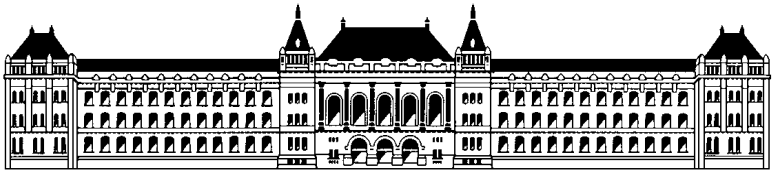
NEM OSZTÁLYOZOTT



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

BIZTONSÁG MENEDZSMENT KUTATÓ CSOPORT

AZ ÜZLETI HÍRSZERZÉS ÉS AZ IPARI KÉMKEDÉS

AJÁNLÁS

2.0 változat

Készítette: Erdősi Péter, CISA

2005

A BIZTONSÁG MENEDZSMENT CSOPORT TAGJAI:

Egerszegi Krisztián	Ph. D. hallgató
Erdősi Péter CISA,	Ph. D. hallgató
Lengyel Csaba	biztonsági vezető
Sántha Péter	vezető szakértő
Dr. Székely Iván	egyetemi docens
Vasvári György CISM,	tiszteleti egyetemi docens (a csoport vezetője)

VÉLEMÉNYEZTE: Vasvári György CISM, tiszteleti egyetemi docens

LEKTORÁLTA **:** **Nágel Imre**, biztonsági szakértő
dr. Rátai Balázs, jogi szakértő

Mi az üzleti hírszerzés és az ipari kémkedés?

Az **üzleti hírszerzés** viszonylag tág körben értelmezhető fogalom. Ide tartozik egyes felosztások szerint – szélsőséges formában – az ipari kémkedés, valamint a piacfelügyelet, a stratégiai (technológiai, versenytárs, kereskedelmi és környezet) felügyelet is. „Értelme csak piacgazdaságban és versenyben van." – állítja [4]. A megállapítás talán túl sommásnak tűnik, azonban abban egyetérthetünk, hogy legtöbbször piac-gazdaságban és versenyhelyzetben fordul elő.

Ezt megerősíti [9] is, mely szerint „gazdasági döntések meghozatalához szükséges releváns és értékes információk folyamatos gyűjtését és elemzését a fejlett országokban már több évtizede sikerrel alkalmazott üzleti hírszerzés módszertana segítheti".

A szavak jelentését boncolgatva az is adódik, hogy „üzleti hírszerzés"-t elkövetve valószínűsíthetően az üzleti élet szereplőiről kíván az aktív fél beszerezni olyan információkat, melyek relevanciával bírhatnak számára. Az más kérdés, hogy az üzleti hírszerzés során alkalmazott módszerek nyilvánvaló módon tipizálhatóak és felhasználhatóságuk nem korlátozódik a piacgazdaságra.

Az ajánlás *célja* az, hogy kizárólag az üzleti világ aspektusából járja körbe ezt a fogalmat – figyelemfelkeltő jelleggel, az informatikai biztonsággal foglalkozók számára, és *nem célja* a terület átfogó boncolgatása, ismertetése, oktatása.

Az **ipari kémkedés** [1] szerint olyan adat-, vagy információszerző tevékenység, ill. a jog által tiltott vagy etikailag kifogásolható viszony, viselkedésforma, amelynek célja a gazdaság, a tudomány, a kereskedelem, az üzleti élet területén jelentkező, esetleg a későbbi várható versenyhelyzetben való szinten maradás fenntartása, a konkurenssel szemben meglévő lemaradás leküzdése, behozása.

Ezt a definíciót a jobb megértés kedvéért érdemes több részre bontani:

1. jogszerűtlen információszerző tevékenység, melynek célpontja a versenytárs
2. (nemcsak piaci) versenyhelyzetben pozíció megőrzése vagy javítása
3. lemaradás gyors behozása (leggyakrabban technológia illegális megszerzése).

Az ipari kémkedés fogalomkörében felmerülhet a „versenytárs" és az „ellenérdekű fél" fogalma is. A „versenytárs" általános fogalom – általában azonos piaci szegmens szereplőit nevezzük így, míg az „ellenérdekű fél" terminus inkább konkrét relációkhoz köthető – a relációk azonban különböző időpillanatban eltérőek is

lehetnek, az adott üzleti érdeknek megfelelően. Megjegyzésre kívánkozik, hogy a rövid távon együttműködésben érdekelt felek viszonyának fennállása alatt sem tűnik kívánatosnak az, hogy, a másik fél a közös munkához nem kapcsolódó információkat megtudhasson a partneréről.

A jogosulatlan információszerző tevékenység végzését megkönnyíthetik a szabályozási hiányosságok és a biztonsági kultúra alacsony szintje (adatszerzés, adatok elvesztése). Ezt leginkább a koncepciótlan és nem egyenszilárdságú szabályozási tevékenység teszi lehetővé, melynek eredményeként a szabályzatok előírásait nemcsak hogy nem ismerik, de ha ismerik, akkor sem tartják kötelező érvényűnek.

Az üzleti hírszerzés és az ipari kémkedés fogalmai fenti szétválasztásának jogosságát megerősíti az Üzleti Hírszerzés Portál [9] is, mikor azt állítja, hogy „az ipari kémkedés többnyire eseti, egy adott titok megszerzésére irányuló, az illegalitás határát súroló vagy azt elérő, tiltott tevékenység, az üzleti hírszerzés (competitive intelligence – CI) kizárólag a törvényes keretek között mozgó információs vezetői döntés-támogatást jelent”

Az üzleti titok védelme

Az Alkotmányról szóló 1949. évi XX. törvény 59. § (1)-ja szerint a Magyar Köztársaságban mindenkit megillet a jóhírnévhez, a magánlakás sérthetetlenségéhez, valamint a magántitok és a személyes adatok védelméhez való jog.

Titoknak minősülnek azok a tények, adatok, következtetések stb., amelyek elleplezéséhez valamilyen érdek fűződik. Ez az érdek bizonyos körben társadalmilag elismert védelem alatt áll, érvényesülését jogszabály biztosítja.

A számtalan titokfajta közül (állami, szolgálati, hivatásbeli stb.) - az Alkotmány 59.§ (1) bekezdésével összhangban, a Ptk. a személyhez fűződő jogok között a levéltitok, a magántitok és **üzleti titok** megőrzését részesíti védelemben.

Annak megítélésénél, hogy a titoksértés és ezzel együtt a személyhez fűződő jog sérelme megvalósult-e, a törvény fenti rendelkezésén túl megfelelően figyelembe kell venni az adott titokfajta megőrzésével kapcsolatos külön szabályokat is.

A Ptk. 81. § (2) bekezdésében definiálta az üzleti titok fogalmát, amely - a vonatkozó külön törvények egyidejű módosítása mellett - mint általános fogalom-meghatározás irányadó minden olyan körben, ahol az üzleti titok felmerül. A törvény értelmében üzleti titoknak azok az adatok, tények, információk minősülnek, amelyek esetében az alábbi hármas **együttes feltétel** megvalósul:

- az érintett gazdasági tevékenységhez kapcsolódnak,
- a jogosult jogszerű pénzügyi, gazdasági, piaci érdekét annak nyilvánosságra hozatala, vagy illetéktelenek általi megismerése és felhasználása sértené vagy veszélyeztetné,

- és ez okból a jogosult a titokban tartás érdekében megtette a szükséges intézkedéseket.

A törvényi feltételek bármelyikének hiányában az adott adat (tény, információ) nem minősülhet üzleti titoknak.

A titoksértés tehát számtalan módon bekövetkezhet, a jogsértő magatartás pontos körülhatárolása szinte lehetetlen. Ezért a törvény a taxatíve meghatározott titokkörben annak bármilyen magatartással megvalósuló megsértését szankcionálja: a titkok jogosulatlan megszerzésétől, az illetéktelen nyilvánosságra hozatalig egyaránt.

A titkos információgyűjtés eszközeit és módszereit [5] az alábbiakban határozza meg – a teljesség igénye nélkül:

- informátor
- megfigyelés, a megfigyelés eredményeinek technikai rögzítése
- bizalmi vásárlás
- telefonkészülék lehallgatása, beszélgetések rögzítése
- helyiségbeli történések megfigyelése, lehallgatása, találtak rögzítése
- számítástechnikai úton keletkezett adatok megismerése

Megjegyezzük, hogy ezeket az eszközöket az erre törvényben feljogosított rendvédelmi szervek bűnüldözés, vagy bűnmegelőzési céllal használhatják, és esetenként bírói engedélyhez kötött az alkalmazásuk.

Az információk szerkezeti osztályozása

Egyes vélekedések szerint az üzleti szempontból fontos információk 70-90%-a nyíltan hozzáférhető. A problémát a keresett információ megtalálása és feldolgozása jelenti. Az információs társadalom korában könnyű „információs bulímiába” esni, így nevezzük az információk válogatás nélküli nagy tömegű „fogyasztását”, ami nem vezet a kívánt eredményre.

Az információ osztályozására egy lehetséges példát az alábbi táblázat tartalmaz:

Az információ szerkezete	*Az információ természete*	*Lehetséges források*
Szöveg típusú (40%)	Formális fehér és fekete	Tudományos publikációk, szabadalmak, szakirodalom, cégadatok, szabványok, külső jelentések technológia, árképzés, termelési adatok (titkos ügyiratkezelés)
Szakértelem típusú (10%)	Formális és informális szürke és fekete	Cég emlékezete, belső adatok

Az információ szerkezete	*Az információ természete*	*Lehetséges források*
Pontatlan típusú (40%)	Informális szürke és fekete	Különböző helyekről érkező emberek
Vásár- és szalon típusú (10%)	Formális és informális fehér és szürke	Reklámok, kiadványok, szóbeli beszámolók

1. táblázat: Az információk egy lehetséges osztályozása

Ebben a megközelítésben formálisnak nevezzük azokat az információkat, amelyeket hivatalosan közzétesznek, míg az informális információ nem hivatalos forrásból származik. A fehér információt tudatosan és nyilvánosan közzétették, a szürke ugyan nem titkos, de nem is adták ki, míg a fekete információ titkos és gyakran csak illegális módon szerezhető meg.

A gazdasági szervezetek nyílt (formális, fehér) információinak megszerzése, összesítése és felhasználása nem törvénytelen, ezzel foglalkoznak például a piackutatók, valamint a külső gazdasági elemzések készítői.

Napjainkban a piaci verseny növekedése magával hozza az egyes cégek érdeklődésének növekedését, más, elsősorban konkurens cégek adatai iránt. Ennek tudható be, hogy lehet találni olyan vállalkozásokat, amelyek készek az ilyen adatokat megszerezni.

Ki kell mondanunk tehát, hogy az ipari kémkedés hazánkban ma már realitás, ezt az „adat”, mint informatikai erőforrás biztonságát fenyegető veszélyforrásként kell kezelnünk, és egy biztonsági átvilágításnál vizsgálnunk kell azt is, hogy tesznek-e ellene valamit.

A STRATÉGIAI HÍRSZERZÉS

Stratégiai hírszerzésen általában egy kifelé irányuló figyelmet értünk, mely folyamatos környezet-figyelést jelent. Szükséges ahhoz, hogy egy adott vállalat a versenyben elfoglalt pozícióját tisztán és világosan meghatározhassa, valamint a piaci mozgásokat szem előtt tartva definiálja és szükség esetén módosíthassa a saját stratégiai irányvonalait.

A stratégiai hírszerzés négy területre bontható fel:

1) **Technológiai felügyelet**: általában a technológiai előnyből adódik minden versenyelőny. Ide tartozik mindaz, ami a termékek továbbfejlesztését befolyásolhatja – mindez teljesen legálisan:
   - szabadalmak figyelése, elemzése
   - szektorok technológiai átvilágítása
   - műszaki piackutatás
   - technológiai lehetőségek felkutatása

- beruházások műszaki kiértékelése

2) **Versenytársak felügyelete**: ide tartoznak azoknak az információknak a figyelése, melyek a versenytársak stratégiájáról tudósíthatnak:
   - versenytársak termékskálájának figyelése, elemzése
   - elosztócsatornák
   - értékesítés és eladás
   - költségelemzés
   - vállalati szervezet és kultúra elemzése
   - a felső vezetés képességeinek elemzése
   - a cégek tevékenységi portfóliója
   - a verseny erőssége

A versenytársak felügyeleténél figyelembe kell venni az üzleti dezinformáció fennállásának lehetőségét is.

3) **Kereskedelmi felügyelet**: itt nem a termékek játsszák a fő szerepet, hanem a versenytársak termékeknek fogadtatását, sikerét vagy bukását, illetve azok okait keressük, és elemezzük ki:
   - termékek fogyása területi megoszlásban
   - termékek áramlása, forgalma
   - reklamációk
   - terméksiker lehetséges okai (termék, előállító, vevői szokások)

Hasonlóan a versenytársak felügyeleténél leírtakhoz, itt is figyelembe kell venni az üzleti dezinformáció lehetőségét is.

4) **Környezet-felügyelet**: ez a legkevésbé definiált terület, ide tartozik mindaz, amit az előző pontokhoz nem tudunk besorolni. Arra vonatkozó információk gyűjtése és elemzése történik meg, hogy mitől lesz egy környezeti változás releváns az adott vállalat életére nézve. Ezek nem feltétlenül kapcsolódnak szorosan a tevékenységhez, de néha igen sok múlik a megszerzésükön. Például egy marketinges számára fontos információ lehet a potenciális vásárlók szokásai, életmódja, vagy az újdonságokhoz való viszonya. Egy bank számára a tőkeerő, szociális helyzet, az aktuális és a várható kamatpolitika jelenthet lényeges információt a termékskála kidolgozásához és értékesítéséhez.

A felügyeleti tevékenység továbbá lehet itt is *aktív és passzív*. Aktívról akkor beszélünk, ha az adatok szolgáltatási rendje előre kialakított és kidolgozott, míg passzív a felügyelet, amikor nincs előre megadott adatkör, amit be kell szolgáltatni („nyitott szemmel járni”). Az optimális eredményt valószínűleg a kettő kombinációjával lehet elérni, mivel az aktív felügyelet rugalmatlanságát kiegészítheti a passzív eljárás, míg a passzív felügyelet ciklusmentességét megtörheti az aktív

adatszolgáltatás rendszeressége. Végezetül meg kell említenünk azt, hogy csak az ember képes arra, hogy egy adott területtől távolinak tűnő információkat asszociáljon a vizsgált területhez.

AZ IPARI KÉMKEDÉS

Feltétlenül azon az álláspontón kell lenni, hogy éles határ húzandó a piackutatás – bővebb értelemben a törvényes üzleti hírszerzés, és az ipari kémkedés – mint az információ-szerzés törvénytelen eleme – közé. Mint a korábbi definíciókból egyértelműen következik, az ipari kémkedés illegális eszközöket használ, és jogosulatlanul szerez meg és használ fel információkat.

Az ipari kémkedés lehetséges céljai:

- a megbízó jogosulatlan előnyhöz juttatása, lehetővé téve a megszerzett adatok, technológiák felhasználását, és
- az adat-tulajdonos cég hátrányos helyzetbe hozása, magyarul kár okozása.

Az ilyen törekvések különösen élesen merülhetnek fel az ipari kutatást végző cégeknél, erős versenyhelyzetben lévő cégeknél, illetve tenderek kiírását követően, sőt sokszor a kiírást megelőzően is.

[9] alapján fel kell még hívnunk a figyelmet arra, hogy több független elemző cég szerint drasztikusan növekszik a világban az elektronikus adatvesztés, adatlopás, illetéktelen behatolás, és az online pénzügyi visszaélések száma. Az információnak van egy olyan tulajdonsága, hogy az egyetlen olyan érték, amit – megfelelő intézkedések hiányában – észrevétlenül ellophatnak tőlünk, és azután is megmarad.

A TÁMADÓ ESZKÖZÖK

Az információ birtoklása az alábbi két módon lehetséges:

- információ-szerzéssel, vagy
- információ-vesztés következtében.

Az információ-szerzés továbbá elvégezhető emberi (humán) közreműködés elérésével vagy technikai eszközök felhasználásával. Ebből adódóan feloszthatjuk a támadási módszereket aktív és passzív csoportra.

Aktív módszerek

Az aktív támadási módszerek (fizikai, logikai) vagy személyes megjelenést, vagy személyes ráhatást igényelnek. Ilyenek például a fizikai vagy logikai behatolás, iratlopás, -másolás, -fényképezés, rosszindulatú szoftverek [trójai faló, kémszoftverek (spyware)] bejuttatása, jogosult személy megtévesztésével cselekvésre való felbujtás – azaz mindazok az ismert aktív támadási módszerek, amelyek az információ jogosulatlan megszerzésére szolgálnak.

A humán módszerek aktív felhasználása a jogosulatlan információk megszerzésében különösen kedvelt eszköz. Emlékeztetünk arra, hogy szakértői jelentések alapján egy információ rendszerben a nagyobb veszélyforrást a humán erőforrások, és nem a technikai eszközök jelentik. Nyilvánvaló módon minden technikai védelmen legalább egy személynek keresztül kell mennie – a jogosult hozzáférés megvalósításakor.

A humán eszközök közül kiemeljük a következőket – a teljesség igénye nélkül:

- **Szándékosság**: a támadó meg akarja találni azt az embert, aki vagy megvásárolható, vagy egyszerűen kárt akar okozni cégének, vagy volt cégének. Ide sorolhatók az alábbi motivációk: meggazdagodás, bosszú, frusztráció, elégedetlenség, meggyőződés...
- **Egyéb aktív módszerek**: a fentieken túl meg kell említenünk az információ-szerzés további lehetséges módozatait is: állítólagos üzleti ajánlat-kérők és tárgyaló-partnerek, felvételi interjún megjelenők szerezhetnek legálisnak tűnő szituációkban információt az adott cégről, üzleti paramétereiről.

Passzív módszerek

Passzív támadási módszereken a fizikai vagy logikai lehallgatás változatos eszközeit értjük, ilyen például a hangpuska, valamint az akusztikus kisugárzás, és a nyilvános vagy zárt helyen történő beszélgetések lehallgatása, a billentyűzet-lehallgató eszközök, továbbá az elektromágneses kisugárzások rögzítése is. A passzív módszerek egy lehetséges csoportosítása az alábbi:

- **Gondatlanság**: melynek oka lehet a személy nem megfelelő képzettsége, figyelmetlensége. Ennek ismert működő megvalósítása [2] a social engineering módszere. Mitnick azt írja, hogy a „social engineering a befolyásolás, és rábeszélés eszközével megtéveszti az embereket, manipulálja vagy meggyőzi őket, hogy a social engineer tényleg az akinek mondja magát. Ennek eredményeképpen a social engineer képes az embereket információszerzés érdekében kihasználni.” Tehát felkelti a bizalmat azért, hogy jogosulatlanul hozzájusson információkhoz. Gondatlan információ-kiadás történhet még stressz, fáradtság, tudatlanság következményeként is, de ide tartozhat az állás-interjúkon kiadott információk megszerzése is. További gondatlanságnak minősíthető a „fecsegők” magatartása. Vannak emberek, akik szeretik a jól értesültet játszani, és tőlük kéretlenül lehet információkat kapni.
- **Szabályozási hiányosságok**: információ-vesztést eredményezhet a hibás szabályozás is. Ha a vállalati folyamat nem zárt az információ védettségére nézve, akkor hiába tartják be a szabályzatot, az önmagában nem elég az egyenszilárdságú védettség megvalósításához.
- **HR-tényezők**: A humán faktor további információ-kiadást eredményező tényezői lehetnek az előírások ismeretének hiánya, az előírások figyelmen kívül hagyása (véletlenül vagy szándékosan), a nem kielégítő képzés, a

kényelmesség, a megszokás, a fenyegetettség ismeretének – egyszóval a biztonsági tudatosság hiánya.

ESETEK

Információ-szerzésről és -vesztésről számos hírt olvashatunk az elektronikus sajtóban, szinte nem telik el olyan hét, hogy ne jelenne meg legalább egy ilyen témájú cikk valamelyik hírportálon. Ebből adódóan nem célunk itt tömérdek esetet felsorolni – némi kereséssel bárki találhat több tucatot. Az alábbi kiragadott példákat inkább annak a ténynek az illusztrálására, igazolására szántuk, hogy a veszélyforrás valós, és reálissá vált a mai, információ-rendszereket működtető vállalatokban. Az adatszerzés és az adatvesztés realitásának alátámasztására az alábbi két – időtávban is jelentősen eltérő – esetet hozzuk fel példának:

- 2001. végén felfedezésre került egy olyan program [7], mely információ-rendszerekbe behatolva hátsó ajtót nyit egy távoli támadó számára, és az információ-rendszerben tárolt adatokhoz hozzáférést biztosít. A program számos speciális tulajdonsággal rendelkezik – elrejtőzés, fájl-továbbító képességek, nyomok eltüntetése –, melyekből valószínűsíthető, hogy információk megszerzésére lett tervezve és alkalmazva.
- 2005. év elején tették közzé, hogy mágnesszalagos adathordozók eltűnésével kb. 1.200.000 ügyfél számla-adata veszett el [8]. Az adathordozók a háttér-központba való továbbítás közben tűntek el. Tartalmaztak számos személyi azonosító elemet és számla-információt is.

A VÉDEKEZÉS MÓDSZEREI

Az üzleti hírszerzés működésének, szervezésének nincsenek sémái, kialakítása – [6] alapján – egyedi elvek alapján történik. Felépítését több tényező befolyásolja:

- ágazati jellemzők
- vállalat fizikai és gazdasági mérete
- vállalati és vezetési kultúra
- külső tényezők.

Az ipari kémkedés vagy a „social engineering” módszereire sem alkalmazható egy egységes sablon – de néhol felfedezhetőek azonos alapelemek a végrehajtások során.

Ebből az következik, hogy nem egyes támadások elleni védekezést kell egy hatékony védelemnek megvalósítania, hanem az információ-rendszer ellenálló-képességét kell oly módon kiterjeszteni, hogy képes legyen az ilyen irányú támadások elleni védekezésre. Emiatt a támadási módszerekkel szemben – véleményünk szerint – egy

egyenszilárdságú, azaz minden pontján legalább egy jól meghatározott ellenálló-képességgel bíró biztonsági alrendszerrel lehetséges teljeskörűen védekezni. A biztonsági rendszer alrendszereit az alábbiakban foglaljuk össze:

1) **a vagyonbiztonsági alrendszer**, amelyben a vagyonbiztonsági védelmi intézkedéseken kívül vannak informatikai védelmi intézkedések is,
2) **az üzembiztonsági alrendszer**, amelyben vannak az üzembiztonsági védelmi intézkedéseken kívül vagyon, és informatikai védelmi intézkedések,
3) **az informatikai biztonsági alrendszer,** amelyben vannak vagyonbiztonsági védelmi intézkedések is."

Emlékeztetünk arra, hogy az „üzleti titok" fennállásának törvényi feltételei között szerepel, hogy „a jogosult a titokban tartás érdekében megtette a szükséges intézkedéseket". Ebből következik, hogy önmagában, a szükséges védelem kialakítása *nélkül* az adott védendő információ nem elégíti ki az üzleti titok törvényben megfogalmazott kritériumait.

A kialakított vállalati biztonsági rendszeren, alrendszereken belül konkrétan az alábbi intézkedések jelenhetnek védelmet a vállalat méltányolható érdekből titokban tartandó adatai számára:

- a nem nyilvános adatoknak a vállalat érdekei ellenére történő nyilvánosságra kerülése ellen, elsősorban az MSZ ISO/IEC 17799 szerint, az osztályozással kell védekezni, és az ennek alapján tett védelmi intézkedések megvalósítását, megvalósulását a tevékenységek naplóinak belső ellenőrzésével rendszeresen ellenőrizni kell.
- Továbbá az osztályozásban megtestesülő biztonsági követelmények szigorításával is lehet védekezni, azaz az adatokat, különösen a biztonság érzékeny adatokat, magasabb biztonsági osztályba kell sorolni (pl. bizalmas, helyett titkos), annak érdekében, hogy erősebb védelmi intézkedést kelljen a megfelelő védelmi szint eléréshez tenni.
- Végül a biztonsági tudatosságot erősíteni kell a nem tudatos hibák (pl. a megtévesztés módszere) elleni védekezés fokozása céljából.

A fentiekből külön kiemeljük a humán, és a szervezési védelem fontosságát, azon belül is a biztonsági tudatosság erősítését, azaz annak megismertetését, hogy hazánkban is már létezik ipari kémkedés – ez alapvető fontosságú a védekezés szempontjából. Ezen belül a „social engineering" (megtévesztés) módszereiről is széles körben javasolt tájékoztatni a munkatársakat, hiszen a szélhámosság ellen nagyon nehéz védekezni.

A technikai védelmen belül tehát különösen ajánlott erős fizikai, és logikai hozzáférés védelem megvalósítása (be- és kilépés ellenőrzés, jelszó menedzsment, jogosultság menedzsment, behatolás védelem, üres íróasztal, üres képernyő),

valamint a hálózatok lehallgatás elleni védelmének megvalósítása csökkenti az ipari kémkedésből adódó kockázatot. Általában az aktív, és passzív támadások ellen ismert védekezési módszerek használhatóak, alkalmazva ezen veszélyforrásra.

Az események detektálásához elengedhetetlen, hogy legyenek jelzések a rendszerben, azaz előzetesen a számonkérhetőséget is meg kell teremteni. Az ellenőrzési folyamatok szintén kritikusak az észlelésben, mivel a rendszer jelzései – kiértékelés hiányában – nem szolgálják kellőképpen a védelem megvalósítását.

Említésre kívánkozik az is – anélkül, hogy különösebb részletekbe bocsátkoznánk, hogy a szakértői anyagok a védekezésben javasolnak kitérni az üzleti hírszerzés elhárítására, és az ipari kémkedés elleni védelemre egyaránt. Ebből az következik, hogy szakértők szerint nem elegendő csupán az ipari kémkedés elleni védelmet megvalósítani, hanem az üzleti hírszerzés tárgyául szolgáló legális információ-kiadás stratégiáját is meg kell tervezni és átgondoltan kell megvalósítani.

Végezetül konzekvenciaként megállapíthatjuk, hogy a védelemnek javasolt mindenképpen egyenszilárdságúnak és az üzleti és biztonsági kockázatokkal arányosnak lennie, ami azt jelenti, hogy az ipari kémkedés elleni védelem is épüljön be a biztonsági alrendszerbe, azaz annak integráns részeként funkcionáljon, a többi intézkedéssel együtt.

FELHASZNÁLT IRODALOM

[1] Információ-biztonság. Több szerző. Kasza és Tsa. BT. Pécel.1997.
[2] Kevin D. Mitnick: A megtévesztés művészete. A legendás hacker. Perfect Pro Kft. Budapest. 2003.
[3] Nyilas Sándor – Nagy Béla: Amit az ipari kémkedésről tudni kell. Raab Karcher Biztonsági szolgálat. Budapest. 1998.
[4] Benczúr Dávid: Internet és üzleti hírszerzés. Alma Mater-sorozat III: Sokszínű e-világ, BME GTK Információ- és Tudásmenedzsment Tanszék, 2002. február.
[5] Erdős István: A titkos információgyűjtés magyar szabályozása, és az általa nyert információ felhasználása a büntetőeljárás során. Miskolc, 2000. november
[6] Jasenszky Nándor: „Hogyan épül fel az üzleti hírszerzői tevékenység optimális szervezeti háttere a vállalaton belül? c. előadás-anyaga „Értékkövető üzleti hírszerzés a vállalati gyakorlatban" Institute for International Research Szakkonferencia 2003. november;
[7] http://www.saveas.hu/documents/publications/esettanulmany-poloska-20020201.pdf
[8] http://www.msnbc.msn.com/id/7032779/
[9] http://www.uzletihirszerzes.hu/index.php?option=com_content&task=view&id=263&Itemid=27