

Az információk megóvása

Jelen írást – nem túl elegáns módon – egy közhellyel kell kezdenem, miszerint a biztonság szempontjából az egyik leggyengébb láncszem az ember.

Egy biztonsági rendszerrel kapcsolatban szintén elmondhatjuk, hogy az adott biztonsági rendszer és/vagy megoldás éppen annyira erős, mint a rendszer leggyengébb eleme. Sajnos a gyakorlati példák számtalan sora bizonyítja, hogy leggyakrabban az emberi tényező bizonyul kritikusnak. Cikkemben a humánbiztonság körét kívánom kicsit körüljárni. A humánbiztonság kifejezés alatt csak és kizárólag a munkavállalók (személyek) információbiztonsági szempontból való megfelelését értem az adott cég, szervezet bizalmas információinak, üzleti titkainak megőrzése érdekében. A biztonság és a munkavállalók egymáshoz való viszonya sok esetben szövevényes és kiismerhetetlen.

Nem szabad elfelejteni – mint kockázati tényezőt – az emberi felelőtlenséget, a szándékos károkozást, az elbocsátott munkavállaló sértettségét, az emberek jóindulatának, hiszékenységének kihasználását (Social Engineering), a meggondolatlan, fölösleges fecsegést. A fenti kockázatok ismeretében különös, hogy a cégek többsége a humánbiztonság megteremtésére és megtartására kevés erőfeszítést tesz, és még kevesebb erőforrást fordít.

Napjainkban a legtöbb vállalatnál, szervezetnél az sincs tisztázva, hogy melyik szervezeti egység feladata a humánbiztonsági ellenőrzések végrehajtása. Az általános gyakorlat szerint a HR szervezet végzi ezt a fajta tevékenységet. Ugyanakkor előfordul, hogy a biztonsági igazgatóság, a bankbiztonság, a belső ellenőrzés és még sorolhatnánk a különböző tevékenységű cégeknél, különböző elnevezéssel és feladatkörrel rendelkező szervezeti egységek felsorolását, folyamatosan vagy esetenként, de szerepet vállalnak a humánbiztonsági feladatok ellátásában. Addig, amíg csak a dokumentumok, okmányok összegyűjtése a feladat (erkölcsi bizonyítvány, önéletrajz, motivációs levél stb.) általában a HR terület munkatársai foglalkoznak a leendő munkatársak-

kal. Attól a pillanattól kezdve, hogy bármiféle komolyabb vagy részletesebb biztonsági szűrést kell végezni, bevonásra kerül valamely biztonsági terület (például bankbiztonság, biztonsági vezető, biztonsági igazgatóság) is.

Az egyik legjellemzőbb hiányosság, hogy a cégek többségénél szinte semmiféle dokumentált szabályozás nem létezik a munkatársakkal szemben támasztott és elvárt humánbiztonsági szempontok érvényesítésére. A humánbiztonság, mint fogalom nem kerül bevezetésre, illetve az adott szervezetek nagy részére a humánbiztonsági kérdéseket érintő feladatokat nem delegálják egyetlen szervezeti egység számára sem. Ez igaz arra, hogy nincsenek meghatározva az új munkatárs kiválasztásával, felvételével kapcsolatos humánbiztonsági teendők, továbbá nincs kialakított és követett eljárás a munkatársak aktív időszaka alatti biztonsági ellenőrzésekre, a lehetséges biztonsági kockázatok csökkentésére, és legvégül nincs megfelelő szabályozás a munkatársak távozásakor követendő humánbiztonsági teendőkről. Mindenképpen ajánlott lenne a cégek számára, hogy saját érdekükben, üzleti titkaik megvédése céljából a fokozódó biztonsági elvárások, illetve az információbiztonság szerepének növekedése miatt kellő hangsúlyt helyezzenek a humánbiztonsági kockázatok kezelésére, és kialakítsák azokat a belső folyamatokat, amelyek segítségével megfelelően képesek szavatolni a szervezet által a munkavállalókkal szemben támasztott humánbiztonsági elvárásokat. Ne feledkezzünk meg arról sem, hogy a kialakításra és bevezetésre kerülő humánbiztonsági rendszer feleljen meg a hazai és európai jogszabályi követelményeknek, maximális hatékonysággal legyen képes a cég humánbiztonsági érdekeit kiszolgálni amellet, hogy a munkatársaknak ne okozzon semmiféle érdeksérelmet vagy esetleg joghátrányt. Ezért javasolt olyan életciklus-



Kiss Péter

Információbiztonsági szakértő, tanácsadó. Rendszeresen tart szervezett képzéseket nagyvállalati környezetben, információbiztonsági témában. Független szakértőként nemzetközi és hazai nagyvállalatoknál segít az információbiztonsági rendszerek kialakításában, felülvizsgálataiban. Több mint öt éves gyakorlati szakmai tapasztalattal rendelkezik az ISO27001-es szabvány bevezetésére való felkészítésben, rendelkezik információbiztonsági auditori képesítéssel, ISACA tag. Szakmai tapasztalatát többek között az Állami Nyomda Nyrt.-nél, banki, biztonsági szektorban szerezte. Folyamatosan részt vesz nemzetközi projekteken.

modellt alkalmazni, amely megfelelően és teljes körűen – a foglalkoztatás első pillanatától a legutolsó pillanatáig – képes lefedni a munkavállalókkal szemben támasztott humánbiztonsági követelményeket.

Példa az életciklus-modellre

1. Kiválasztás, felvétel humánbiztonsági követelményei
2. Aktív, munkaviszony alatti követelmények
3. Kilépés, elbocsátás humánbiztonsági követelményei

Sok esetben találkozni olyan megoldással, amely inkább szokásokon alapul, látszat-tevékenység, mintsem valódi biztonsági jellegű ellenőrzés vagy szűrés. Tipikusan ilyen az erkölcsi bizonyítvány megkövetelése. Az erkölcsi bizonyítvány bemutatásával a munkavállaló a büntetlen előéletét tudja hitelt érdemlően igazolni. Az erkölcsi bizonyítvány önmagában azonban kevés ahhoz, hogy felelősséggel meg lehessen mondani valakiről, hogy biztonsági kockázatot jelent-e az adott cég számára vagy sem. Szeretném felhívni a figyelmet, hogy az erkölcsi bizonyítványok terén a leggyakoribb eljárás, hogy az újonnan belépő munkatárs esetén – felvétel alatt – megkövetelik, de a felvétel után

¹ Érdemes tudni, hogy az erkölcsi bizonyítvány a kiállításától számított három hónapig érvényes.

² Természetesen ez függ az elkövetett bűncselekménytől, de lehetnek olyan esetek, amikor a munkaadó nem értesül.

már soha többet nem kéri az erkölcsi bizonyítványt¹. Amennyiben a munkatárs a felvétele után – az alkalmazása alatt érintett lesz valamilyen bűncselekményben – és ezt önmagától nem jelzi a cégénél, akkor vélhetően erről a munkaadó nem is biztos, hogy értesülni fog.²

Néhány alkalmazható módszer

Az alábbi módszerek közül néhányat (legalább öt-hat) együttesen alkalmazva a vállalat kijelölt szervezeti egysége képes lehet arra, hogy a humánbiztonsági kockázatokat a megfelelő és elvárt szinten tartsa.

- Önéletrajz
- Iskolai bizonyítványok, diplomák és egyéb okmányok eredetijének bekérése, ellenőrzése

- Erkölcsi bizonyítvány
- Referenciák kérése és tényleges ellenőrzése
- Személyes elbeszélgetés
- Szakmai teszt
- Grafológiai vizsgálat
- Pszichológiai szűrés, teszt
- Poligráfós vizsgálat

A fenti módszerek elsősorban az üzleti életben, civil szervezeteknél kerülnek alkalmazásra. Különleges kormányzati, rendvédelmi, katonai szervezeteknél használatos eljárásokra (például környezettanulmány, nemzetbiztonsági átvizsgálás) és azok sajátosságaira jelen cikk nem tér ki.

A fenti módszerek alkalmazása során tudni kell, hogy egyes módszereket csakis szakember segítségével lehet eredményesen

alkalmazni, illetve van közöttük olyan, amelynek az alkalmazása kizárólag az alany kifejezett beleegyezése és jóváhagyása mellett, az egyéb vonatkozó jogszabályok maradéktalan betartásával engedélyezett. Gyakori hiba – a sajnálatosan elszaporodott okirat-hamisítások miatt –, hogy az iskolai végzettséget, nyelvtudást vagy egyéb végzettséget igazoló dokumentumok eredetiségének vizsgálatát elmulasztják a munkaadók. Ennek a mulasztásnak a kiküszöbölése az első és legfontosabb lépés a megfelelő humánbiztonság megteremtése felé. Nem árt tisztázni, hogy a jelentkező valóban az-e, mint akinek kiadja magát, és hogy valóban rendelkezik-e azokkal a háttérismeretekkel és szükséges végzettségekkel, amelyeknek meglétét állítja magáról.