Som Zoltán[412]**: Interoperabilitási kérdések és informatikai biztonsági tükrében a közigazgatásban**

Absztrakt
Magyarországon a 2013. évi CCXX. törvény az állami és önkormányzati nyilvántartások együttműködésének általános szabályairól ír elő interoperabilitási kötelezettséget. Ezen túlmenően be kívánom mutatni, hogy milyen további jogforrások léteznek, különös tekintettel az Európai Unió irányelvekre. Az Európai Unió tagjaként számos környező ország érintett Magyarországon kívül. Ha országhatárok nélkül tekintjük, akkor pedig magyar állampolgárok, Európai Uniós viszonylatban pedig az összes uniós állampolgár, nemzetiségtől függetlenül. Tekintettel az egyes kormányok és az EU e-kormányzati törekvéseire, a 2014-2020-as akciótervek alapján jelentős változások indulnak meg, melyek mindannyiunk életére hatással lesznek. Tanulmányomban át kívánom tekinteni, hogy a növekvő e-kormányzati infrastruktúra milyen szükséges előzetes felkészítést igényel az állampolgárok és az őket kiszolgáló, az infrastruktúrát kezelő és üzemeltető személyzet és oktatásuk szempontjából, mindezt elsősorban informatikai biztonsági szempontból megvizsgálva.

Előszó helyett

Információs társadalomban élünk[413], hétköznapi életünk során számtalan információs, elektronikus rendszert használunk. Azonban a közvetlenül használt eszközökön kívül, szinte minden igénybe vett szolgáltatás mögött információs rendszerek állnak. Ilyenek a közlekedési rendszerek, víz, gáz és áramszolgáltatás, az állami és közigazgatási, banki szolgáltatások, stb. Az információs közmű képezi mindezek alapját. Az információs közmű az állam és állampolgárok életének minden egyes területén jelen van. Voltaképpen az elektromos áram és az információs szolgáltatások nélkül minden, ami a mai modern környezetünk jellemzi, minden egyes további közmű megszűnne működni. Tételes felsorolásra nem vállalkozom, de a víz és gázelosztó rendszerek, a logisztikai és közlekedési irányítók, pénzügyi és egyéb szektorok mögött mind információs rendszerek tartják fent a működést. A nemzetközi és hazai kutatások és események, mind azt mutatják, hogy az információ és az információs rendszerek feletti befolyásra napjainkban már komoly figyelmet kell fordítani, kiterjesztve az említett rendszerek működésének garantálására,[414] a benne lévő információk védelmére, annak bizalmasságára, sértetlenségére és a rendelkezésre állására.[415] A globális kibertér eseményeire a kiberfenyegetésekre, kiberhadviselésre, a kibertámadásokra, kiber terrorizmusra, stb. mindezekre számos példát lehet felsorolni. És bár a szakirodalom gyakran szinonimaként használja a kiber, az információ és informatikai biztonság szavakat, a lényeg, hogy az információ különböző megjelenési formáival, azok feletti kontrollokkal foglalkozni szükséges. A közigazgatás kitettsége jelentős, mivel „…tény, hogy közigazgatás megszervezése a mai világban informatikai számítástechnikai eszközök nélkül nem lehetséges”.[416] [417]A kibertudatosság[418] szinten tartása, növelése, a szervezeti egyenszilárdság megteremtése[419] érdekében komoly lépéseket kell tenni. Ezen

[412] Nemzeti Közszolgálati Egyetem, Közigazgatás-tudományi kar, Közigazgatás-tudományi Doktori iskola és a Technológia es Innováció Kutatóközpont PhD hallgatója, az E-közszolgálati Fejlesztési Intézet munkatársa som.zoltan.kdi@office.uni-nke.hu
[413] Som Zoltán: *Az internet veszélyei és ajánlás ennek kezelésére, elsősorban a tizenéves általános iskolások vonatkozásában.* Módszertani közlemények: tanítók és tanárok számára 2012- 53:(2) pp. 21-32., 2013
[414] Dr. Bukovics István: *A fenntartható közigazgatás, fenntartható biztonság elmélete.*
[415] Som Zoltán: *Hitelesítési kérdések a magyar (e-) közigazgatásban*, Tavaszi szél konferencia 2014
[416] A fenntartható közigazgatás, fenntartható biztonság elmélete, Dr. Bukovics István
[417] Bukovics István: *A kritikus infrastruktúrák rendszerkoncepciója*, Fejezetek a kritikus infrastruktúra védelemből, ISBN 978-963-08-6926-3, 2013
[418] 2013. évi L. törvény: az állami és önkormányzati szervek elektronikus információbiztonságáról
[419] Som Zoltán – Pál Attila 2013: *Tudatosság oktatás az infobiztonsági törvény alapján, közigazgatási tapasztalatok*. Elhangzott: Budapest, ITBN konferencia 2013.09.26

lépéssorozat egyike a Nemzet Közszolgálati Egyetemen elindult képzés[420] is, melynek meglátásom szerint nagyobb volumenű eredményeit évek múlva lehet csak kimutatni. Ennek oka feltételezhetően az, hogy a szervezeti egyenszilárdság megteremtése kultúra kérdése is, azaz nem lehetséges csak tisztán szabályozással, a szabályozás változásával gyors és tartós sikereket elérni. Képzésre, tudatossági oktatásokra van szükség.

Magyarországon a Nemzetközi Gyermekmentő Szolgálat karolta fel az Európai Unió Safer Internet[421] Programjának a támogatását. Önkéntes oktatók és programok, rendezvények segítségével igyekszik felhívni a figyelmet arra a jelenségre, hogy ezen ismereteket, amelyekre a modern információs társadalomban szükség van[422] nem tartalmazza – még – az iskolarendszerű képzés.

Az első digitális lábnyom

Az Európai Unió Safer Internet Programjának önkéntes oktatójaként sokszor teszem fel a kérdés, mikor keletkezik az első digitális lábnyomunk? Úgy gondolom, számos jó válasz létezik a kérdésre. Ezek egyike lehet, hogy születéskor nyilvántartásba kerül mindenki, egyesek ezzel párhuzamosan a helyi újság „megérkeztünk" rovatában is megjelennek. Ezt megelőzően, azonban már az első ultrahang felvételek is bekerülhetnek orvosi, elektronikus rendszerekbe. Ha pedig tovább boncolgatjuk a kérdés, akkor talán a szülő digitális lábnyomához tartozik még a terhességi teszt megvásárlásának bankkártyás fizetési lenyomata. Ez a digitális adattest életünk során velünk növekszik. Továbblépve az első digitális lábnyom kérdéskörén, általában vizsgálva a kérdést, minden ide tartozik, amely a felhasználó online jelenléte után megmarad és amelyből következtetni lehet a tevékenységére, vagy személyére, [423] vagy további adatgyűjtésre alkalmas. Mindezek alapján belátható, hogy a digitális lábnyom, a digitális adattesttel kapcsolatos tudatosság már nem csak a fiatal korosztály oktatása kapcsán kiemelt fontosságú. Gyorsan változó világunkban a tanulási folyamat már nem feltétlen a szülő – gyerek másolódás révén jön létre és ez kiemelten igaz az információs technológiák használtára is [424] A nemzetközi és hazai törekvéseken belül a közigazgatási rendszerek fejlesztése kiemelt terület, fontos megteremteni tehát ezen rendszerek használathoz szükséges kompetenciákat is. A közigazgatásban is egyre nagyobb teret nyerő infokommunikációs technológiák felhasználáshoz számos területen kell párhuzamos fejlesztéseket megvalósítani. Ezen fejlesztések azonban nem csak kizárólag tudás, nem csak kizárólag infrastruktúra, stb. területeken kell, hogy megnyilvánuljanak. Számos kutatás támasztja alá, hogy az igénybevett szolgáltatás kapcsán a felhasználó saját tudásáról alkotott képe is legalább ugyan olyan fontos tényezőként esik latba. [425] A felhasználó, aki képes saját digitális identitását tudatosan kezelni, nagyobb valószínűséggel fogja használni az információs rendszereket, akár a közigazgatásban is. Ez pedig társadalmi - gazdasági előnyökkel is járhat.

---

[420] NKE Elektronikus információbiztonsági vezető szakirányú továbbképzési szak

[421] A Safer Internet konzorcium tagjai: Nemzetközi Gyermekmentő Szolgálat – Konzorcium-vezető, tudatosság-növelő központ, Kék Vonal Alapítvány – Helpline, Puskás Tivadar Közalapítvány - CERT Hungary – Hotline

[422] Som Zoltán: *Az internet veszélyei és ajánlás ennek kezelésére, elsősorban a tizenéves általános iskolások vonatkozásában.* Módszertani közlemények: tanítók és tanárok számára 2012- 53:(2) pp. 21-32., 2013

[423] Digitális lábnyom, http://netpedia.hu/digitalis-labnyom, Letöltve: 2014.06.30.

[424] Som Zoltán, *Kibertudatossággal a kiberhadviselés ellen*, 13. Robothadviselés konferencia,

[425] Döme Zsolt - Reich Jenő, Közszolgálat a közigazgatásban, ÁROP 2011/1.1.12, Elhangzott: Időpont: 2014.03.18. NKE

Információbiztonság

Az információbiztonság, mint kifejezést megértéséhez számos további tényezőt kell figyelembe venni. Egyrészt gyakran az informatikai biztonság szinonimájaként használják tévesen ezt a kifejezést. Másrészt az információ már valamilyen értelmezést takar. Azaz valamely adat értelmezése, összefüggések feltárása révén válik információvá. Ezért a legtöbbet az adat szintjén tehetünk az információbiztonság és – védelem érdekében. Ennek érdekében a leg alacsonyabb szinten, szinteken, az adat szintjén kell megtenni a szükséges óvintézkedéseket. Általában véve igaz, hogy a legtöbbet, tudatossággal lehet tenni. Ennek érdekében a stratégia része kell, hogy legyen a tudatosság kialakítása, tudatossági oktatási stratégia megtervezése, amely nem csak szigorúan a közigazgatásban, hanem a közigazgatás ügyfeleire, az állampolgárokra, vállalkozásokra, stb. is ki kell, hogy terjedjen. Ezen kompetenciák kialakítására és folyamatos fejlesztésére komoly, a jelenleginél nagyobb hangsúlyt szükséges fektetni. Egyrészt, mivel ez a terület még nem épült be az oktatásba, semelyik szinten.[426] Másrészt viszont a hétköznapi életünk során már jól érezhetően jelen van a virtuális tér és a kettő közötti határvonal összemosódik. Annak érdekében, hogy valódi és digitális világunkban létező identitásunkat egyaránt meg tudjuk védeni, olyan széleskörű oktatási program meghirdetésére lenne szükség, amely egyszerre képes az összes korosztályt megszólítani. Hiszen a közoktatásba való beépítése csak részeredmény lehet a közigazgatás ügyfeleinek népes táborát tekintve.

Kutatási területemen, az információbiztonságnak a fentieken belül egy szűkebb szeletét vizsgálom kiemelt alapossággal. A közigazgatásban, munkaszervezeti szinten teszem fel a kérdést, hogyan lehetséges mérni az információbiztonsággal összefüggő tudatossági szintet, milyen képzési lehetőségek állnak rendelkezésre annak fejlesztésére.

Jogszabályi környezet és közigazgatás

Magyarország EU viszonylatban is „alapvetően jól áll" az információbiztonság szabályozottságának vonatkozásában és ez elsősorban a szakmai közösségen kívül a 2013. évi L. törvénynek[427] és az azt követő végrehajtási rendeleteknek[428] köszönhető. Fel kell, hogy hívjam azonban a figyelmet, hogy több tucatra tehető azon keretrendszerek, irányelvek, ajánlások, jogszabályok és egyéb vonatkozó dokumentumoknak a száma, amelyet a közigazgatásban és információs rendszerek tervezésétől az üzemeltetéséig terjedő intervallumban érintett szervezeteknek figyelembe kell venniük.[429] Ezek nem minden esetben szigorúan vett jogszabályok. Sokkal inkább olyan ajánlások a tervezéshez, kivitelezéshez, üzemeltetéshez, amelyek segítségével majd olyan távlati célok is elérhető közelségbe kerülhetnek, mint a tervezhetőség, költséghatékonyság, információbiztonság, interoperabilitás.

Az interoperabilitás szemszögéből vizsgálva az egyes rendszerek közötti interoperabilitás képessége és megvalósulása, egyaránt érdeke a közigazgatásnak és az ügyfeleinek. A közigazgatás így képessé válhat összetett adatok és összefüggések értelmezésére, valamint olyan szolgáltatások és magas szintű kiszolgálás lebonyolítására, amely jelenleg még csak papír alapon és eltérő alrendszerből lehetséges.

A teljesség igénye nélkül mindenképpen érdemes kiemelni hazai viszonylatban a Nemzeti Infokommunikációs Stratégiát[430], a 2013. évi L. törvényt és annak végrehajtási rendeleteit. Nemzetközi viszonylatban pedig az EU COM(2010) 743 (végleges) dokumentumot. Ez voltaképpen egy action plan, ami az interoperabilitást, az elektronikus aláírást és a digitális azonosítást jelöli meg, mint fő megoldandó szakterületeket. Erre épül rá az European Interoperability Framework (EIF).

[426] Krasznay Csaba: *A modern kor gyermekkatonái – hogyan védjük az ifjú hackereket?* 2012, 2012.09.25, II. Nemzetközi Konferencia: Az internet hatása a gyermekekre és a fiatalokra, Budapest, Magyar Tudományos Akadémia

[427] A 2013. évi L. törvény, az állami és önkormányzati szervek elektronikus információbiztonságáról.

[428] A 301/2013. (VII. 29.) Korm. Rendelet, 26/2013. (X. 21.) KIM rendelet, 77/2013. (XII. 19.) NFM rendelet, 36/2013. (VII. 17.) BM rendelet, 36/2013. (VII. 17.) BM rendelet, 36/2013. (VII. 17.) BM rendelet

[429] Som Zoltán: *Hitelesítési kérdések a magyar (e-) közigazgatásban*, Tavaszi szél konferencia 2014

[430] Nemzeti Infokommunikációs Stratégia 2014-2020

Szervezeti szinten pedig European Union Agency for Network and Information Security ajánlásai (EU ENISA) melyeket az Unió a szervezeteinek és tagállamainak bocsát ki.
A közigazgatás kapcsán ki kell térni a szabályozott elektronikus ügyintézési szolgáltatásokra. Ezekből a 2004. évi CXL. Törvény a közigazgatási hatósági eljárás és szolgáltatás általános szabályairól (KET) a Ket. 172. § j) pontja szerinti szolgáltatásokból 32 darab létezik taxatíve felsorolva. Fontos kiemelni a a 2004. évi CXL. törvény 2010-es módosításakor bekerült: „8. § Az eljárás megindítására irányuló kérelmet benyújtó ügyfél és az eljárás egyéb résztvevője – e törvény keretei között – az egyes kapcsolattartási formák közül szabadon választhat."

Ügyfél elvárások és informatikai biztonság

„Az infokommunikációs és az IT ipar alkotta IKT-szektor a magyar GDP mintegy 12%-át adja, és az ágazatban foglalkoztatottak száma az OECD országok többségével összevetve kiemelkedően magas hazánkban … Az IKT-szektor makrogazdasági súlyához mérten nemzetközi összevetésben ugyanakkor alacsony a magyar lakosság és a KKV-k körében az infokommunikációs eszközök tudatos használata, ami súlyosan korlátozza az infokommunikációs eszközöknek és szolgáltatásoknak tulajdonítható kedvező hatások érvényesülését."[431] A közigazgatás ügyfelei, az állampolgárok, KKV-k vonatkozásában számos tanulmány tükrözi azt a törekvést, hogy csökkenteni kívánják az adminisztrációs terheket, ezzel is növelve a versenyképességet.[432] Nem kérdés, hogy az információs rendszerek fejlesztése nemzetközi és hazai viszonylatban is kiemelt fontosságú kérdésként van kezelve.[433] Pár fontos, ezzel szorosan összefüggő tényezőt azonban érdemes figyelembe venni. A közigazgatásban az állampolgár az ügyfél, a jó állam pedig odafigyel ügyfeleire, a közigazgatásban az állam célja az elégedett ügyfél.[434] Törvényileg szabályozásra kerültek az ügykörök, amelyekkel egyablakos ügyintézésre nyílik lehetőség.[435] Ezen ügyfél a szolgáltatások igénybevételekor döntést hoz, hogy azt milyen formában kívánja igénybe venni.[436] [437] Ezen döntésnek több dimenziója van, nem csak kizárólag a szolgáltatás nyújtóján, az adott közigazgatási szervezeten múlik a döntés kimenetele. Az állampolgár saját technikai felszereltségével és a technikába vetett bizalmával, saját tudásáról alkotott képével is jelentősen befolyásolja saját döntését.[438] A bizalmi szolgáltatások közös jellemzője, hogy minden szereplője megbízik a szolgáltatóban. Ez a bizalom olyan tekintetben áll fenn, hogy nem kételkednek a szolgáltatások felhasználói a szolgáltatások minőségében, megbízhatóságában és biztonságában sem. Ezt a bizalmat nehéz megteremteni, de adott esetben egy incidens következtében könnyű elveszíteni. Ezért a szolgáltatást nyújtók, és az azokat felhasználók elemi érdeke, hogy a szolgáltató a bizalmat minden körülmények között fenntartsa. Ennek egyik eleme a szolgáltatások nyújtásának, folyamatainak és kontrolljainak megtervezése, szabály szerinti működtetése, másik eleme pedig a rendszeres felügyelet.[439] Mindezen szabályozási környezetek hatékonyan képesek hozzájárulni az értékteremtéshez és ahhoz, hogy a nemzetközi kiberincidensek hazánkban ne, vagy csak kisebb következményekkel fordulhassanak elő. A téma egyik jelentős,

[431] Nemzeti Infokommunikációs Stratégia 2014-2020
[432] Frank Hogrebe - Wilfried Kruse: *One Stop eGovernment for Small and Medium- Sized Enterprises,* Bled Conference 2008
[433] Communication from the commission, 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 Letöltve: 2014.06.30
[434] Papp Gergely: *Ügyfélelégedettség mérés a közigazgatási ügyfélkiszolgálásban*, 2014
[435] 2013. évi 515 (XII. 30.) Korm. rendelet 1. melléklet meghatározza a kormányablakokban azonnal intézhető ügyeket
[436] Meg kell említeni a Posta konverziós kézbesítési rendszert: A Hibrid kézbesítési és konverziós rendszerrel a Magyar Posta olyan szolgáltatásokat teremt, amelyek lehetővé teszik az ügyfelek számára, hogy a közigazgatási eljárási folyamatokban a küldeményeket hitelesen kézbesítve küldhessék akár elektronikus, akár hagyományos módon, garantálva a szükséges bizonyító erőt.
[437] Som Zoltán: *Hitelesítési kérdések a magyar (e-) közigazgatásban*, Tavaszi szél konferencia 2014
[438] Döme Zsolt - Reich Jenő: *Közszolgálat a közigazgatásban*, ÁROP 2011/1.1.12, Elhangzott: Időpont: 2014.03.18. NKE
[439] Erdősi Péter Máté: *Magyar bizalmi szolgáltatások felügyeletének összehasonlító elemzése*, 2014

megkerülhetetlen, kérdéseket felvető Digitális Mohács című értekezése, amely nemzetközi színtéren vizsgálva elég közel állhat a valósághoz, egy lehetséges szcenáriót vizsgálva. [440]

Nemzetközi kitekintés

Az élet néha hihetetlenebb dolgokat produkál, mint a gondolatkísérlet, vagy mintha a fantasztikum területéről vennénk a példáinkat. Az alábbiakban ismertetésre kerülő események azt támasztják alá, hogy információs társadalmunk kitettsége az információs rendszereknek igen magas, közel sem elhanyagolható. Modern életünk során, az igénybe vett közművek és szolgáltatások mindegyike valamilyen információs rendszeren alapul, így az információs közmű ellen intézett támadás, hatással lehet az élet minden területére. A közigazgatás területére szűkítve a kérdést, ott is igaz, hogy az egyre digitalizálódó infrastruktúra nagyobb kitettséget eredményezhet, amennyiben nem kezeljük ezen változásokból fakadó fenyegetettségeket. Azonban „…tény, hogy közigazgatás megszervezése a mai világban informatikai számítástechnikai eszközök nélkül nem lehetséges". [441] Így a közigazgatási információs rendszerek fejlesztése nem kérdés, sokkal inkább az a feladat, hogy ezen rendszerek megfelelő védelmére megvalósuljon. Különösen igaz ez az alábbi két röviden ismertetett nemzetközi esemény tanulságait levonva.

A 2007-es Észtországi események során a parlamentet, minisztériumokat, kiemelt kormányzati szerveket, hírportálokat támadtak meg. Ezek elsősorban szolgáltatás megtagadásra irányuló támadások voltak. Tömeges kéretlen levélküldéssel kombinálták, összehangolt támadás, megtévesztés, weblapok deface-elése, azaz módosították a hírközlő weblapok tartalmát, megtévesztés, pánikkeltés, félrevezetés. Hetekig tartó támadás sorozat oka vélhetőleg politikai-gazdasági okokra és erődemonstrációs célokra vezethető vissza, kirobbantó oka viszont egy szobor áthelyezése volt.

Az iráni atomprogram elleni támadás 2007-2010 között valósult meg. A Stuxnet nevű számítógépes program segítségével több éven keresztül nem csak információkat szereztek meg, hanem az urándúsítás hatásfokát is rontották az ipari vezérlőmechanizmusokba történő beavatkozással.[442] Ez a típusú célzott támadás az előbbi Észtországi példától teljesen különböző. Vélhetőleg több tíz fős programozói csapat több éves munkája állhatott a háttérben és célzottan erre a feladatra hozták létre.

A nemzetközi jog kis késéssel és utólag természetesen reagál ezen eseményekre, például felmerül a kérdés, hogy harci cselekménynek minősül-e egy ilyen tevékenység? A Tallinn Manual, amely a NATO felkérésére készült el, értelmezni és kezelni próbálja az ilyen eseményeket jogi, katonai, nemzetközi szempontból.[443] Ennek elkészülte már önmagában is azt vetíti előre, hogy a jelenleginél is komolyabban kell kezelni az információs rendszerek elleni támadásokat.

Kiberfenyegetések, kiberhadviselés, globális kibertér, kibertámadások

A fentiekben már ismertetésre került hatásokra az Európai Unió szervezete az ENISA[444] is számos ajánlást adott és ad közre a tagországi és uniós szervezeteknek. Elkészült a NATO megbízásából a Tallinn Manual. És a 2013. évi L. törvény is már definiálja a témával összefüggő fogalmakat is. Általánosságban is érdemes megvizsgálni, hogy miért tűnik úgy, hogy növekvő tendenciát mutatnak ezen információbiztonsággal kapcsolatos események? A jelenség hátterében az állhat, hogy a motiváció nem változik vagy nem változott, ellenben a technológiai fejlődéssel és fejlettséggel egyre

[440] Kovács – Krasznay: *Digitális Mohács*, *Nemzet és Biztonság*, 2010
[441] A fenntartható közigazgatás, fenntartható biztonság elmélete, Dr. Bukovics István
[442] Cserháti András, A Stuxnet vírus és az iráni atom program, http://wwwold.kfki.hu/fszemle/archivum/fsz1105/CserhatiAndras.pdf
[443] *The Tallinn Manual on the International Law Applicable to Cyber Warfare*, NATO Cooperative Cyber Defence, Centre of Excellence Tallinn, Estonia, https://www.ccdcoe.org/, http://issuu.com/nato_ccd_coe/docs/tallinnmanual?e=5903855/1802381, Letöltve: 2014.06.30
[444] European Union Agency for Network and Information Security, http://www.enisa.europa.eu/

több eszköz áll rendelkezésre.[445] Ezek segítségével pedig gyorsabban, hatékonyabban képesek szervezetek, országok elérni a céljaikat.[446] Ezen célok kivitelezése, most szigorúan az informatikai biztonsági incidensek vonatkozásában vizsgálva sokkal előnyösebb lehet valamilyen nyílt támadásnál, vagy fizikai, helyszíni információszerzésnél, mivel:

- hosszú ideig, akár teljesen észrevétlen maradhat az adatszivárgás
- folyamatos adatszerzésre nyílik lehetőség
- költséghatékony (olcsó, vagy olcsóbb, mint direkt (katonai) konfliktus)
- kevésbé meghatározható a támadó kiléte és célja,
- politikailag indokolhatóbb, nincs emberáldozat
- párhuzamosítható és növelhető a folyamat intenzitása
- kicsi a való világban tapasztalható tettenérés és bizonyítás valószínűsége
- alacsonyan tartható humánerőforrás költségek, automatizmus lehetősége
- digitális adat sajátossága: nem szerezhető vissza,
- egyéb (például: iparág specifikus tényezők).

Az információs rendszereket érő támadások ellen az első vonal és egyben épp ezért talán leghatékonyabb védekezés a tudatossági képzés. Az egyenszilárdság megteremtése kiemelten fontos, hiszen a leggyengébb láncszem, a legkönnyebben megtéveszthető elem: a felhasználó, a legkönnyebben megfertőzhető számítógép jelentheti a belépési pontot. Ezen belépési pont védelme érdekében egységesen magas szintet kell produkálnia a szervezetnek, a logikai és fizikai belépési pontjain egyaránt. A részletekre való kitérés mellőzésével tapasztalható, hogy Magyarországon is egyre gyakoribbak és nagyobb intenzitásúak az adathalászattal, spam küldéssel, megtévesztést használó, kártékony kódokat terjesztő támadások. Ezen támadások régebben bizonyos szektorokra koncentrálódtak, a fókuszban elsősorban bizonyos iparágakat tartottak, például a bankszektort (hitelkártya adatok megszerzése, stb.). Napjainkban azonban ez már szinten minden területre kigyűrűzött, mert általánosan igaz, hogy az információszerzés a cél, amelyet később többféle célra fel lehet használni, például: további, más támadásoknál.[447]

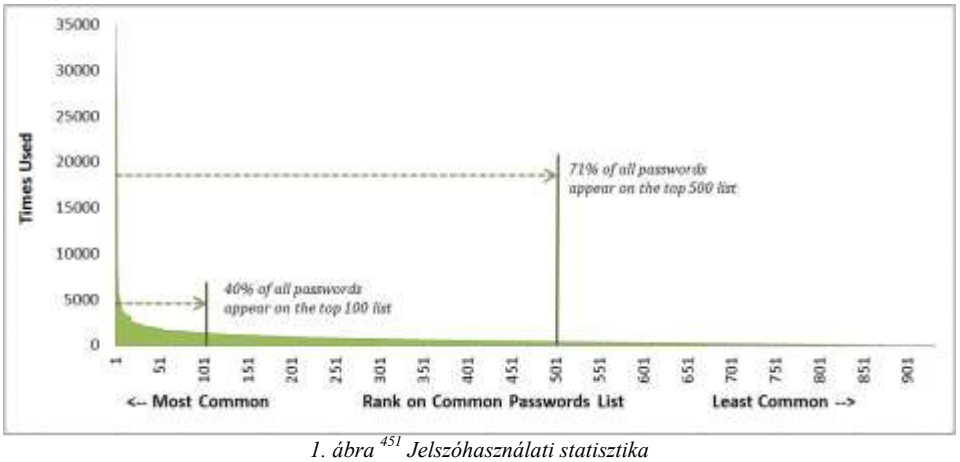
A jó jelszó

Napjainkban már nem tekinthető kiemelten komoly védelemnek a felhasználónév – jelszó páros. Ennek okait részletezve elegendő annyit megemlíteni, hogy a technikai fejlődés, az egyre gyorsabb és nagyobb számítási kapacitás, valamint a jelszavak nagy tömegű kompromittálódása[448] miatt a kevés szekvenciát[449] tartalmazó, rövid jelszavak kifejezetten gyengének tekinthetőek, azok célzott feltörésére irányuló kísérletek, csillapítás[450] nélkül komoly sikerrel kecsegtethetnek.
Az alábbi ábráról hat millió egyedi felhasználónév – jelszó páros feldolgozásával készült el és az leolvasható róla, hogy:

- 4.7%-a a felhasználóknak a „password” szót használja jelszónak
- 8.5%-a a „password” vagy az „123456” szavakat használja jelszónak
- 9.8% a a „password” vagy az „123456” vagy az „12345678” szavakat használja jelszónak

[445] Munk Sándor, *Az információs műveletek típusai és modelljei*, 2002
[446] Munk Sándor: *Az információs fölényről*, 2001, Hadtudomány 2001. évi 3. szám
[447] Négyesi Imre: *A információ szerepe a katonai – vezetői információs rendszerekben.* Hadtudományi Szemle 2009. (II.) 1., 119-123. o.
[448] Számos nemzetközi szolgáltatónál történt adatvesztés következtében több millió ügyféladat és jelszó került nyilvánosságra.
[449] A jelszavak összeállításánál négy féle szekvenciát alkalmazhatunk: kisbetű, nagybetű, szám és speciális karakter. Javasolt mind a négy szekvencia egyidejű használata.
[450] Csillapításnak nevezzük azokat az eljárásokat, amikor valamilyen megkötést, megszorítást alkalmazunk. Ilyen lehet a fizikai hozzáférés megkövetelése, vagy a próbálkozások száma akár.

- 14% a leggyakoribb 10 jelszó közül használja valamelyiket
- 40% jelszava rajta van a top 100-as listán
- 79% jelszava rajta van a top 500-as listán
- 91% jelszava rajta van a top 1000-es listán



1. ábra [451] Jelszóhasználati statisztika

A fentiekben bemutatásra került elrettentő tapasztalat is arra enged következtetni, hogy nagy szükség van az oktatási tevékenységre. Ez annál is inkább igaz, mivel az interneten online formában számtalan információ elérhető és megfelelő szakmai tudás birtokában dönthető el csak, hogy az adott információ releváns-e.[452] A jelszavakkal kapcsolatosan is folyamatosan változnak, fejlődnek az ajánlások, röviden a legfontosabbakat összefoglalva: [453]

- legyen legalább 8 karakter hosszúságú,
- tartalmazzon minél több szekvenciát, akár mind a négyet,
- ne tartalmazzon személyes vagy hozzánk köthető adatot,
- ne legyen jelmondat, vagy triviálisan visszaalakítható szó,[454]
- ne használjunk online jelszógenerátort, [455]
- változtassuk meg rendszeresen,
- ne írjuk le sehova,
- ne adjuk meg senkinek,
- egy jelszót csak egy helyre, hozzáféréshez használjunk,
- a jelszó személyes használatra való, ne használjunk közös jelszavakat,
- használjunk jelszószéfet,
- ne jegyeztessük meg a programokkal, például:a böngészővel,
- ne írjuk be idegen, közösen használt számítógépen, vagy ha igen, akkor utána változtassuk meg amint lehetséges

[451] 10,000 Top Passwords, https://xato.net/passwords/more-top-worst-passwords/#.UtbzrJ55OQq
[452] Léteznek már kifejezetten a felhasználók megtévesztésére létrehozott weboldalak, amelyeket hamis, megtévesztő tartalommal töltenek fel.
[453] Som Zoltán: *Jó-e az én jelszavam*, megjelenés alatt.
[454] A jelmondat használata alapvetően elfogadott, bár egyes ajánlások már ezt sem támogatják.
[455] A jelszógenerátor alapvetően jó és hasznos dolog, azonban online változatot használva azonnal online módon kompromittálódik is az elkészült jelszó. Ettől függetlenül ötletadáshoz használható: http://passwordsgenerator.net/

A fenti okokból kifolyólag nem javasolt a jelszavak online, biztonsági tesztelése, azonban kizárólag demonstrációs céllal megemlítem, hogy már erre is van lehetőség az interneten. [456] A jelszavakkal kapcsolatos további gond, hogy a léteznek úgynevezett rainbow táblák, amelyek előre legenerált módon tárolják a jelszavakat, így amennyiben hash vagy más módon tárolt jelszavakat szereznek meg a támadók, akkor is elképzelhető, hogy vissza tudják fejteni, komolyabb számítási kapacitás nélkül is, egyszerű kereséssel.
A jó jelszó használata tehát önmagában nem képes garantáltan megvédeni, azonban az automatikus próbálkozások és automata támadások, összességében a támadások ellen az első védelmi vonalat jelentheti. Napjainkban már a többfaktoros autentikáció, vagy a tanúsítvány használat, biometrikus adatok jelenthetnek nagyobb, kiemelt védelmet.

Felmérés a közigazgatásban

Jelentős változások indultak meg a közigazgatásban is az információbiztonság vonatkozásában. Egyrészt a 2013. évi L. törvény és a végrehajtási rendeletek által definiált feladatok tekintetében. Másrészt az olyan fontos felmérések által, amelyekből lehetséges elindulni, építkezni és láthatóvá válik, hogy mi az aktuális helyzet az információbiztonság tekintetében.[457] Azt, hogy ezen folyamatok mennyi idő alatt gyűrűznek be a közigazgatás minden területére nem lehet megjósolni. Azonban az, hogy a 2013. évi L. törvény előírja megfelelő szakképesítésű információbiztonsági szakember alkalmazását és az a Nemzeti Közszolgálati Egyetemen, Elektronikus információbiztonsági vezető szakirányú továbbképzési szakán az ilyen képzések elindultak, komoly bizakodásra ad alapot.[458] Hozzá kell tenni, hogy az így kiképzett szakemberek tudásának szétterítéséhez az adott munkaszervezetben várhatólag további időre van szükség.
Az alábbi felmérésben[459] adott válasz, a szervezet információbiztonságával kapcsolatos kérdéscsoport vonatkozásában:
A válaszadók 88%-a nyilatkozta, hogy van informatikai biztonsággal foglalkozó részleg a munkahelyén, amely válasz egyik jelentése, hogy 12% olyan munkaszervezetnél dolgozik, ahol nincs ilyen. Vélhetően itt komoly informatikai biztonsági gondok lehetnek, hiszen ebből következik, hogy ott a felső vezetés sem kap valós képet az információs és informatikai biztonságról. A munkavállalók nem részesülnek semmilyen képzésben vagy felvilágosításban. Az üzemeltetés által végzett feladatokról ebben a vonatkozásban nincs visszacsatolás sem az üzemeltetés, sem a felső vezetés felé.

A magasnak tűnő 88%-ot azonban érdemes megvizsgálni további kérdések tükrében:

- 8% nem érzi biztonságosnak a számítógépét adatlopásokkal szemben.
- 14%-a a válaszadóknak talált már trójai programot a gépén.
- 25% inkább úgy gondolja, hogy csak az IT-részleg feladata a biztonság garantálása.
- 26%-a azt mondja, hogy megadta már másnak a céges jelszavát.
- 33% nem tudja miről ismerhető fel valamilyen átverős (spam) levél.
- 40%-a állítja, hogy nem venné észre, ha feltörnék a számítógépét.
- 49% pedig mindezek ellenére úgy gondolja, hogy megfelelően elegendő informatikai biztonsági képzésben részesült. Hozzászámolva a bizonytalanokat ez az arány 61%-ra növekszik.[460]

[456] Saját jelszavunkat ne írjuk be ismeretlen helyeken, kizárólag demonstrációs célokat szolgálva, jelszavunk jósága itt tesztelhető: https://howsecureismypassword.net/
[457] ÁROP 2.2.17 „Új közszolgálati életpálya" (Nemeslaki-Illéssy-Som)
[458] http://vtki.uni-nke.hu/szakiranyu-tovabbkepzes/projektbol-fejlesztett-szakiranyu-tovabbkepzesi-szakok/elektronikus-informaciobiztonsagi-vezeto-szakiranyu-tovabbkepzesi-szak
[459] ÁROP 2.2.17 „Új közszolgálati életpálya" programban részvétel informatikai szakértőként
[460] Illéssy-Nemeslaki-Som: Elektronikus információbiztonság-tudatosság a magyar közigazgatásban, Információs társadalom, ISSN 1587-8694

A számok értelmezése többféleképpen történhet, azonban a kutatás során, elsősorban a mélyinterjúk tapasztalataira és a számokra is alapozva erősen eltúlzottnak tűnik a biztonsággal kapcsolatos kép a felhasználók fejében. Azaz tévesen és túlzott biztonságban gondolják magukat tapasztalataim szerint.
Talán a biztonság fenntartásán kívül a legfontosabb kérdés, hogy mikor tekinthető sikeresnek, eredményesnek az adott folyamat működtetése, vagy az adott projekt. Az információbiztonság sikeressége az elkerült incidensekben mérhető, amely viszont pont ennél fogva, hogy nem lett belőle incidens, nem igazán válik mérhetővé. Ezen kívül az információbiztonság nem termel közvetlen nyereséget, így csupán a költségoldala az, amelyik markánsan meghatározható.

Siker mérőrendszer
Mi szükséges a sikerhez, mi a siker, ki, hogyan és miben méri? Kinek a szempontjából sikeres? Ilyen és számos további kérdések merülnek fel a sikeresség vizsgálatának kapcsán. Ezen téma összetettségét jól mutatja az alábbi táblázat:[461]

Kategória	E-kereskedelem (DeLone és McLean 2003)	E-közigazgatás
Rendszer minősége	Alkalmazkodóképesség Elérhetőség Megbízhatóság Válaszidő Használhatóság	Alkalmazkodóképesség Elérhetőség Megbízhatóság Válaszidő Használhatóság Interoperabilitás
Információ minősége	Teljesség Könnyű megértés Személyre szabás Relevancia Biztonság	Teljesség Könnyű megértés Személyre szabás Relevancia Biztonság
Szolgáltatás minősége	Bizalom Empátia Reagáló képesség	Ügyfélközpontúság Bizalom/Szakmai színvonal szavatolása Empátia Reagáló képesség
Használat	Használat jellege Navigációs minták Látogatók száma a honlapon Végrehajtott tranzakciók száma	Használat jellege Navigációs minták Látogatók száma a honlapon Végrehajtott tranzakciók száma és jellege
Felhasználói elégedettség	Vásárlások megismétlése Látogatások megismétlése Felhasználói felmérések	Ismételt ügyintézés Honlap ismételt felkeresése Felhasználói felmérések
Nettó haszon	Költségmegtakarítás Piacbővülés További eladások növekedése Csökkentett keresési költségek Időmegtakarítás	Költségmegtakarítás Időmegtakarítás Átláthatóság Demokrácia növelése Szolgáltatások bővülése

2. ábra: A siker mérőrendszer

[461] Dr. Orbán Anna: *E-közigazgatás fejlettségi szintjének a mérése*, 2014

Azaz komplexen, számos tényező összességét kell vizsgálni a közigazgatási rendszerek fejlesztése, üzemeltetési, általánosan a szolgáltatások kapcsán.

Összegzés és várt eredmények

A jelenlegi Magyarországi helyzet és irányvonal összhangban van az Európai Unió törekvéseivel, mind az e-közigazgatási rendszerek fejlesztése, mind az információbiztonság vonatkozásában. Az információbiztonság és az információs rendszerek interoperabilitása tekintetében is igaz, hogy a hosszabb időre van szükség a megfelelő szakembergárda kinevelődéséhez és ahhoz, hogy tudásukat tovább tudják adni az adott munkaszervezetekben. Ezen tudásnak be kell épülnie a folyamatokba, már a rendszerek tervezésekor érvényre kell, hogy jusson. A későbbiekben ezek a tényezők hozzájárulhatnak a szervezeti tudás és a rendszerek közötti interoperabilitási képesség növeléséhez. Ezen folyamatoknak a hozadéka lehet a szigetszerű képződmények és elszigetelt egyedi szolgáltatások megszüntetése, központosítása.

Meg kell jegyezni, hogy az e-közigazgatási rendszerek használatához azt használni képes ügyfélkör is szükséges. Ezért, ezzel párhuzamosan fejleszteni szükséges a digitális kompetenciákat és információbiztonsági, tudatossági oktatásokra is szükség van. Első és másodlagos digitális szakadék megszüntetésére párhuzamosan törekedni szükséges. [462]

Gazdasági szempontból is komoly költségmegtakarítás érhető el, ha a lokális szerverszobák üzemeltetése, fenntartása, hűtése és egyéb járulékos költségei csak egyetlen, központi telephelyen jelentkeznek. Ennek járulékos további haszna lehet a biztonságosabb üzemeltetés. Hosszú távon ezen folyamatok az ország kibertudatossági szintjének általános emelkedését is generálhatják, ami nemzetgazdasági érdek. Fontos tisztában lenni azzal, hogy a fenyegetettségekkel minden esetben számolni kell, mert csak akkor lehetséges a kockázatértékelés elvégzése és felkészülni rá, mivel nincs tökéletes biztonság, ezért is kiemelten fontos az egyenszilárdság megteremtése.

Összefoglaló

A 2013. évi L. törvénnyel elindult folyamatok révén növekedhet a közigazgatás információbiztonsága. Ezen folyamatok érvényre jutásához, a szakembergárda kiképzéséhez és ahhoz, hogy tudásuk munkaszervezeti tudássá váljon, időre van szükség.

A megkezdett folyamatok révén megszűnhetnek a szigetszerű szolgáltatások, növekedhet a rendszerek közötti interoperabilitás, az információbiztonság kezelésére is központilag nyílik lehetőség, gazdasági előnyökkel is járhat a központosított szolgáltatás megvalósítása.

Az e-közigazgatási rendszerek használatához azt használni képes ügyfélkör is szükséges. Ezért fejleszteni szükséges a digitális kompetenciákat és információbiztonsági, tudatossági oktatásokra is szükség van. Első és másodlagos digitális szakadék megszüntetésére párhuzamosan törekedni szükséges. [463]

Hosszú távon ezen folyamatok az ország kibertudatossági szintjének általános emelkedését is generálhatják, ami nemzetgazdasági érdek. Fontos tisztában lenni azzal, hogy a fenyegetettségekkel minden esetben számolni kell, mert csak akkor lehetséges a kockázatértékelés elvégzése és felkészülni rá, mivel nincs tökéletes biztonság, ezért is kiemelten fontos az egyenszilárdság megteremtése.

Felhasznált irodalom:

[1] 2013. évi 515 (XII. 30.) Korm. rendelet 1. melléklet meghatározza a kormányablakokban azonnal intézhető ügyeket.

[2] 2013. évi L. számú törvény az az állami és önkormányzati szervek elektronikus információbiztonságáról.

[3] 2013. évi L. törvény: az állami és önkormányzati szervek elektronikus információbiztonságáról

[4] Bukovics István, A fenntartható közigazgatás, fenntartható biztonság elmélete,

[462] Nemzeti Infokommunikációs Stratégia 2014-2020

[463] Nemzeti Infokommunikációs Stratégia 2014-2020

[5] Bukovics István, A kritikus infrastruktúrák rendszerkoncepciója, Fejezetek a kritikus infrastruktúra védelemből, ISBN 978-963-08-6926-3, 2013
[6] Communication from the commission, 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 Letöltve: 2014.06.01
[7] Döme Zsolt - Reich Jenő, Közszolgálat a közigazgatásban, ÁROP 2011/1.1.12, Elhangzott: Időpont: 2014.03.18. NKE
[8] Elektronikus információbiztonsági vezető szakirányú továbbképzési szak, http://vtki.uni-nke.hu/szakiranyu-tovabbkepzes/projektbol-fejlesztett-szakiranyu-tovabbkepzesi-szakok/elektronikus-informaciobiztonsagi-vezeto-szakiranyu-tovabbkepzesi-szak
[9] ENISA, European Union Agency for Network and Information Security, http://www.enisa.europa.eu/
[10] EU direktíva a 2006/123/EC számút, amely az EU belső szolgáltatásainak harmonizációját, a szükségtelen adminisztrációs terhek csökkentését célozta meg.
[11] European Interoperability Framework (EIF), European Commission, http://ec.europa.eu/isa/documents/isa_annex_ii_eif_en.pdf
[12] Frank Hogrebe - Wilfried Kruse, One Stop eGovernment for Small and Medium- Sized Enterprises:, Bled Conference 2008
[13] Illéssy Miklós – Nemeslaki András – Som Zoltán, Elektronikus információbiztonság-tudatosság a magyar közigazgatásban, Információs Társadalom, ISSN 1587-8694
[14] Kovács – Krasznay, Digitális Mohács, Nemzet és Biztonság, 2010
[15] Krasznay Csaba, A modern kor gyermekkatonái – hogyan védjük az ifjú hackereket? 2012, 2012.09.25, II. Nemzetközi Konferencia: Az internet hatása a gyermekekre és a fiatalokra, Budapest, Magyar Tudományos Akadémia
[16] Muha Lajos - Krasznay Csaba: Kibervédelem Magyarországon: áldás vagy átok? Forrás: http://www.hwsw.hu/hirek/50206/kibervedelem-biztonsag-jog-torveny.html letöltve: 2014.06.01.
[17] Munk Sándor, Az információs fölényről, 2001, Hadtudomány 2001. évi 3. szám
[18] Munk Sándor, Az információs műveletek típusai és modelljei, 2002
[19] Négyesi Imre, A információ szerepe a katonai – vezetői információs rendszerekben. Hadtudományi Szemle 2009. (II.) 1., 119-123. o.
[20] Nemeslaki András, Vállalati internetstratégia, Budapest, Akadémiai Kiadó, 2012. 271 ISBN:978 963 05, 2012
[21] Nemzeti Infokommunikációs Stratégia 2014-2020
[22] Papp Gergely, Ügyfélelégedettség mérés a közigazgatási ügyfélkiszolgálásban, 2014, Letöltve:2014.06.01 Forrás: http://ktk.uni-nke.hu/kutatas-es-tudomanyos-elet/esemenyek_-konferenciak?tag=2014
[23] Som Zoltán – Pál Attila 2013: Tudatosság oktatás az infobiztonsági törvény alapján, közigazgatási tapasztalatok. Elhangzott: Budapest, ITBN konferencia 2013.09.26
[24] Som Zoltán, Az internet veszélyei és ajánlás ennek kezelésére, elsősorban a tizenéves általános iskolások vonatkozásában. Módszertani közlemények: tanítók és tanárok számára 2012- 53:(2) pp. 21-32., 2013
[25] Som Zoltán, Biztonság támogatása, tantárgyi jegyzet, NKE, ÁROP 2.2.21
[26] Som Zoltán, Hitelesítési kérdések a magyar (e-) közigazgatásban, Tavaszi szél konferencia 2014
[27] Som Zoltán, Kibertudatossággal a kiberhadviselés ellen, 13. Robothadviselés konferencia,
[28] Som Zoltán, Laws aiding cyber security in the EU, Central and Eastern European eGov Days 2014