Nemeslaki András – Sasvári Péter

Az információbiztonság-tudatosság empirikus vizsgálata a magyar üzleti és közszférában

BEVEZETÉS

A gazdasági életben és lassan hétköznapi életünkben is egyre nagyobb szerepet játszanak az egyedi számítógépek és a hálózatba kötött számítógépes rendszerek. A termelésben és a mindennapi életvitelünkben folyamatosan növekvő szerepet kap az információs rendszerek használata, egyre inkább függővé válunk ezektől. Ezen változások miatt az információ egyre nagyobb értéket képvisel, és ez elengedhetetlenül maga után vonja a védelmével kapcsolatos problémákat és azok megoldási lehetőségeit.[1] Kutatásunk középpontjában az *információbiztonság-tudatosság* vizsgálata áll a magyar üzleti és a közszférában.

Információ alatt értjük a bizonyos tényekről, tárgyakról vagy jelenségekről hozzáférhető formában megadott megfigyelést, tapasztalatot vagy ismeretet, amely valakinek a tudását, ismeretkészletét, annak rendezettségét megváltoztatja, átalakítja, alapvetően befolyásolja, bizonytalanságát csökkenti vagy megszünteti.[2]

Muha szerint az *információbiztonság* a szóban, rajzban, írásban, a kommunikációs, informatikai és más elektronikus rendszerekben, vagy bármilyen más módon kezelt adatok védelmére vonatkozik.[3]

Az *üzleti szféra* számára az egyik legfontosabb védendő adat az üzleti titok. Az 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 pénzügyi, gazdasági vagy piaci érdekét sértené vagy veszélyeztetné, feltéve, hogy a titok megőrzésével kapcsolatban a vele jogszerűen rendelkező jogosultat felróhatóság nem terheli.[4]

Hiába szereljük fel rendszereinket a legkifinomultabb biztonsági eszközökkel, hiába védjük vállalati adatainkat jelszavakkal, hozzáférés-védelemmel, ha felhasználóink, munkatársaink nem tudnak, vagy nem akarnak felelősségteljesen viselkedni rendszereink használatakor.

Magyarország Országgyűlése 2013-ban elfogadta az állami és önkormányzati szervek elektronikus információbiztonságról szóló törvényt (a továbbiakban információbiztonsági törvény, Ibtv.), amely kiemelkedő csúcspontja annak az összetett kormányzati stratégiának, amely szerint a magyar állam kezelni kívánja azokat a modern kihívásokat és fenyegetéseket, amelyeket az egyre jobban elterjedő digitális infrastruktúra és a kibertér jelent.[5]

A *közszféra* számára pedig kiemelten fontos – a napjaink információs társadalmát érő fenyegetések miatt – a nemzeti vagyon részét képező nemzeti elektronikus adatvagyon,[6] valamint az azt kezelő információs rendszerek, illetve a létfontosságú információs rendszerek és rendszerelemek biztonsága.[7]

Hiába szereljük fel rendszereinket a legkifinomultabb biztonsági eszközökkel, hiába védjük vállalati adatainkat jelszavakkal, hozzáférés-védelemmel, ha felhasználóink, munkatársaink nem tudnak, vagy nem akarnak felelősségteljesen viselkedni rendszereink használatakor.[8] E megállapítás fokozottan érvényes a kis- és középvállalatokra, mivel rájuk kevésbé jellemző a nagyvállalatoknál általános központi szabályozottság.[9]

Az információbiztonsági követelményeket alapvetően három csoportra oszthatjuk, melyek lefedik mind a technikai-technológiai hátteret, mind pedig a menedzsmentrendszereket:[10]

– fizikai védelem,
– logikai védelem,
– humánbiztonság, adminisztratív védelem.

A *fizikai védelem* a fizikai térben megvalósuló fenyegetések elleni védelem, amelynek fontosabb részei a természeti csapás elleni védelem, a mechanikai védelem, az elektronikai jelzőrendszer, az előerős védelem, a beléptetőrendszer, a megfigyelőrendszer, a tápáramellátás, a sugárzott és vezetett zavarvédelem, klimatizálás és a tűzvédelem.[11]

A *logikai védelem* az elektronikus információs rendszerben információtechnológiai eszközökkel és eljárásokkal (programokkal, protokollokkal) kialakított védelem;[12]

Az *adminisztratív védelem* pedig a védelem érdekében hozott szervezési, szabályozási, ellenőrzési intézkedések, továbbá a védelemre vonatkozó oktatás (tulajdonképpen a menedzsmentrendszerek megfelelősége).[13]

Régóta közhelynek számít, hogy az információbiztonság kockázati tényezői között igen előkelő, egyes felmérések szerint vezető helyen áll az *emberi tényező*.[14] A megfelelő információbiztonsági szint elérése és fenntartása érdekében a fizikai és logikai védelmen túl feltétlenül vizsgálnunk és kezelnünk kell a humán faktor okozta fenyegetettségeket is. Ezek elsősorban a szükséges ismeretek hiányára és a tevékenységekhez kapcsolódó ok-okozati összefüggések tudatosításának alacsony szintjére vezethetők vissza.

Az *információbiztonság-tudatosság* a szervezet kultúrájának része, olyan gondolkodás- és magatartásmód, amely biztosítja, hogy a szervezetek alkalmazottjai elkötelezettségből elismerik a biztonsági intézkedések jogosságát, betartják azokat, és másokkal is megismertetik, illetve betartatják ezeket.[15]

A *digitális műveltség* a legfontosabb, és ugyanakkor a legtöbb kihívást jelentő területe a mindenki számára elérhető információs társadalom megteremtésének.[16] A tudástársadalom mindennapi életünk részévé vált, ugyanakkor új hézagokat is teremtett a társadalom különböző csoportjai között. A digitális műveltség alapvető létszükségletté, kompetenciává vált, amely-

Nemeslaki András a Nemzeti Közszolgálati Egyetem, Közigazgatás-tudományi Kar, E-közszolgálati Fejlesztési Intézet vezetője és egyetemi tanára.

Sasvári Péter a Nemzeti Közszolgálati Egyetem, Közigazgatás-tudományi Kar, E-közszolgálati Fejlesztési Intézet egyetemi docense.

nek hiánya akadályozza, vagy megnehezíti a társadalmi integrációt és a személyes fejlődést. A nem megfelelő információs-kommunikációs technológiai felkészültséggel, hozzáféréssel vagy használattal rendelkezők hátrányos helyzetbe kerül(het)nek a munkaerőpiacon alkalmazottként, vagy fogyasztónként is.[17]

Az Európai Bizottság jelentésének munkadefiníciója a következő: a *digitális műveltség* mindazoknak a jártasságoknak az összessége, amelyek a digitális kompetencia megszerzéséhez szükségesek.

A digitális műveltség területei:[18]

– Hálózatinformatika. Minden olyan kommunikációs rendszer, amelyben meghatározott csomópontok között, előre definiált közegekben és rögzített szabályok szerint zajlik a kommunikáció.[19]

– Hardverismeret. A számítástechnikában hardvernek nevezzük magát a számítógépet és minden kézzel megfogható tartozékát, a számítógép elektromos és mechanikus alkatrészeit (melyekből összeszerelték a számítógépet).

– Szoftverismeret. Szoftvernek nevezzük a számítógépre írt programokat (operációs rendszer, szövegszerkesztő stb.) és az ezekhez mellékelt írásos dokumentációkat. A szoftvereket programozók készítik, szellemi termékek, kézzel nem megfoghatóak.

– valamint Információbiztonság-ismeretek.

1. ADATVÉDELEM, ADATBIZTONSÁG FOGALMA

Az *adat* fogalma a BS 7799 Brit informatikai szabvány szerint tények, elképzelések, utasítások formalizált ábrázolása ismertetés, feldolgozás, illetve távközlés céljából.[20]

A magyar szaknyelvben elkülönül az adatvédelem és az adatbiztonság fogalma. Az *adatvédelem* azt mondja meg, hogy mit kell, és a biztonság kritikussága függvényében mennyire kell megvédeni, míg az *adatbiztonság*, az informatikai biztonság azt határozza meg, hogy az adatvédelmi, titokvédelmi osztályozást figyelembe véve az informatikai erőforrásokat hogyan kell megvédeni, valamint a védelmi intézkedéseket meg is teszi.

Az *adatbiztonság*ról a magyar adatvédelmi törvény a következőket mondja ki:[21]

– Az *adatkezelő* köteles gondoskodni az adatok biztonságáról, köteles továbbá megtenni azokat a technikai és szervezési intézkedéseket és kialakítani azokat az eljárási szabályokat, amelyek e törvény, valamint az egyéb adat- és titokvédelmi szabályok érvényre juttatásához szükségesek.

– Az *adatokat* védeni kell különösen a jogosulatlan hozzáférés, megváltoztatás, nyilvánosságra hozás vagy törlés, illetőleg a sérülés vagy megsemmisülés ellen.

Tehát adatbiztonság alatt az adatok védelme érdekében tett technikai megoldásokat és intézkedéseket szoktunk érteni.

2. AZ INFORMÁCIÓBIZTONSÁG-TUDATOSSÁG KONCEPCIONÁLIS MODELLJE

A kutatásunkhoz alapul szolgáló SANS kérdőívet információbiztonsági szakértők dolgozták ki az USA-ban 2012-ben. Ezzel a hétköznapi felhasználói szokásokat méri fel és azokhoz rendel 1–5-ig terjedő skálán egy értéket, majd az összesített értékek alapján öt kockázati kategóriába sorolja a válaszadókat.[22, 23]

– Az *első kategóriába* tartozó munkavállalók jellemzője, hogy tisztában vannak a biztonsági alapelvekkel és veszélyekkel, jól képzettek, mindennapi viselkedésük megfelel a munkahelyi biztonsági szabályoknak és irányelveknek.

– A *második kategóriába* tartozó munkavállalók már vettek részt valamilyen információbiztonsági képzésen, tisztában vannak a veszélyekkel, de mégsem követik teljes mértékben a vonatkozó biztonsági alapelveket és szabályokat.

– A *harmadik kategóriába*, az átlagos veszélyt jelentő kockázati csoportba azok a munkavállalók tartoznak, akik tisztában vannak a veszélyekkel, és tudják, hogy bizonyos biztonsági alapelveket be kellene tartaniuk, de továbbképzésre szorulnak a témában. Itt már nem ismerik fel az informatikai incidenseket, és nem tudják, mi a teendő ilyen esetben.

– A *negyedik kategóriába* tartozók nincsenek tisztában a biztonsági alapelvekkel és veszélyekkel, sem pedig munkaszervezetük biztonsági szabályzatával.

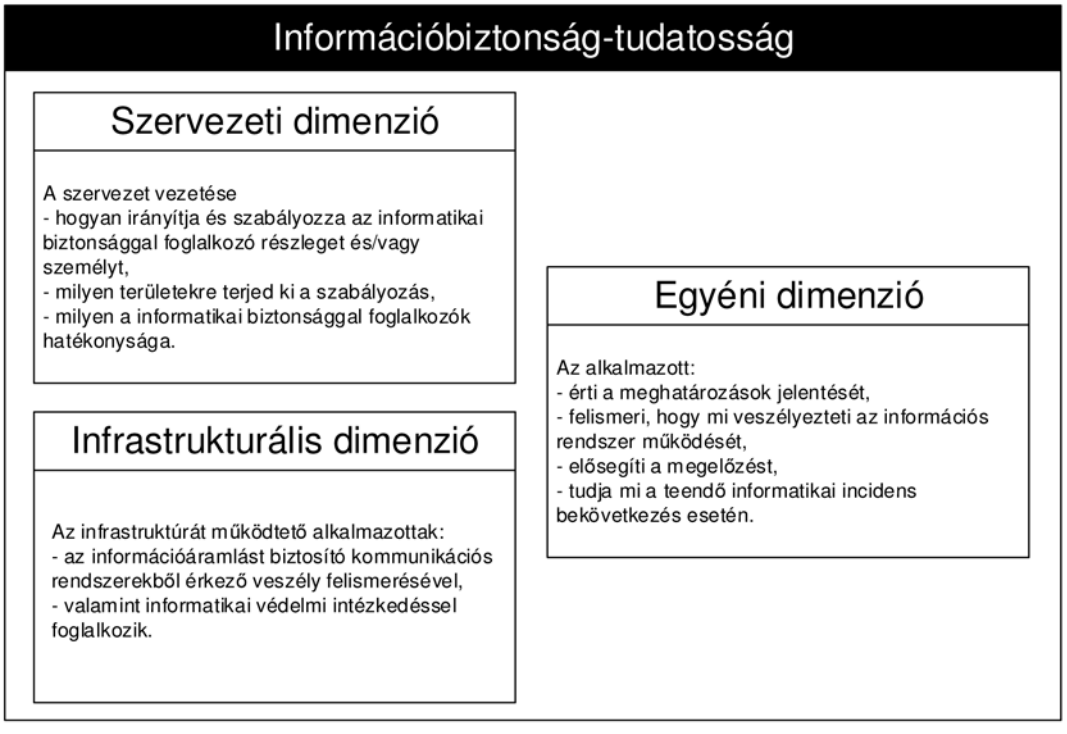
– Végül az *ötödik kategóriába* tartozó munkavállalók nincsenek tisztában a veszélyekkel, és nem tartják be a biztonsági szabályzatokat sem.

Annak érdekében, hogy a globális értékelésen túl részletesebb képet kapjunk a területről, a válaszokat Illésy, Nemeslaki és Som írása alapján három nagyobb dimenzió mentén különítettük el:[24]

– A *szervezeti dimenzió*, ahol a szervezeti szokásokat és eljárásokat mérjük.

– Az *egyéni dimenzió*, ahol a szervezetnél dolgozó általános ismereteit és szokásait mérjük és elemezzük.

– Az *infrastrukturális dimenzió*, amely a szervezet környezeti, informatikai állapotáról megfogalmazott véleményeket tartalmazza.



1. ábra: A vizsgálati modell felépítése

A menedzsment módszertanok a biztonsági kultúra megvalósítását lehetővé tevő sikertényezők között első helyen tartalmazzák a *felsővezetés* elkötelezettségét, és az ebből következő *szervezeti* tudatosságot, *dimenziót*.[25]

Tehát a szervezeti dimenzió alatt azt értjük, hogy a szervezet vezetése

– hogyan irányítja és szabályozza az informatikai biztonsággal foglalkozó részleget és/vagy személyt,

– milyen területekre terjed ki a szabályozás,

– milyen az informatikai biztonsággal foglalkozók hatékonysága.

A szervezeti tudatosságra külső (pl. jogszabályok, szabványok, politikai hatások, piaci hatások, természeti hatások) és belső tényezők (pl. szabályzatok, a közvetlen vezetés utasításai, humánpolitika és ellenőrzés) egyaránt hatással vannak.[26]

Az *egyéni dimenzió* esetén az *alkalmazottak* informatikai tudását, készségét és képességét kívánjuk mérni. Az információs társadalom lehetőségeivel csak azok a dolgozók tudnak megfelelő módon élni, akik tudatosan alkalmazzák az informatikai eszközöket, ezért a fejlesztési feladatok meghatározása során elsősorban az eszközök ismeretére, az eszközökkel megvalósítható lehetőségek feltérképezésére és az alkotó felhasználásra kerül a hangsúly.[27] Ez információbiztonság-tudatosság esetén ez azt jelenti, hogy a dolgozó:

– érti a meghatározások jelentését, azaz hogy pontosan miről beszélünk,

– felismeri, hogy mi veszélyezteti az információs rendszer működését,

– elősegíti a megelőzést,

– tudja, mi a teendő informatikai incidens bekövetkezés esetén.

Az információtechnológia fejlődése és eszközeinek rohamos elterjedése az egyes információs rendszerek és erőforrások előbb szervezeti szintű, majd regionális és világméretű összekapcsolódásából is egy új, egyre bővülő infrastruktúra-típus alakult ki, amely átszövi az üzleti és közszférát egyaránt. Az információs környezet alapvető összetevőit a helyi – egy adott földrajzi helyen elhelyezkedő, egységes irányítás alatt álló – információs környezetek képezik, amelyek maguk is két részből állnak. Az elsőbe a helyi környezet információs eszközei és más technikai erőforrásai (végberendezései és kommunikációs elemei), információi és alkalmazásai, valamint a *működtető szervezetek és személyek* tartoznak. A másikat az adott környezet szereplői – információszolgáltatói és felhasználói – alkotják. Az információs környezet további lényeges összetevőjét képezi az információs *infrastruktúra,* amely egyrészt a helyi információs környezetek közötti információáramlást biztosító kommunikációs (hálózati) rendszerek, eszközök és erőforrások; másrészt azon szervezetek, eszközök és más erőforrások összessége, amelyek más alapvető vagy értéknövelő (információvédelmi, logisztikai stb.) szolgáltatásokat nyújtanak.[28] Ebből következik, hogy az infrastrukturális dimenzió tartalmazza az infrastruktúrát működtető alkalmazottak:

– az információáramlást biztosító kommunikációs rendszerekből érkező veszély felismerésével,[29]

– valamint informatikai védelmi intézkedéssel foglalkozik.

Veszélynek, illetve *veszélyforrásnak* tekinthető mindaz, amelynek hatására, illetve bekövetkeztekor az informatikabiztonság sérül, egy vagy több informatikai rendszerelem működésében nem kívánt változás áll be.[30]

A *digitális műveltség* szintje öt kategóriába sorolható:

– *kiváló,* mivel felismeri az információszükségleteit, hosszú idő óta kiválóan kezeli a hálózati informatikát, magas szinten áll a hardver- és a szoftverkezelés területén, végül jól ismeri a hálózati veszélyeket és védekezni is tud ellenük.

– *jó,* mivel majdnem mindig felismeri az információszükségleteit, a hálózati kommunikációt alkalmazza, valamint egyes hardver- és szoftverkezelés területen kiváló, valamint az információbiztonság területén is járatos.

– *közepes,* mivel segítséggel felismeri saját információs szükségleteit, irányítással használja a hálózati informatikát, hiányosságai vannak hardver- és szoftverkezelés területén, végül információbiztonság területén néha hibázik.

– *rossz,* mivel képzés és tapasztalat hiányában nem ismeri fel saját információs szükségleteit, a hálózati kommunikációra nem képes, nagy hiányosságai vannak a szoftver- és hardverismeretek területén, valamint a hálózati veszélyeket nem ismeri fel.

– *nagyon rossz,* mivel információs szükségleteit nem ismeri, a hálózati kommunikációs alapismeretekkel sem rendelkezik, szoftver- és hardverismeretekkel nem rendelkezik.

3. A VIZSGÁLAT TÁRGYA ÉS MÓDSZERE

A társadalmi igények kielégítése bármelyik országban három nagy szféra (üzleti, köz- és civil szféra) közreműködésével történik, amelyek között a fejlett gazdaságokban sokirányú együttműködés érvényesül.

Az üzleti szféra az alábbi részekre bontható: *mikro-, kis- és középvállalkozás*okra,[31] valamint *nagyvállalatra*.

A közszolgáltatás a szolgáltatások speciális fajtája: közszolgáltatás a közszükségletek kielégítése, és ezen belül közfeladat, ha *nonprofit* jellegű, illetve közérdekű szolgáltatás, ha *profitorientált* jelleggel végzik. A *közszférán belül* az elmondottak alapján két szűkebb terület, az *állam,* illetve az *önkormányzatok* szerepvállalása kiemelkedően fontos. Mind az államnak, mind az önkormányzatnak lehetnek nonprofit és profitorientált szervezetei.

A képzési reformokat, az azt meghatározó közigazgatás fejlesztési stratégiát, illetve az annak irányait kijelölő közpolitikai gondolkodást döntően az állam szerepéről, nagyságáról és kiterjedtségéről való diskurzus határozza meg.[32] Akár erős, kiterjedt, nagy állam szerepében gondolkozunk, akár kicsi, kiszervezésen alapuló, ún. „éjjeli őr" funkciót betöltő államban, a közszféra és azon belül a közszolgálat határa közel sem egyértelmű, hanem igen elmosódott.[33] Gajdushek szerint a legszűkebben értelmezett közszolgálat a közigazgatási hivatalokat jelenti, a legtágabb pedig az állami szféra összes intézményét jelentheti; a három államhatalmi ág szervezeteit (törvényhozói, végrehajtói és bírósági szervezetek), de azon túlmenően a fegyveres testületeket, iskolákat, kórházakat, szociális intézményeket, állami vállalatokat vagy akár közfeladatot ellátó közalapítványokat is.

Magyarországon a közigazgatási, illetve közszolgálati képzés nagy ívű reformja zajlik 2012 óta, lényegében a Nemzeti Közszolgálati Egyetem megalakulásával. A magyar közigazgatási reformstratégia, a Magyary-terv négy pillérre alapozva jelölt ki fejlesztési irányokat a hazai közigazgatásban:

a) szervezetfejlesztés (magyar közigazgatás szervezetrendszerének átalakítása)

b) feladatrendszerfejlesztés (feladatkataszter kialakítása, az állam feladatainak rendszerezése és harmonizálása)

c) folyamathatékonyság (különösen az állampolgári egyablakos ügyintézés, a Kormány Ablakok kialakítása, elektronikus szolgáltatások fejlesztése)

d) humánerőforrás-fejlesztés, illetve karrierpályák kidolgozása.

Különösen az utolsó pillér vonatkozásában lényeges az egységes közszolgálati szemlélet, hiszen a karrier utak megtervezése, az ehhez szükséges képzések és átképzések rendszere, az élethosszig tartó tanulás nélkül nem biztosítható stabil karrierpálya a köztisztviselők, katonák, rendőrök, katasztrófa védelmi szakemberek számára a folyamatosan változó, átalakuló közintézmények rendszerében.[34]

Primer kutatásunk alapjául

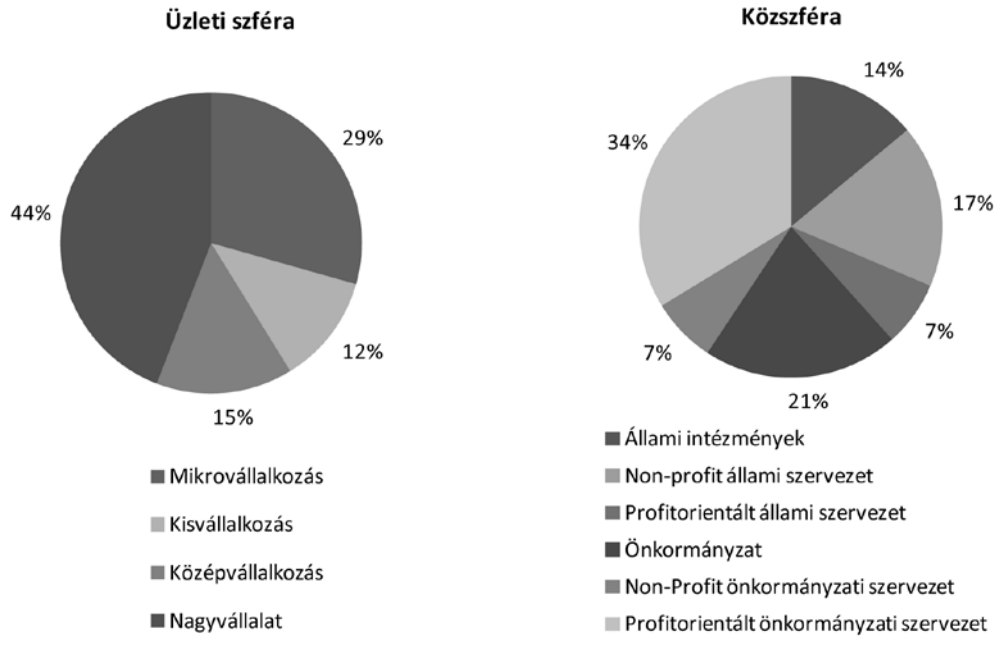
– egy, már 2012-ben Bond, Stephens és Piscitello által kidolgozott és használt Security Awareness Survey (SANS);

– valamint a 2014-ben Illéssy és Nemeslaki által továbbfejlesztett, korábban a magyar Nemzeti Közszolgálati Egyetemen lekérdezett[35]
kérdőív szolgált.

A digitális műveltség szintjét a kutatás alapjául szolgáló kérdőív területenkénti több kérdéssel mértük fel. A hálózati informatika használatának felméréséhez a mobil hálózati eszközök ismeretét, valamint az internet használatának hosszát vettük alapul. A hardverismeretet a tárolóeszközökre való kérdéssel és a számítógép használat idejére vonatkozó kérdés segítségével határoztuk meg. A szoftverismeret szintjét a számítógépre történő telepítés és a telepítésre vonatkozó kérdéssel mértük meg. Végül az általános információbiztonsági ismeretet a számítógépes vírusokra vonatkozó kérdésekkel határoztuk meg.

A kérdőívek kitöltése a Miskolci Egyetem hallgatói segítségével papíron és online formában történt, a kitöltőre vonatkozó demográfiai és munkahelyadatoktól függetlenül.

A miskolci kérdőívet 2014 áprilisáig 316 fő töltötte ki. A munkahellyel rendelkező kitöltők száma 120, azzal nem rendelkezőké pedig 196. Az üzleti szférából (pl. mikro-, kis- és középvállalkozásoknál vagy nagyvállalatnál) alkalmazottaktól és vállalkozóktól 34, közszférából (pl. állami intézmény, állami tulajdonú szervezet, önkormányzat, önkormányzati tulajdonú szervezet) pedig 86 darab kitöltött kérdőív érkezett be a kitűzött határidőre.



2. ábra: Munkahellyel rendelkező, az információbiztonság-tudatossági kérdőívet kitöltők megoszlása

A kérdőív 4 részből állt:

• *Demográfiai kérdések*. A kitöltő legfontosabb demográfiai adatai mellett (pl. nem, születési év, iskolai végzettség, jövedelmi helyzet) megkérdezésre került az informatikai jártassága is.

• *Munkahely jellemzője.* Ha a kitöltő munkaviszonnyal rendelkezik, akkor megkérdezésre került, hogy melyik szférában és régióban dolgozik.

• *Információbiztonság-tudatossági kérdések.* Az alábbi témákat érintették: a munkaszervezet és szabályozás, információbiztonsággal kapcsolatos ismeretek mindennapi felhasználása, informatikai eszközök használata és adatkezelés, általános számítógép-használati szokások.

• *Egyéb kérdések*. Egyéb adatbiztonsági területeket érintő kérdések.

A vizsgált üzleti és közszférából kitöltött kérdőívek egy feltáró kutatás részét képezik. A *feltáró kutatásunk* célja, hogy belelássunk az információbiztonság-tudatosság természetébe és megismerjük az üzleti és a közszféra egyes szervezeteinek helyzetét. Kevés az előzetes ismeretünk erről a problémáról, mivel azelőtt még így senki nem vizsgálta. A kvalitatív módszerünk az üzleti és közszféra szervezeteinek helyzetét és fejlesztési szükségleteit segíti mélyebben megérteni.

A feltáró kutatásunk célja, hogy belelássunk az információbiztonság-tudatosság természetébe és megismerjük az üzleti és a közszféra egyes szervezeteinek helyzetét. Kevés az előzetes ismeretünk erről a problémáról, mivel azelőtt még így senki nem vizsgálta.

4. AZ INFORMÁCIÓBIZTONSÁG-TUDATOSSÁG HELYZETE MAGYARORSZÁGON, 2014-BEN

A globális képet tekintve megállapítható, hogy a vizsgált üzleti és közszférában tevékenykedő szervezetek közül kettő, az állami intézmények, valamint az állami profitorientált szervezetek a legbiztonságosabb első-, valamint a második kategóriához tartoznak. Hasonlóan jó eredménnyel rendelkeznek a mintában szereplő nagyvállalatok, valamint a nonprofit állami szervezetek is. Igaz, itt már a válaszadók közel 8%-a a harmadik, az átlagos veszélyt jelentő kockázati csoportba került.

Minősítés	Sorrend	Megnevezés	Első kategória	Második kategória	Harmadik kategória
Fejlett	1	Profitorientált állami szervezet	40%	60%	0%
	2	Állami intézmények	27%	73%	0%
Jó	3	Nagyvállalat	31%	61%	8%
	4	Nonprofit állami szervezet	22%	71%	7%
Átlagos	5	Középvállalkozás	33%	33%	34%
	6	Profitorientált önkormányzati szervezet	30%	44%	26%
	7	Önkormányzat	7%	71%	22%
Alacsony	8	Nonprofit önkormányzati szervezet	0%	67%	33%
	9	Kisvállalkozás	0%	100%	0%
	10	Mikrovállalkozás	0%	78%	22%

1. táblázat: A magyar információbiztonság-tudatosság minősítése az üzleti és a közszférában

Ennél rosszabb aránnyal rendelkeznek a 250 főnél kevesebbet foglalkoztató középvállalkozások, valamint az önkormányzati tulajdonú profitorientált szervezetek és maguk az önkormányzatok. Itt már a szervezetek közel negyedénél az alkalmazottak továbbképzésre szorulnának.

Végül az utolsó kategóriába azok a szervezetek tartoznak, ahol a szervezetek egyike sem bír első kategóriás válasszal. Itt találhatóak meg a közszférából az önkormányzati tulajdonú nonprofit szervezetek, valamint az üzleti szférából az 50 főnél kevesebbet foglalkoztató kisvállalatok és a mikrovállalkozások.

4.1. Az információbiztonság-tudatosság szervezeti dimenziója

A közszférában az állami szektor, a nonprofit állami szervezet, az önkormányzat, valamint az önkormányzat nonprofit szervezet 100%-a nyilatkozott úgy, hogy van *informatikai biztonsággal foglalkozó részleg* a munkahelyén. Magas értékkel találkozhatunk még az állami és önkormányzati tulajdonú profitorientált (83%) szervezeteknél is. Az üzleti szféra szereplői közül a legnagyobb értékkel a nagyvállalatok bírnak (93%). Őket követik a 250 főnél kevesebb főt foglalkoztató középvállalkozások (80%), majd a kisvállalkozások (75%) következnek. A legalacsonyabb értékkel, 40%-os aránnyal az alacsony tőkével és emberi erőforrással bíró mikrovállalkozások zárják a sort.

A *szervezeti dimenzió* kockázati besorolását mérő válaszokat illetően jó eredményekkel (első és második kategóriával) csak a profitorientált állami intézményeknél, a nagyvállalatoknál, az állami intézményeknél, valamint az önkormányzati tulajdonú nonprofit szervezeteknél találkozhatunk.

Sorrend	Megnevezés	Első kategória	Második kategória	Harmadik kategória	Negyedik kategória
1	Profitorientált állami szervezet	0%	100%	0%	0%
2	Nagyvállalat	15%	85%	0%	0%
3	Állami intézmények	9%	73%	18%	0%
4	Nonprofit önkormányzati szervezet	0%	100%	0%	0%
5	Nonprofit állami szervezet	7%	57%	36%	0%
6	Profitorientált önkormányzati szervezet	22%	39%	26%	13%
7	Középvállalkozás	0%	67%	33%	0%
8	Kisvállalkozás	0%	50%	50%	0%
9	Önkormányzat	0%	50%	43%	7%
10	Mikrovállalkozás	0%	33%	44%	22%

2. táblázat: A magyar információbiztonság-tudatosság szervezeti dimenzió szerinti minősítése az üzleti és a közszférában

Meglepődve tapasztaltuk, hogy az önkormányzatok és az önkormányzati tulajdonú profitorientált szervezetek egyes tagjai a negyedik kategóriába tartoznak, ami információbiztonság szempontjából aggasztó lehet.

Minden vizsgált szervezeti egységnél meg kell vizsgálni, hogy *van-e szabályzat az informatikai eszközök használatáról* vagy olyan általános szabályzat, amely kitér az informatikai eszközök használatára. A megkérdezettek átlagosan negyede nem tudta megmondani, hogy van-e ilyen szabályzat a munkahelyén. Ez az arány az állami intézményeknél, az önkormányzatoknál eléri a 40%-ot. A mikrovállalkozások több mint 80%-ánál, az önkormányzatok közel kétharmadánál, valamint az önkormányzati tulajdonú szervezetek felénél nincs ilyen informatikával kapcsolatos szabályzat. A nagyvállalatok és az állami tulajdonú nonprofit szervezetek kétharmadánál külön IT szabályzat található. Ez az állami intézményeknél 20%, de általános szabályzaton belül az IT 30%-ánál található meg.

A mikrovállalkozások több mint 80%-ánál, az önkormányzatok közel kétharmadánál, valamint az önkormányzati tulajdonú szervezetek felénél nincs ilyen informatikával kapcsolatos szabályzat.

A vállalkozásoknál dolgozók több mint 50%-a megfelelőnek találja az információbiztonság területén tartott *képzések* színvonalát. A mikro- és kisvállalkozásoknál 50%, a középvállalkozásoknál 75%, a nagyvállalatoknál eléri a 80%-ot azoknak a dolgozóknak az aránya, akik elégedettek az ezen a területen kapott oktatással. A közszféránál ennél rosszabb értékeket mértünk. Az önkormányzatoknál és az állami intézményeknél a megkérdezettek alig 40%-a látja úgy, hogy megfelelő képzést kaptak az információbiztonság témakörében. Az állami profit- és nonprofit szervezeteknél dolgozók több mint a fele gondolja úgy, hogy megfelelő volt az oktatás. Az önkormányzati tulajdonú szervezeteknél már csak minden harmadik alkalmazott gondolja ezt.

A *szervezeti dimenzió része a weboldalak* látogatásának, munkahelyi szabályozásának a vizsgálata is. Általánosságban elmondható, hogy az üzleti szférában a nagyvállalatok több mint 90%-a szabályozza az elérhető tartalmakat, miközben a mikrovállalkozások alig 20%-a, a kis- és a középvállalkozások alig 40%-a köti jogosultsághoz az internet használatát.

Az önkormányzatok és az önkormányzati tulajdonú nonprofit szervezetek 80%-ánál semmilyen korlátozást nem vezettek be a munkahelyi internetezéssel kapcsolatban. Ezzel szemben állami intézmények 90%-ánál, az állami tulajdonú profit és nonprofit szervezetek közel 70%-ánál vannak bizonyos előírások ennek használatával kapcsolatban.

A *szervezeti dimenzió* további *része* még a *levelezőrendszerek* szabályozása. Itt is elmondható, hogy ha a szervezet mérete – mind az alkalmazottak számát, mind eszközértékét tekintve – nő, akkor a szabályozás mértéke is erősödik. Az állami intézmények, az állami tulajdonú nonprofit szervezetek és a nagyvállalatok 80%-ánál előírások vannak a levelezőrendszer használatára. Ezzel szemben a mikrovállalkozások és az önkormányzatok, valamint az önkormányzati tulajdonú nonprofit szervezetek alig 20%-a foglalkozik az elektronikus levelezés alkalmazottak általi használatával. A kis- és középvállalkozásoknál, valamint az állami és önkormányzati tulajdonú profitorientált szervezeteknél közel a fele nem szabályozza a levelezőrendszerek használatát.

A *felhőalapú számítástechnika* kialakulásának hátterében az a gondolat áll, mely szerint az információfeldolgozás sokkal hatékonyabb, ha hálózaton keresztül elérhető, központilag összehangolt számítógép- és adattároló rendszereken történik. Ez is a *szervezeti dimenzió része*. A „felhő” kifejezés az internet hálózati diagramokon való ábrázolásából ered, azzal jelölik a rendszer ismeretlen, vagy irreleváns részeit. A felhőalapú számítástechnika egy olyan modell, amelynek segítségével bárhonnan, kényelmesen, és igény szerint hozzáférhetünk a testreszabott informatikai erőforrások megosztott halmazához (pl. hálózatokhoz, szerverekhez, tárhelyekhez, alkalmazásokhoz, szolgáltatásokhoz), miközben a rendelkezésre bocsátás minimális adminisztrációs tevékenységet és szolgáltatói beavatkozást igényel. A kérdőívet kitöltők közel 40%-a – szférától és mérettől függetlenül – nem tudja, hogy az adott szervezetnél szabályozott-e a felhőalapú számítástechnika használata. A nagyvállalatoknál, az önkormányzati tulajdonú nonprofit szervezeteknél és az állami intézményeknél nem, vagy csak kis hányaduknál engedélyezett a használatuk.

A mikrovállalkozásoknál, az önkormányzatoknál és a profitorientált állami szervezeteknél a megkérdezettek közel 20%-a tudja úgy, hogy használhatnak pl. iCloud, Dropbox és Google Drive alkalmazást intézményi, vállalati adatok tárolására.

4.2. Az információbiztonság-tudatosság egyéni dimenziója

Az *egyéni dimenzió* vizsgálatánál a kérdőívet kitöltők általános informatikai ismereteit vizsgáljuk. Ez nagyban függ az alkalmazottak korábbi években szerzett gyakorlatától is. A vizsgált szervezeti egységeknél a kérdőívet kitöltők átlagosan 12 és 20 év közötti időtartamot jelöltek meg a számítógéphasználat tekintetében. Az internethasználatnál viszont átlagosan 8 és 15 év közötti értékeket találunk az üzleti és közszféra egyes alkalmazottjainál. Ha a napi számítógép-használatot vizsgáljuk, akkor megállapítható, hogy minden vizsgált vállalkozás, intézmény esetén elmondható, hogy az ott dolgozók átlagosan napi 5 és 8 óra közötti időt töltenek el a számítógép előtt. Ebből azt a következtetés vonhatjuk le, hogy a kérdőívet kitöltők szférától függetlenül hasonló gyakorlattal rendelkeztek a mintában.

A középvállalkozásoknál, a nonprofit állami szervezeteknél, az állami intézményeknél, a profitorientált állami szervezeteknél, valamint a nagyvállalatoknál az első- és második kategóriás válaszadók aránya meghaladta a 66%-ot, ami nagyon jónak mondható. Ami mégis óvatosságra inthet minket, hogy a nonprofit állami szervezetek és a nagyvállalatok 8%-ánál az alkalmazottak egy része nincs tisztában a biztonsági alapelvekkel és veszélyekkel.

Sorrend	Megnevezés	Első kategória	Második kategória	Harmadik kategória	Negyedik kategória	Ötödik kategória
1	Középvállalkozás	67%	0%	33%	0%	0%
2	Nonprofit állami szervezet	29%	64%	0%	7%	0%
3	Állami intézmények	36%	45%	18%	0%	0%
4	Profitorientált állami szervezet	20%	60%	20%	0%	0%
5	Nagyvállalat	38%	31%	23%	8%	0%
6	Profitorientált önkormányzati szervezet	39%	35%	17%	0%	9%
7	Mikrovállalkozás	0%	78%	22%	0%	0%
8	Önkormányzat	7%	64%	29%	0%	0%
9	Kisvállalkozás	0%	50%	50%	0%	0%
10	Nonprofit önkormányzati szervezet	0%	67%	0%	33%	0%

3. táblázat: A magyar információbiztonság-tudatosság egyéni dimenzió szerinti minősítése az üzleti és a közszférában

Ennél nagyobb problémával a profitorientált önkormányzati szervezeteknél találkoztunk, ahol a válaszadók 9%-a az ötödik kategóriába esett. Az információbiztonság egyéni dimenzió vizsgálatánál a mikro-, kisvállalkozások, az önkormányzatok valamint a nonprofit önkormányzati szervezetek zárják a sort.

Az *egyéni dimenzió részeként* vizsgáltuk az alkalmazottakat, hogy észre vennék-e, ha *a számítógépüket feltörnék*. A számítógép feltöréséről akkor beszélünk, ha valaki a számítástechnikai rendszer védelmét szolgáló intézkedés megsértésével vagy kijátszásával jogosulatlanul belép vagy belépési jogosultságai kereteit túllépve, illetőleg azt megsértve bent marad az adott rendszerben. A nagyvállalatoknál, profitorientált állami szervezeteknél dolgozók több mint 80%-a úgy gondolja, hogy észrevenné a feltörést. Ezzel szemben a kisvállalkozások alig negyede gondolja ezt így. A többi vizsgált szervezetnél közel 60%-os gyakoriság figyelhető meg.

Az *egyéni dimenzió keretében vizsgáltuk* szervezetenként, hogy az alkalmazottak milyen arányban adták meg *önként* más felhasználóknak a *céges jelszavukat*. A jelszó egy titkos karakterlánc, amellyel személyek jelentkezhetnek be, férhetnek hozzá egy számítógéphez, fájlokhoz, programokhoz és más erőforrásokhoz.

A válaszadók legnagyobb arányban (40%) az állami intézményeknél és a nagyvállalatoknál adják meg céges jelszavukat. A saját vállalati jelszót a legkevésbé (10%) a kis- és középvállalkozásoknál, nonprofit állami szervezeteknél és mikrovállalkozásoknál adják át másoknak. A többi szervezetnél 16%-os arányt tapasztaltunk.

Ehhez kapcsolódó kérdés, hogy *kérte-e* már el a kérdőívet kitöltő főnöke a beosztott *céges jelszavát*. Meglepő módon ez a nagyvállalatok közel felénél már előfordult. Alacsony előfordulást – 7% alatt – az önkormányzatoknál és a közepes méretű vállalkozásnál tapasztaltunk. A többi vizsgált egységnél 10 és 17%-os értékeket mértünk.

Újra és újra felröppennek a hírek, hogy neves portálok feltörésével több százezer vagy több millió felhasználó jelszava kerül napvilágra. Komoly biztonsági kockázatot jelent, hogy sokan *ugyanazt a jelszót* használják mindenhol. Az egyéni dimenzió keretében megvizsgáltuk, hogy a kérdőívet kitöltők mennyire óvatosak ebben a tekintetben. A válaszadók tizede állította, hogy ugyanazt a jelszót használja a munkahelyén és a magánéletében is. A középvállalkozásoknál ennek épp a duplája, míg az állami intézményeknél és a kisvállalkozásoknál senki sem használja a privát jelszavát a munkahelyén.

Ha megvizsgáljuk, hogy *hol előírás a jelszóváltoztatás,* és vajon *meg is változtatják-e a jelszavakat*, akkor megállapítható, hogy a mikrovállalkozások kétharmadánál, a középvállalkozások felénél, valamint az önkormányzatok 60%-ánál nem előírás a jelszó változtatás és nem is változtatják meg azt.

Ezzel szemben a nagyvállalatok, állami intézmények és profitorientált állami szervezetek közel 90%-ánál előírás a jelszóváltoztatás, és meg is teszik azt az ott dolgozók. Az önkormányzati tulajdonú nonprofit szervezetek kétharmadánál ugyan nem előírás a változtatás, de mégis megteszik azt.

Itt kell vizsgálni még az *illegális szoftvertelepítést* és -használatot, valamint a személyes használatú fájlletöltést. Az illegális szoftverhasználat azt jelenti, hogy valaki egy számítógépes programot jogosulatlanul másol le és használ, ezzel megsértve a szerzői jogi törvényt, valamint a szoftver-licencszerződésben leírt feltételeket.[36] Az illegális szoftverhasználat és személyes használatú fájlletöltés a mikrovállalkozások 70%-ánál, a középvállalkozások 60%-ánál és a kisvállalkozások felénél volt jellemző. Az üzleti szférában a legalacsonyabb értékkel a nagyvállalatoknál találkozunk. Itt minden ötödik vállalatnál találkoztunk saját célú letöltéssel és jogosulatlan használattal. A közszférában a legnagyobb értékkel a nonprofit állami szervezeteknél (53%), az állami intézményeknél (42%) és a profitorientált önkormányzati szervezeteknél (40%) találkoztunk. Alacsonyabb gyakoriságot az önkormányzatoknál (30%), az önkormányzati tulajdonú nonprofit szervezeteknél (20%) és a profitorientált állami szervezeteknél (17%) találtunk.

4.3. Az információbiztonság-tudatosság infrastrukturális dimenziója

Az *infrastrukturális dimenziónál* számos kérdésre adott válaszban jelenik meg valamilyen tudás hiánya vagy valamilyen infrastruktúrának a túlértékelése. Ilyen lehet például az, hogy az alkalmazott számítógépén lévő információ nem értékes a hackerek számára. Az internet értelmező kisszótár szerint a *hacker* megszállott szoftverszakértő, aki az internetre kapcsolt rendszerek szisztematikus letapogatásával megkeresi azok gyenge pontjait és behatolási lehetőségeit.[37]

Az üzleti és a közszférában dolgozók több mint a harmada meg van győződve arról, hogy a számítógépük a hackereknek nem célpontjuk.

Az üzleti és a közszférában dolgozók több mint a harmada meg van győződve arról, hogy a számítógépük a hackereknek nem célpontjuk. Ennél nagyobb aránnyal az üzleti szférában csak a mikrovállalkozásoknál (50%) és nagyvállalatoknál (40%) találkozunk. A kis- és középvállalkozásoknál minden negyedik személy szerint nem célpontjai egy ilyen típusú támadásnak.

A közszféra vizsgálatánál az önkormányzatoknál dolgozók 55%-a gondolja úgy, hogy az adataik nem érdekesek másoknak. A vizsgált szervezetek közül az állami intézményekben dolgozók 90%-a véli úgy, hogy a munkahelyi számítógépén tárolt információk érdekesek lehetnek a hackerek számára.

Az állami intézmények és az állami tulajdonú profitorientált szervezetek szerepeltek a legjobban a magyar *információbiztonság-tudatosság infrastrukturális dimenzió* szerinti minősítésben. Igen jó első kategóriás adatokkal bírtak még a középvállalkozások is. Bár itt az alkalmazottak harmada a harmadik kategória besorolása miatt továbbképzésre szorul. A nagyvállalatoknál ez az arány 8%, ami hasonló nagyságú, mint a nonprofit állami szervezeteknél mért adat (7%). Bár ez utóbbi szervezeteknél dolgozók 7%-a nincs tisztában a biztonsági alapelvekkel és veszélyekkel (negyedik kategória).

Sorrend	Megnevezés	Első kategória	Második kategória	Harmadik kategória	Negyedik kategória
1	Állami intézmények	36%	64%	0%	0%
2	Profitorientált állami szervezet	20%	80%	0%	0%
3	Középvállalkozás	67%	0%	33%	0%
4	Nagyvállalat	38%	54%	8%	0%
5	Nonprofit állami szervezet	36%	50%	7%	7%
6	Profitorientált önkormányzati szervezet	35%	48%	17%	0%
7	Mikrovállalkozás	22%	78%	0%	0%
8	Önkormányzat	29%	50%	21%	0%
9	Kisvállalkozás	0%	100%	0%	0%
10	Nonprofit önkormányzati szervezet	0%	100%	0%	0%

4. táblázat: A magyar információbiztonság-tudatosság infrastrukturális dimenzió szerinti minősítése az üzleti és a közszférában

Az önkormányzatoknál dolgozók ötödének szintén továbbképzésre volna szüksége az információbiztonság-tudatosság területén.

Az *infrastrukturális dimenzió* körében vizsgáltuk a *feltelepített, frissített és engedélyezett víruskereső programok* meglétét. A vírusirtó program a számítástechnikában egy szoftveres vagy hardveres architektúra, amelynek célja annak biztosítása, hogy a hálózatba, vagy egy adott számítógépbe ne juthasson be olyan állomány, mely károkozást, illetéktelen adatgyűjtést vagy bármely, a felhasználó által nem engedélyezett műveletet hajt végre. Ilyenek például a vírusok, trójai programok és egyéb kártékony programok. A vizsgált szervezeteknél dolgozók 90%-a nyilatkozott arról, hogy van víruskereső program a számítógépén. Az állami intézményeknél, a profitorientált állami szervezeteknél és nonprofit önkormányzati szervezeteknél mindegyik kérdezett úgy nyilatkozott, hogy antivírusprogramot használ.

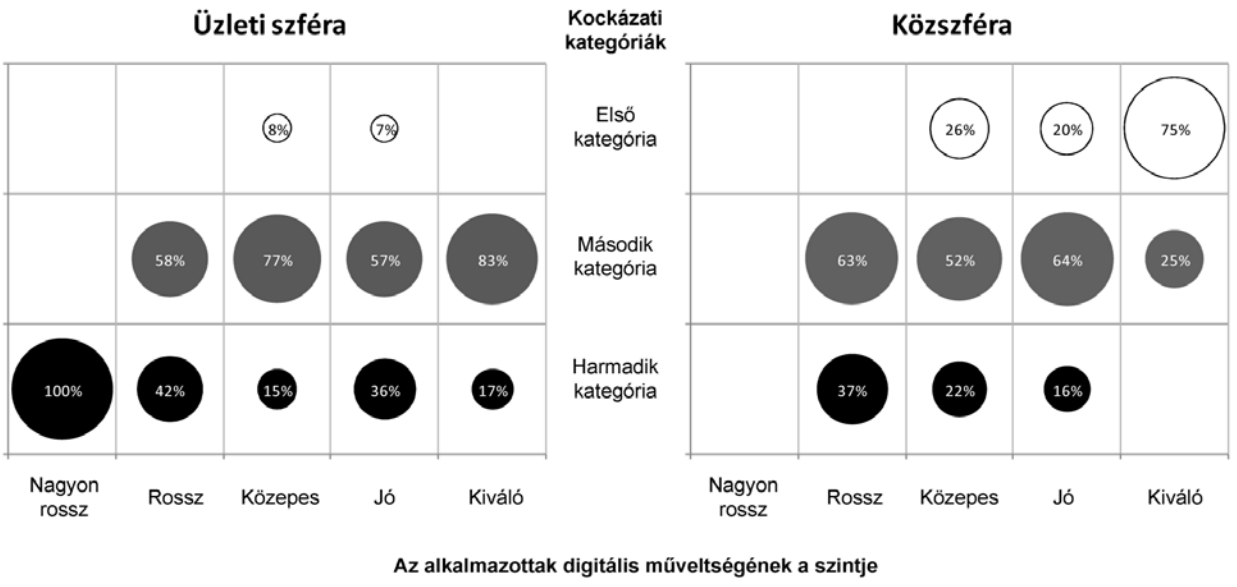
Átlag alatti gyakorisággal a nonprofit állami szervezeteknél (80%), kisvállalkozásoknál (75%) találkoztunk.

Egy másik kérdéssel arra kerestük a választ, hogy az *alkalmazott talált-e már vírust számítógépén*. A számítógépes vírus olyan program, amely saját másolatait helyezi el más, végrehajtható programokban vagy dokumentumokban. Többnyire rosszindulatú, más állományokat használhatatlanná, sőt teljesen tönkre is tehet. A válaszadók közel negyede állítja azt, hogy talált számítógépes vírussal a munkahelyi gépén. Ennél nagyobb aránnyal a nonprofit önkormányzati szervezeteknél (50%), a kisvállalkozásoknál (50%), a középvállalkozásoknál és az önkormányzatoknál (40%) találkozhatunk. A legalacsonyabb gyakoriságot az állami intézményeknél (közel 10%) találtuk. A mikrovállalkozásoknál, az állami intézményeknél, valamint a profitorientált önkormányzati és állami szervezeteknél dolgozók közel 10% nem tudta megmondani, hogy valaha volt-e a számítógépén ilyen nem kívánt program.

Az *infrastrukturális dimenzió* keretében vizsgáltuk az *automatikus frissítés* gyakoriságát az üzleti és a közszférában. Automatikus frissítésről akkor beszélünk, amikor a fontos frissítések akkor kerülnek telepítésre, amikor azok elérhetővé válnak. A vizsgált szervezetek közel 70%-ánál az automatikus frissítést használják. A nagyvállalatok 13%-ánál, önkormányzatok 12%-nál és az önkormányzati tulajdonú szervezetek 40%-ánál nem tudták megmondani, hogy működik-e az automatikus frissítés a munkahelyén, illetve a saját számítógépén.

Megállapítható, hogy az információbiztonság-tudatosság és az alkalmazottak digitális műveltsége között szoros kapcsolat figyelhető meg. Az *üzleti szféra* esetén a nagyon alacsony és rossz digitális műveltséggel rendelkezők mindegyike a harmadik kockázati kategóriába került. A válaszok alapján a rossz informatikai jártassággal rendelkezők 40%-a a harmadik, 60%-a a második kockázati kategóriában található. Azok az alkalmazottak, akik segítséggel ismerik fel saját információs szükségletüket, több mint háromnegyedük a második kockázati kategóriába került, ötödük a harmadik, míg a megkérdezettek 8%-a a legjobb első kategóriában volt megtalálható. Meglepő módon a jó és a kiváló informatikai alapismerettel rendelkezők leggyakrabban a második kategóriában szerepeltek a legnagyobb számban. Első kockázati kategóriában csak a jó digitális műveltséggel rendelkezők 7%-a volt, miközben a harmadik kategóriába a harmaduk szerepelt. Szomorúan állapítható meg, hogy a kiváló ismeretekkel rendelkezőknek kevesebb mint az ötöde a harmadik információbiztonsági kategóriában volt az üzleti szférában.

Megállapítható, hogy az információbiztonság-tudatosság és az alkalmazottak digitális műveltsége között szoros kapcsolat figyelhető meg.



3. ábra: A globális kockázati kategóriák és az alkalmazottak digitális műveltsége közötti kapcsolat

Közszférában a kiváló digitális műveltséggel rendelkezők háromnegyede a globális információbiztonság-tudatosság területén a legjobb első kategóriában, a fennmaradt negyedük a második kategóriában található. Jó informatikai tudással rendelkezők ötöde a legmegbízhatóbb kategóriába tartozik, kétharmaduk a második, de 16%-uk csak a harmadik kockázati kategóriában szerepel. Azok az alkalmazottak, akik segítségre szorulnak informatikából, negyede magas, fele jó, ötöde közepes információbiztonság-tudatossággal bír. Végül a rossz informatikai ismeretekkel bírók kétharmada második, egyharmada harmadik kockázati kategóriába sorolható.

ÖSSZEFOGLALÁS

Tanulmányunkban áttekintettük az üzleti és a közszférában az információbiztonsági-tudatosság helyzetét, egymáshoz viszonyított állapotát.

Az információbiztonsági-tudatosság *fejlettnek* mondható a közszférában az állami intézményeknél, valamint az állami tulajdonú szervezeteknél. Az itt dolgozó munkavállalók jellemzője, hogy tisztában vannak a biztonsági alapelvekkel és veszélyekkel, már vettek részt valamilyen információbiztonsági képzésen, jól képzettek és majdnem mindig követik a vonatkozó biztonsági alapelveket és szabályokat. Az alkalmazottak egy kisebbik része nem venné észre, ha a számítógépét feltörnék; a dolgozók egy része a céges jelszavát másoknak is megmondta, és kisebb hányada úgy gondolja, hogy a munkahely adatainak védelme kizárólag az IT-biztonsági részleg feladata. Egyesek az gondolják, hogy nem értékesek a számítógépükön tárolt adataik, sokan közülük nem hallottak a felhő szolgáltatásokról, néhányan céges adatokat tárolnak a mobiltelefonjukon, sokan közülük saját, személyes célra töltöttek le adatokat a munkahelyi számítógépükre.

Jónak mondható az információbiztonság-tudatosság az üzleti szférában a nagyvállalatoknál, a közszférában az állami tulajdonú nonprofit szervezeteknél. Az alkalmazottak már vettek részt valamilyen információbiztonsági képzésen, tisztában vannak a veszélyekkel, de továbbképzésre szorulnak a témában. Az itt dolgozók egy kisebbik része nem venné észre, hogy a számítógépét feltörték, a harmada utasításra vagy önként a céges jelszavát másoknak is megmondta, és úgy gondolja, hogy nagyon biztonságos a számítógépe adatlopással szemben. Az alkalmazottak ötöde nem elégedett a képzéssel, amit ezen a területen kapott, a harmada meg van győződve arról, hogy a számítógépén tárolt adatok nem értékesek a hackerek számára, sokan közülük nem hallottak a felhő szolgáltatásokról.

A információbiztonság-tudatosság *közepes színvonalúnak* tekinthető a középvállalkozásoknál, az önkormányzatoknál, valamint az önkormányzati tulajdonú profitorientált szervezeteknél. Ebbe a csoportba részben azok a munkavállalók tartoznak, akik tisztában vannak a veszélyekkel, és tudják, hogy bizonyos biztonsági alapelveket be kellene tartaniuk, de továbbképzésre szorulnak a témában. Az alkalmazottak tizede nem tudja, hogy kihez kell fordulnia abban az esetben, ha számítógépét feltörték, harmada nem venné észre, ha a számítógépét feltörnék, és nem tudja, hogy a munkahelyem adatainak és infrastruktúrájának a védelme kinek a feladata. Az alkalmazottak harmada nem elégedett a korábbi képzésekkel, tizede pedig nem tudja, hogy mi az a spam, néhányan nem tudják megmondani, hogy van-e telepítve víruskereső program a számítógépükön. Egyharmaduk meg van győződve arról, hogy a számítógépén tárolt adatok nem értékesek a hackerek számára, sokan közülük nem hallottak a felhő szolgáltatásokról, a harmada céges adatokat tárol a mobiltelefonján, a fele saját célra töltött le már személyes célú adatot a munkahelyi gépére. A szervezetek felénél nincs előírás a levelezőrendszer használatára és nincs szabály a weboldalak látogatására.

Alacsony színvonalúnak mondható az információbiztonság-tudatosság az üzleti szférában a mikro- és kisvállalkozásoknál, a közszférában az önkormányzati tulajdonú nonprofit szervezeteknél. Azok a munkavállalók tartoznak ide, akik részben tisztában vannak a veszélyekkel és az esetek túlnyomórészében tudják, hogy bizonyos biztonsági alapelveket be kellene tartaniuk, de továbbképzésre szorulnak a témában. Egyesek nincsenek tisztában a biztonsági alapelvekkel és veszélyekkel, sem pedig munkaszervezetük biztonsági szabályzatával. Az itt dolgozók harmada nem venné észre, hogy a számítógépét feltörték, tizede odaadta céges jelszavát másnak, az alkalmazottak harmada nem elégedett a korábbi képzésekkel, tizede pedig nem tudja, mi az a spam, és nem tudja megmondani, hogy van-e telepítve víruskereső program a számítógépén. A harmada meg van győződve arról, a számítógépén tárolt adatok nem értékesek a hackerek számára, sokan közülük nem hallottak a felhő szolgáltatásokról, harmada céges adatokat tárol a mobiltelefonján, fele személyes fájlok letöltésére is használja a munkahelyi számítógépét. A szervezetek felénél nincs informatikai biztonsággal foglalkozó részleg, kétharmadánál nincs előírás a levelezőrendszer használatára és szabály a weboldalak látogatására.

Jónak mondható az információbiztonság-tudatosság az üzleti szférában a nagyvállalatoknál, a közszférában az állami tulajdonú nonprofit szervezeteknél.

Megfigyelhető még, hogy a *magasabb digitális műveltséggel* rendelkező alkalmazottak a közszférában alacsonyabb kockázati kategóriában szerepelnek, mint az üzleti szféra esetén.

Jegyzetek

1 Bulgurcu, Burcu – Cavusoglu, Hasan – Benbasat, Izak: Information Security Policy Compliance: An Empirical Study Of Rationality-Based Beliefs And Information Security Awareness, MIS Quarterly 2010/34. pp. 523–548.

2 2013. évi L. törvény az állami és önkormányzati szervek elektronikus információbiztonságáról (a továbbiakban: Ibtv.)

3 Muha Lajos: Az informatikai biztonság egy lehetséges rendszertana, Bolyai Szemle 2008/17. pp. 137–156.

4 Claburn, Thomas: The Threats Get Nastier. IT threats are growing in number, sophistication, and ill intent. Think you've got them under control? Just wait till tomorrow. InformationWeek, Aug 29, 2005. http://www.informationweek.com/story/showArticle.jhtml?articleID=170100709 [2014.09.01.]

5 Ibtv.

6 Magyarország Nemzeti Kiberbiztonsági Stratégiájáról szóló 1139/2013. (III. 21.) Korm. határozat

7 Dinya László: A közszféra szerepe a régiók versenyképességének növelésében, „Versenyképesség-regionális versenyképesség", JATEPress, Szeged, 2010. pp. 117–123.

8 Hoffman, Donna L. – Novak, Thomas P. – Peralta, Marcos: Building Con Trust Online, How merchants can win back lost consumer trust in the interests of e-commerce sales, Communications Of The Acm 1999/42, p. 4.

9 Kürt Zrt.: Informatikai biztonsági tudatosság oktatása http://www.kurt.hu/megoldasaink/informatikai-biztonsagi-tudatossag-oktatasa/ [2014.09.01.]

10 Kodaj Katalin: A Nemzeti Elektronikus Információbiztonsági Hatóság, 2013. http://kifu.gov.hu/kifu/sites/default/files/NFM_Ibtv_NEIH_2013_12_18.pdf [2014.09.01.]

11 Gordon A., Lawrence – Martin P., Loeb – Lucyshyn, William – Richardson, Robert: 2006 CSI/FBI Computer Crime and Security Survey. Computer Security Institute, 2006, http://i.cmpnet.com/gocsi/db_area/pdfs/fbi/FBI2006.pdf [2014.09.01.]

12 Ibtv.

13 Vinçotte International Hungary Kft.: A Vinçotte komplex megoldáscsomagja a közigazgatásban és a kormányzati szférában működő szervezeteknek. http://www.vincotte.hu/Tanusitas/Informaciobiztonsag-a-kormanyzati-szektorban [2014.09.01.]

14 Desman, Mark B.: The Ten Commandments of Information Security Awareness Training. Information Systems Security, 2003, January/February, pp. 39–44.

15 Chen, Charlie C. – Shaw R. S. – Yang, Samuel C.: Mitigating Information Security Risks by Increasing User Security Awareness: A Case Study of an Information Security Awareness System, Information Technology, Learning, and Performance Journal 2006/24. pp. 1–11.

16 CETF ICT Digital Literacy Initiative: Consensus Document, 2008. november http://www.ictliteracy.info/rf.pdf/California%20ICT%20Assessments%20and%20Curriculum%20Framework.pdf [2014.09.01.]

17 Kovácsné Koreny Ágnes: Digitális műveltség Európában, Tudományos és Műszaki Tájékoztatás, Könyvtár- és információtudományi szakfolyóirat 2009/6.

18 Jártasság és felkészültség: a lakosság infokommunikációs attitűdjei, 2009, http://pmsz.org/hu/kutatasok/j%C3%A1rtass%C3%A1g-%C3%A9s-felk%C3%A9sz%C3%BClts%C3%A9g-lakoss%C3%A1g-infokommunik%C3%A1ci%C3%B3s-attit%C5%B1djei [2014.09.01.]

19 Kardos Zoltán: Hálózati kommunikáció, Nemzeti Szakképzési és Felnőttképzési Intézet, 2008, http://www.kepzesevolucioja.hu/dmdocuments/4ap/17_0061_011_101030.pdf [2014.09.01.]

20 United Kingdom Government's Department of Trade and Industry (DTI): Code Practice for Information Security Management BS 7799, 2000.

21 2011. évi CXII. törvény az információs önrendelkezési jogról és az információszabadságról, 7. §

22 Bond, Trenton – Stephens, Cortney – Piscitello, Dave: Security Awareness

Survey, 2012, http://www.securingthehuman.org/media/resources/planning/Stage03-03-HumanRiskSurvey.docx [2014.09.01.]
23 Illéssy Miklós – Nemeslaki András – Som Zoltán: Elektronikus információbiztonság-tudatosság a magyar közigazgatásban, Információs Társadalom 2014/1. pp. 52–73.
24 Illéssy Miklós – Nemeslaki András – Som Zoltán i. m.
25 Kodaj Katalin i. m. p. 5.
26 Kodaj Katalin i. m. p. 9.
27 Kenneth, J. Knapp – Ferrante, Claudia J.: Policy Awareness, Enforcement and Maintenance: Critical to Information Security Effectiveness in Organizations, Journal of Management Policy and Practice 2012/5. pp. 66–80.
28 Munk Sándor: Információs színtér, információs környezet, információs infrastruktúra, Nemzetvédelmi Egyetemi Közlemények, 2002, http://uni-nke.hu/downloads/konyvtar/digitgy/20022/vszt/munk.html#_ftn35 [2014.09.01.]
29 Shaw, R. S. – Chen, Charlie C. – Harris, Albert L. – Huang, Hui-Jou: The impact of information richness on information security awareness training effectiveness, Computers and Education 2009/1. pp. 92–100.
30 Muha Lajos: Fogalmak és definíciók: 2.4. in: Maha L. (szerk.) Az informatikai biztonság kézikönyve: Informatikai biztonsági tanácsadó A-tól Z-ig., Budapest: Verlag Dashöfer, 2004. pp. 1–37.
31 2004. évi XXXIV. törvény a kis- és középvállalkozásokról, fejlődésük támogatásáról.
32 Magyarország Nemzeti Biztonsági Stratégiájáról szóló 1035/2012. II. 21. Korm. határozat.
33 Gajdushek György: Közszolgálat. A magyar közigazgatás személyi állománya és személyzeti rendszere az empirikus adatok tükrében. 2008, Budapest. KSZK.
34 Chang, Liua – Jack T., Marchewkab – June, Luc – Chun-Sheng, Yu: Beyond Concerns: A Privacy-Trust-Behavior Intention Model, Information & Management (I&M) 2005/1, pp. 289–304.
35 Nemeslaki Andras – Illéssy Miklós: Information Security Awareness in the Hungarian Public Sector: Result of an Empirical Study, in: Alexander Balthasar, Hendrik Hansen, Balázs Kőnig, Robert Müller-Török, Johannes Pichler (eds.): Central and Eastern European eGov Days 2014 – eGovernment: Driver or Stumbling Block for European Integration. Austrian Computer Society, Wien, 2014.
36 Nyugat-magyarországi Egyetem: A szoftverhasználat rendje, 2009, http://info.nyme.hu/index.php?id=4933 [2014.09.01.]
37 Internet értelmező kisszótár: Hacker, 2009, http://www.ujmagyarevezred.nl/mikrosz.html [2014.09.01.]