

Lehallgatásvédelem az üzleti szférában 2. rész

A LEHALLGATÁSVÉDELEM CÉLJA

A lehallgatás költségeinek nyilvánvalóan arányban kell állniuk az általuk megszerzeni kívánt információ értékével. Ha figyelembe vesszük a rejtett megfigyeléssel járó jogi, erkölcsi, üzleti és technikai jellegű kockázatokat is, a megszerezhető haszonnak legalább egy, de inkább több nagyságrendnyivel meg kell haladnia a ráfordításokat. A költségeket a megfigyelőeszköz árán túl növelik a beépítéssel, telepítéssel, a vételi hely fenntartásával kapcsolatos kiadások.

A védelem szempontjából vizsgálva az összefüggés megfordítható, tehát a védett információ értéke alapján következtethetünk arra, hogy milyen költségvonzatú, és ebből eredően milyen technikai színvonalú megfigyelőeszköz alkalmazásával kell számolnunk fenyegetésként. Továbbá a védett információ értéke általában meghatározza az ellentevékenységre fordítható anyagi forrásokat is.

A rejtett megfigyelés észlelésén és közvetlen elhárításán túl, az ellentevékenységnek egyben megelőző jellegű hatása is van. Ha az ellenérdekelt félnek nem kell jelentős ellentevékenységgel számolnia, a megfigyelőeszköz választását alapvetően technikai jellegű megfontolások határozzák meg. Azaz várhatóan olyan megfigyelőeszközt fog alkalmazni, amely technikaiilag még éppen alkalmas a feladat ellátására, de semmilyen a felfedést nehezítő, speciális funkcióra nincs szükség.

A megfigyelés költsége tehát egy elsősorban technikai jellegű követelményekkel (hatótávolság, táplálás stb.) meghatározott minimumra korlátozható.

Ha a megfigyelt területen számolni kell ellentevékenységgel, a megfigyelés már nem valószínűsíthető meg ezen a technikai alapköltségen, mert szükség van az eszköz rejtett működését biztosító speciális funkciókra, és nem hagyható figyelmen kívül az esetleges bukás kockázata sem. A különleges eszközök beszerzése, a speciális ismereteket igénylő alkalmazási módszerek szükségessége és a növekvő kockázat kivédése

érdekében teendő intézkedések mind-mind növelik a költségeket és az előkészítésre fordítandó időt. Az ellentevékenységre fordított kiadások a barikád másik oldalán tehát hatványozott ráfordítási igényt és kockázatot generálnak. Ráadásul egy bizonyos technológiaszint fölött a lehallgatóberendezések bekerülnek a nemzetközileg ellenőrzött technológiák sorába, így az ipari és üzleti kémkedés résztvevői számára (elméletileg) elérhetetlenekké válnak.

A lehallgatásvédelem célja tehát kettős. A közvetlen cél természetesen az esetleg telepített lehallgatóberendezések megtalálása, egy-egy tárgyalás, rendezvény biztosítása. Hosszú távon, a megelőzés oldaláról vizsgálva azonban az elsődleges cél az, hogy a foganatosított intézkedésekkel, rendszabályokkal és alkalmazott technikai eszközökkel, az elfogadható kockázat mellett végezhető lehallgatás költségeit oly mértékben megnöveljük, hogy az már aránytalan kiadásokkal járjon, és/vagy az ellenérdekelt fél számára hozzáférhetetlen technológiát igényeljen.

Általánosságban az ellentevékenység bizalmas jellegű feladat, de ezen belül a területek differenciáltan kezelhetők. A dilemma hasonlít a középkori hajóskapitányéra, aki nek el kell döntenie, hogy az új tizágyús teherhajójára hány ágyúnyílást festessen. Ha nem készítet egyet sem, akkor ugyan könnyű zsákmánynak fog tűnni, a kalózokat azonban meglepi az ágyú, és így könnyű győzelmet arathat. Viszont ha a tíz helyett húszat festet fel, a kalózok a nagy tűzerő láttán lehet, hogy meg sem támadják, így elkerülheti a kétes kimenetelű harcot. Bár ha mégis megtámadják, bajba kerül.

Amennyiben sikerül az ellentevékenység tényét titokban tartani, az ellenérdekelt fél ugyan lehet, hogy könnyebben szánja rá magát a rejtett megfigyelőeszköz alkalmazására, de várhatóan könnyelműen jár el, így nagyobb eséllyel számolhatunk tevékenységének felfedezésére. Az ellentevékenység tényének korlátozott ismertetése ugyanakkor bizonyos mértékű visszatartó, elrettentő hatással bírhat, de ezzel egyidejűleg nagyobb felkészültségre kényszerít,

ha mégis a lehallgatás alkalmazása mellett dönt az ellenérdekelt fél.

A rendszeres technikai ellentevékenység tényét, de különösen a lehallgatásvédelem érdekében hozott szervezési intézkedéseket tartósan és teljesen nem lehet eltírtkolni, ezért nincs is sok értelme az erőfeszítésnek. Megítélésünk szerint az a tény önmagában, hogy az adott szervezetnél ilyen jellegű biztonsági tevékenység folyik, legfeljebb bizalmas jellegűnek tekinthető. A tevékenységre vonatkozó konkrét adatok azonban kifejezetten titkosak. Így különösen zártan kell kezelni az ellentevékenység módszereire, az alkalmazott eljárásokra és elhárítóberendezésekre vonatkozó adatokat, valamint a tervezett ellenőrzések helyét és idejét. A hely és idő vonatkozásában célszerű kifejezetten törekedni a rendszeresség és kiszámíthatóság elkerülésére is.

HA TALÁLUNK VALAMIT...

Annak ellenére, hogy mint láttuk, a lehallgatásvédelem elsődleges célja a megelőzés, célszerű előzetesen felkészülni arra, hogy az ellenőrzés során lehallgatóberendezést találunk. Előfordul az is, hogy a lehallgatásvédelem kiépítése éppen egy ilyen készülék véletlen megtalálásával kezdődik.

Ami nem kétséges, hogy a lehallgatóberendezést szakértők bevonásával, a lehetőségek szerint legalaposabban célszerű megvizsgáltatni. A kérdések, amire a szakértők válaszolhatnak segíthetik tisztázni a rejtett megfigyelőeszköz beépítésének körülményeit, leszűkíteni a lehetséges beépítő és megbízó kilétét, a lehallgatás során vélhetőleg eddig továbbított adatok körét, az okozott kár nagyságát. A hatótávolság meghatározásával esetleg lehetőség nyílik a vételi pont behatárolására, kutatás vagy megfigyelés megszervezésével megtalálására is.

Ha valaki akár véletlenül, akár tervezett technikai ellentevékenység eredményeként lehallgatóberendezést talál, első – nem kis részben indulatoktól vezérelt – gondolata, hogy kitépi azt a helyéről, majd kihívja az összes létező tévétársaságot, hogy jogos felháborodásának hangot adhasson. Természetesen ez a legrosszabb megoldás. Sajnos az esetek jelentős hányadában mégis győznek az indulatok, és a hálás témát a média megfelelően kiszínezve, bő

terjedelemben találja. A hírekből természetesen az eszköz telepítője is értesül a „bakiról”, és sietve intézkedik a hozzá vezető nyomok eltüntetéséről, esetleg a kiesett eszköz más, magasabb színvonalúval való pótlásáról. A szálak sikeres felgöngyölítésére ilyen körülmények között alig-alig marad remény.

Ha a sikeres felderítés tényét nem verjük nagydobra, sokkal jobb eséllyel kísérelhetjük meg a telepítő kilétének megállapítását. Ehhez – különösen, ha a felfedett eszköz rendszeres beavatkozást igényel, például elem- vagy rögzítőmemória cseréje – elég megszervezni a telepítési hely folyamatos rejtett figyelését. A siker alapfeltétele, hogy a megfigyelőeszköz felfedésének ténye és az intézkedések titokban maradjanak.

Végül szóljunk a harmadik lehetőségről: a dezinformációról. A megfigyeléssel együtt lehet élni, csak tudjunk róla, mert mondanivalónk megválogatása ezek után már viszonylag könnyen megy. A felfedett lehallgatóberendezés nem jelent veszélyt, hiszen a kényes információkat máshol is megoszthatjuk partnereinkkel, viszont lehetőséget teremt a telepítő dezinformálására. Ráadásul, amíg a megtalált eszköz megfelelően működik, valószínűleg nem kerül sor másik, esetleg jóval nehezebben felfedhető készülék telepítésére (itt azért szükséges az óvatosság). A dezinformációval egyidejűleg természetesen lehetőség van a vételi pont vagy esetleg a megfigyelőeszköz üzemeltető személy felfedésére irányuló intézkedések megtételére is.

A LEHALLGATÁSVÉDELEM MÓDSZEREI

Bármilyen nagy is a rejtett megfigyelőeszközök sokfélesége, meg lehet határozni azokat a védekezési pontokat, amelyek az ellentevékenység alapjául szolgálnak. Ezek azok a pontok, ahol a megfigyelőeszköz működési elvéből adódóan lehetőség nyílik jelenlétének észlelésére, működésének detektálására vagy megakadályozására. A védekezési pontokat jól ábrázolhatjuk a lehallgatás megvalósítását tükröző ábrán. A jel útját követve vizsgáljuk meg az ellentevékenység lehetőségeit:

■ **Az informatív jel szűrése, árnyékolása, zavarása** • A lehallgatóberendezés működésének elengedhetetlen feltétele, hogy az informatív jel eljusson annak bemenetére.

Ha ezt valamilyen úton meg tudjuk akadályozni, a továbbított jel már nem tartalmaz információt, tehát értéktelen. Ez a módszer gyakorlatilag az informatív jel terjedési távolságának csökkentésére irányuló eszközöket foglalja magába, beleértve többek között a hangszigetelést, a tárgyalóhelyiség falainak és épületgépészeti berendezéseinek megrezgetését speciális, a beszéd spektrumát elfedő zajszerű jellel, de tágabb értelemben akár a tárgyalóhelyiség vagy beszélgetés helyének megfelelő megválasztását is.

■ **Fizikai átvizsgálás** • A fizikai átvizsgálás célja felkutatni, ellenőrizni és lehetőség szerint lezárni minden olyan helyet, amely potenciálisan alkalmas lehet lehallgatóberendezés rejtett telepítésére, beleértve ebbe a táplálást és az átviteli közegeként való felhasználást is. Az átvizsgálásnál nagyon hasznosak lehetnek az ellenőrzés előkészítése során beszerzett információk a közelmúltban történt átalakításokról, javításokról, esetleg előző rendezvényekről, bérletéről, a helyiség(ek) felügyeletéről és belépéti rendjéről. A fizikai átvizsgálás a technikai elhárítás talán legtöbb tapasztalatot, intuíciót igénylő területe. A műszerek ugyan segítenek, de a tapasztalat és a megérzés legalább ilyen fontos. A terület egyes pontjain, berendezési és használati tárgyaként külön-külön kell mérlegelni a vizsgálat mélységét, módszerét. Mindent ellenőrizni lehetetlen, a döntésben csak a tapasztalat, a fenyegetés és a rendelkezésre álló adatok helyes értékelése, valamint a telepítő fejével való gondolkodás segíthet.

■ **A lehallgatóberendezés áramfelvételének észlelése** • A lehallgatóberendezés működéséhez energiára van szükség,

amit gyakran környezete elektromos berendezéseiből, illetve az erős- vagy gyengeáramú vezetékeiből vesz fel. Az energiafelvétel olyan aktív tevékenység, ami megfelelő műszeres ellenőrzéssel kimutatható.

■ **Az átviteli út ellenőrzése** • Ahhoz, hogy a lehallgatóberendezés a jelet a vételi pontba juttassa, azt egy megfelelően megválasztott átviteli közegen keresztül továbbítja. A potenciális átviteli közegek vizsgálatával ez a jel detektálható. A problémát csak a lehetséges átviteli közegek sokfélesége okozza. A legkézenfekvőbb rádiós átvitelen túl számolni kell a valamennyi fellelhető vezetékfajta (erősáramú, telefon, számítógéphálózati, vagyonvédelmi stb.) felhasználásával, de indokolt esetben az infravörös és ultrahangtartomány sem maradhat ki. Az ellenőrzés megszervezésekor célszerű figyelembe venni, hogy a lehallgatóberendezések egy része távvezérelhető. Ez lehetővé teszi, hogy csak a kellő pillanatban kapcsolják adásra. Értelemszerűen ezeket a berendezéseket az átviteli út ellenőrzésével észlelni is csak adás közben lehet. Ezért mindenképpen célszerű az ellenőrzést munkaidőben, a tárgyalást megelőzően vagy akár közben is elvégezni.

■ **Az átviteli út szűrése, árnyékolása, zavarása** • A lehetséges átviteli utakon a jel továbbítása meg is akadályozható, ami lehetetlenné teheti bizonyos típusú megfigyelőeszközök használatát. Ide tartoznak a különböző vezetékekre felszerelhető szűrők, az árnyékolás, vagy akár zavaróberendezés használata is.

(Folytatjuk)

Dr. Töltési Imre

műszaki igazgató – Carinex Kft.

Fizikai biztonság,
szervezési
és rezsim
intézkedések

