HADMÉRNÖK

XI. Évfolyam 2. szám – 2016. június

Som Zoltán - Papp Gergely Zoltán
som.zoltan.kdi@office.uni-nke.hu - papp.gergely.kdi@office.uni-nke.hu

TUDÁSFEJLESZTÉS A KIBERBŰNÜLDÖZÉSBEN – LEHETŐSÉGEK ÉS KIHÍVÁSOK

Absztrakt

Napjainkban az infokommunikációs eszközök széles körben elterjedtek, a hétköznapi élet minden területén jelen vannak. Ezek az eszközeink értéket képviselnek, mint ahogy értéket képviselnek azon adatok, információk is, amelyek ezen eszközökön tárolódnak. Sok esetben maga az információ megszerzése a cél, a tároló eszköztől függetlenül, vagy fordítva. Fel van-e készítve a felhasználók arra, hogy milyen módon óvhatják meg adataikat? Legalább ennyire fontos, hogy fel vannak-e készítve a nyomozati szervek, hogy az új társadalmi változásokra, tendenciákra reagáljanak? Ezen logika mentén három fő érdekcsoportot különböztethetünk meg. Az első az állampolgárok köre, akik információs rendszereket és eszközöket használnak. A második fő csoport, akik információs rendszerekkel kapcsolatos visszaéléseket követnek el, eszközök vagy információk megszerzésében érdekeltek. A harmadik csoportot pedig a nyomozati szervek alkotják, akik a meglévő eszközparkkal, saját vagy külső erőforrásból próbálják fenntartani a rendet. A külső erőforrások vonatkozásában az igazságügyi szakértőkre gondolunk elsősorban, akik szakmai és műszaki felkészültségükkel képesek a nyomozati szervek munkáját segíteni. Mélyebben és összefüggéseiben vizsgálva a kérdést, ezen folyamatok kihatással lehetnek az e-szolgáltatások elterjedésére, az e-befogadására, a teljes IKT szegmensre és a GPD-re is. Így az infokommunikációs folyamatokból eredő változások feladatokat indukálnak számos területen, mind a kormányzati, a szolgáltatói, a bűnüldözői és a nyomozati tevékenységet folytató szervezeteknél egyaránt.

The use of various info-communication tools are widely spread, they are present in all areas of our every-day lives. These tools represent values to us, just as various data and information stored on them do. In numerous cases the goal is to acquire information with no special regard to the storage device or it might even be the other way around. Are users adequately prepared to be able to protect their data? Are they familiar with the right methods to do so? Just as importantly, are investigative bodies prepared to react to tendencies and changes of this new society? Following this logic, there are three major interest groups. The first one being the citizens using IT systems and tools. The second major group consists of those who are interested in acquiring information or equipment for which they abuse IT systems. And the investigative bodies make up the third group who try to maintain order using instruments they already own, utilizing their personal resources or some external ones. By external resources, we primarily mean judicial experts who are well prepared both professionally and technically

speaking and thus would be able to aid the work of investigative bodies. Reviewing the question at hand in context and more deeply, it becomes visible that these processes may affect the spreading of e-services, e-acceptance, and the ICT segment as a whole or even the GDP. As a result, changes in info-communication processes induce objectives to be set by service providers and bodies engaged in both governmental activities as well as law enforcement and investigation.

Kulcsszavak: *információbiztonság, informatikai bűnesetek, informatikai szakértő, információbiztonsági és tudatossági oktatás, e-befogadás, e-közigazgatás ~ information security, IT crime, IT expert, information security education and awareness, e-acceptance, e-(public) administration*

INFORMÁCIÓS RENDSZEREK NAPJAINKBAN

Az Európai Unió EU2020 programjának része, hogy polgárai minél több szolgáltatást vehessenek igénybe elektronikusan, ehhez pedig minden szükséges feltétel, például a szélessávú internetelérés lehetősége is rendelkezésre álljon.[1] Ezzel összhangban van a Nemzeti Infokommunikációs Stratégia 2014-2020, a technológiai változások és lehetőségek gyors kiszélesedése azonban más megközelítést igényel az állampolgárok részéről is. Felkészítéseket kell tartani tudatossági képzésekkel, ismeretterjesztő anyagokkal annak érdekében, hogy a gyors változásokkal járó kockázatokat csökkenteni lehessen, az állampolgárok megfelelő kompetenciával, rendelkezzenek, megfelelő tudatossági szinten legyenek saját adataik védelme érdekében.[2] Az állampolgárok általános csoportján kívül azonban számos más halmaz és érdekeltségi kör mentén is lehet csoportokat definiálni.

Az Európai Unió és Magyarország Kormányának, 2020-ig előirányzott stratégiai tervei [3], [4] további, nagymértékű fejlődést terveznek az elektronikus szolgáltatások, az IKT szektor és az e-közigazgatási szolgáltatások területén is. Ilyen nagyságú és gyorsaságú fejlődésre és változásra fel kell készíteni az érintetteket, az állampolgárokat, a közigazgatásban dolgozókat, megfelelő információbiztonsági szintet kell elérni.[5], [6]

Hétköznapi életünk minden területén jelen vannak és nélkülözhetetlenné váltak az információs rendszerek, különös tekintettel arra, hogy minden további közműszolgáltatás, szállítás, stb. is ezen rendszerek összehangolt irányítása mellett valósul meg.[7] A felhasználók jelentős része könnyen megtéveszthető, sokan a közvetlen környezetünkben napi szinten használt eszközök működési elvével sincsenek tisztában (például okostelefon, világítás, egyéb elektronikus vezérlésű rendszerek). Ennek egyik oka az, hogy a rendszer szállítója jellemzően el is rejti a „motorháztető alatt” annak elemeit, mivel a kezelőnek, felhasználónak elegendő bizonyos gombokat megnyomnia, nem szükséges ismernie a háttérben zajló folyamatokat. Ebből következik, hogy nem is érdemes ezen ismereteket oktatni (hiszen a technika fejlődésével mindez folyamatosan változik), sokkal inkább egy általános biztonságtudatossági magatartás és gondolkodás kialakítására, fejlesztésére van szükség, leginkább ezzel készíthető fel az állampolgár a lehetséges veszélyekre.

LOKÁLIS ÉS NEMZETKÖZI ESEMÉNYEK

Jól példázza a változó trendeket a 2007-es Észtországi kiberháború és 2010-es Iráni atomprogram[8] elleni támadás is.[9] Észtország esetében megmutatja, hogy mélyen, elemi folyamatokban vannak jelen az információs rendszerek, amelyek elleni célzott támadás rövid időn belül képes megbénítani a normál hétköznapi folyamatokat, akár egy egész ország életét. Az iráni atomprogram elleni Stuxnet vírustámadás pedig jó példa arra, hogy rendszereink összetettsége olyan méreteket öltött, amely már nehezen követhető. Strukturáltsága olyan bonyolult, hogy csupán más rendszerek segítségével vagyunk képesek működésüket fenntartani.

Léteznek szervezett bűnözői csoportok, amelyek fő profiljuk mellett alkalmanként más területeken is próbálkoznak, a meglévő adataikból próbálnak minél nagyobb profitra szert tenni. Az internetes feketepiacon minden adatnak értéke, ára van. Megadott összegekért cserél gazdát egy e-mail cím adatbázis, vagy bankkártya adatok, stb. minden pénzzé tehető. Általában véve igaz, hogy olyan gyorsan változik a technológia, amelyet rendkívül nehéz

szabályozási keretek között kezelni. A teljesség igénye nélkül jó példa erre a bitcoin [11] fizetési megoldás, vagy a Tor projekt [12], amely teljes anonimitást garantál.[13] Azonban az internet rendkívül polarizáló ereje révén, ezen eszközök is többféle célra, így illegális tevékenységre is alkalmasak.

A kiberteret [14], az Ibtv[15] alapján értelmezve könnyen belátható, hogy olyan globális hálózatot használunk, amelyben a potenciális fenyegetettség és támadások szempontjából szinte csak logikailag értelmezhető a magyar vagy más kibertér. A globális kibertér kifejezés jól reprezentálja, hogy nincsenek országhatárok, a visszaélési lehetőségek átlépik azokat. Egyetlen globális kibertér van, ahol természetesen vannak földrajzi eltérések, de ezek nem értelmezhetőek túl szigorúan. A Budapesten megalkotott – és számos további EU tagország által ratifikált –, a kiberbűnözés visszaszorításáról szóló egyezmény kereteit napjainkra túlhaladta az informatika világa. A kapcsolódó jogsértések is teljesen megváltoztak, így szükségszerű a terület újraszabályozása és folyamatos monitorozása. A tudomány fejlődési ütemét tekintve bizonyos, hogy az internetalapú digitális gazdaság a hazai fejlődés fontos tényezője lesz a következő években.[16] Az információs rendszerek polarizáló hatása figyelhető meg.

Összegezve egy olyan koordináta rendszerben képzelhetjük el az információs rendszereket, a globális kiberteret, amelynek az abszcisszáján az érdekeltségi motiváció található (azaz nemzetállamok, bűnszervezetek, ipari vállalatok, egészen a lakossági felhasználásig megtalálhatóak), míg az ordinátán az adott tevékenység pénzügyi hatása ábrázolható. Így talán a „legkisebbnek" tekinthető okostelefon és az ahhoz köthető adateltulajdonítás, valamint az ipari kémkedés reprezentálására egyaránt alkalmas a rendszer.

ÁLTALÁNOS GYAKORLAT ÉS TUDATOSSÁGI SZINT

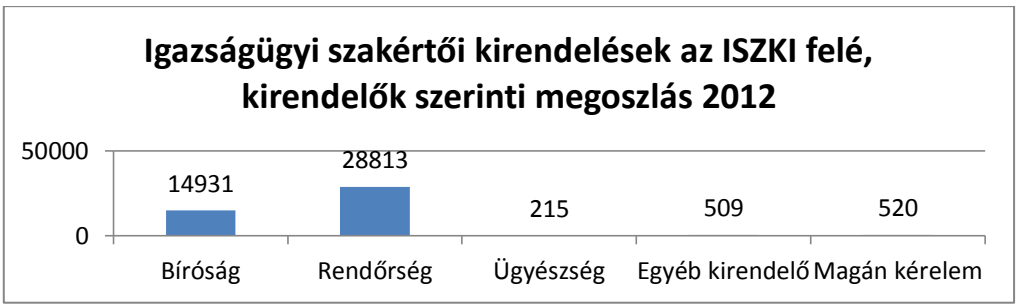
Az információs rendszerek széles körben elterjedtek, további növekedésük prognosztizálható. A nemzetközi és hazai kutatások, események mind azt mutatják, hogy az információra és az információs rendszerek feletti befolyásra napjainkban már komoly figyelmet kell fordítani, kiterjesztve az említett rendszerek működésének garantálására, a benne lévő információk védelmére, annak bizalmasságára, sértetlenségére és a rendelkezésre állására [17]. A globális kibertér eseményeire számos példát lehet felsorolni.[18] A közigazgatás kiszolgáltatottsága jelentős, mivel „…tény, hogy közigazgatás megszervezése a mai világban informatikai számítástechnikai eszközök nélkül nem lehetséges" [19]. A kibertudatosság [20] szinten tartása, növelése, a szervezeti egyenszilárdság megteremtése érdekében komoly lépéseket kell tenni. Ezen lépéssorozat egyike a Nemzet Közszolgálati Egyetemen elindult EIV képzés [21] is, amelynek reális eredményeit várhatóan csak évek múlva lehet kimutatni majd. Ennek oka feltételezhetően az, hogy a szervezeti egyenszilárdság megteremtése kultúra kérdése is, azaz nem lehetséges csak tisztán szabályozással gyors és tartós sikereket elérni.

Az is megállapítható, hogy alapszintű biztonságtudatos magatartással az ilyen visszaélések túlnyomó része megelőzhető lenne a virtuális térben [22]. Kutatások azt is igazolják, hogy a tudatos magatartást jelentősen befolyásolja az informatikai eszközökkel, rendszerekkel kapcsolatos felhasználói attitűd [23]. A jelenlegi információbiztonsági szint további, mélyebb elemzésre szorul, mivel a kutatások alapján valószínűsíthető, hogy a tudás sok esetben

megvan, de a gyakorlatba, a hétköznapokba nem minden esetben épült még be. [24] Magyarország ettől függetlenül jól áll szabályozás és alapok tekintetében az EU-n belül.[25] Nem várható el széles társadalmi rétegektől, hogy a technológia minden részletét ismerjék. Az ilyen jellegű visszaélések és nyomozati tevékenység ellátására, támogatására lett létrehozva a szakértői rendszer. Az általános gyakorlat természetesen valamilyen optimumra törekszik. Azaz a kisebb büntetési tételű vagy kisebb anyagi kárt jelentő ügyekben kisebb mértékben történik meg „energia kifejtés". Míg a 3-5 évnél nagyobb büntetési tételek, életellenes cselekmények esetében sokkal gyakoribb a szakértők bevonása. A szakértői rendszer részletes áttekintése nélkül két fontos dolgot kívánunk kiemelni. Az egyik, hogy a sok apró ügy summázása összességében olyan gazdasági értéket képviselhet, amellyel már érdemes lenne központilag foglalkozni. Ennek érdekében viszont olyan folyamatra, technikai és oktatási modernizációra van szükség, amely révén lehetséges az egyébként kis volumenű esetek kezelése is. A másik, hogy a látszólagosan kis fajsúlyú esetekben jelenleg még nem kezelik az eltűnt adatokat, jellemzően csupán az adathordozó notebook, telefon, stb. eszközökre koncentrálnak a nyomozati tevékenység során.

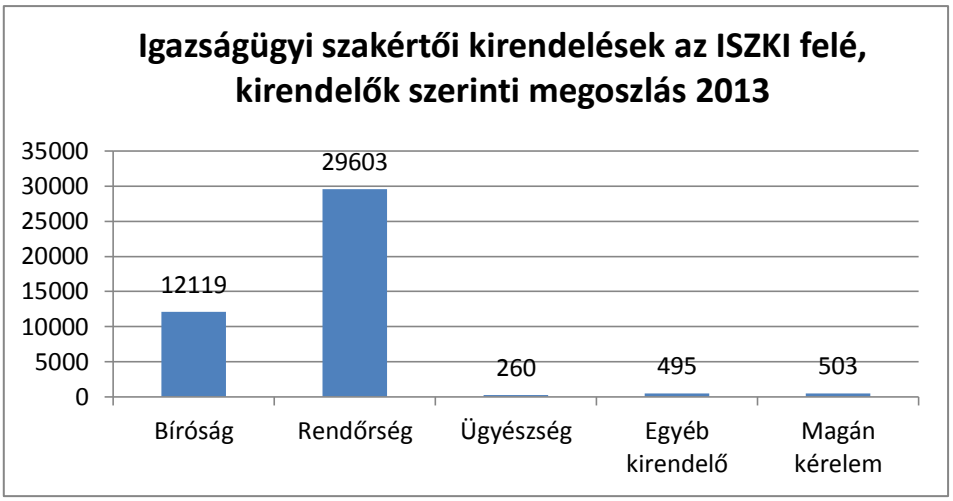
SZAKÉRTŐI KIRENDELÉSEK SZÁMA

Az igazságügyi szakértői rendszer működésének egyik lényege, hogy a tudomány aktuális, legfrissebb állásának megfelelő eredményeket felhasználva lehessen egyes esetekben eljárni, a szakterület legjobbjaitól segítséget kérni. Tekintsük meg a kirendelések számát, amely nem országos összesítés (csak az ISZKI felé érkező kéréseket mutatja), mégis reprezentatívnak tekinthető.[26]



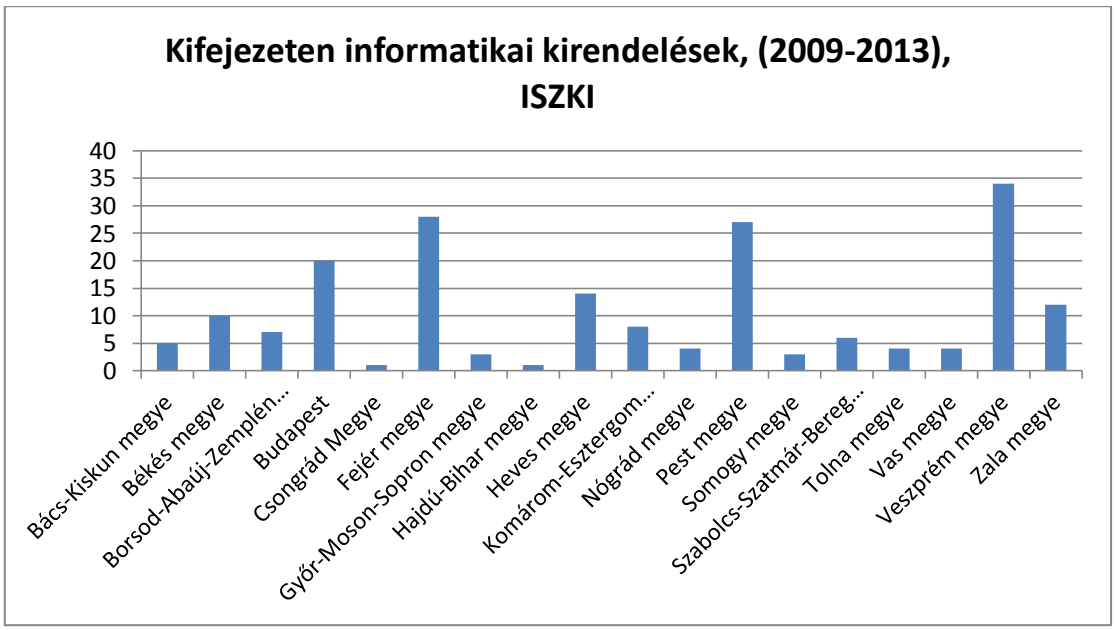
1.ábra Igazságügyi szakértői kirendelések az Igazságügyi Szakértői és Kutató Intézetek felé, 2012-ben[26]

A fenti 1. sz. ábrán az ISZKI felé intézett kirendelések és megkeresések száma figyelhető meg. A 2. sz. ábrán pedig a 2013-as évre vonatkoztatott adatok láthatóak. Látható, hogy nagyságrendi különbségek nincsenek, nagy változások nem tapasztalhatóak.



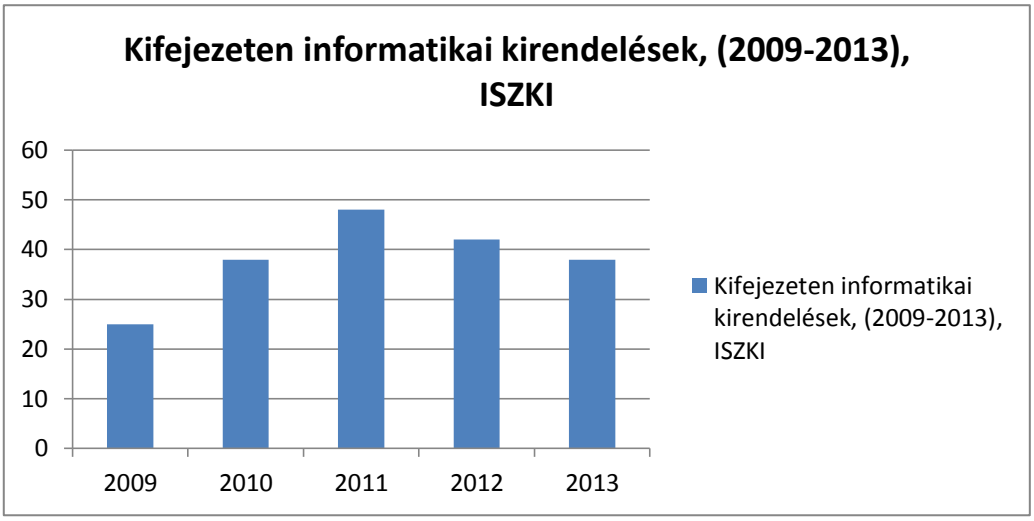
2. ábra Igazságügyi szakértői kirendelések az Igazságügyi Szakértői és Kutató Intézetek felé, 2013-ban [26]

Majd vizsgáljuk meg, a kifejezetten informatika témában történő kirendeléseket is a 2009-2013 intervallumban.



3. ábra Igazságügyi szakértői kirendelések az Igazságügyi Szakértői és Kutató Intézetek felé, informatikai ügyekben 2009-2013, megyénkénti eloszlásban [26]

A 4. ábrán pedig a 2009-2013 közötti, informatikai témában történő esetszámot láthatjuk, kirendelő szerinti bontásban.



4. ábra Igazságügyi szakértői kirendelések az Igazságügyi Szakértői és Kutató Intézetek felé, informatikai ügyekben 2009-2013, évenkénti eloszlásban [26]

Jól láthatóan egészen alacsony számban vannak informatikai kirendelések, felkérések, a teljes számossághoz viszonyítva. Ennek egyik oka lehet, hogy még a nyomozati tevékenységben, kriminalisztikai oktatásban, valamint a felhasznált eszközök tekintetében jelentős fejlesztésre lenne szükség. További oka lehet, hogy sok esetben közvetlenül keresik meg a hatóságok a szakértőket – elsősorban azért, hogy árversenyt indukáljanak. Pedig tudhatjuk, hogy „olcsó húsnak híg a leve", hiszen a jó szakértőnek fent kell tartani az eszközparkot, képeznie kell magát, hogy a kor követelményeinek megfelelve, magas tudományos szinten legyen képes az adott ügyet kivizsgálni.

Fontos tehát, hogy csupán technikai fejlesztés nem hozhat hosszú távú eredményeket. Erre jó példa, hogy „hiába" van rendszám, vagy akár arcfelismerő alkalmazás és rendszer, hiába van letárolva az adott nagy mennyiségű információ az adatbázisban, ha nincs ott a megfelelő szakértelemmel rendelkező humán-erőforrás, amely ezt feldolgozni képes. Tehát minden összetevőre szükség van ahhoz, hogy általánosan fordítani lehessen a jelenlegi tendencián. Az ember, a humán tényező és annak képzése, a képzett munkaerő kapacitása is kiemelten fontos a rendszerben, különös tekintettel arra, hogy az információs technológiák segítségével elkövetett, vagy éppen ennek segítségével felderíthető eseték száma prognosztizálhatóan növekszik. A társadalmi szokások változása miatt elképzelhető, hogy a táblagépek és okostelefonok sok esetben másodlagos célként jelennek meg, elsődlegesen már a rajtuk tárolt adatokon, azok megszerzésén, felhasználásán van a hangsúly. Ezen esetek felderítése technológiai értelemben nem lenne már lehetetlen, sokkal inkább humán-erőforrás függvénye.

MI VÁRHATÓ A JÖVŐBEN?

Az információbiztonság helyzetét vizsgálva Magyarországon láthatóan koncepcionális és szisztematikus munka valósul meg[31],[32], az EU direktívákkal összhangban. Az információbiztonság, annak mérése, az egyéni- és szervezeti tudatossági szint felmérése komoly kihívás, mivel bizonyos esetekben kimutatható, hogy a válaszadók a kérdéseknek akarnak megfelelni.[32] A többi Uniós tagállamhoz hasonlóan Magyarországon is működik az Európai Unió Safer Internet[33] programja, amelyet a Nemzetközi Gyermekmentő Szolgálat karolt fel. Összességében azt feltételezhetnénk, hogy jól állunk – és ez szabályozási szempontból valóban érvényes is –, azonban az tapasztalható, hogy még nem képezi a rutin

részét, nincs beidegződve a biztonságtudatos viselkedés. Bár ismertek az ajánlások, de még nem épültek be a szokásokba.

„Meg nem kerülhető kérdés a felhasználói tudatosság. A tapasztalatok szerint a minden IT újdonságra nyitott, gyakran a biztonsági minimumokat is elkerülő felhasználók zömét a fiatal korosztály adja. Az alap- és középfokú képzésben, majd a szakmai vagy felsőfokú szakirányokban kiemelt szerep hárul az oktatásban közreműködőkre annak érdekében, hogy a ma csak Y generációnak nevezett, néhány év múlva a gazdaság vérkeringésébe bekerülő tömegek személyes és egyéb szenzitív adatokat tudatosan, biztonságosan, készség szinten helyezzenek el, kezeljenek. A jelenleg hiányos, IT biztonság tárgyú oktatási anyagok és oktatói ismeretek pótlására hatékony finanszírozási eszközt kell biztosítania a fenntartónak."[33] Várhatóan növekedni fog azon események száma, amikor például nem csak az okos telefon lesz a célpont, nem csak az adathordozót tulajdonítják el, hanem a rajta lévő adatokkal is megkísérelnek majd visszaélni. Az adott eszközzel kapcsolatos figyelmeztetés akár törvényi kötelezettség is lehetne. „A kormány az Európai Unióban elsőként lépett a hatékonyabb, biztonságosabb, nagyobb tudású, ugyanakkor olcsóbb informatikai rendszer kialakításának, azaz a kormányzati felhőszolgáltatás elindításának útjára." [32] Hozzá kell tenni, hogy ez a tendencia állampolgári szinten is megjelenik. Azaz gyakorlatilag az okostelefon alkalmazások, a közösségi hálózatok, levelezés, mind olyan alkalmazások, amelyek jellemzően a felhőben, valahol a kibertérben találhatóak.

A további, várhatóan újabb platformokon megjelenő jogellenes cselekmények felderítése, szakszerű bizonyítása további kihívást jelent az igazságszolgáltatás valamennyi szereplője számára. A sok esetben felhőben tárolt, fizikai adathordozó lefoglalása nélkül feltárt összefüggések tényadatokkal való alátámasztása, szakvéleményben való objektív és érthető közlése még inkább nélkülözhetetlen lesz az ügyek hatósági szereplői számára. Hogy a jogszabály betűje szerinti kötelezettség teljesítése érdekében szükséges bizonyítási eszköztár és ismeretanyag többlet finanszírozása hogyan oldható meg a kötelezettek oldalán, egyelőre erősen nyitott kérdés.[32] További aggodalomra ad okot, hogy jelenleg sajnos nincs ezen a területen szakértői életpálya modell.

AZ INFORMÁCIÓS TÁRSADALOM GAZDASÁGI VETÜLETEI

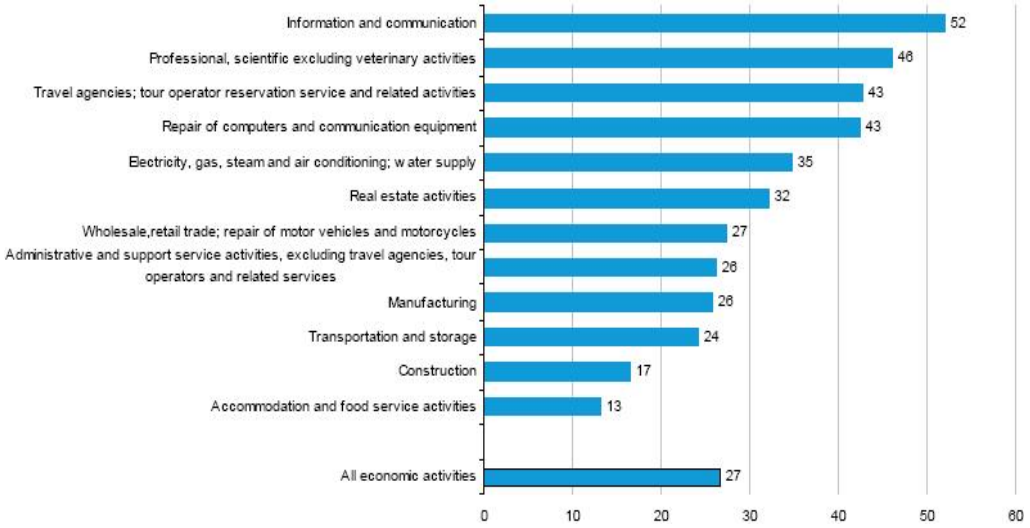
Minden évben, az európai állampolgárok 40%-a (kb. 200 millió fő) vásárol az interneten. Az IKT szektor önmagában majdnem 6%-át reprezentálja az EU GDP-jének és EU IKT szektor és az IKT-hoz kapcsolódó befektetések szállítják hozzávetőleg a felét a termelékenység növekedésének, emellett pedig az internet-gazdaság generálta a 21%-át az EU GDP növekedésének az elmúlt 5 évben. Az ENISA 2012-es jelentése[34] azt mutatja, hogy a kiberbiztonsági incidensek a munkahelyteremtést és a gazdasági növekedést is veszélybe sodorhatják.

Top Threats	Current Trends	Top Emerging Trends					
		Mobile Computing	Social Technology	Critical Infrastr.	Trust Infrastr.	Cloud	Big Data
1. Drive-by exploits	↑	↑	↑	↑		↑	↑
2. Worms/Trojans	↑	↑	↑	↑		→	↑
3. Code Injection	↑	→		↑		↑	
4. Exploit Kits	↑	↑	→	↑			↑
5. Botnets	↑	↑		→		→	
6. Denial of Service	→			→	↑	→	
7. Phishing	→	↑	↑	→			→
8. Compromising Confidential Information	↑	↑		↑	→	↑	↑
9. Rogueware/ Scareware	→		→				
10. Spam	↓		→				→
11. Targeted Attacks	↑		↑	↑	→	↑	→
12. Physical Theft/Loss/Damage	↑	↑	↑	↑	→	→	
13. Identity Theft	↑	↑	↑		→	↑	↑
14. Abuse of Information Leakage	↑	→	↑		→	↑	↑
15. Search Engine Poisoning	→						
16. Rogue Certificates	↑				↑		

Legend: ↓ Declining, → Stable, ↑ Increasing

5. ábra ENISA: Fenyegetettségi térkép 2013 áttekintő [34]

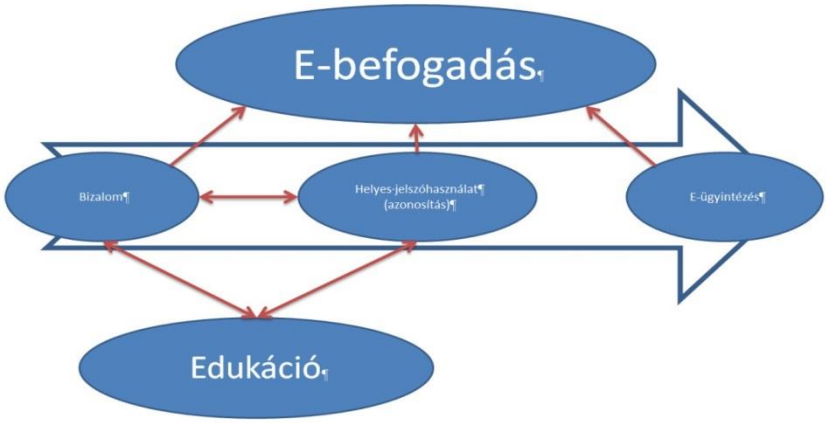
Az 5. sz. ábrán jól látható, hogy szinte minden potenciális támadási-területen minimum stagnálás, mailben irtam de jellemzően emelkedés tapasztalható a kiber bűncselekmények előfordulásában. A stagnáláshoz hozzátartozik, hogy az internetképes eszközök száma növekszik, így a puszta stagnálás is növekedést jelenthet.



6. ábra Az EU GDP és ICT kapcsolata [35]

Éppen ezért kiemelten fontos, hogy erre a nemzetközileg jellemző tendenciára Magyarország, és a hazai bűnüldöző szervek is felkészüljenek. Az igazságügyi szakértők szakmai és műszaki felkészültségükkel képesek a nyomozati szervek munkáját segíteni, mert már számos technikai lehetőség rendelkezésükre áll a tevékenységük támogatására, elegendő ha a számos, nyilvános területen található kamerára gondolunk, vagy a mobiltelefonok nyújtotta lokalizációs és képrögzítési lehetőségre. A megfelelő oktatás segítségével továbbá olyan társadalmi folyamatok is indukálhatóak, amelyek – összhangban a Magyarország

Nemzeti Infokommunikációs Stratégiájával és az EU 2020 célkitűzéseivel – szinergikus folyamatokat indíthatnak el. Mindezek nem csak az e-szolgáltatások elfogadottságát, az e-befogadást, az IKT szektor fejlődését erősíthetik, hanem kimutatható módon a GDP növekedéséhez is jelentős mértékben hozzájárulhatnak. Mindehhez természetesen komplexen látni kell nem csak az egyes folyamatokat, hanem az azok közötti összefüggéseket is.



7. ábra Az ügyfélbizalom, mint feltétel [36]

A FELHASZNÁLÓI BIZALOM ÉS AZ INFORMATIKAI BIZTONSÁG ÖSSZEKAPCSOLÓDÁSA

Ezen szolgáltatások támadása, nem csak és kizárólag anyagi veszteségeket, elmaradt bevételt produkál, hanem hosszú távon az ügyfélbizalom elvesztése révén sokkal komolyabb hatásai lehetnek. Az ügyfélbizalom helyreállítása sokkal költségesebb lehet, mint a prevenciós tevékenység, sőt bizonyos esetekben nem is lehetséges. Ezen a ponton tehát az informatikai biztonság és a felhasználói bizalom között nagyon szoros összefüggés mutatható ki.

Ahogy már említésre került, nem csupán az elkövetéssel érintett tárgy vagyoni értékét szükséges vizsgálni, nem csak az adott esetben érintett információ és információhordozó értékét, hanem az éves szinten summázott érték valószínűleg széles társadalmi mérésekkel összevethető módon befolyásolja azt az ügyfélbizalmat is, amelynek megerősítése és szinten tartása mára a modern gazdaságokban elengedhetetlen feltétel. Mindezeket áttekintve számos területen lehet megfogalmazni tennivalót, kicsit előre tekintve pedig már most láthatóak olyan, jelenleg még nem szabályozott területek, amelyek a technika gyors változásából következőleg olyan módszer kidolgozására sarkalják a szakmában érintetteket, amelyben a törvényi szabályozás gyorsasága összemérhetővé válik a technikai változásokkal. Azaz, ha új, még a törvényekben, eljárásrendekben nem szereplő visszaélési módszerek bukkannak fel, akkor azokat is nagyon gyorsan kezelni lehet, annak nem jelenlegi, hanem várható és összegzett súlya alapján. Így tehát az oktatásnak és a megfelelő eszköz- és humán erőforrásnak a szabályozási területen, a tudatossági képzéseken, az információbiztonsági vezetők rendelkezésre álló forrásaiban, a nyomozati tevékenységet ellátó szervezetek belső- és külső humánerőforrásainak tekintetében is meg kell jelennie. Nem utolsó sorban pedig az igazságügyi szakértő háttérrendszer megerősítésében, hiszen ezek nélkül nem jön létre, nem indulhat be az a szinergikus folyamat, amely révén széles társadalmi rétegekhez jut el a tudás, a tudatosság és nem alakul ki az a széleskörű bizalmi háló sem, támogatva az e-befogadást és erősítve a gazdasági tényezőket.

ÖSSZEGZÉS

Összegezve kijelenthető, hogy a humán faktor, az emberi tényező minden egyes folyamatban jelen van. Azaz nem elegendő és nem lehet megoldás csak a technológia fejlesztése, annak kiválasztása, beüzemelése, működtetése minden esetben humánerőforrást és döntést igényel. Mindehhez pedig olyan magasan képzett, a rendszert jól ismerő személynek kell rendelkezésre állnia, amely átlátja a megfelelő összefüggéseket, megfelelő kapacitással rendelkezik ahhoz, hogy a nagyszámú eseményt – amelyre irányulóan a technika csak elő feldolgozást képes végezni – le tudja kezelni. A tendenciák, nemzetközi és hazai szinten egyaránt jelen vannak, mint ahogy a kibertér képzeletbeli határai is nehezen rajzolhatóak meg. Így az oktatás és a felkészítés területén – amelyek mind a szakembereket, mind pedig széles társadalmi rétegeket érintenek – sok tennivaló van még. A szakértői rendszer vonatkozásában olyan életpályamodellt lenne érdemes kialakítani, amely hatékony támogatást képes nyújtani ahhoz a célhoz, hogy az egyre növekvő információ rendszerekkel összefüggő esetek, visszaélések, ezek terjedése ne öltsön még nagyobb méreteket. Határozott koncepciót kell kialakítani, hogy ne utólag kelljen az e-bizalom visszaállítására, az e-befogadás újra-fejlesztésére horribilis forrásokat elkülöníteni.

Felhasznált irodalom

[1] Europe 2020, A European strategy for smart, sustainable and inclusive growth, http://ec.europa.eu/eu2020/pdf/COMPLET%20EN%20BARROSO%20%20%20007%20-%20Europe%202020%20-%20EN%20version.pdf, 2016.05.01.

[2] Z. Som: Laws aiding cyber security in the EU. Central and Eastern European eGov Days, 2014.

[3] EU 2020 Programterv az ICT szektorra, http://ec.europa.eu/programmes/horizon2020/en/h2020-section/information-and-communication-technologies, 2016.05.01.

[4] Nemzeti Infokommunikációs Stratégia 2014-2020, http://www.nisz.hu/sites/default/files/u1/nemzeti_infokommunikacios_strategia_2014_2020.pdf, 2016.05.01.

[5] Magyarország Nemzeti Biztonsági Stratégiájáról szóló 1035/2012. (II. 21.) Korm. határozat, 31. pont a kiberbiztonságról http://2010-2014.kormany.hu/download/f/49/70000/1035_2012_korm_hatarozat.pdf, 2016.05.01.

[6] Magyarország Nemzeti Kiberbiztonsági Stratégiájáról szóló 1139/2013. (III. 21.) Korm. határozat, http://njt.hu/cgi_bin/njt_doc.cgi?docid=159530.238845, 2016.05.01.

[7] Z. Som: Cyber security legislation in the EU in: The information technology as Public Utility. Nispace, 2014.

[8] A. Cserháti: A stuxnet vírus és az iráni atomprogram, http://fizikaiszemle.hu/archivum/fsz1105/CserhatiAndras.pdf, 2016.05.01.

[9] Z. Som: Kibertudatossággal a kiberhadviselés ellen. 13. Robothadviselés konferencia, 2013.

[11] A Bitcoin fizetési eszköz, https://bitcoin.org/hu/, 2016.05.01.

[12] A Tor Projekt, https://www.torproject.org/, 2016.05.01.

[13] P. Sasvári, Z. Som: Az információbiztonság-tudatosság vizsgálata a magyar üzleti- és közszférában. ITBN, 2016.05.01.

[14] [15] 2013. évi L. törvény az állami és önkormányzati szervek elektronikus információbiztonságáról, http://kozlonyok.hu/nkonline/MKPDF/hiteles/MK13069.pdf, 2016.05.01.

[16] Cs. Lente: Mérlegen az informatikai biztonság. ITBN, http://miszk.hu/hir/merlegen-az-informatikai-biztonsag.html, 2016.05.01.

[17] Z. Som: Hitelesítési kérdések a magyar (e-) közigazgatásban. Tavaszi szél konferencia, http://www.kozszov.org.hu/dokumentumok/UMK/UMK_2014_2/20_esemeny_Orszagos_doktorandusz_konf.pdf, 2014.

[18] G. Z. Papp, Z. Som: Jelszóhasználati trendek és az ügyfélbizalom értéke, avagy a jelszó, a bizalom és az e-befogadás és ezek kapcsolata napjainkban. http://www.academia.edu/9393609/Jelsz%C3%B3haszn%C3%A1lati_trendek_%C3%A9s_az_%C3%BCgyf%C3%A9lbizalom_%C3%A9rt%C3%A9ke._A_jelsz%C3%B3_a_bizalom_%C3%A9s_az_e-befogad%C3%A1s_%C3%B6sszef%C3%BCgg%C3%A9sei_napjainkban, 2016.05.01

[19] I. Bukovics: A fenntartható közigazgatás, fenntartható biztonság elmélete. http://docplayer.hu/9743088-Bukovics-istvan-a-fenntarthato-kozigazgatas-fenntarthato-biztonsag-elmelete.html, 2016.05.01.

[20] 2013. évi L. törvény az állami és önkormányzati szervek elektronikus i nformációbiztonságáról, http://kozlonyok.hu/nkonline/MKPDF/hiteles/MK13069.pdf, 2016.05.01.

[21] NKE Elektronikus információbiztonsági vezető szakirányú továbbképzési szak, http://vtki.uni-nke.hu/szakiranyu-tovabbkepzes/szakiranyu-tovabbkepzesi-szakok/elektronikus-informaciobiztonsagi-vezeto-szakiranyu-tovabbkepzesi-szak, 2016.05.01.

[22] Z. Som, G. Z. Papp: Információbiztonsági alapok és jelszóhasználati statisztikák. A jelszó, a bizalom és az e-befogadás összefüggései napjainkban. http://www.academia.edu/9393569/Inform%C3%A1ci%C3%B3biztons%C3%A1gi_alapok_%C3%A9s_jelsz%C3%B3haszn%C3%A1lati_statisztik%C3%A1k._A_jelsz%C3%B3_a_bizalom_%C3%A9s_az_e-befogad%C3%A1s_%C3%B6sszef%C3%BCgg%C3%A9sei_napjainkban, 2016.05.01.

[23] J. Reich, Zs. Döme: Közszolgálat a közigazgatásban. ÁROP-2011/1.1.12.

[24] M. Illéssy, A. Nemeslaki, Z. Som: Elektronikus információbiztonság-tudatosság a magyar közigazgatásban. Információs társadalom, Társadalomtudományi folyóirat, XIV. évfolyam, 1. szám (p.:52-73) ISSN:1587-8694.

[25] 2013. évi L. törvény az állami és önkormányzati szervek elektronikus információbiztonságáról, http://kozlonyok.hu/nkonline/MKPDF/hiteles/MK13069.pdf, 2016.05.01.

[26] Igazságügyi Szakértői és Kutató Intézetek. Nyilvános, weblapról származó információk, beszámolók, negyedéves jelentések hivatalos 2009-2014. évi adatszolgáltatása alapján saját feldolgozás és elemzés. http://www.iszki.hu/, 2016.05.01.

[27] Digitális Megújulás Cselekvési Terv. Egyszerű Állam: a vállalkozások adminisztratív terheit csökkentő középtávú kormányzati program. Magyary Zoltán Közigazgatás-fejlesztési Program. Magyarország Nemzeti Kiberbiztonsági Stratégiája. Nemzeti Infokommunikációs Stratégia 2014-2020. Ibtv.

[28] Z. Som, G. Z. Papp: Információbiztonsági alapok és jelszóhasználati statisztikák. A jelszó, a bizalom és az e-befogadás összefüggései napjainkban. http://www.academia.edu/9393569/Inform%C3%A1ci%C3%B3biztons%C3%A1gi_alapok_%C3%A9s_jelsz%C3%B3haszn%C3%A1lati_statisztik%C3%A1k._A_jelsz%C3

%B3_a_bizalom_%C3%A9s_az_e-befogad%C3%A1s_%C3%B6sszef%C3%BCgg%C3%A9sei_napjainkban, 2016.05.01.
[29] M. Illéssy, A. Nemeslaki, Z. Som: Elektronikus információbiztonság-tudatosság a magyar közigazgatásban. Információs társadalom, Társadalomtudományi folyóirat, XIV. évfolyam, 1. szám (p.:52-73) ISSN:1587-8694.
[30] EU Safer Internet Program, https://saferinternet.hu, 2016.05.01.
[31] Digitális Megújulás Cselekvési Terv. Egyszerű Állam: a vállalkozások adminisztratív terheit csökkentő középtávú kormányzati program. Magyary Zoltán Közigazgatás-fejlesztési Program. Magyarország Nemzeti Kiberbiztonsági Stratégiája. Nemzeti Infokommunikációs Stratégia 2014-2020. Ibtv.
[32] Cs. Lente: Mérlegen az informatikai biztonság. ITBN, http://miszk.hu/hir/merlegen-az-informatikai-biztonsag.html, 2016.05.01
[33] Enisa. Threat Landscape 2013. Overview of current and emerging cyber-threats. 11 December 2013.
[34] Enisa. Threat Landscape 2013. Overview of current and emerging cyber-threats. 11 December 2013.
[35] Eurostat weboldal. Figure 10. http://ec.europa.eu/eurostat/documents/4168041/5947469/KS-QA-10-049-EN.PDF/15c0d269-9f5f-4ab6-aefb-6db976cb22cd , 2016.05.01.
[36] Z. Som: Hitelesítési kérdések a magyar (e-) közigazgatásban. Tavaszi szél konferencia, http://www.kozszov.org.hu/dokumentumok/UMK/UMK_2014_2/20_esemeny_Orszagos_doktorandusz_konf.pdf, 2014.