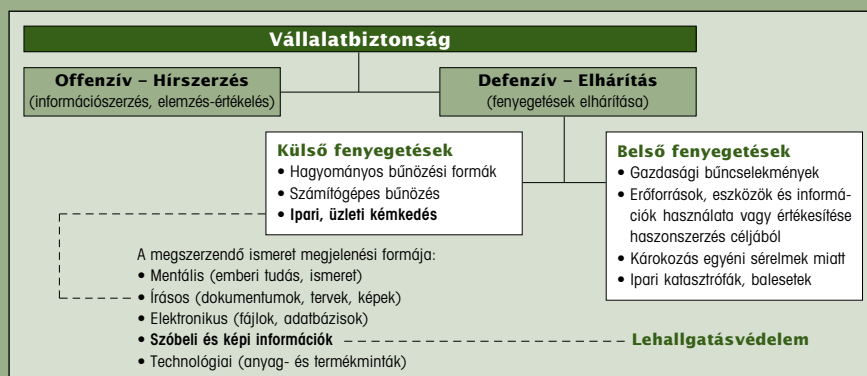


Lehallgatásvédelem az üzleti szférában 1. rész

A vállalatbiztonság területén zajló változások fontos mozgatója a felismerés, hogy a vállalatok vagyonának egyre nagyobb hányadát képviseli az az ismeret, információ, amely az üzleti, kutatási és termelési folyamatok során keletkezik. Ez az információhalmaz kiterjed a vállalat működésének minden területére, magába foglalja a stratégiai terveket, az értékesítési és beszerzési folyamatokat, a kutatási eredményeket és technológiai ismereteket, a vállalat teljes kapcsolatrendszerét, üzemeltetési, ügyviteli és biztonsági adatokat. Az információ megjelenési formája legalább ennyire változatos, kezdve az egyes kulcsfontosságú munkatársak által felhalmozott átfogó ismeretektől, a különböző papír vagy elektronikus alapú dokumentumokon keresztül, az új termékek prototípusáig.



LEHALLGATÁSVÉDELEM

A vállalat biztonsági rendszerének feladata megakadályozni ezen információk véletlen kiszivárgását vagy szándékos megszerzését más, ellenérdekelt piaci résztvevők által. Míg korábban (és jobbra ma is) a védelmi tevékenység a hagyományos

vagyonvédelmen túl az informatikai rendszerre koncentrált, a támadó fél oldaláról – talán épp az informatikai védelem fejlődése miatt – előtérbe kerülnek az információ más megjelenési formáira irányuló támadások. E tendencia mentén egyre gyakrabban találkozhatunk – akár csak a médiá-

ba kiszűrődő híreket figyelve is – a lehallgatás alkalmazásával.

E cikkben áttekintjük a lehallgatás, mint az ipari, üzleti kémkedés eszközének főbb jellemzőit és az ellene való védekezés lehetőségeit. Megjegyezzük, hogy bár a lehallgatást az ipari, üzleti kémkedés eszközékként tárgyaljuk, de megjelenhet belső fenyegetésként is, akár egyéni haszonszerzés céljából végzett információlopás, akár bosszú motiválta károkozás esetén. Külső támadás, kémkedés során is jellemző valamilyen módon megnyert, esetleg kényszerített belső munkatárs részvétele.

VESZÉLYEZTETETT TERÜLETEK

Lehallgatás alatt azt a műveletet, eljárást értjük, amelynek során technikai eszköz(ök) szándékos és rejtett alkalmazásával, a résztvevők vagy ezek egy részének tudtán kívül, megszerzik valamely tárgyalás, találkozó, tevékenység, személyes vagy távközlési eszközön történt megbeszélés során átadásra került, megjelenített, bizalmas információkat. A meghatározás leglényegesebb eleme, hogy az információszerezés a résztvevők tudtán és akaratán kívül történik, hiszen éppen ez indokolja a technikai eszközök rejtett alkalmazását. Viszonylag gyakran előfordul az az eset is, amikor a megfigyelés az egyik résztvevő fél érdekében és tudtával történik, a másik fél kárára (pl. kompromittálás, bizonyíték szerzése, dokumentálás).

A védett információk megszerzésére irányuló tevékenység komoly tervező és előkészítő munkát igényel a kémkedést folytató fél részéről. Ennek során mérlegelni kell, hogy a szükséges információ milyen forrásokból és milyen úton szerezhető

meg a legkisebb kockázat és költség mellett. A lehallgatás ebből a szempontból két kritikus tulajdonsággal is bír, amelyek szűkítik alkalmazási lehetőségeit. Egyrészt a lehallgatóberendezés megfelelő rejtett telepítése különleges tudást, az alkalmazás helyszínének előzetes ismeretét, illetve az esetek többségében az oda való bejutást igényli. Ugyanakkor a telepített eszköz, megtalálása esetén, egyértelműen bizonyítja a lehallgatás tényét, és utalhat az elkövető kilétére is. Másrészt a lehallgatóberendezés alkalmazása helyhez és időhöz kötött. Lehallgatással olyan szóbeli vagy képi információkat lehet megszerezni, amelyek megjelenése egyszeri és megismételhetetlen. Így a sikeres alkalmazás feltételezi, hogy az alkalmazónak előzetesen ismernie kell a megfigyelni kívánt tárgyalás vagy egyéb esemény helyét és legalább hozzávetőlegesen idejét.

E korlátozó tényezők mellett természetesen vannak olyan körülmények is, amelyek a lehallgatás alkalmazását indokolhatják. Normális üzleti munkafolyamatok mellett is gyakran előfordulnak olyan tárgyalások, szóbeli döntések és eljárások, amelyekről egyáltalán nem készül más formában feljegyzés, vagy mire az elkészül, az információ már elveszti időszerűségét, értékét. Gondoljunk csak egy többfordulós szóbeli alkufolyamatra vagy egy ajánlat beadási határideje előtt közvetlenül meghozott döntésre. Mire az információ hagyományos úton megszerezhetővé válik, már rég érdektelenné vált.

Jellemző alkalmazási kör az informális megbeszélések, megállapodások rejtett dokumentálása. Ezekről az aktusokról, a dolog természetéből adódóan, semmilyen formában nem készül feljegyzés, ugyanakkor valamelyik félnek érdeke fűződhet a későbbi reprodukálhatósághoz. Az igazi veszélyt az jelenti, hogy a lehallgatást ebben az esetben az esemény egyik legális résztvevője követi el, ezért elhárítása rendkívül nehéz. A lehallgatás része lehet egy szélesebb körű játszmának is, amely provokációra vagy kompromittálásra alapul. Ebben az esetben a lehallgatás, mint segédeszköz, a cselekmény dokumentálására szolgál.

Talán furcsa, de a hagyományos információszerző módszerekre kiterjedő szilárd védelmi rendszer kiépítése is kikényszerítheti lehallgatás alkalmazását. Ha ugyanis

nincs mód az adatok más, kevésbé kockázatos módon történő megszerzésére, a támadás áthelyeződhet a rendszer legkevésbé védett részére. Ez ma nagyon gyakran a lehallgatásvédelem.

Nem szigorúan szóbeli vagy képi információk megszerzésére irányul, de hasonló technikai eszközei és módszerei miatt meg kell említsük azokat a lehallgatóberendezéseket is, amelyek alkalmazásának célja az informatikai, beléptető- és más hasonló technikai rendszerekhez történő hozzáférés megszerzése. Összességében a lehallgatás megjelenésével számolnunk kell mindazokon a területeken, ahol kiélezett a piaci verseny, és egy döntés idő előtti megismerése nagy előnyt jelent.

AZ INFORMATÍV JEL

A rejtett megfigyelés célja minden esetben valamely bizalmas információ megszerzése. Az absztrakt információhoz ugyanakkor mindig valamilyen konkrét megjelenési forma társul. A megszülető gondolat semmilyen eszközzel nem fogható fel, de mihamarabb (pl. szóban) megosztjuk azt másokkal, olyan jellé (esetünkben hanggá) alakul át, amely alkalmassá válik arra, hogy technikai eszközökkel felfogjuk, kezeljük, így egyben a rejtett megfigyelés alapjává legyen. Az információ, cseréje, rögzítése, feldolgozása során, átalakul olyan fizikai jellé, amely felfogható, rögzíthető, és belőle az információ helyreállítható. Ez az informatív jel képezi a rejtett megfigyelés alapját. A lehallgatóberendezés felfogja, feldolgozza (erősíti, digitalizálja, tömöríti stb.), majd egy megfelelően kiválasztott átviteli úton továbbítja az informatív jelet a vételi pontba, ahol a vett jelből az ismeret ismét helyreállítható. Az informatív jel vizsgálata azért különösen fontos, mert a lehallgatás csak ennek jelenlétében lehetséges, így terjedésének távolsága egyben meghatározza a védendő területet is. Informatív jelként számolnunk kell a következő fizikai jelenségekkel:

► A levegő akusztikus rezgése (a hang). – A hang terjedése és felfoghatóságának távolsága erősen függ a környezeti körülményektől. Helyiségeken belül, hivatalos rendezvényeken gyakorlati szabályként fogadhatjuk el, hogy a zárt tér akusztikája, a beszélő által választott hangerő, az esetleges hangosítás általában azt eredményezi, hogy a beszéd elvárható érzékenységgé

mikrofonnal a helyiség minden pontján megfelelő minőségben észlelhető. Ne feledjük, a hangokat jól vezetik az épületek szellőzőcsatornái is.

► Falszerkezetek, nyílászárók, épületgépeszeti berendezések akusztikus rezgései. – A hang terjedése során ütközik a környező tárgyakkal, felületekkel, és rezgésbe hozza ezeket. Ezek a rezgések megfelelő berendezésekkel a hanghoz hasonlóan felfoghatók és felhasználhatók. A rezgések terjedési távolsága a közeg függvényében meglehetősen eltérő.

► Az elektromos berendezések vezetékein megjelenő szórt jelek és szórt elektromágneses sugárzás. – A hang rezgésbe hozza a környezetünkben lévő elektromos berendezések alkatrészeit is, amelyek eseténként mikrofonként működve az akusztikus rezgést elektromos jellé alakíthatják. (Egyes elektronikus eszközeink egyébként is tartalmaznak mikrofont.) Ezek az elektromos jelek, a berendezés hibás működése vagy gyenge elektromos paraméterei miatt, megjelenhetnek a hozzájuk csatlakozó vezetékeken vagy kisugárzódhatnak elektromágneses jelek formájában.

► Irodai távközlési eszközök. – Sok mindennapos irodai berendezés továbbítja a hangot elektromos jelek formájában, vezetéken vagy rádiós úton. Ezek használata annyira megszokottá vált, hogy gyakran nem is gondolunk a bennük rejlő biztonsági kockázatra. A rádiós mikrofonok, konferencia- és tolmácsberendezések kisugárzott jelei több száz méterről vehetők, és a kihangosítható vezetékes telefonok jelentős részénél is aktivizálható a behallgatás funkció kívülről, a megfelelő szervizkód ismeretében, hogy csak a leggyakoribb eseteket említsük.

A lehallgatásvédelem tehát sohasem ér véget az adott helyiség határainál, hanem csak ott, ahol az informatív jel különböző típusai már bizonyosan nem foghatók fel semmilyen ésszerűen számba jöhető technikai eszközzel. A védelemnek egyik fő célja az informatív jel terjedési távolságának redukálása, hiszen ezzel lényegesen csökkenthetők a lehallgatási lehetőségei, illetve a védendő, ellenőrizendő terület nagysága.

(Folytatjuk)

Dr. Tótlási Imre

műszaki igazgató – Cainex Kft.