VÉDETT HELYISÉGEK BIZTONSÁGÁNAK SZEMPONTJAI

SAFETY ACPECTS OF PROTECTED AREAS

BRÉDA GÁBOR PhD-hallgató
Óbudai Egyetem, Biztonságtudományi Doktori Iskola

Abstract

In today's informational society the protection of data and information is of great importance. There are adequate and safe solutions from the aspect of the protection of recorded information. Nonetheless, upon closer inspection, areas where data of economic value is spoken out loud, the protection against information leak cannot be considered sure in all cases. The organization of the protection of spoken information is closely linked to the establishment of the physical environment's protection. It is necessary to define the notion of a protected area from the perspective of the subject. In the public sector data assets and information are protected with the help of legal provisions, on the other hand, in the pure private sector it depends mostly on the personal skills and fiscal opportunities of data administrators. Renowned manufacturers are working out protection solutions in IT environments that later appear in regulatory environments. But other widely known ways of acquiring information and the protection against them is not very much spoken of. This paper wishes to provide an explanation about the interpretation data and information, and then it adumbrates the theoretical approach to classic, open-source intelligence solutions. Upon choosing the technical guideline, the article uses an own grouping to negotiate the relevant basic parameters of independent technical hardware that appeared with the presence of internet open market.

1. Bevezetés

Az adat és információvédelem kiemelt jelenőséggel bír információs társadalmunkban. Minden ember illetve szervezet igyekszik megóvni bizalmas adatait, információit, az arra illetéktelenek elől. A fizikai adathordozóra rögzített adatok és információk megalkotott védelmi mechanizmusai, túlnyomórészt egy helyiség vagy épületkomplexum meghatározott falai közé szorulnak. A napi valóság élethelyzeteit áttekintve azonban megállapíthatjuk, hogy azok nem csak rögzített formában és az erre kialakított helyeken fordulnak elő, hanem más környezetben is, sokszor a szokások által befolyásolva.

A témát kutatva meghatározom a problémával kapcsolatos feltevést, körülhatárolva egy védett helyiség biztonsági igényeit. Áttekintem a témához kapcsolódó hatályos intézkedéseket, valamint csoportosítom az internet által kínált, nagy számban megjelent, fokozott biztonsági kockázatot jelentő autonóm információrögzítő eszközök paramétereit és működési tulajdonságait.

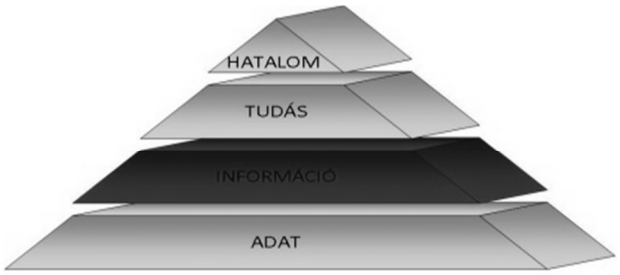
2. Adat és információ

A köznapi kommunikációban sokszor beszélünk adatról, információról a fogalmakat egymással szinonimaként is használjuk. Először tisztázni szükséges a kettő közötti különbséget. Az adatokat birtokolni és ismerni, nem jelenti önmagában azt, hogy információ

birtokában vagyunk, tovább gondolva, ha információink vannak, az sem jelent azt, hogy tudásunk lenne. A világ szervezeteinek információs hátterét szemügyre véve az tapasztalható, hogy nagy mennyiségű adatot gyűjtenek, raktároznak és halmoznak fel, anélkül, hogy a továbbiakban bárminemű kialakult tervük, vagy előre meghatározott céljuk lenne azokkal. Ez minden bizonnyal idővel majd egy túlcsordulást okoz, amely újabb problémákat generál. Másrészről egy ellentmondás is felmerülhet, miszerint előfordulhat, hogy az adathalmazok sokaságában, nem biztos, hogy minden olyan adat, megfelelő módon és mennyiségben, teljességében rendelkezésre áll, amely egy optimális döntés meghozatalát tökéletes háttérrel tudja ellátni a megfelelő információk megalkotásához.

Az emberiség fejlődése során, valamint jelleméből fakadóan mindig információéhséggel küzdött. Az elmúlt kétszáz évben, közeledve napjainkhoz, a technológia fejlődésével az elektronikus hírszerzés lehetőségei hatványozott mértékben nőttek. Az emberiség történelmében, eddig még soha nem látott minőségű és gyorsaságú hírközlési berendezések állnak a hétköznapi ember rendelkezésére. Egy, a világban történő változás szinte minden esetben valamilyen adatot generál, amelyek rögzítését sokszor állami fenntartású cégek végzik. A tárolt mennyiség ellenére, azonban nem egyértelmű, hogy mi a kimeneti cél. Nincs minden esetben kimeneti koncepció az adatok több szempontból való feldolgozásával kapcsolatban. Tulajdonképpen a nagy kihívást manapság, nem az adatok megszerzése és raktározása, hanem az azokból nyerhető információ létrehozása, valamint hasznosítható formába történő alakítása jelenti. Az adat, az információ és a tudás nem ugyan azt jelenti. A Russel Ackoff (1988) által megfogalmazott elméleti kapcsolatot a piramis modell szemlélteti a legjobban az 1.ábrán. Az adat az alap pillér, melynek feldolgozásával juthatunk az információhoz. Az információk összessége tudás halmazt képez, amely hozzájárul a bölcsesség, vagy hatalom kialakulásához. Az adatok gyűjthetőek automatikus rendszerek útján, azonban a további feldolgozásuk során képesnek kell lenni megfelelő jelentéssel felruházni azokat. Az adatok gyűjtése során szem előtt kell tartani az abból előállítható információt, illetve a megszerezni kívánt tudást. Míg az információ sajátos jelentésjelleggel bír, addig a tudás az információk birtoklójának újabb lehetőségeket kínál. Egy információ, az alapjául szolgáló adatok révén, több beágyazott jelentéstartalmat is kifejezhet (Bellinger, Castro, Mills, 2004). A megfelelő tudáshalmazok logikai kezelésével bölcsesség és hatalom érhető el, amely logikai rendezéssel további döntéstámogató értéket képvisel. Az információkból rendelkezésre álló tudás, elengedhetetlen a jó döntések meghozatalához (Zoltayné 2005).

1. ábra. Modell az adat, információ, tudás, hatalom kapcsolatára
Figure 1. Flowchart model of Data, Information, Knowledge, and Wisdom



Forrás: Russel Ackoff alapján; saját szerkesztésű ábra

A tudásszintet tovább elemezve, Polányi (1966) szerint a tudást kétféle módon értelmezhetjük. Egyik módja a rejtett tudás a másik az egyértelmű, közvetlen tudás. Míg a rejtett tudás a tapasztalatokon, emberi tulajdonságokon, szándékon képzeleten és kreativitáson valamint helyzetfelismerésen alapul, úgy a közvetlen (explicit)tudás direkt kapcsolódik az információhoz a racionális logikus gondolkodáshoz. Fontos megállapítás továbbá, hogy a tudás nem alakul ki magától. A tudás egy folyamat terméke, azaz keletkezik. Nonaka és Takeuchi (1995) kutatásukban használták Polányi tudáskategóriáit,elméletük szerint tudást lehet szerezni az információk ismeretéből, megérteni az üzenetét a már létrehozott tudásnak. Továbbá létezik az a fajta tudás, amely az adatok saját feldolgozásából ered, így az információ, majd a tudás a megalkotójuk munkáján keresztül válik kész értékké. Érdekes megállapítás, hogy a rejtett, vagy nevezhetjük hallgatólagos tudás mechanikáját nehéz megértenünk, mert mint az már említett módon nagyban emberi tényezőktől függ. A közvetlen tudás mechanizmusa viszont jól áttekinthető, hisz ez a fajta információ alapú tudás, világos belső logikájú, könnyen átadható. Először elmagyarázza a mögöttes logikát, majd biztosítja a hiányzó adatokat és információkat. Amennyiben a meglévő adatokat logikai úton különböző formában kombináljuk új adatokkal, úgy új információk előállítása válik lehetségessé.

A jó döntések meghozatalához lényeges az adatok megfelelő elemzése, a helyes összeillesztés és az információ előállítása. Minél több információ áll rendelkezésünkre egy probléma megoldása során, annál megfelelőbben lehet meghatározni a lehetőségeinket. Azonban a teljes tudás megszerzése az összes információ magunkévá tétele szinte lehetetlen feladat. Előfordul, hogy nincs elég időnk, vagy nincs hozzáférésünk, vagy elég anyagi erőnk megszerezni mindet. Amennyiben egy döntés előtt megtudnánk szerezni minden információt lehetséges, hogy annak mennyisége olyan hatalmas mértéket öltene, hogy nem tudnánk feldolgozni azt. A döntések velejárója nagy általánosságban az információ hiánya és a bizonytalanság, így válik értékké a megszerzett információ mennyisége és pontossága. Az információt, mint döntéssegítő tudást értékelve, a jó információ lehet: pontos, időszerű, átfogó, alapos (Szikora, Tóth, 2015). Összegezve, egy információ nem mondja meg, hogy mit kell tennünk, csak segít eldönteni annak végrehajtását. Az élet adta döntési helyzetek nem sablonosak, minden esemény saját körülményei környezetében zajlik, így nem tudunk pontos modellt adni egyik helyzet megoldására sem. Amennyiben az információ korlátlan mennyiségben hozzáférhetővé válik az ember számára a következő akadályt maga az ember jelenti, mert korlátozott az információ feldolgozó kapacitása, saját magát hátráltatva (Miller, 1956; Simmel 1950; March, Hevner, Ram, 2000). A tárgyaltak miatt válik fontossá, hogy adott témát illetően, értékkel bíró kész információkhoz juthassunk, amelyek a döntési bizonytalanságot megfelelően kompenzálhatják. Az okfejtésből kiindulva válik relevánssá az információ védelmének kialakítása.

2.1. Védett helyiségek

A védett helyiségek kialakításának meghatározása, mindig a megoldani kívánt védelmi feladat szemszögéből kell, hogy megvalósuljon. Példákat állítva válik egyértelművé a téma szempontjából tárgyalt védett helyiség mechanizmusának megértése, mert a következőekben láthatjuk, hogy számtalan alapkövetelményt állíthatunk egy ilyen helyiséggel kapcsolatban.

A legklasszikusabb esetben a fizikálisan megfogható értéktárgy biztonságba helyezése a cél. Az ilyen helyiség tipikusan a bankokban található széf. Továbbá feladat lehet egy élőlény ki, vagy be jutása elleni védelem megalkotása is, ez tipikusan az állatkerti ketrec,

vagy a börtöncella megvalósítása. Más megközelítésben védett helyiség kialakítható a természet elemi ereje ellen is, főként az amerikai kontinensen találhatunk ilyen helyiségeket a nagyerősségű szélviharok elleni védelemre kialakítva. A témához közeledve ismert a katonaság, valamint a polgári védelem által létrehozott védett objektumok és óvóhelyek létezése is, amely szintén a védett helyiség kategóriába sorolható, és itt szintén elsősorban a fizikai védelem kialakítása a cél a pusztító, az emberi szervezetet károsító hatásokkal szemben. Itt már követelmény lehet a stabil kommunikációs rendszer kiépítése, valamint ellentevékenység indítására alkalmas helyiség megalkotása. Védett helyiségről beszélhetünk a fizikai, biológiai kutató intézmények esetén is, mikor különböző a kutatás tárgyát képező káros hatásoktól kell megóvni a kutatók valamint a környezet épségét, vagy épp a külső szennyeződésektől kell megóvni a vizsgált folyamatot (Bréda, 2016).

2.2. A téma szempontjából releváns védett helyiség meghatározása

A téma szempontjából a védett helyiség fogalmát meghatározva, az olyan elhatárolt térrészt nevezünk védett helyiségnek: ahol érzékeny, értékkel bíró adatok és információk, (az arra jogosult helyen, minősített adatok és információk) fordulnak elő bármilyen ismert fizikai formában. A megvalósítani kívánt cél az, hogy azok az adatok és információk amelyek ebben a védett helyiségben előállnak, azok illetéktelen számára ne legyenek hozzáférhetőek, valamint azok jogosulatlan fél általi megszerzése, ne legyen lehetséges. Cél egy egységes védelmi szilárdság kialakítása, és annak fenntartása.

3. Az adatvédelem

A különböző adathordozókon rögzített anyagok fizikai védelme megoldottnak tekinthető, mivel különböző védelmi intézkedések és szabályok alkalmazása esetén a hozzáférés jól definiálható. Egy helyiség védelmét, ahol a védeni kívánt adatunk és információnk tárolt formában jelen vannak, alapesetben mechanikai és elektronikus vagyonvédelmi eszközökkel látjuk el. Sőt, ezen túlmenően élőerős őrzés megszervezése is kialakítható, amely jó hatékonysággal biztosíthatja a helyiség illetéktelenek behatolása elleni védelmét, vagy alapesetben jelzést kaphatunk egy behatolási kísérlet tényéről.

Áttekintve az érvényben lévő intézkedéseket, az informatikai berendezések üzemeltetése és az IT biztonság szinten tartásának elősegítésére számos gyártó dolgozik védelmi megoldások létrehozásán és fejlesztésén. Támogatást nyújtva a saját rendszereihez, napi szintű frissítéseket dolgoznak ki a megjelenő újabb támadások elleni védekezéshez. A jól karbantartott rendszerek, kis idő elteltével integrálják a kiadott frissítéseket. A témában szabványok érhetőek el, amelyek komplexen kezelik az IT biztonság területét. Ezek közül csak egyet említve az „MSZ ISO/IEC 27001:2014 Informatika. Biztonságtechnika. Információbiztonság-irányítási rendszerek. Követelmények.” elnevezésű szabvány, amely alkalmazása meglehetősen komplex megoldást nyújthat a védelem megalapozása terén.

Az állami és közigazgatási ágazatban az adat és információ védelme első megközelítésben, szabályzók által lefedettnek tekinthető. Az állam törvények, rendeletek és helyi szinteken utasítások előírásával szervezi és védi a minősített és érzékeny adatait. A témakörben a legfontosabb jogi intézkedések felsorolva a következőekben láthatóak:

- 2009. évi CLV. Törvény; A minősített adat védelméről
- 2013. évi L. Törvény; Az állami és önkormányzati szervek elektronikus információbiztonságáról

- 90/2010 (III./26) Kormányrendelet; A Nemzeti Biztonsági Felügyelet működésének, valamint a minősített adat kezelésének rendjéről
- 92/2010 (III./31) Kormányrendelet; Az iparbiztonsági ellenőrzés és a telephely biztonsági tanúsítvány kiadásának részletes szabályairól
- 161/2010 (V./6) Kormányrendelet; A minősített adat elektronikus biztonságának, valamint a rejtjeltevékenység engedélyezésének és hatósági felügyeletének részletes szabályairól

A magánszektorban szintén az értékkel rendelkező adatok, információk megóvása a cél viszont más jellegű háttérrel. A különbség az, hogy míg egy állami szerv, vagy hivatal illetve az azokkal kapcsolatban álló civil cég törvény által kötelezett a minősített és érzékeny adatok, információk védelmére, a tisztán magánszférában csupán a saját érdek védelme a mozgatórugója az információvédelemnek. A magáncégek esetén az adat és információvédelem sokszor az adatgazda szakértelmén valamint az anyagi lehetőségein múlik, törvényi védelmét az üzleti és magántitokról szóló jogszabályok alkotják ([1], [2], [3], [4], [5]).

Az üzleti titok védelme az alábbi két jogszabály segítségével valósul meg ([7], [8], Cégvezetés 2002.)

- Polgári Törvénykönyvről szóló 2013. évi V. törvény (Ptk) 2:47. §. *[Az üzleti titokhoz való jog. Know-how (védett ismeret)]*
  - **2:47. §** (1) Üzleti titok a gazdasági tevékenységhez kapcsolódó minden nem közismert vagy az érintett gazdasági tevékenységet végző személyek számára nem könnyen hozzáférhető olyan tény, tájékoztatás, egyéb adat és az azokból készült összeállítás, amelynek illetéktelenek által történő megszerzése, hasznosítása, másokkal való közlése vagy nyilvánosságra hozatala a jogosult jogos pénzügyi, gazdasági vagy piaci érdekét sértené vagy veszélyeztetné, feltéve, hogy a titok megőrzésével kapcsolatban a vele jogszerűen rendelkező jogosultat felróhatóság nem terheli.
  - (2) Az üzleti titokkal azonos védelemben részesül az azonosításra alkalmas módon rögzített, vagyoni értéket képviselő műszaki, gazdasági vagy szervezési ismeret, tapasztalat vagy ezek összeállítása (e törvény alkalmazásában: védett ismeret), ha a jóhiszeműség és tisztesség elvét sértő módon szerzik meg, hasznosítják, közlik mással vagy hozzák nyilvánosságra. E védelemre nem lehet hivatkozni azzal szemben, aki a védett ismerethez vagy az azt lényegében helyettesítő hasonló ismerethez
  - *a)* a jogosulttól független fejlesztéssel vagy
  - *b)* jogszerűen megszerzett termék vagy jogszerűen igénybevett szolgáltatás vizsgálata és elemzése útján jutott hozzá.
  - (3) Az üzleti titok megsértésére nem lehet hivatkozni azzal szemben, aki az üzleti titkot vagy a védett ismeretet harmadik személytől kereskedelmi forgalomban jóhiszeműen és ellenérték fejében szerezte meg.

- 1996. évi LVII. törvény (Tpt.); A tisztességtelen piaci magatartás és a versenykorlátozás tilalmáról;
  - **4. §** (1) Tilos a Polgári Törvénykönyvben meghatározott üzleti titkot tisztességtelen módon megszerezni vagy felhasználni, valamint jogosulatlanul mással közölni vagy nyilvánosságra hozni.

- (2) Üzleti titok tisztességtelen módon való megszerzésének minősül az is, ha az üzleti titkot a jogosult hozzájárulása nélkül, a vele üzleti kapcsolatban – ideértve az üzletkötést megelőző olyan tájékoztatást, tárgyalást és ajánlattételt is, amelyet nem követ szerződéskötés – vagy bizalmi viszonyban – így különösen munkaviszonyban, munkavégzésre irányuló egyéb jogviszonyban vagy tagsági viszonyban – álló személy közreműködésével szerezték meg.

3.1. Az elhangzott szó védelme

Az előzőekben említett adatvédelmi intézkedéseket és a munkahelyeken előforduló hagyományos kommunikáció megvalósulását tanulmányozva felvetődik egy a téma szempontjából fontos kérdés. Az adatok és az információk védelme, az általánosságban elterjedt és előírt információvédelmi megoldások alkalmazása és betartása mellett vajon minden szempontból megoldottnak tekinthető-e?

Az elhangzott szó védelmére konkrétan egyetlen hatályos kormányrendelet intézkedik utasítással amely a következő ([6]):

- 90/2010. (III. 26.) Kormány rendelet, A Nemzeti Biztonsági Felügyelet működésének, valamint a minősített adat kezelésének rendjéről
  - 59. § (2) A minősített adatot kezelő szerv vezetője biztosítja, hogy azok a biztonsági területek, ahol „Titkos!” vagy ennél magasabb minősítési szintű minősített adatokról rendszeresen tárgyalnak, lehallgatás mentesek legyenek.

A fenti kormányrendelet szintén csak a minősített adat témaköréhez kapcsolható és szó szoros értelemben csak a „Titkos!” minősítési szinttől határoz meg irányelvet az elhangzott szó védelmében. Tovább kutatva a témát, nem találunk megfelelő utasítást, valamint technikai paramétert a lehallgatás mentes tárgyalás kivitelezésére. A kutatásom egyik céljának tekintem egy ilyen környezet definiált létrehozását, valamint az egyenszilárdság fenntartásához való intézkedések meghatározását (Erdősi 2005, Vaszari 2007, Környei 2015).

4. Biztonsági rés meghatározása, hipotézis

A hagyományos munkaszervezésben az adatok és információk feldolgozásának folyamata, valamint az azokból nyert eredmények, információk, gyakran hangzanak el élő szóban a munkamegbeszéléseken. Ezzel létrehozva egy újabb fizikai közeget, ahol az információ, természetes közegében az ember számára talán a legkönnyebben megérthető formában előfordul. Feltevésem szerint az eddigi kutatásaim eredményeit figyelembe véve, ma Magyarországon nincs megfelelő definiált intézkedés az érzékeny (esetenként minősített) adatok szóbeli tárgyalási helyszínének kialakítására, valamint definiált műszaki leírás egy megfelelő védett helyiség megalkotására.

Ebből a megállapításból fakadóan további kutatást kell végezni az akusztikai közegből nyerhető információszerzés terén és meg kell vizsgálni az elhangzott szó tartalmának fizikai védelmére vonatkozó megoldásokat.

4.1. Technikai információszerzés

Az információszerzést, két nagy csoportra osztható. Az egyik a humán megközelítés, miszerint az embert, mint eszközt használva, történik meg az információk megszerzése. A másik csoport a technikai jellegű, melynek elemeit a következőekben láthatjuk:

- Nyílt források kutatása az interneten
- Adatbányászat
- Rádiós közlemények elfogása, demodulálása, az információ visszafejtése
- Informatikai támadások
- Hamis weboldalak létrehozása
- Lehallgatás

Ebben az esetben az információk megszerzésére, valamilyen a technika által kínált megoldás nyújt segítséget.

A témát tekintve az utolsó pont, a „lehallgatás" bizonyul a legnagyobb fenyegetésnek a védett helyiségek szempontjából. A következőekben egy megjelenő új probléma eszközrendszerét tekintem át a védett helyiségek fenyegetése szempontjából (Vadász, 2014).

4.2. Új fenyegetettség megjelenése

A kérdéskört megvizsgálva, találhatunk egy biztonsági problémát, amely napjaink technológiai és gyártástechnológiai fejlődésének eredménye.

Századunk felgyorsult világában, az információhoz való gyors hozzáférés, valamint a hírközlő technológiák alkalmazása napi szintű gyakorlattá vált. Míg a 90' években pár száz MB információ elektronikus úton történő rögzítésére és annak továbbítására szolgáló kisméretű eszköz, egyszerű ember számára szinte hozzáférhetetlen és megfizethetetlen volt, addigra napjainkban, szinte bárki hozzáférhet sokkal nagyobb tudású készülékhez, akár anonim módon internetes vásárlás segítségével. A világhálón található kínálatot áttekintve szembetűnik, hogy egy egész iparág épült a kisméretű kép és hang információgyűjtő berendezések gyártására.

Egy új probléma adódott, amióta az internet mindenki számára elérhető lett, és az áruszállítás nemzetközi szinten is akadálytalanná vált. Azóta mindennemű termék eladási rátája rohamosan megnövekedett. Ezért elsősorban az internetes kereskedést tartjuk felelősnek. Jelenleg a helyzet azt mutatja, hogy a kereskedelmi piacon, az információrögzítő berendezések széles spektrumát találjuk.

Az információszerzés az esetek többségében, különböző normáknak megfelelve etikus formában történik. A valóságot analizálva és a napi sajtót szemügyre véve azonban gyakran találunk olyan cikkeket, amelyeknek tartalma etikátlan hírszerzési, információszerzési metódusból származhat, vagy maga az ilyen információszerzési módszer ténye kerül napvilágra. Hazánkban csak a bűnüldöző szervek, külön engedély birtokában alkalmazhatják a rejtett megfigyelést lehetővé tevő technikákat nyomozati céllal. A polgári használata az ilyen módszert használó technikai berendezéseknek tilos. Mégis újból és újból kiderül, hogy létezik a probléma.

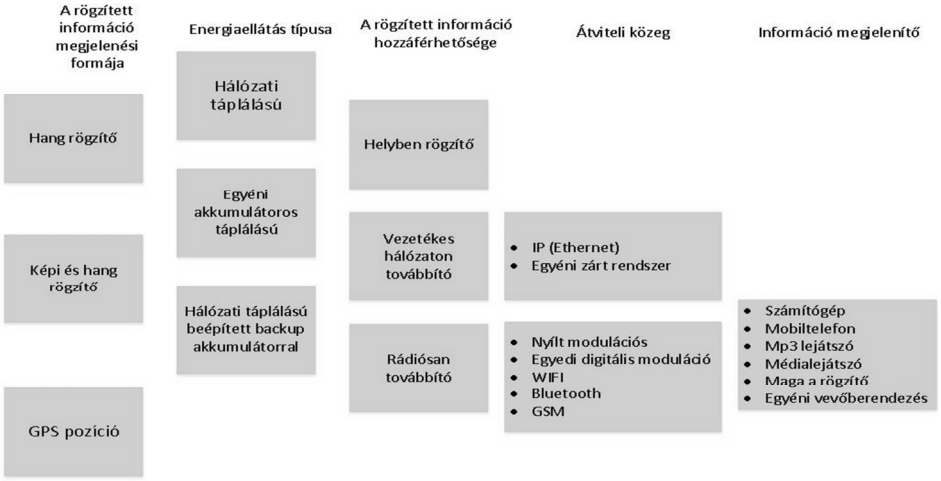
4.3. Autonóm információrögzítő hardverek áttekintése

A kutatási téma szempontjából fontos az önálló adatrögzítő berendezések vizsgálata, mivel egy védett helyiségben semmilyen módon nem kívánatos a következőekben tárgyalt berendezések bekerülése és alkalmazása. (Itt kell megemlítenem, hogy jelen téma nem foglalkozik az IT rendszereken történő információszerzéssel és azok elemeivel.)

Áttekintettem az internetes áruházakban hirdetett, a téma szempontjából releváns készülékek alapműködését és csoportosítottam azokat amely a 2. ábrán látható. A felhozott kínálatot áttekintve látható, hogy egy egész iparág épült a kisméretű rögzítő berendezések gyártására, függetlenül a rögzíteni kívánt fizikai közegtől. A rögzített felvételek formátuma mára már kizárólag digitális jellegű, az analóg technikákat teljesen kizárva

2. ábra. Az interneten található információrögzítő berendezések osztályozása működés szerint

Figure 2. Classification information gathering equipment operating principle found on the internet



*Forrás:*saját kutatás alapján, saját készítésű ábra

Látható, hogy a megfigyelni kívánt fizikai információ, amelyeket az áttanulmányozott berendezések érzékelni képesek, tulajdonképpen három rögzíthető alapparaméter köré tagolódnak. Kép, hang és földrajzi koordináta. Ez a három fő paramétercsoport, valamint ezek kombinációi.

Mivel elektromos berendezésekről van szó, meg kell, oldani azok villamos táplálását. A vizsgált eszközök lehetnek közvetlen hálózati táplálásúak, egyéni akkumulátoros-elemes táplálásúak valamint hálózatról működőek, valamint időszakos energia kiesést saját beépített akkumulátorról áthidaló típusok.

A rögzített fájlokhoz való hozzáférés módja, szintén három csoportba sorolható. Az első a helyben rögzítő típus. Itt önálló szigetüzemről beszélhetünk. Ezek az adatrögzítők valahová elhelyezve a típusuknak megfelelően magukon tárolják a rögzített eseményt. A rögzítményhez való hozzáféréshez szükséges az eszközhöz való újbóli hozzáférés.

A következő típuscsoport, amelynek adattartalma illetve információtovábbító képessége távolról is elérhető. A hozzáférés kiviteltől függően lehetséges rádiós úton, vagy vezetékes megoldás révén. Ennél a megvalósításoknál nem szükséges a berendezéshez való állandó fizikai hozzáférés, elég egy egyszeri elhelyezés. Végiggondolva egy gondolatbeli

elhelyezést, vezetékes megoldás alkalmazása esetén nem elég csupán az elhelyezés helyszínére történő egyszeri hozzáférés, itt konkrét kábelező feladat, vagy Ethernet hozzáférés szükséges. Párhuzamot vonva gondoljunk egy biztonsági kamerarendszer kiépítésére és az azzal járó kiépítési feladatok elvégzésére. Feltehetően az ilyen berendezések elhelyezése bonyolult, de az üzembiztonságuk szempontjából valószínűleg a leg stabilabb. A rádiós típusokat megvizsgálva tulajdonképpen az alap analóg modulációs eljárástól, napjaink telekommunikációs szabványainak megfelelő rádiós kommunikációs eljárásokig szinte a teljes paletta megtalálható. Egy egyéni analóg, vagy saját modulációs eljárással rendelkező adó hallhatósági hatósugara nagyban függ az adó kimenő teljesítményétől, addig WIFI, Bluetooth valamint GSM technológia esetén maximalizált, a technológia szabványára jellemző teljesítményviszonyokkal számolhatunk. A rádiós hírközlési szabványokat támogató berendezések önálló elérhetőségi távolsága ugyan nem növelhető egy bizonyos mértéken túl az adó teljesítményének növelésével, azonban ha rendelkezésre áll a technológiájuknak megfelelő szabványos hálózat és ahhoz csatlakoztatva helyezik el azokat, szinte bármilyen távolságból elérhetővé válnak.

Az információs tartalom megjelenítők, tulajdonképpen a szokványos digitális média lejátszást támogató berendezésekkel elképzelhetőek mint számítógép, mobiltelefon, médialejátszó. Hang és képrögzítő készülék esetén lehetséges, hogy magán a felvevő berendezésen is lejátszható a rögzített esemény.

Az eredmények kimutatják, hogy a technológia rohamos fejlődése és az árak rohamos csökkenése, valamint a szabad piac miatt a hozzáférés szabadabbá vált, vagyis mindenki számára elérhetővé váltak a tárgyalt eszközök. Az internet előtti időszakban az ilyen adatrögzítő eszközök beszerzése gyakorlatilag lehetetlen volt. Ez önmagában még nem is lenne baj, de társadalmunk sajnos a rossz irányba tart a bizalom terén. Előfordulhat, hogy aki hobbyként élt az ilyen eszközök adta lehetőségekkel, az hirtelen társai ellen használhatja, társadalmunk jóságának megítélését rontva. Akár csak egyet a tárgyalt berendezések közül jogszerűtlenül alkalmazva, súlyos etikai és jogi problémák vetődhetnek fel. A média csatornáinak hírközléseit, valamint a téma eddigi kutatási eredményeit összevetve, eltolódás várható az információszerzés módszerei tekintetében (Töltési 2006).

5. Összegzés

A cikk témáját végigtekintve megállapítható, hogy probléma van az információ védelem területén. Egy hipotézist határozok meg, miszerint az elhangzott szó védelme nem kifejezetten definiált. Az elérhető előírások, nem határoznak meg elég konkrét védelmi intézkedéseket az információval rendelkező szó védelmében. Az átfogó kutatás során, az internetet mint multi-funkciós felületet kihasználva, olyan technológiai és információszerzési indirekt felületet is igénybe vehetünk, amely a világháló előtti korszakban szinte elképzelhetetlen lett volna. Az adatrögzítő technológiák fejlődésével, a technikai berendezéseink mérete exponenciális mértékben csökkent, már-már szinte a kézzel alig fogható méretre. A rögzítő technológiák méretcsökkenésével az információrögzítő hardverek mérete is arányosan csökkent, így lehetőséget biztosítva azok rejtett formában történő használatának megvalósítására.

Véleményem szerint a tárgyalt terület védelmének meghatározására, valamint a technológiák alkalmazásának egyértelműsítésére, előírást kellene kidolgozni az érintett szabályozói környezetben, mivel azok nincsenek adaptálva a jelenlegi technológiai feltételrendszerre (Lazányi 2015).

Amennyiben a protokollok (SOP) nem tudják lekövetni a technológiák gyors változásait, az emberi tényezőben kell változást előidéznünk. A tudatos odafigyelés, megerősíti a rendszert. Lehetséges viselkedési előírások alapján, még jobb lenne, ha ez az egyének tudatos önérdek követő magatartása szerves részévé válna a rendszernek (Lazányi 2016).

Felhasznált irodalom

Ackoff, R. L., (1989): "From Data to Wisdom", Journal of Applies Systems Analysis, Volume 16, pp. 3–9.

G. Bellinger, D. Castro, A. Mills, (2004): "Data, Information, Knowledge, and Wisdom", http://www.systems-thinking.org/dikw/dikw.htm

Zoltayné Paprika Zita (2005): "Döntéselmélet", Aliena kiadó, Budapest.

Polányi, Michael, (1966): "The Tacit Dimension". Garden City: Dou-bleday and Company.

Nonaka, Ikujiro; Takeuchi, Hirotaka (1995): "The knowledge creating company: how Japanese companies create the dynamics of innovation", New York: Oxford University Press. p. 284.

Tóth László, Szikora Péter (2015): Data, information, knowledge in FUTÁR: Case study of a public transportation information system; Science Journal of Business and Management; 2015; 3(1-1): pp. 66–72 Published online January 16,;doi: 10.11648/j.sjbm.s.2015030101.21; ISSN: 2331-0626 (Print); ISSN: 2331-0634; http://article.sciencepublishinggroup.com/pdf/10.11648.j.sjbm.s.2015030101.21.pdf

Miller, George A. (1956):"The Magical Number Seven, Plus or Minus Two: Some Limits on Our Capacity for Processing Information", The PsychologicalReview, vol. 63, pp. 81–97.

Simmel, G. (1950). "The metropolis and mental life", In K. H. Wolff (Ed.), "The sociology of Georg Simmel" , New York: Free Press.

S. March, A. Hevner, S. Ram (2000). "Research Commentary: An Agenda for Information Technology Research in Heterogeneous and Distributed Environments", Informs Pubs Online. http://dx.doi.org/10.1287/ isre.11.4.327.11873 (accessed:30 Nov 2014)

Bréda Gábor (2016): Tavaszi Szél konferencia Absztraktkötet, Óbudai Egyetem p. 303.

MSZ ISO/IEC 27001:1014 Informatika. Biztonságtechnika. Az információbiztonság irányítási rendszerei. Követelmények; http://www.mszt.hu

[1] 2009. évi CLV. törvény a minősített adat védelméről. Hatályos 2015. 12. 24 http://njt.hu/cgi_bin/njt_doc.cgi?docid=126195.316499; letöltve: 2016. május 10.

[2] 90/2010 (III. 26.) Kormány rendelet A Nemzeti Biztonsági Felügyelet működésének, valamint a minősített adat kezelésének rendjéről. Hatályos 2014. 09. 05 http://njt.hu/cgi_bin/njt_doc.cgi?docid=132266.269659; letöltve: 2016. május 10.

[3] 92/2010. (III. 31.) Kormány rendelet az iparbiztonsági ellenőrzés és a telephely biztonsági tanúsítvány kiadásának részletes szabályairól Hatályos 2015. 08. 08. http://njt.hu/cgi_bin/njt_doc.cgi?docid=132295.297256; letöltve: 2016. május 10.

[4] 161/2010. (V. 6.) Korm. rendelet a minősített adat elektronikus biztonságának, valamint a rejtjeltevékenység engedélyezésének és hatósági felügyeletének részletes szabályairól Hatályos: 2015. 11. 07.; http://njt.hu/cgi_bin/njt_doc.cgi?docid=133060.313440; letöltve: 2016. május 10.

[5] 2013. évi L. törvény Az állami és önkormányzati szervek elektronikus információbiztonságáról; Hatályos: 2016. 01. 01.; http://njt.hu/cgi_bin/njt_doc.cgi?docid =160206.314734; letöltve: 2016. május 10.

[6] 90/2010 (III. 26.) Kormány rendelet A Nemzeti Biztonsági Felügyelet működésének, valamint a minősített adat kezelésének rendjéről. 59. § 2. pontja. Hatályos 2014. 09. 05.; http://njt.hu/cgi_bin/njt_doc.cgi?docid=132266.269659; letöltve: 2016. május 10.

[7] 2013 évi v. törvény ; 2:46. § A polgári törvénykönyvről; A magántitokhoz való jog. Hatályos 2016. 07. 01.; http://njt.hu/cgi_bin/njt_doc.cgi?docid=159096.323414; letöltve: 2016. október 15.

[8] 1996 évi LVII. törvény, A tisztességtelen piaci magatartás és a versenykorlátozás tilalmáról.; http://njt.hu/cgi_bin/njt_doc.cgi?docid=26902.294660; letöltve: 2016. október 15.

Cégvezetés 2002 november 01. 55. szám.; http://cegvezetes.hu/2002/11/az-uzleti-titok- vedelme/
Erdősi Péter (2005): CISA; Az üzletihírszerzés és az ipari kémkedés ajánlás, 2. változat, BME-GTK-ITT
Vaszari Ádám (2007): Üzleti hírszerzés a multinacionális cégeknél és a kis és középvállalkozásoknál; BGF-KFK
Vadász Pál (2014): Információkeresés a gazdasági hírszerzésben; Hadmérnök IX. évfolyam 2. szám – 2014. június.
Környei Mátyás, (2015): Üzleti titokvédelem; PTE ÁJK ;http://onszak.hu/folyoirat/wpcontent/uploads/2015/04/171_2nd.pdf
Töltési Imre Dr. (2006): Lehallgatásvédelem az üzleti szférában 1. Detektor plus 2006. 07. pp. 32–33, *www.detektor.siteset.hu/fajl.php?id=8281*
Töltési Imre Dr. (2006): Lehallgatásvédelem az üzleti szférában 2. Detektor plus 2006. 08–09. pp. 58–59; *www.detektor.siteset.hu/fajl.php?id=8282*
Töltési Imre Dr. (2006): Lehallgatásvédelem az üzleti szférában 3. Detektor plus 2006. 10–11. pp. 47–49; *www.detektor.siteset.hu/fajl.php?id=8283*
Lazányi Kornélia, (2015): A biztonsági kultúra; TAYLOR Gazdálkodás- és szervezéstudományi folyóirat 2015. 1–2 szám; Szeged 2015, p. 398–405. http://vikek.hu/wpcontent/uploads/2015/10/TAYLOR_2015-nyomdai.pdf
Lazányi Kornélia, (2016): A biztonsági kultúra szerepe a vezetői döntések támogatásában; TAYLOR Gazdálkodás- és szervezéstudományi folyóirat 2016. 1. szám; Szeged 2016, p. 143–150. http://vikek.hu/wpcontent/uploads/2016/05/Taylor2016.1.sz%C3%A1mNo22.pdf