki kell képezni. Amennyiben haladéktalan és elháríthatatlan elfoglaltság, vagy akadály miatt nem tud személyesen megjelenni, úgy el kell számára küldeni a krízismenedzsment folyamatot, szerepeket, felelősségeket és a találkozó összefoglalóját. A távolmaradó tagnak értesítenie kell a biztonsági szervezetet, hogy az anyagokat megkapta és megértette.

Minden olyan olyan esetben, amikor egy új tag került kinevezésre a krízismenedzsmentbe haladéktalanul meg kell kapnia a krízismenedzsment oktatást a krízismenedzsment folyamatgazdájától (a biztonsági szervezet tagja, aki felelős a krízismenedzsment folyamatért), hogy biztosítva legyen ezáltal a krízismenedzsment teljes működőképessége. Ezt az egyedi oktatást ugyanúgy kell dokumentálni és jelenteni, mint az általános képzést és gyakorlatot is.

**Krizismenedzsment gyakorlat követelményei**

**Elméleti gyakorlat**

Az elméleti gyakorlat során felülvizsgálatra kerül a krízismenedzsment folyamat és egy tanácskozás keretében vitatják meg a tagok, hogy miként lenne szükséges reagálni az adott helyzetben. Általában a krízismenedzsment tagjain kívül más személyek és szervezetek nem kerülnek bevonásra az ilyen típusú gyakorlatok során. Az elméleti gyakorlatot a biztonsági szervezet koordinálja.

**Szimulációs gyakorlat**

A szimulációs gyakorlat a krízismenedzsment központ aktiválásával kezdődik, a szükséges személyzet és erőforrások bevonásra kerülnek. A krízismenedzsment tagjain kívül más személyek és szervezetek is bevonásra kerülhetnek a szimulációs gyakorlatba. Az ilyen típusú gyakorlat tervezése és koordinálása a biztonsági szervezet feladata, de elindításától kezdve az egész krízismenedzsment felelős a hatékony végrehajtásért. A szimulációs gyakorlatok kiterjedhetnek több helyszínre és több katasztrófaelhárító csoportra is. Így lehetőség nyilik több különböző földrajzi helyszíneken lévő egységek tevékenységének összehangolására, eljárásaink, berendezéseink, fel szereléseik tesztelésére is [41].

**Gyakorlat tervezése**

Minden egyes gyakorlatot előre meg kell tervezni [36] [84]. A terv meghatározza a tervezésben részt vevő személyeket, a gyakorlat célját, a gyakorlat tervezett lefolyását, a bevonásra kerülő
személyeket, szervezeteket, a gyakorlat idő tartamát, külső erőforrások, szervek, bevonását és a terv felülvizsgálatára vonatkozó célokat, lehetséges eredményeket. A gyakorlat céljai között szerepelnek kell a következőknek: lepróbálni és megerősíteni a krízismenedzsment és katasztrófaelhárítási terveket, teszteni a készenléti képességet, képezni a résztvevőket és feltárni az esetleges hiányosságokat, valamint kidolgozni a javító intézkedéseket és folyamatokat. A gyakorlat végrehajtását és értékelését dokumentálni kell.

A gyakorlatot legalább évente végre kell hajtani, illetve ha azt valamilyen helyi jogszabály, vagy szabályzat ennél gyakoribb időintervallumban előírja, akkor az szerint kell eljárni. Minimum követelményként a következő szempontok alapján szükséges teszteni és dokumentálni a kriszismenedzsment folyamatot négy éves periódus alatt (minden évben legalább egy gyakorlatot végre kell hajtani): tűzeset, politikai, vagy polgári demonstrációk, tüntetések, zavargások, fenyegetések (bomba, vagy személyes), személy, vagy tulajdon elleni erőszakos cselekmények, természeti, vagy ember által okozott katasztrófa helyzetek, illetve ezek hatásai.

A gyakorlat értékelése

Minden gyakorlat értékelésénél meg kell állapítani, hogy a kitűzött célokat sikerült-e elérni a gyakorlat során, illetve dokumentálni kell azokat a területeket, amelyeket fejleszteni szükséges.

A gyakorlatok időzítésének tervezése és jelentése

Célszerű, ha minden év első negyedévében a helyi biztonsági igazgatók benyújítják az éves tervezetüket a biztonsági főigazgató felé.

4.6.4 A Kriszismenedzsment terv

Az elkészített és mindig frissített tervet megfelelő védelmű helyen kell tárolni digitális és nyomtatott változatban is.

A tevnek tartalmaznia kell a következő elemeket [85]: az elsődleges és az alternatív kriszismenedzsment központ kijelölése, a krízismenedzsment tagjainak és helyetteseinek kijelölése (pl.: kriszismenedzsment vezetője, helyettese, jogi, személyzeti, biztonsági, kommunikációs, gyártási, munka és egészségvédelmi, pénzügyi, létesítményi, stb. vezetők), a biztonsági szervezetek felül kell vizsgálni és frissíteni a tervet negyedévente (nevek, helyettesek, telefonszámok, stb.).
Jelentési kötelezettség

Azonnal jelenteni kell minden vészhelyzeti eseményt a helyi biztonsági szervezetnek, illetve a munkahelyi vezetőnek. A munkahelyi vezető jelenti tovább a felettesének. Előzetes jelentést kell készítenie a biztonsági szervezetnek és folyamatosan ki kell egészítenie az újabb rendelkezésre álló információkkal. Minden biztonsági eseményt jelenteni kell a biztonsági központnak, ha ilyen van, ha nincs, akkor a helyi biztonsági szervezetnek.

Az esemény utólagos értékelése

A biztonsági szervezetnek ki kell vizsgálnia minden egyes vészhelyzetet, amely indokolta a križismenedzsment aktiválását, erről írásos összefoglalót kell készítenie és azt eljuttatni a biztonsági főigazgatóhoz.

Megfelelősségi nyilatkozat

A helyi biztonsági igazgatónak évente írásban értesíteni kell a helyi üzleti vezetőt, illetve a biztonsági főigazgatót, hogy a križismenedzsment minden követelményének megfelel a vezetése alatt álló helyszín.

4.7 A humánbiztonság

Mit értünk humánbiztonság alatt? Véleményem szerint a humán-(emberi) biztonságon, tágabb értelemben minden olyan biztonsági területet, tevékenységet értetünk, ami az emberrel kapcsolatos. Ez meglehetősen széles skálát felölelhet a munkavédelemtől kezdődően a terrorizmusig, vagy az éghajlati változások emberre gyakorolt biztonsági hatásáig is. Úgy gondolom, hogy a biztonsági vezetőknek nem indokolt ennyire globálisan foglalkozni a kérdéssel. Egy lényegesen szűkebb értelmezés szerint a humánbiztonság jelentése az emberek, emberi értékek védelme, a más jellegű értékeink (fizikai, intellektuális, adat, stb.) védelme az embertől, illetve az ő szándékosságától, vagy gondatlan károkozásától. Valójában, szakmai körökben ennél még szűkebben értelmezzük a humánbiztonság fogalmát, és szinte kizárólag a munkatársak feddhetetlenségének megkövetelését és az annak érvényt szerző szabályokat, folyamatokat, vizsgálatokat értjük alatta.

Napjainkban az ilyen jellegű biztonsági követelmények aléget nehéz érvényt szerezni, gondolok itt a személyes adatok védelmére, jogszerűségre. Úgy is mondhatnám, hogy munkatársaink

Négyféle összeférhetetlenséget ismerünk, az általános, a gazdasági, a személyi és a szervezeti összeférhetetlenséget. Nem jogi, szakszerű szóhasználattal érve, az általános azt jelenti, hogy a vállalat dolgozója nem szerezhet részesedést (kivéve részvény) olyan gazdálkodó szervezetben, amely olyan, vagy hasonló tevékenységet végez, mint az a vállalat, ahol alkalmazásban áll, illetve a két vállalat között nem lehet rendszeres gazdasági kapcsolat. A gazdasági összeférhetetlenségről akkor beszélünk, a fenti példa mentén, amikor a vállalat dolgozója (résztesedés helyett) másik munkaviszonyt létesít. Személyi összeférhetetlenség az, amikor közeli hozzátartozók alá- és főlérődeltségi, ellenőrzési, utalványozási viszonyba kerülnek egymással. Szervezeti összeférhetetlenség, pedig akkor akakot ki, ha a dolgozó önmaga fölött ellenőrizhet, illetve magának utalványozhat. A vezetőkre ennél szigorúbb követelmények vonatkoznak, nekik nem lehet engedély nélkül más munkaviszonyuk, sőt azt is be kell jelenteniük, ha közeli hozzáértelmezőjük esetében kialakult az összeférhetetlenség.

Folyamatában úgy működhet a humánbiztonság, hogy a Munka Törvénykönyvére támaszkodva el kell készíteni a szabályzati hatteret, majd minden dolgozóval ki kell töltetni egy formanyomtatványt, amiben nyilatkoznak arról, hogy nem áll fenn összeférhetetlenség az említett kategóriákat illetően. Ezt a nyilatkozatot a dolgozó vezetője leellenőrzi és igazolja, hogy rendben van. Amennyiben összeférhetetlenség áll fenn, akkor több lehetősége van a munkáltatói joggyakorló vezetőnek, felszólíthatja a dolgozót az összeférhetetlenségi ok azonnali, vagy egy meghatározott határidőn belüli megszüntetésére, illetve szankcionálhatja is, sőt legsúlyosabb esetben rendkívüli felmondási oknak is tekintheti.

4.7.1 A humánbiztonság lényegi elemei

A humánbiztonság lényegének bemutatásán keresztül teljesebb képet kaphatunk a területről, és rá lehet világítani arra az oldalára is, ami megmutatja, hogy minden mindig szabályszerűen történik a vállalat és a dolgozók érdekében is. Ez a folyamat nemcsak a vállalatnak, hanem a dolgozóknak is segítséget tud nyújtani, védelmezni képes, azáltal, hogy időben jelzi a kockázatokat. A humánbiztonság folyamatának rá kell épülnie az összeférhetetlenségi folyamatra [98].
A humánbiztonsági folyamat elsődleges célja, a vállalat gazdasági érdekeinek védelme. A vállalat alapvető érdeke, hogy a dolgozóival kapcsolatos kockázatokat csökkenteni tudja. Arra kell törekednie, hogy megelőzze, felderítse és megszüntesse mindazon szándékos, vagy gondatlan dolgozói magatartásokat, illetve a dolgozók személyes körülményeiben rejlő, befolyásolás vagy zsarolás jellegű támadásokat lehetővé tevő kockázatokat, amelyek a vállalatnak anyagi, vagy erkölcsi károkat okozhatnak [89].

A humánbiztonsági tevékenység másik célja továbbá az is, hogy segítse, növelje a munkavállalók biztonsági tudatosságát úgy, hogy jelzi a személyes körülményeikben felmerült biztonsági kockázatokat, azokat értékelni, így a dolgozók ellen irányuló befolyásoló törekvésekkel és támadásokkal szemben is védelmet nyújtt.

A vállalat, mint munkáltató köteles a humánbiztonsági tevékenységgel kapcsolatos jogszabályok (adatvédelmi törvény, munka törvénykönyve) és a belső szabályzatok (munkavállalói adatok kezelése, adatosztályozás) rendelkezéseit a humánbiztonsági tevékenység során betartani. A humánbiztonsági tevékenység során a munkáltató és a tevékenységet végző személy köteles a munkavállalók személyiségési jogait tiszteletben tartani.

A humánbiztonsági tevékenység körébe tartozik a dolgozók humánbiztonsági vizsgálatainak végrehajtása, valamint a humánbiztonsági tevékenységre vonatkozó szabályzat kidolgozása.

A humánbiztonsági vizsgálattal összefüggésben kezelt (benyújtott, beszerzett, keletkezett) munkavállalói személyes és különleges (személyes) adatokat kizárólag a biztonsági szervezet vezetője, illetve a biztonsági szervezethez tartozó vizsgálatot végző kollégái ismerhetik meg. Ezen személyeken felül, a belső szabályozottság szerint, általában megismerni még a vállalat legfőbb vezetője, valamint kockázati tényező felmerülése esetén a vizsgálat dolgozó munkáltatói jogkört gyakorló vezetője.

A tevékenység céljából kezelt adatok csak a humánbiztonsági tevékenységgel összefüggésben használhatóak fel. Azok más folyamatokban, mint személyügyi vagy munkajogi folyamatokban (pl. értékelés, jutalmazás) nem használhatóak fel.

A vizsgálatoknál kezelt nem lényegi dokumentumok a vizsgálat végeztével megsemmisítésre kell, hogy kerüljenek. Megőrzendő viszont a dolgozó által kitöltött adatlap, és a vizsgálatban való önkéntes részvételt igazoló, valamint adatkezelési hozzájáruló nyilatkozatok, a humánbiztonsági ellenőrzésről készült tájékoztató, illetve az azt alátámasztó dokumentumok.
A vizsgálattal kapcsolatos megőrzendő dokumentumokat a vonatkozó jogszabályi rendelkezések és a vállalat iratkezelési és adatosztályozási szabályainak betartásával kell kezelni és tárolni, azok bizalmasnak minősülnek. A bizalmas adatok hozzáférése csak felhatalmazott személyekre korlátozódhat, azokat illetéktenen személyek hozzáférérsétől a biztonsági szervezetnek fizikai és logikai eszközökkel szükséges védenie.

A megőrzés (adattárolás) legfeljebb az adott dolgozó munkaviszonyának fennállásáig tarthat. Ez alól kizárólag az képez kivételt, ha a dolgozó ellen munkaviszonyának fennállása alatt büntetőeljárás indult, továbbá, ha a munkavállaló munkakörével összefüggésben szándékosan vagy gondatlanul okozott kár miatt polgári peres, vagy munkaügyi bírósági eljárás indul, illetve a munkaviszonyal összefüggésben munkaügyi bírósági jogvitát kezdeményezett a munkavállaló. A jelzett esetekben az adattárolás időtartama az eljárások jogerős befejezéséig hosszabbodhat meg.


A dolgozó tájékoztatást kérhet a humánbiztonsági vizsgálat céljáról, a felvett személyes adatok köréről, kezelésének rendjéről, a személyes adatok megismerésre jogosultak köréről, az adattárolásról/adatmegsemmisítésről, az adatkezeléssel kapcsolatos jogokról, a jogorvoslati jogosultságokról.

A dolgozó házassági jogalapján való együttműködésének önkéntességi alapon kell működnie. Az együttműködés megtagadása miatt a dolgozót semmilyen jogtalan hátrány nem érheti, azonban a vállalat megfontolhatja, hogy az együttműködés megtagadása az adott körülmények között önmagában kockázatként értékelhető-e?

A dolgozókat a betöltött vagy betöltendő beosztás alapján kerülnek biztonsági besorolásra. A humánbiztonsági vizsgálat az a tevékenység, amelynek során a biztonsági szervezet adatot gyűjt, a részére átadott adatokat áttekinti, azokat a jogszabályok által biztosított törvényes eszközökkel, a vizsgálat alá vont dolgozó személyhez fűződő jogainak tiszteletben tartása mellett ellenőriz, és értékelni, hogy a vállalat vonatkozásában fennáll-e humánbiztonsági kockázat, és amennyiben igen, úgy az milyen mértékű.
A humánbiztonsági vizsgálatokat a beosztás elnyerését, illetve a dolgozó beosztásának változását megelőzően, ezután három-négyévente, ismételten célszerű elvégezni, illetve szúrópróbaszerűen vagy biztonsági kockázat felmerülése esetén, vagy megelőzésképpen bármikor.

A dolgozó a tájékoztató átvételét követően dönt arról, hogy együttműködik-e a humánbiztonsági vizsgálatban, és hozzájárul-e az ehhez szükséges adatkezeléshez. Amennyiben az érintett a hozzájárulását megadja, kitölti az adatlapot.

A biztonsági szervezet munkatársa az adatlapot átvételekor a dolgozóval közösen áttekinti, szükség esetén segítséget nyújt a dolgozónak a teljes kitöltéshez, válaszol az adatlapmal és a vizsgállattal kapcsolatos kérdésekre, illetve tisztázó kérdéseket tehet fel a dolgozónak.

Az adatlapon megadott információk ellenőrzésére és a biztonsági kockázat értékelése céljából a biztonsági szervezet munkatársa a vállalat szervezetéitől bekéri az ott fellelhető adatokat, és lefolytatják a biztonsági ellenőrzést. Az ellenőrzés keretében az alábbi eszközök/módszerek használhatóak a szükséges adatok beszerzéséhez, ellenőrzéséhez és értékeléséhez [90]:
- A vállalat területén, működő biztonsági és informatikai eszközök által rögzített adatok megismerése,
- Egyéb belső és külső nyilvános forrásokból, valamint a vállalat tulajdonában lévő eszközök ből kinyerhető és adatbázisokban rögzített adatok beszerzése, értékelése, a vizsgállattal érintett meghallgatása (humánbiztonsági interjú), a vállalat adott vizsgállattal nem érintett dolgozójának meghallgatása, informálódás a korábbi munkahelyen, a vagyonyvédelmi társaságokkal érvényben lévő szerződésekben foglalt törvényes információszerző eszközök alkalmazása, poligraf, pszichológiai teszt, grafológiai vizsgálat.

A vizsgálat eredménye lehet: merült fel kockázat vagy nem merült fel kockázatra utaló körülmény. Amennyiben merült fel kockázat, az kockázatértékelés alapján a következő minősítéseket eredményezheti: rendszeresen ellenőrizendő kockázat merült fel, értékelendő kockázat merült fel, kizáró kockázat merült fel.

Kizáró kockázati minősítés esetén a kockázat az adott munkakör betöltése mellett a kockázat jellege és mértéke miatt potenciálisan és közvetlenül veszélyezteti a vállalat jogos gazdasági érdekeit.

Értékelendő kockázati minősítés esetén a kockázat egyéb körülmények fennállása mellett potenciálisan veszélyeztetetheti a vállalat jogos gazdasági érdekeit.

Rendszeresen ellenőrizendő kockázati minősítés esetén a kockázat a vállalat jogos gazdasági érdekeit közvetlenül nem veszélyeztet vagy azok távoli veszélyeztetésére alkalmas, azonban a
körülmények változása következtében ez bármikor módosulhat, ezért annak rendszeres utóellenőrzése szükséges.

A biztonsági szervezetnek értesítenie kell a humánbiztonsági vizsgálat eredményéről és megállapításairól, az esetlegesen felmerült biztonsági kockázatokról és azok súlyosságáról, minősítéséről a belső szabályzatban meghatározott vezetőt.

Az értesíts megőrzentével a humánbiztonsági folyamat végére értünk, amit a fentiek szerint, amennyiben szükséges, vagy időszakonként meg lehet ismételni.

**ÖSSZEFOGLALÓ**

Összegezte megőrzentheto, hogy az összeférhetetlenségi folyamat arra képes lehet arra, hogy biztosítsa azt, hogy a vállalat gazdasági érdekei ne sérüljenek a dolgozóival kapcsolatos kockázati tényezők miatt. Ehhez szükségeltetik egy olyan szabályozott, kontrol alatt működő szigorú rendszer, amely a törvényekre és a belső szabályokra támaszkodva képes garantálni a szakszerűséget a vállalat és dolgozói számára, amihez egy korrekt, a dolgozók részére biztonságot nyújtó és bizalmat keltő tevékenység társul.

4.7.2 Összeférhetetlenség

Általános rendelkezések

A vállalat értekeinek védelme mentén kialakult bizalmi viszony a vállalat és az alkalmazottak között, amely szerint az egyik legfontosabb feladata az alkalmazottaknak, hogy a vállalat eszközeit ki-zárólagosan, illetve a munkavégző képességeiket, munkaerüjéket elsősorban a vállalat jogos üzleti érdekeinek előrése céljából használják. Ennek a célnak az eléréséhez minden vezetőnek és alkalmazottnak el kell kerülni minden olyan helyzetet, illetve tartózkodni kell minden olyan intézkedéstől, ami a vállalati és a személyes érdekek ütközését okozhatja, illetve megzavarhatják a pártatlan és objektív döntések meghozatalában. [23] [44] [53]

Ennek alapján és a jogszabályokkal, szabályzatokkal összhangban a vállalat jogos gazdasági érdekeinek, alkalmazottainak védelme és az összeférhetetlenséggel veszélyeztető helyzetek elhárítása érdekében ellenőrzői folyamatot kell létre hozni. Ennnek érdekében, hogy az összeférhetetlenségi konfliktushelyzetek ne alakulhassanak ki, illetve ha egy alkalmazott ilyen helyzetben találna magát, akkor segítségére a vállalat egy nyilatkozat alapú összeférhetetlenségi folyamatot kell működtetni és az alapján iránymutatást adni. [37] [99]
Körülmények, amelyek különösen veszélyeztethetik a vállalat jogos gazdasági érdekeit

Összeférhetetlenség, akkor keletkezik, ha a vezető, vagy az alkalmazott személyes érdekeit zavarja, vagy úgy tűnik, hogy zavarja a vállalat üzleti érdeke és ez magában hordozhatja a vállalat jogos gazdasági érdekeinek a potenciális veszélyeztetetését. Ilyen veszélyeztetettség fordulhat elő a következő esetekben.

Általános összeférhetetlenség, ha a munkavállaló részesedést szerez (nyilvános részvényvásárlás kivételével), olyan társaságban, amely a vállalattal azonos, vagy hasonló tevékenységet végez, vagy rendszeres gazdasági kapcsolatban áll.

Gazdasági összeférhetetlenség, ha a munkavállaló a vállalatnál fennálló munkaviszonyán kívül létesített, vagy létesíteni kíván további munkaviszonyt, vagy egyéb munkavégzésre irányuló jogviszonyt.

Személyi összeférhetetlenség, ha a munkavállaló, vagy hozzátartozói olyan munkakörökben tevékenykednek, amelyekben egymással közvetlen alá- és fölérendeltségi, ellenőrzési, utalványozási, átvételi viszonyba kerülnek.

Szervezeti összeférhetetlenség, ha a munkavállaló saját magával kapcsolatosan tud költségeket engedélyezni, illetve saját magát ellenőrizni.

További követelmények vezetők számára

A vezető nem alakíthat ki további munkavégzésre irányuló egyéb jogviszonyt, kivéve tudományos, oktatói, illetve szerzői jogviszonyt.

A vezető nem köthet a saját nevében, vagy javára a vállalat tevékenységi körébe tartozó ügyleteket.

A vezető nem szerezhet részesedést (a nyilvános forgalmú részvényszerzés kivételével) a vállalattal azonos vagy ahhoz hasonló tevékenységet is végző, vagy a vállalattal rendszeres gazdasági kapcsolatban álló más gazdálkodó szervezetben.

A vezető köteles továbbá bejelenteni, ha közeli hozzátartozója tagja lett (részzesedést szerzett), vagy vezetőként munkavégzésre irányuló jogviszonyt létesített a vállalattal azonos, vagy ahhoz hasonló tevékenységet folytató, vagy a vállalattal rendszeres gazdasági kapcsolatban álló gazdasági társaságban.
Részletes felelősségek

A munkavállaló jelentési kötelezettségei

Általános összeférhetetlenség esetén, ha részesedést szerzett, vagy már korábban fennálló részesedéssel rendelkezett valamely gazdálkodó szervezetben, amely azonos, vagy hasonló tevékenységet folytat, mint a vállalat, vagy a gazdálkodó szervezettel a vállalat rendszeres gazdasági kapcsolatban áll, a nyilvános részvényszerzés kivételével.

Gazdasági összeférhetetlenség esetén, ha létre kíván hozni, vagy már létrehozott további munkaviszonyt, vagy munkavégzésre irányuló egyéb jogviszonyt.

Személyi összeférhetetlenség esetén, ha közvetlen hozzátartozója létesít, vagy már létesített a vállalattal munkaviszonyt, vagy munkavégzésre irányuló egyéb jogviszonyt.

Bármilyen okból kifolyólag kialakult szervezeti összeférhetetlenséget, amiben az alkalmazott egyéni megértettségével kapcsolatban áll, új nyilatkozatot kell kitölteni.

Ha az alkalmazottnak nincs érvényes nyilatkozata harminc napon belül az intézkedés hatályba lépését követően. Ha változás történt az összeférhetetlenséget kiváltó körülményekben, vagy jogviszonyban, akkor tizenöt napon belül új nyilatkozat szükséges. Új alkalmazottak esetében öt munkanapon belül szükséges nyilatkozni. Munkaszerződés módosítás esetén öt munkanapon belül kell nyilatkozni. Jogi állományból visszatérés esetén, ha a távollét meghaladta a kilencven napot, akkor öt munkanapon belül kell a nyilatkozatot kitölteni.

Új nyilatkozatot kell kitölteni

A beszerzési területre vonatkozó speciális követelmények

Azokra a döntéshozó vezetőkre és alkalmazottakra vonatkozik, akik részesei a beszerzési folyamatnak, amennyiben saját maguknak, illetve közeli hozzátartozóiknak munkaviszonyuk, vagy munkavégzésre irányuló egyéb jogviszonyuk, vagy részesedésük van, nyilvános részvényszerzés kivételével, vagy a tenderen indult gazdasági társaságban.

A nyilatkozatot a munkáltatói joggyakorló vezetőnek kell benyújtani. A vezető a biztonsági szervezethez fordulhat szakmai segítségért, illetve támogatásért az összeférhetetlenség kiértékelésében és kezelésében. Ez a speciális nyilatkozat nem mentesít az általános nyilatkozat benyújtásától, ez a speciális beszerzői nyilatkozat az általános nyilatkozatra épülő addicionális kontrollt valósít meg.
Nagy értékű beszerzés esetén (pl.: 100 M HUF) feletti értékű beszerzések esetén a biztonsági szervezetet tájékoztatni kell, hogy el tudja végezni az összeférhetetlenségi nyilatkozatokban szereplő adatok ellenőrzését.

**Nyilatkozatok kiértékelése**

A nyilatkozatok kiértékelése a munkáltatói joggyakorló vezető folyamatos felelőssége.

A munkáltatói joggyakorló vezetőnek abban az esetben is jóvá kell hagynia, aláírnia a nyilatkozatot, ha abban nem áll fenn semmilyen jellegű összeférhetetlenség, vagyis az alkalmazott nem jelzett és nem kérelmezett más munkaviszonyt, illetve munkavégzés jellegű más jogviszonyt és nem tüntetett fel összeférhetetlenségi körülményt.

Az alkalmazottnak tizenöt nap áll rendelkezésére, hogy nyilatkozatát benyújtsa a munkáltatói joggyakorló vezetője felé. Amennyiben vezetője nem tudja eldönteni, hogy fennáll-e az összeférhetetlenség, úgy fordulhat a biztonsági szervezethez szakmai támogatásért.

Amennyibe összeférhetetlenség áll fenn a vezető dönthat úgy, hogy számára a körülmény fennállása ismert, nem lát benne kockázatot és engedélyezi annak fenntartását, vagy meghatározhat egy határiderint, ameddig az alkalmazottnak fel kell számolnia az összeférhetetlenséget, illetve az összeférhetetlenségi körülmény haladéktalan felszámolására is adhat utasítást.

Amennyiben a munkáltatói joggyakorló vezető nem ad visszajelzést tizenöt napon belül, akkor úgy kell tekinteni, hogy részéről összeférhetetlenségi körülmény nem áll fenn az alkalmazott nyilatkozatával kapcsolatban. Annak megállapításához, hogy a vállalati tevékenységi körök összeférhetetlenségben vannak-e az alkalmazott által jelentett tevékenységi körökkel a cégnyilvántartás az irányadó.

**Összeférhetetlenségi vizsgálat kezdeményezése**

Összeférhetetlenségi vizsgálat elindítását kezdeményezheti a munkáltatói joggyakorló vezető, ha nem áll rendelkezésére elengő információt ahhoz, hogy megalapozott döntést tudjon hozni a nyilatkozat elbármásítása során. A munkáltatói joggyakorló vezető kezdeményezheti a vizsgálat megindítását, azzal, hogy értesíti a biztonsági szervezetet. A vizsgálat lefolytatásához a benyújtott összeférhetetlenségi nyilatkozatot kell alapul venni.

A vizsgálat lefolytatása után a biztonsági szervezet értesíti a munkáltatói joggyakorló vezetőt a vizsgálat eredményéről, aki, amennyiben szükséges, az intézkedéseket foganatosítja.
A nyilatkozatok véletlenszerű ellenőrzése

A nyilatkozatok véletlenszerű ellenőrzését, az azokban foglalt adatok helyességének vizsgálatát a biztonsági szervezet végzi a személyzeti osztály (HR) szervezet bevonásával.

Jogi következmények

A követelményeknek való nem megfelelés, illetve azok szándékos, vagy gondatlan megsértése esetén a vállalat és az alkalmazott közötti jogviszony tekintetében a fennálló jogszabályok az irányadóak.
Összegzett következtetések

Összegezeve megállapítható, hogy a hazai biztonságmenedzsment előzmények, alapok nélkül, több irányban is jelentős eredményeket tud felmutatni a magánszférában, határozott fejlődésen ment keresztül, de az összefogó, rendszerező, standardizáló feladatok még előttünk vannak. Ehhez nyújt iránymutatást ez a tanulmány, melynek célját egy külföldi példán keresztül a saját elgondolásonomat felvázolva, mintegy követhető elképzelésként, annak érdekében, hogy a kivánatossá vált és egységes, komplex vállalati biztonságmenedzsment rendszer kialakításra kerülhessen. Célkitűzésem volt, hogy értekezésem megírásával hozzá járuljak ahhoz, hogy a biztonsági szakmán belül kialakulhasson a hazai komplex biztonságmenedzsment szemlélet, melyhez egy követhető irányvonalat is felvázoltam. A jövőbeli célon alapvetően erre az értekezésre támaszkodva, ehhez kapcsolódva a komplex vállalati biztonságmenedzsment további területeinek a lefedéséhez szükséges eljárások felvázolása, pl.: a biztonsági folyamatok dokumentálása, a folyamatleírások, folyamatábrák és végrehajtási utasítások mintaszerű kialakításával, a biztonsági szolgáltatók egyszerű és hatékony minőségi ellenőrző rendszerének bemutatásával. A rendszer nem zárt, ahhoz mindig hozzá lehet építeni további szükséges modulokat, illetve ki lehet hagyni az adott vállalat tevékenységének és biztonsági szükségleteinek megfelelően [92].

Értekezésemben feldolgoztam a magyarországi vállalati biztonságmenedzsment jelenlegi helyzetét, vázoltam egy lehetséges, általam javasolt komplex irányú megközelítést, elkészítettem egy törzsanyagot, amire építkezhetnek a biztonsági vezetők, biztonsági szakemberek, illetve ez a disszertáció a vállalati biztonságmenedzsment oktatási anyagát is képezheti. Áttekintettem a hazai biztonságmenedzsment történeti, elméleti és gyakorlati előzményeit, hátterét. Elvégeztem a kapcsolódó nemzetközi és hazai szakirodalom és szakmai előzmények összegyűjtését (szakmai konferenciák, beszélgetések, kérdőív, stb.) és szakmai véleményemmel való ütköztetését.
Új tudományos eredmények

1. Bizonyítottam, hogy a szervezeteknél/vállalatoknál egy bizonyos szint felett a biztonságmenedzsment az adott szervezet biztonságát közvetlenül, pozitíván befolyásoló védelmi erőforrás.

2. Igazoltam, hogy szükséges a vállalat biztonságmenedzsmentet lefedő új elméleti és gyakorlati tartalommal rendelkező törzsanyag létrehozása, amelyre tudnak támaszkodni a biztonsági vezetők, biztonsági szakemberek és oktatók.

3. Kutatásaimmal bizonyítottam, hogy a multinacionális vállalatoknál, de bizonyos nemzetközi jelentőséggel rendelkező nagyvállalatoknál a biztonságmenedzsment szervezete nincs megfelelő helyen a szervezeti struktúrában és ezért a biztonságmenedzsmentet nem az indokolt fontossága szerint kezeli a vállalat vezetősége, így a vállalat biztonságmenedzsmentje nem tudja a leghatékonyabb módon ellátni a feladatát, a vállalati értékek védelmét.

4. Igazoltam, hogy a vállalati biztonságmenedzsment törzsanyagának alkalmazásával a biztonsági vezetők jobb eredményeket tudnak elérni, a kockázati tényezőket csökkenteni tudják a vállalati értékek megvédésének szempontjából, illetve szakmai elismertségük növekedhet a vállalat vezetőségén belül, így a biztonságmenedzsment jelentősége és érdekérvényesítő képessége is magasabbra kerülhet a vállalati hierarchiában.

5. Bebizonyítottam, hogy különböző vállalatoknál eltérő, és a vállalati biztonságmenedzsment nem minden területet átfogó biztonsági szabályzat-rendszer működik.

6. Létrehoztam a korábbi eredmények figyelembe vételével a vállalati komplex biztonságmenedzsment törzsanyagát, amelyben kidolgoztam a vállalati biztonságmenedzsment főbb témakörei szerinti követelményeket és ezen követelmények eléréséhez vezető javasolt eljárási rendet.
Ajánlások

A “Komplex biztonságmenedzsment” című doktori értekezésem eredményeinek hasznosíthatósága alapján az alábbi javaslatokat fogalmazom meg a kutatási eredmények tükrében, az alábbi területeken:

1. A biztonság területén tevékenykedő kutató és elméleti szakemberek számára ajánlom az álta lapse elkészített komplex biztonságmenedzsment törzsanyag használatát, amely alapot adhat a vállalati biztonságmenedzsment hatékony tudományos megközelítéséhez, fejlesztéséhez és a gyakorlati kiterjesztéséhez.

2. A biztonsági területtől foglalkozó oktatók számára ajánlom az értekezés használatát, kiindulópontként, lehetséges tananyag vázaként, illetve egy komplett vállalati biztonságmenedzsment modulként való felhasználását is.

3. Az állami szektorban dolgozó vezetők és biztonsági vezetők számára ajánlom az általam kiderített értekezés alkalmazását, amely használatával hatékonyabb és biztonságosabbá tehetik biztonsági szervezetük működését, valamint támogatást nyújthat számukra korunk vállalatbiztonsági kockázatainak csökkentéséhez, illetve felszámolásához.

4. Ajánlom a magánbiztonság megbízói területén munkáskodó biztonsági vezetőknek, akik a disszertációval felhasználásával feljegyzhetik biztonsági rendszerüket, ezáltal hatékonyabb működést tudnak elérni és a rájuk bizott vállalati értékeket megfelelően, kevesebb veszteséggel tudják védelmezni.

5. A biztonsági szolgáltatóknak ajánlom, akik az értekezésem felhasználásával közelebb kerülhetnek a megfelelő biztonsági megoldásokat ajánlani a megbízóiknak, amelyekre azoknak szükségük van. Így stabilabb és magasabb pozícióba kerülhetnek a biztonsági szolgáltatói piacon.
Hivatkozások


[22] HUTTON, Alex and HUBBARD, Doug: Measuring IT Risk. CSO, ISSN 1540-90X, 2011/03. 26-33. o.

[23] DRAZ, Daniel: Fraud Prevention, Improving Internal Controls. CSO, ISSN 1540-90X, 2011/05. 32-35. o.


[31] LOKEY, William M: Don’t let Plan Be the Disaster. Security Management, ISSN 0145-9406, 2009/06. 70. o.


[34] SPADANUTA, Laura: Threats in the Mail. Security Management, ISSN 0145-9406, 2010/08. 16-18. o.


[93] Zólyomi Zsolt: Detektor Plusz, ISSN 1217-9175, a Behatolás a biztonság elmélete és gyakorlata, Biztonsági irányítási rendszer és önellenőrzés, 2012. 2. szám 22-23. o.

[94] Zólyomi Zsolt: Detektor Plusz, ISSN 1217-9175, a Behatolás a biztonság elmélete és gyakorlata, Motozás, beléptető-rendszerek, 2011. 1. szám 16-17. o.


[99] Zólyomi Zsolt: Detektor Plusz, ISSN 1217-9175, a Behatolás a biztonság elmélete és gyakorlata, Összeférhetetlenség, 2011. 3. szám 17-18. o.

[100] Zólyomi Zsolt: Detektor Plusz, ISSN 1217-9175, a Behatolás a biztonság elmélete és gyakorlata, A biztonsági szervezet pénzügyi kontroll modellje, 2012. 3. szám 6-7. o.


[106] Az egészségügy és az ápolás általános alapelvi, Dr. Papp Katalin, Ujváriné Dr. Siket Adrienn (2014) Debreceni Egyetem Egészségügyi Kar, 5. Az alapvető emberi szükségeletek és
kielégítésük, 19. kép, Maslow szükségleti piramisa,
Felhasznált irodalom


[5]. 2012. évi C. törvény a Büntető Törvénykönyvről

[6]. A Kormány 1035/2012. (II. 21.) Korm. határozata Magyarország Nemzeti Biztonsági Stratégiájáról


[8]. A létfontosságú rendszerek és létesítmények azonosításáról, kijelöléséről és védelméről szóló 2012. évi CLXVI törvény 2. számú melléklete

[9]. A magánbiztonság aktuális nemzetközi trendjei, rövid hazai helyzetértékeléssel, In: Gaál Gyula, Hautzinger Zoltán (szerk.): Modernkori veszélyek rendszerszerte aspektusai, Pécsi Határőr Tudományos Közlemények, XV. Pécs, 2015, 57-64. oldalak, ISSN: 1589- 1674


[14]. Az üzleti hírszerzés és az ipari kémkedés Budapesti Műszaki és Gazdaságtudományi Egyetem Gazdaság-, és Társadalomtudományi Kar Információ-, és Tudásmenedzsment Tanszék Biztonságmenedzsment kutató csoport, Készítette: Erdősi Péter, CISA 2005


[20]. BM rendelet a személy-, és vagyonvédelmi, valamint a magánnyomozói tevékenység szabályairól szóló 2005. évi CXXXIII. törvény végrehajtásáról 68/2012. (XII.14.)

[21]. BM rendelet rendészeti feladatokat ellátó személyek, a segédfelügyelők, valamint a személy- és vagyonőrök képzéséről és vizsgáztatásáról


[28]. Country Evacuation Planning Guidelines; OGP International Association of Oil &Gas Producers; 209-2015 Blackfriars Road London SE1 8NL United Kingdom; September 2012; Report No. 472 (Version 1.1)

[30]. Cynthia Hetherington; Business Background Investigations; Cynthia Hetherington and BRB Publications, Inc.; PO Box 27869 Tempe, AZ 85285 800.929.3811; 2010; ISBN 978-1-889150-49-9

[31]. CSO (Cheif Security Officer): by CXO Media Inc., 492 Old Connecticut Path, P.O. Box 9208, Framingham, MA01701-9208, ISSN 1540-904X. következő kiadványai: 2010. 02, 03, 04, 05, 06, 07-08, 09, 11; 2011. 12-01, 02, 03, 04, 05, 09, 10, 11; 2012. 05, 06, 07-08, 09; 2013. 09.


[43]. Firearms and the use of force; OGP International Association of Oil &Gas Producers; 209-2015 Blackfriars Road London SE1 8NL United Kingdom; February 2010; Report No. 320, revision 2


[47]. General Security Risk Assessment Guideline; ASIS International; 1625 Prince Street, Alexandria, Virginia 22314-2818 USA; 2003; 703-519-6200


[52]. Integrating security in major projects – principles & guidelines; OGP International Association of Oil &Gas Producers; 209-2015 Blackfriars Road London SE1 8NL United Kingdom; April 2014; OGP Report No. 494


[57]. Kiss Péter: Humánbiztonság – módszerek alkalmazása, Információbiztonság, 2008/május, 6-7. oldalak
[60]. Magánbiztonsági képzés – nem középiskolás fokon. IN: Biztonságpiac évkönyv, 2015., 119-120. oldalak
[63]. Márkus Csaba: Magyar biztonságtechnika I., Fejezetek a magyar biztonságtechnika történetéből, SLV Press Kiadó 2009
[68]. Munka Törvénykönyve (2012. évi I. tv.) 8.§-11.§, 52.§
[69]. Nagy Rudolf: A kritikus infrastruktúra védelme elméleti és gyakorlati kérdéseinek kutatása, PhD értekezés, Zrínyi Miklós Nemzetvédelmi Egyetem Hadmérnöki Doktori Iskola, 2011
[71]. Pádár Péter: Üzletmenet folytonosság menedzsment
[72]. Péczeli Anna: A humán biztonság elmélete és gyakorlata Kanada és Japán példáján, Grótius, 2012


[76]. Response to demonstration at company premises; OGP International Association of Oil &Gas Producers; 209-2015 Blackfriars Road London SE1 8NL United Kingdom; March 2010; Document No. 308

[77]. Response to demonstration at offshore facilities; OGP International Association of Oil &Gas Producers; 209-2015 Blackfriars Road London SE1 8NL United Kingdom; March 2010; Document No. 309


[80]. Schutzbach Mártonné: Az informatikai biztonság általános koncepciója és gyakorlata a védelmi szférában, Nemzetvédelmi Egyetemi Közlemények, 7. évfolyam, 2. szám, 2003, 155. oldal


[82]. Security Management System; OGP International Association of Oil &Gas Producers; 209-2015 Blackfriars Road London SE1 8NL United Kingdom; July 2014; OGP Report No. 512

[83]. Security Management: by ASIS International, 1625 Prince St., Alexandria, VA22314; 703/519-6200, ISSN 0145-9406. következő kiadványai: 2006. 09, 10, 11, 12; 2007. 01, 02, 03, 05, 06, 09; 2008. 05, 11, 12; 2009. 03, 04, 05, 06, 07, 08, 09, 10, 11, 12; 2010. 01-12; 2011. 01-12; 2012. 01-12; 2013. 01, 03, 04, 05, 06, 08, 09; 2014. 06-12; 2015.01-03.
[84]. Sik Zoltán Nándor: A kritikus információs infrastruktúra védelem kormányzati feladatai az információs hadviselés korában
letöltve: 2013. december 17.


[88]. Szenes Katalin: Informatikai biztonsági módszerek kiterjesztése a vállalatiirányítás, a működés, és a kockázatkezelés támogatására; Minőségés Megbizhatóság; nemzeti minőségpolitikai szakfolyóirat, kiadja: az European Organization for Quality (EOQ) Magyar Nemzeti Bizottsága, XLVI. év. 2012. / 5. sz., 252-257. oldalak, ISSN: 0580-4485

[89]. Szövényi György: Biztonságvédelmi szabályzat, Budapest, KJK-Kerszőv, 2000


[102]. Tóth Attila - Tóth Levente: Biztonságtechnika, Nemzeti Közszolgálati Egyetem Rendészettudományi Kar, Budapest, 2010

[103]. Tóth Attila - Tóth Levente: Biztonságtechnika, Nemzeti Közszolgálati Egyetem Rendészettudományi Kar, Budapest, 2010


[108]. W. Barry Nixon, Kim M. Kerr; Background Screening and Investigations; Elsevier Inc.; 30 Corporate Drive, Suite 400, Burlington, MA 01803, USA; Linacre House, Jordan Hill, Oxford OX

1995. 548 First St., Crete, IL 60417, U.S.A. (708) 672-4200.


[111]. Utassy Sándor: Komplex villamos rendszerek biztonságtechnikai kérdései, doktori (PhD) értekezése 2009
letöltve: 2019.09.01.17:00
Ábrajegyzék

1. ábra A vagyonvédelem .......................................................................................... 10
2. ábra Utassy féle vagyonvédelem ........................................................................ 11
3. ábra A biztonsági rendszer ................................................................................ 12
4. ábra Tevékenység szerinti megoszlás ................................................................ 19
5. ábra Szervezeti szint szerinti megoszlás ............................................................. 20
6. ábra Felelősségi terület szerinti megoszlás ........................................................... 21
7. ábra Szervezeti felépítés szerinti megoszlás ......................................................... 22
8. ábra Szabályzati lefedettség szerint .................................................................... 23
9. ábra ábra Szabályzati hiányosságok megoszlása .................................................. 24
10. ábra Szabályzati lefedettség átlaga ...................................................................... 25
11. ábra A biztonságirányítási rendszer hierarchiája .................................................. 31
12. ábra A biztonságirányítási rendszer szintjei ............................................................ 32
13. ábra A biztonságirányítási rendszer folyamszemlélet irányából ......................... 32
14. ábra Kockázatértékelés ....................................................................................... 47
15. ábra A kockázatértékelés ponthatárai ................................................................... 47
16. ábra Válságkezelés helyzete az üzletmenet-folytonosságban .............................. 95
17. ábra A válságkezelés bizonyított eredménye ....................................................... 95
18. ábra A vállalat krízismenedzsment rendszere ..................................................... 98
19. ábra Krízismenedzsment tervek szintenénti kapcsolódása .................................. 102
20. ábra A krízismenedzsment szervezeti felépítése .................................................. 111
21. ábra A magyarországi biztonsági vezetők egyesületének névsora .................... 152
22. ábra A legnagyobb nyereséget termelő cégek ....................................................... 153
23. ábra A 10 legnagyobb foglalkoztató .................................................................... 154
24. ábra Az 50 legnagyobb export-árbevételű magyar cég .......................................... 155
A szerző publikációi

1. A védelmi rendszer humán tényezői (ipari üzemek, gyárak tekintetében), Az XY Kft. védelme 2000/11, A Detektor Plusz országos pályázatán elért „Az év biztonságvédelmi menedzsere különdíj” a szakma legjobbjai pályázaton. Az adományozó az Országos Bűnmegelőzési Tanács.

2. Védekezzünk a terror ellen, biológiai terrorizmus, Nemzetközi Testőr és Biztonsági Szolgálatok Szövetsége (IBSSA) konferencia 2002/01.

3. Termelő üzem felszámolása során a biztonsági igazgatóság feladata, Magyarországi Biztonsági Vezetők Egyesülete (MBVE) IV. konferencia, 2003/03.

4. Madárinfluenza, MBVE VII. konferencia, 2006/03.


8. Harc az olajért, MBVE XI. konferencia, 2010/03.


12. Kérdezz-felelek rovat létrehozása és folyamatos írása a Detektor Plusz, a biztonság lapjában, ISSN 1217-9175, a Behatolás a biztonság elmélete és gyakorlata címmel, „Behatolás” a biztonság elméletébe és gyakorlatába, 2010. 5-6. sz. 15. o.


18. Összeférhetetlenség, 2011. 3. szám 17-18. o.
29. A MOL krízismenedzsment rendszere, együttműködés az iparbiztonsági szabályozás mentén, 2012/05/30, Budapest, BM OKF Iparbiztonsági konferencia
30. A kritikus infrastruktúra biztonsági aspektusai a MOL-nál, 2012/09/18, Budapest, Változó környezet, változó biztonság, kiberfenyegetések kihívásainak napjainkban, Nemzetközi tudományos-szakmai konferencia
34. A MOL, mint kritikus infrastruktúra, Vezérkari tanfolyam, VKT-24, NKE 2013/02/11.
36. MOL érdekeltségek védelme Pakisztánban és Irakban, külföldi harcosok bevonásával, “A terrorizmus Rubik-kockája, avagy a fenyegetések komplex megközelítése” Nemzetközi tudományos-szakmai konferencia, 2013/10/01. Budapest, angol nyelven


39. MOL Csoport kitermelési helyek és szállítási útvonalak biztonsági helyzete és biztosítottsága, NKE Hadtudományi PhD képzés, Budapest, 2014/04/15.

40. Biztonsági kihívások a délszláv régióban, Nemzetbiztonsági Intézet Konferencia, Biztonság a Nyugat-Balkánon, NKE, Budapest, 2014/06/05.


### Mellékletek

#### 1.sz. melléklet

A Magyarországi Biztonsági Vezetők Egyesületének névsora

Az egyesület honlapja bemutatja a szervezetet és közli a tagok listáját (2017. szeptember 24-állapot szerint).

"A Magyarországi Biztonsági Vezetők Egyesülete a hazai szakmai elit reprezentatív érdekképviselete.

<table>
<thead>
<tr>
<th>NÉV</th>
<th>TAGSÁG</th>
<th>CÉG</th>
</tr>
</thead>
<tbody>
<tr>
<td>Baranyai Zoltán</td>
<td>Szakmai</td>
<td>MÁV Ingatlankezelési Kft</td>
</tr>
<tr>
<td>Batyik Géza</td>
<td>Szakmai</td>
<td>MBVE szakértő</td>
</tr>
<tr>
<td>Bazsó László</td>
<td>Szakmai</td>
<td>Provident Financial Zrt</td>
</tr>
<tr>
<td>Bedő Csaba</td>
<td>Szakmai</td>
<td>Citibank Zrt.</td>
</tr>
<tr>
<td>Bertényi Kornél</td>
<td>Szakmai</td>
<td>MBVE szakértő</td>
</tr>
<tr>
<td>Boda József dr.</td>
<td>Tiszteletbeli</td>
<td>Nemzeti Közszolgálati Egyetem Rendészettudományi Kar</td>
</tr>
<tr>
<td>Borbély Tibor</td>
<td>Szakmai</td>
<td>UniCreditbank Hungary Zrt</td>
</tr>
<tr>
<td>Bozsik Frigyes dr.</td>
<td>Szakmai</td>
<td>MBVE szakértő</td>
</tr>
<tr>
<td>Cselovszki Zoltán</td>
<td>Szakmai</td>
<td>Szerencsejáték Zrt</td>
</tr>
<tr>
<td>Czintula György dr.</td>
<td>Szakmai</td>
<td>Pro-M Zrt</td>
</tr>
<tr>
<td>Czirkus László</td>
<td>Szakmai</td>
<td>MBVE szakértő</td>
</tr>
<tr>
<td>Dósa Imre dr.</td>
<td>Szakmai</td>
<td>Budapest Bank Nyrt</td>
</tr>
<tr>
<td>Duba Róbert</td>
<td>Szakmai</td>
<td>Szerencsejáték Zrt</td>
</tr>
<tr>
<td>Farkas Gábor</td>
<td>Szakmai</td>
<td>Csongrád Megyei Kormányhivatal</td>
</tr>
<tr>
<td>Feke László</td>
<td>Szakmai</td>
<td>Justice Security Kft</td>
</tr>
<tr>
<td>Fialka György dr.</td>
<td>Szakmai</td>
<td>MBVE szakértő</td>
</tr>
</tbody>
</table>
Gerencsér István dr.  Szakmai  Flextronics International Kft.
Görombei László  Szakmai  Syngenta Seeds Kft.
Holló Attila Csaba  Szakmai  MNB-Biztonsági Zrt
Iszály Mihály dr.  Szakmai  ÁNY Biztonsági Nyomda Zrt
Jakab Péter  Szakmai  MBVE szakértő
Jónás Endre dr.  Szakmai  Fővárosi Közterület Fenntartó Zrt
Kakas Nándor  Szakmai  MBVE szakértő
Kalmár István dr  Szakmai  MBVE szakértő
Károlyi László dr.  Szakmai  Magyar Posta Zrt/ MBVE alelnök
Kárpáti Miklós  Szakmai  NISZ Zrt.
Klézl Marina  Pártoló  Detektor Plusz Biztonságvédelmi szaklap
Kovács György  Szakmai  Justice Security Kft
Kovács Olivér  Szakmai  MET Services
Kovács Roland  Szakmai  OTP Bank Nyrt.
Kovács Tim  Szakmai  General Electric
Major László dr.  Szakmai  Magyar Posta Zrt.
Markó Béla  Szakmai  Pénzjegynyomda Zrt
Mayer Gyula  Szakmai  EMEA Távolsági Szolgáltató Zrt
Mészáros István  Szakmai  Semmelweis Egyetem
Mohácsi Péter  Szakmai  Lego Manufacturing Kft
Nagy Lajos  Szakmai  Coca-Cola HBC Magyarország Kft
Nagy László dr.  Tiszteletbeli  ASVA (Audióvizuális Művek Szerzői Jogait Védő Közhasznú Alapítvány
Németh Árpád Dávid  Szakmai  MBVE szakértő
Németh Gyula  Szakmai  Siemens Real Estate
Pallagi András  Szakmai  MBVE szakértő
Papp András dr.  Szakmai  EGIS Nyrt
21. ábra A magyarországi biztonsági vezetők egyesületének névsora
A legnagyobb nyereséget termelő cégek

![Table Image]

22. ábra A legnagyobb nyereséget termelő cégek

http://hvg.hu/gazdasag/20161111 ime_a_legnagyobb_nyereseget_termelo_cegek_top500

(letöltés: 2017.09.24. 16:43)
3. sz. melléklet

A 10 legnagyobb foglalkoztató:

<table>
<thead>
<tr>
<th></th>
<th>létszám (fő)</th>
<th>változás (százalék)</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. OTP Bank Zrt.</td>
<td>35796</td>
<td>-5</td>
</tr>
<tr>
<td>2. Magyar Posta Zrt.</td>
<td>33084</td>
<td>-1</td>
</tr>
<tr>
<td>4. Magyar Államvasutak Zrt.</td>
<td>17094</td>
<td>0</td>
</tr>
<tr>
<td>5. MÁV-Start Zrt.</td>
<td>14229</td>
<td>107</td>
</tr>
<tr>
<td>6. Spar Magyarország Kereskedelmi Kft.</td>
<td>14015</td>
<td>3</td>
</tr>
<tr>
<td>7. Budapesti Közlekedési Zrt.</td>
<td>11760</td>
<td>-1</td>
</tr>
<tr>
<td>8. Richter Gedeon Vegyészeti Gyár Nyrt.</td>
<td>11759</td>
<td>3</td>
</tr>
<tr>
<td>9. Magyar Telekom Távközlési Zrt.</td>
<td>11050</td>
<td>-3</td>
</tr>
<tr>
<td>10. Audi Hungaria Motor Zrt.</td>
<td>10868</td>
<td>14</td>
</tr>
</tbody>
</table>

23. ábra A 10 legnagyobb foglalkoztató

https://444.hu/2015/07/23/30-legnagyobb-ceg

(letöltés: 2017. 09. 24. 16:55)

A bemutatott vállalati top-listák alapján összességében megállapítható, hogy a válaszadók a magyarországi gazdasági élet vezető vállalatainál töltenek be biztonsági vezetői beosztást és így válaszaik mértékadóak a hazai vállalati biztonságmenedzsment szempontjából.
# Az 50 legnagyobb export-árbevételi magyarországi cég 2015-ben

<table>
<thead>
<tr>
<th>Helyezés</th>
<th>Cégnév</th>
<th>Ágazat</th>
<th>Külföldi árbevétel</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>3. GE Infrastructure CEE Holding Kft.*</td>
<td>vegykereskedés</td>
<td>4 483 809 122</td>
</tr>
<tr>
<td>2.</td>
<td>4. Mol Magyar Olaj és Gázipari Nyrt.**</td>
<td>energiaipar</td>
<td>2 998 282 14</td>
</tr>
<tr>
<td>3.</td>
<td>5. Audi Hungaria Motor Kft.</td>
<td>autógyártás</td>
<td>2 509 054 12</td>
</tr>
<tr>
<td>4.</td>
<td>6. Mercedes-Benz Manufacturing Hungary Kft.</td>
<td>autógyártás</td>
<td>1 062 038 20</td>
</tr>
<tr>
<td>5.</td>
<td>7. Samsung Electronics Magyar Zrt.</td>
<td>elektronikaipar</td>
<td>627 977 9</td>
</tr>
<tr>
<td>6.</td>
<td>8. Magyar Suzuki Zrt.</td>
<td>autógyártás</td>
<td>580 646 26</td>
</tr>
<tr>
<td>7.</td>
<td>9. Wizz Air Hungary Kft.</td>
<td>gépjárműipar</td>
<td>493 292 26</td>
</tr>
<tr>
<td>8.</td>
<td>10. Electrónica International Kft. (x)</td>
<td>elektronikaipar</td>
<td>469 051 12</td>
</tr>
<tr>
<td>9.</td>
<td>11. MV Máv Magyar Villamos Művek Zrt.*</td>
<td>vegykereskedés</td>
<td>463 662 37</td>
</tr>
<tr>
<td>10.</td>
<td>12. Robert Bosch Elektronika Kft.</td>
<td>autógyártás</td>
<td>458 589 12</td>
</tr>
<tr>
<td>11.</td>
<td>13. Bimbo Hungria Zrt.</td>
<td>vegykereskedés</td>
<td>451 934 7</td>
</tr>
<tr>
<td>13.</td>
<td>15. PCE Paragon Solutions Kft.</td>
<td>elektronikaipar</td>
<td>284 648 0</td>
</tr>
<tr>
<td>14.</td>
<td>16. BoschChem Zrt.</td>
<td>vegykereskedés</td>
<td>284 470 3</td>
</tr>
<tr>
<td>15.</td>
<td>17. GDF-Suez Földgázkereskedési Kft.</td>
<td>vegykereskedés</td>
<td>275 787 133</td>
</tr>
<tr>
<td>17.</td>
<td>19. sanofi-aventis /Chinon*</td>
<td>vegykereskedés</td>
<td>261 486 3</td>
</tr>
<tr>
<td>18.</td>
<td>20. Harman Becker Kft.</td>
<td>autógyártás</td>
<td>250 113 53</td>
</tr>
<tr>
<td>19.</td>
<td>21. Jabil Circuit Magyarország Kft.</td>
<td>elektronikaipar</td>
<td>232 337 1</td>
</tr>
<tr>
<td>20.</td>
<td>22. Electroly Lelő Hűtőgázgyár Kft.</td>
<td>autógyártás</td>
<td>230 081 2</td>
</tr>
<tr>
<td>21.</td>
<td>23. MOL Petrolkémia Kft. (vált TVK)</td>
<td>vegykereskedés</td>
<td>225 028 17</td>
</tr>
<tr>
<td>22.</td>
<td>24. Lék Savaria Küplanygyár Kft.</td>
<td>autógyártás</td>
<td>222 382 16</td>
</tr>
<tr>
<td>23.</td>
<td>25. Continental Automotive Hungary Kft.</td>
<td>autógyártás</td>
<td>219 915 5</td>
</tr>
<tr>
<td>24.</td>
<td>26. Michelin Hungária Automoszgégyár Kft.</td>
<td>autógyártás</td>
<td>218 975 4</td>
</tr>
<tr>
<td>25.</td>
<td>27. Hankook Tire Magyarország Kft.</td>
<td>autógyártás</td>
<td>211 988 45</td>
</tr>
<tr>
<td>26.</td>
<td>28. Alba-Kölem Kft.</td>
<td>vegykereskedés</td>
<td>204 796 16</td>
</tr>
<tr>
<td>27.</td>
<td>29. Delphi Hungary Kft.</td>
<td>autógyártás</td>
<td>193 434 7</td>
</tr>
<tr>
<td>28.</td>
<td>30. Tero Gépgyártó és Székhely Zrt.*</td>
<td>vegygyár és -magyarság</td>
<td>186 192 14</td>
</tr>
<tr>
<td>29.</td>
<td>31. Lear Corporation Hungary Kft.</td>
<td>autógyártás</td>
<td>180 317 8</td>
</tr>
<tr>
<td>30.</td>
<td>32. Denso Gyár Kft. Magyarország Kft. (x)</td>
<td>autógyártás</td>
<td>178 704 19</td>
</tr>
<tr>
<td>31.</td>
<td>33. Ni Hungary Kft.</td>
<td>elektronikaipar</td>
<td>168 643 4</td>
</tr>
<tr>
<td>32.</td>
<td>34. SE-CEE Schneider Electric Kft.</td>
<td>vegykereskedés</td>
<td>162 986 10</td>
</tr>
<tr>
<td>33.</td>
<td>35. Opel Southeast Europe Kft.</td>
<td>autógyártás</td>
<td>160 645 19</td>
</tr>
<tr>
<td>34.</td>
<td>36. Berg-Warner Rözköly Kft.</td>
<td>autógyártás</td>
<td>135 293 16</td>
</tr>
<tr>
<td>35.</td>
<td>37. Synopsys Global Kft.</td>
<td>vegygyár és -magyarság</td>
<td>113 653 26</td>
</tr>
<tr>
<td>36.</td>
<td>38. Glencore Grain Hungary Kft.</td>
<td>vegykereskedés</td>
<td>108 444 10</td>
</tr>
<tr>
<td>37.</td>
<td>39. Vako Auto-Electric Magyarország Kft.</td>
<td>autógyártás</td>
<td>107 571 29</td>
</tr>
<tr>
<td>38.</td>
<td>40. Johnson Controls Mér Bl.</td>
<td>autógyártás</td>
<td>107 046 0</td>
</tr>
<tr>
<td>39.</td>
<td>41. Porsche Hungária Kft.</td>
<td>autógyártás</td>
<td>102 147 7</td>
</tr>
<tr>
<td>40.</td>
<td>42. SMP Automotive Mirror Technology Bl. (x)</td>
<td>autógyártás</td>
<td>100 054 13</td>
</tr>
<tr>
<td>41.</td>
<td>43. Robert Bosch Automotive Steering Kft.</td>
<td>autógyártás</td>
<td>97 382 53</td>
</tr>
<tr>
<td>42.</td>
<td>44. Ixion Hungary Kft.</td>
<td>autógyártás</td>
<td>97 259 18</td>
</tr>
<tr>
<td>43.</td>
<td>45. Egyes Güvészfőnökség Zrt.**</td>
<td>vegygyár</td>
<td>97 150 3</td>
</tr>
<tr>
<td>44.</td>
<td>46. Videoton Holding Zrt.*</td>
<td>vegygyár</td>
<td>97 120 5</td>
</tr>
<tr>
<td>45.</td>
<td>47. Magyar Telekom Távközlési Nyrt.**</td>
<td>teleközlés</td>
<td>89 758 7</td>
</tr>
<tr>
<td>46.</td>
<td>48. Apcoa CE Kft.</td>
<td>vegykereskedés</td>
<td>89 215 256</td>
</tr>
<tr>
<td>47.</td>
<td>49. Celoplast Hungary Kft.</td>
<td>vegygyár és -magyarság</td>
<td>85 417 15</td>
</tr>
<tr>
<td>48.</td>
<td>50. Grundfos Magyarország Kft.</td>
<td>vegygyár</td>
<td>83 242 45</td>
</tr>
<tr>
<td>49.</td>
<td>51. Bunge Növényiparipari Kft.</td>
<td>vegygyár és -magyarság</td>
<td>83 205 2</td>
</tr>
<tr>
<td>50.</td>
<td>52. Zoltec Kft.</td>
<td>vegygyár és -magyarság</td>
<td>81 678 151</td>
</tr>
</tbody>
</table>


24. ábra Az 50 legnagyobb export-árbevételi magyar cég

[http://hvg.hu/enesacegem/20160724_Top_50_HVGtoplista_a_legnagyobb_magyar_cegekrol](http://hvg.hu/enesacegem/20160724_Top_50_HVGtoplista_a_legnagyobb_magyar_cegekrol)

(letöltés: 2017. 09. 24. 17:13)
5.sz. melléklet

KÉRДŐÍV

1. Név: …………………………… beosztás:……………………… Cég:………………………………………

2. Válassza ki a legmegfelelőbbet felelőssége területe szerint!* 
   - régiós (több ország)
   - országos
   - helyi

3. Munkavállalók száma az Ön felelősségi területén:……………………………………

4. Saját szervezet létszáma: 
   alkalmazott: …………………alvállalkozó:……………………………………

5. Ki a közvetlen vezetője üzleti vonalon?* (munkáltatói joggyakorló) 
   - a vállalat elsőszámú vezetője
   - második szintű vezető, beosztása: ………………………………………
   - harmadik szintű vezető, beosztása: ………………………………………

6. Ha ettől eltérő pl. mátrix rendszer esetén a biztonsági felettes:*  
   - a vállalat csoportszintű (legfőbb) biztonsági vezető
   - régiós biztonsági vezető
   - országos biztonsági vezető

7. Van-e biztonsági szabályzat a cégnél?* 
   - igen
   - más szervezettel közös
   - nincs

8. Ha van, akkor mely fejezeteket tartalmazza?*  
   - fizikai biztonság
   - információ biztonság
   - humán biztonság
   - krízismenedzsment
   - vizsgálatok
   - biztonsági oktatás
   - egyéb:……………………………………
9. Hozzájárulok, hogy az általam megadott adatokat Zólyomi Zsolt felhasználhassa a doktori értekezéséhez:*
   - igen
   - nem

10. Hozzájárulok, hogy az általam megadott adatokat a nevem és a cégnév kivételével Zólyomi Zsolt felhasználhassa a doktori értekezéséhez:*
    - igen
    - nem

* A megfelelő választ kérem, húzza alá.

Budapest, 2014/10/14. ..................................................

aláírás
6.sz. melléklet

Kockázatelemzés dokumentáció

(elkészítésének gyakorisága: évente)

Az objektum neve:…………………………………Címe:……………………………………………

A szabályzat 3.4.4 pontja alapján, kategorizálja az objektumot.

<table>
<thead>
<tr>
<th>Szsz.</th>
<th>Kategória nevek</th>
<th>Az objektum kategóriába sorolása:</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>0-s kategória: (FEKETE)</td>
<td></td>
</tr>
<tr>
<td>2</td>
<td>1-es kategória: (PIROS)</td>
<td></td>
</tr>
<tr>
<td>3</td>
<td>2-es kategória: (SÁRGA)</td>
<td></td>
</tr>
<tr>
<td>4</td>
<td>3-as kategória: (ZÖLD)</td>
<td></td>
</tr>
<tr>
<td>5</td>
<td>4-es kategória: (FEHÉR)</td>
<td></td>
</tr>
</tbody>
</table>

A szabályzat 3.4.4 pontja alapján, végezze el a kockázatelemzési dokumentációt.

<table>
<thead>
<tr>
<th>A lkategória</th>
<th>Nincs</th>
<th>Alacsony</th>
<th>Közepes</th>
<th>Magas</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. Terrorizmus</td>
<td>0</td>
<td>1</td>
<td>2</td>
<td>3</td>
</tr>
<tr>
<td>2. Munkahelyi erőszak</td>
<td>0</td>
<td>1</td>
<td>2</td>
<td>3</td>
</tr>
<tr>
<td>3. Közveszélyes bűncselekmény, belső</td>
<td>0</td>
<td>1</td>
<td>2</td>
<td>3</td>
</tr>
<tr>
<td>4. Közveszélyes bűncselekmény, külső</td>
<td>0</td>
<td>1</td>
<td>2</td>
<td>3</td>
</tr>
<tr>
<td>5. Természeti és emberi eredetű katasztrófa</td>
<td>0</td>
<td>1</td>
<td>2</td>
<td>3</td>
</tr>
</tbody>
</table>

Összesen:
Adja meg, hogy az objektum mely veszélyeztetettségi kategóriába tartozik:

<table>
<thead>
<tr>
<th>Pont</th>
<th>Alacsony</th>
<th>Közepes</th>
<th>Magas</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>ZOLD</td>
<td>SÁRGA</td>
<td>PIROS</td>
</tr>
</tbody>
</table>

0–5   6–10   11–15

Jelölje X-el az objektum veszélyeztetettségi fokát:

A dokumentációt készítette:……………………………………

Dátum: ………………………………………

A következő teszt időpontja: ………………………………………
7.sz. melléklet

Kritikus közművek meghatározása

(élkészítésének gyakorisága: évente)

Az objektum neve: ...........................................................................................................

Címe: .................................................................................................................................

A szabályzat 4.1.2. pontja alapján, azonosítsa, határozza meg, sorolja fel az objektumban található kritikus közműveket:

<table>
<thead>
<tr>
<th>Ssz.</th>
<th>A kritikus közmű megnevezése – leírása - helye</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td></td>
</tr>
<tr>
<td>2</td>
<td></td>
</tr>
<tr>
<td>3</td>
<td></td>
</tr>
<tr>
<td>4</td>
<td></td>
</tr>
<tr>
<td>5</td>
<td></td>
</tr>
<tr>
<td>6</td>
<td></td>
</tr>
<tr>
<td>7</td>
<td></td>
</tr>
<tr>
<td>8</td>
<td></td>
</tr>
</tbody>
</table>

A dokumentációt készítette: .................................................................

Dátum: .................................................................

A következő teszt időpontja: .................................................................
8.sz. melléklet

Az objektum bejáratainál lévő biztonsági berendezések felülvizsgálata

(elkészítésének gyakorisága: 90 naponta)

Az objektum neve: ..............................................................................................................

Címe: ...............................................................................................................................

A szabályzat 4.1.3 pontja alapján, azonosítsa, határozza meg, működőképességét vizsgálja meg, sorolja fel az objektum bejáratainál lévő biztonsági berendezéseket:

<table>
<thead>
<tr>
<th>Ssz.</th>
<th>A berendezések helye:</th>
<th>A biztonsági berendezések neve:</th>
<th>Működőképes: igen/nem</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>2</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>3</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>4</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>5</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>6</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>7</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

A dokumentációt készítette: ..................................................

Dátum: ...........................................

A következő teszt időpontja: ..............................................
9.sz. melléklet

**Egyéb bejutási pontok**

*(elkészítésének gyakorisága: évente)*

Az objektum neve: .............................................................................................................

Címe: .............................................................................................................................

A szabályzat, 4.1.7 pontja alapján, azonosítsa, határozza meg, sorolja fel, hogy hol találhatóak a
vagyonvédelmi technikával védett objektumba, épületekbe történő behatolásra alkalmas védetlen, kevésbé
nyilvánvaló pontjai. (például szellőzőrácsok, lefolyók, aknafedők, közműalagutak, napfénytetők, tetőablakok
vagy szellőzők)

<table>
<thead>
<tr>
<th>Ssz.</th>
<th>Egyéb bejutási pontok helye:</th>
<th>Védettsége: nincs / rács, lakat, stb...</th>
<th>Egyéb:</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>2</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>3</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>4</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>5</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>6</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>7</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

A dokumentációt készítette: ..........................................................

**Dátum:** ..................................................

A következő teszt időpontja: .............................................
10.sz. melléklet

Rejtőzködésre alkalmas helyek

(élkészítésének gyakorisága: évente)

Az objektum neve: ………………………………………………………………………………………………………

Címe: ………………………………………………………………………………………………………………………

Ellenőrizze le a szabályzat 4.1.8 pontja alapján, hogy az objektum kerítése vagy telekhatára mellett a külső oldalon, attól egy méteren belül telepített kertészeti elemek találhatóak-e, vagy nem.

igen □ nem □

Ellenőrizze le a szabályzat 4.1.8 pontja alapján, hogy az objektum kerítése vagy telekhatára mellett a külső oldalon, attól egy méteren belül olyan tárgyat, amely alkalmas robbanó szerkezet elrejtésére, például szemetes kuka, konténer, újrafelhasználható anyagok gyűjtője, stb. találhatóak-e, vagy nem.

igen □ nem □

Szükséges intézkedések felsorolása:

________________________________________________________________________________________________________

________________________________________________________________________________________________________

________________________________________________________________________________________________________

________________________________________________________________________________________________________

________________________________________________________________________________________________________

________________________________________________________________________________________________________

________________________________________________________________________________________________________

________________________________________________________________________________________________________

________________________________________________________________________________________________________

________________________________________________________________________________________________________

________________________________________________________________________________________________________

________________________________________________________________________________________________________

________________________________________________________________________________________________________

________________________________________________________________________________________________________

A dokumentációt készítette: …………………………………

Dátum: …………………………………………………

A következő teszt időpontja: ………………………………………
Biztonsági riasztók ellenőrzése

(elkészítésének gyakorisága: 90 naponta)

Az objektum neve:……………………………………………………………………………………………………

Címe:…………………………………………………………………………………………………………………………

A szabályzat 4.2.2 pontja alapján, ellenőrizze le, tesztelje a biztonsági riasztó rendszer minden elemét (riasztókat).

<table>
<thead>
<tr>
<th>Ssz.</th>
<th>Riasztó pontos elhelyezkedése / típusa</th>
<th>A riasztó működik</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td>Igen</td>
</tr>
<tr>
<td>1</td>
<td></td>
<td></td>
</tr>
<tr>
<td>2</td>
<td></td>
<td></td>
</tr>
<tr>
<td>3</td>
<td></td>
<td></td>
</tr>
<tr>
<td>4</td>
<td></td>
<td></td>
</tr>
<tr>
<td>5</td>
<td></td>
<td></td>
</tr>
<tr>
<td>6</td>
<td></td>
<td></td>
</tr>
<tr>
<td>7</td>
<td></td>
<td></td>
</tr>
<tr>
<td>8</td>
<td></td>
<td></td>
</tr>
<tr>
<td>9</td>
<td></td>
<td></td>
</tr>
<tr>
<td>10</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

A dokumentációt készítette:………………………………………

Dátum: ………………………………………

A következő teszt időpontja: ………………………………………

11.sz. melléklet
12.sz. melléklet

A vállalat korlátozott hozzáférésű területei
(elkészítésének gyakorisága: 90 naponta)

Az objektum neve:……………………………………………………………………………………
Címe:…………………………………………………………………………………………………..

A szabályzat 4.2.6. pontja alapján határozza meg van-e az objektumban korlátozott hozzáférésű terület.

Korlátozott hozzáférésű terület □ van □ nincs □
az objektumban.

Ha van korlátozott hozzáférésű terület az objektumban:

A belépési kód cseréje megtörtét □ igen □ nem □
A kódcsere időpontja:………………………………………………………………………………

A korlátozott hozzáférésű területek beléptető rendszerében nem szereplő személyek

belépése - kilépése naplózott □ igen □ nem □

A korlátozott hozzáférésű területek naplójának felülvizsgálata megtörtént, a napló a helyi vezető

aláírásával és dátummal ellátott □ igen □ nem □

A napló felülvizsgálatának időpontja:………………………………………………………………
A korlátozott hozzáférésű terület beléptető

rendszer adatait átvizsgálva: □ igen □ nem □

Ellenőrizze le, hogy a korlátozott hozzáférésű terület szerkezeti elemei nem átjárhatóak,
vagy elektronikus riasztó rendszer van bekapcsolt: □ rendben □ nem megfelelő □

Ellenőrizze le, hogy a belső mozgásérzékelők bekapcsoltak, amikor a helyszínen nem tartózkodnak. □ rendben □ nem megfelelő □
Ellenőrizze le, hogy a vészkijáratokon és a csak
kijáratra használt ajtók riasztóval ellátottak. rendben □ nem megfelelő □

Ellenőrizze le, hogy a külső ablakok a földszinten,
polikarbonát üvegezést vagy más szilánkmentes
megoldással ellátottak. rendben □ nem megfelelő □

Ellenőrizd le, hogy minden külső ablakon
riasztó van elhelyezve: rendben □ nem megfelelő □

A dokumentációt készítette:……………………………………

Dátum: ………………………………………

A következő teszt időpontja: ………………………………………
13.sz. melléklet

**Főkulcsok elszámolása**

(elkészítésének gyakorisága: évente)

Az objektum neve:………………………………Címe:…………………………………………

A szabályzat 4.2.13. pontja alapján, határozza meg, milyen biztonsági kulcsokat használnak az objektum területén?

<table>
<thead>
<tr>
<th>Sz.</th>
<th>Kulcs megnevezése</th>
<th>Igen/Nem</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Főkulcs</td>
<td></td>
</tr>
<tr>
<td>2</td>
<td>Csoportkulcs</td>
<td></td>
</tr>
<tr>
<td>3</td>
<td>Szintkulcs</td>
<td></td>
</tr>
<tr>
<td>4</td>
<td>Egyedi kulcs</td>
<td></td>
</tr>
<tr>
<td>5</td>
<td>„Blank.” kulcs (kulcsmásolatok)</td>
<td></td>
</tr>
</tbody>
</table>

**Ha van főkulcs rendszer az objektumban**, úgy a szabályzat 4.2.13 pontja alapján, ellenőrizze le, hogy megvalósulnak-e az alábbi biztonsági feltételek.

<table>
<thead>
<tr>
<th>Srsz</th>
<th>Meghatározás</th>
<th>Igen/Nem</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>A biztonsági szolgálat kezeli a kiadásra kerülő kulcsokat?</td>
<td></td>
</tr>
<tr>
<td>2</td>
<td>A főkulcsok, csoportkulcsok, szintkulcsok napi leltárban vannak?</td>
<td></td>
</tr>
<tr>
<td>3</td>
<td>A biztonsági vezető hagyja jóvá a főkulcs használatát?</td>
<td></td>
</tr>
<tr>
<td>4</td>
<td>A kulcsmásolatokat, a „blank” kulcsokat elzárt, biztonságos helyen őrzik?</td>
<td></td>
</tr>
<tr>
<td>---</td>
<td>---</td>
<td></td>
</tr>
<tr>
<td>5</td>
<td>A kulcsok kódjait csak az erre felhatalmazott személyzet ismeri?</td>
<td></td>
</tr>
<tr>
<td>6</td>
<td>Rendelkezésre áll-e kulcsmásoló berendezés az objektumban?</td>
<td></td>
</tr>
<tr>
<td>7</td>
<td>Ha rendelkezésre áll kulcsmásoló berendezés, az kontrollált, elzárt helyen van?</td>
<td></td>
</tr>
</tbody>
</table>

A dokumentációt készítette: ............................................

Dátum: ..................................................

A következő teszt időpontja: ............................................
Az objektum neve: ........................................................................................................

Címe: .........................................................................................................................

<table>
<thead>
<tr>
<th>Srsz</th>
<th>Kulcs megnevezése</th>
<th>Kulcs kódja</th>
<th>Kiadott</th>
<th>Security</th>
<th>Összesen</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Főkulcs</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>2</td>
<td>Csoportkulcs</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>3</td>
<td>Szintkulcs</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>4</td>
<td>Egyedi kulcs</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>5</td>
<td>„Blank” kulcs</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>6</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>7</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>8</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

A dokumentációt készítette: .................................................................

Dátum: ...............................................................
Ideiglenes belépőkártyák nyilvántartásának ellenőrzése
(élkészítésének gyakorisága: 6 havonta)
Az objektum neve: ………………………………………………………………………………………

### Ideiglenes belépőkártya nyilvántartás ellenőrzése

#### Ellenőrzés időpontja:

<table>
<thead>
<tr>
<th></th>
<th>Összesen</th>
<th>Kiadott</th>
<th>Recepció</th>
<th>Tiltott</th>
</tr>
</thead>
<tbody>
<tr>
<td>napi belépőkártyák</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>beszállítói (sárga)</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>vállalati (zöld)</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>látogató (visitor) (piros)</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

### Összesen

#### Egyéb, a belépőkártyákkal kapcsolatos információk:

Az ellenőrzést végezte: …………………………………………………

Dátum: …………………………………………………

A következő ellenőrzés időpontja: ………………………………………
16.sz. melléklet

**Beszéd és adatrögzítő berendezés ellenőrzése a biztonsági szolgálat által**
(elsősorosításának gyakorisága: napi)

Az objektum neve:……………………………………………………………………………………

Címe:…………………………………………………………………………………………………..

Ha van beszéd és adatrögzítő berendezés az objektumban, a szabályzat 4.2.22 pontja alapján ellenőrizze le azt és rögzítsze az alábbi adatokat:

---

**A beszéd és adatrögzítő berendezés ellenőrzésének eredménye:**

A berendezés hibátlanul működik: 

| igen □ | nem □ |

A napi ellenőrzést végző személy neve, beosztása:……………………………………

Az ellenőrzés időpontja: ……………………..

---

**Az alábbiakat akkor kell kitölteni, ha a berendezés meghibásodott.**

Ha a berendezés nem működőképes, az jelentve lett a biztonsági szervezet felé:

| igen □ | nem □ |

---

**A berendezés javítását végezte:**

<table>
<thead>
<tr>
<th>Cégnév</th>
<th>Javítás végző neve</th>
<th>Beosztása:</th>
<th>Belépőkártya száma:</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

---

Az üzemképes állapot időpontja:………………………………………………………………………..

---

Dátum:……………………………………………

---

Aláírás:…………………………………………
Nyilatkozat a munka önállóságáról, irodalmi források megfelelő módon történt idezéséről

Alulírott Zályomi Zsolt kijelentem, hogy a „Komplex biztonságmenedzsment” című benyújtott doktori értekezést magam készítettem, és abban csak az irodalmi hivatkozások listáján megadott forrásokat használtam fel. Minden olyan részt, amelyet szó szerint, vagy azonos tartalomban, de titkosításra más forrásból átvettem, egyértelműen, a forrás megalázasával megjelöltem.

Budapest, 2019. szeptember 17.

(aláírás)
Köszönetnyilvánítás

Elsősorban kiemelt köszönettel tartozom Professzor Dr. Berek Lajos egyetemi tanár Úrnak, témavezetőmnek, a tanulmányaimban, a felkészülésben és az értekezéssel kapcsolatos munkámban nyújtott folyamatos, önzetlen, iránymutató, magasszintű szakmai segítéségéért és mindvégig türelmes támogatásáért.

Köszönettel tartozom

- Professzor Dr. Rajnai Zoltán dékán Úrnak, az Óbudai Egyetem Biztonságtudományi Doktori Iskola vezetőjének tanulmányaimhoz nyújtott segítségért.

- a Nemzeti Közszolgálati Egyetem Hadtudományi és Honvédtisztképző karán a Katonai Műszaki Doktori Iskolában és az Óbudai Egyetem Biztonságtudományi Doktori Iskolában tevékenykedő valamennyi tanáromnak és adminisztrációs dolgozónak, akik tanítottak, inspiráltak, segítették és támogattak a kutatói munkámban.

- minden volt, és jelenlegi munkatársamnak, akikkel együtt munkálkodtunk azon, hogy a biztonság magasabb szintre kerüljön.

- a szerető és türelmesen mögöttem álló kedves családomnak.