SPILÁK VIKTOR – KOSZTYÁN ZSOLT TIBOR

SZERVEZETI KULTÚRA, VEZETŐI SZEREPEK, AZ INFORMÁCIÓBIZTONSÁG ÉS A FELHŐALAPÚ MEGOLDÁSOK KAPCSOLATA

Az információs technológiák és az általuk szavatolt biztonság napjainkra kritikus szerepet töltenek be a szervezetek mindennapi életében, és nagyban képesek támogatni azok sikerességét. A tanulmány elsődleges célja feltárni, hogy milyen változásokat okoz a vezetésben és a szervezet kultúrájában egy-egy információbiztonsági kérdés felmerülése, valamint a felhőmegoldások alkalmazása. A szervezeti kultúra, vezetői szerepek, információbiztonság és a felhőszolgáltatások vizsgálata korábban közös modellben nem történt meg, ezért nem volt arra lehetőség, hogy a hatásokat egy rendszerben vizsgálják és megértsék. Ebben az esettanulmányban a szerző bemutatja, hogy e területek kölcsönhatásban vannak egymással és hatékony együttműködésükhöz szükséges összehangolásuk, esetleg működési átalakításuk, mely képes hatni a vállalati kultúrára és a vezetésre is. Kidolgoz egy olyan új modellt (kiemelt hangsúlyt fektetve az információbiztonsági kiválóságra és a felhőalapú megoldásokra), mely segítséget nyújt a szervezetek működési területei között létező kölcsönhatások későbbi feltárásában. Vizsgálja a felhőmegoldások alkalmazásának hatásait az információbiztonságért felelős szervezet működésére, valamint a szervezet e szolgáltatásokkal szemben támasztott biztonsági elvárásait.

Kulcsszavak: szervezeti kultúra, vezetői szerep, Cameron-Quinn, információbiztonság, felhőalapú megoldások, információbiztonság-menedzsment

A vállalatok keresik, hogy miképpen tudnák felülmúlni versenytársaikat, ebben pedig óriási szerepük van az információs technológiáknak, mint az innovációs teljesítmény egyik befolyásoló tényezőinek (Yang et al., 2015). E technológiák segítik az ügyfelek által támasztott elvárások és igények érzékelését és megértését (Roberts & Varun , 2014). Az üzleti világban lezajlódó gyors változások, többek között a start-up vállalatok megjelenése, folyamatos fejlődése kihívást jelent a piac minden szereplőjének (Kollman et al., 2015). Az elkövetkező években ennek hatása tovább fog erősödni, mivel az európai start-up-ok iránti érdeklődés az amerikai piac irányából is egyre erősödik. A létrehozott termékek és szolgáltatások további fejlesztése és terjesztése erős felvásárló esetén további támogatást kaphat (Pisoni & Onetti, 2018). A nagyobb szervezeteket lassan reagáló, sok esetben a változásoknak ellenálló működés jellemezi (Shaul et al., 2011). Problémát jelent továbbá, hogy az informatikai beruházások hasznosságát nehéz mérni (Fehér et al., 2016). A vezetők ugyanis nincsenek tisztában azzal, hogy az egyes komponensek milyen hatást képesek egymásra gyakorolni, esetleg az egyik területen végrehajtott változtatás egy másik területet negatívan befolyásolhat, vagy megkövetelheti annak átalakítását is (Spilák & Kosztyán, 2013).

A kutatás időszerűségét alátámasztja továbbá, hogy intenzív árverseny esetén a vállalatok szenvedhetnek a decentralizált működéstől (Pekgünk et al., 2016), a technológiai előnyök viszont képesek új lehetőségeket biztosítani a termelés/szolgáltatás átfutási idejének rövidítésére (Marchese et al., 2015). Az informatika mára olyan eszközzé vált, amely Marchese, Crane, Haley megállapítását is figyelembe véve képes hozzájárulni egy szervezet versenyképességéhez, illetve nem hatékony működésének következtében ellentétes hatást kifejteni. A szervezetek igyekeznek a technológiákban rejlő lehetőségeket és kapacitásokat úgy kiaknázni, hogy legyenek képesek a közben a felmerülő költségeket minimalizálni vagy legalább megosztani tudják. Ezért a nagyvállalati környezetre jellemző a közös használatú erőforrások létrehozása és üzemeltetése. Ezáltal a meglévő szervereket felbontják kisebb alkotó elemekre, úgynevezett virtuális gépekre, így pedig egy időben a korábbiakhoz képest sokoldalúbb felhasználásra nyílik lehetőség (Fehér et al., 2016). A magas rendelkezésre állást igénylő megoldásokhoz használható rendszerek esetében kritikus jelentőséggel bír a pontos tervezés, valamint a későbbi költséghatékony üzemeltetés és stabil működés (Metzler, 2009).

Korábban kevés olyan kutatás történt, amely a szervezeti kultúrát, a vezetői szerepeket, az információbiztonsági kiválóságot és felhőalapú megoldásokat együttesen vizsgálta volna. Azonban e területek összekapcsolása segíthet abban, hogy megértsük a felhőalapú megoldások alkalmazásának és az információbiztonsági kérdéseknek a szervezetre gyakorolt hatásait, figyelembe véve a szervezet kultúráját, valamint a vezetői szerepeket.

A tanulmány további részeiben áttekintjük a kutatáshoz kapcsolódó szakirodalmakat, bemutatjuk a létrehozott modellt. Ezt követően az esettanulmányt, valamint annak eredményeit ismertetjük. Összegezzük a levonható következtetéseket, illetve meghatározzuk munkánk további fejlesztési lehetőségeit is.

A kutatáshoz kapcsolódó irodalmi áttekintés

A fejezetben bemutatjuk a kutatáshoz kapcsolódó fontosabb irodalmakat. Ismertetjük a kultúramodellt, a vezetői szerepeket, az információbiztonsággal kapcsolatos elvárásokat, valamint a felhőalapú megoldások alkalmazásának kritériumait.

A kultúramodellek

A témával foglalkozó kutatások, irodalmak sokrétűsége is jól mutatja az akadémiai érdeklődést a vállalati kul-

túra iránt (Oju, 2009). A kultúra fogalmának meghatározása több aspektusból közelíthető meg és nincs egységesen elfogadott értelmezés, Kroeber és Kluckhohn több mint 160 definíciót gyűjtött össze (Kroeber & Kluckhohn, 1978). A kultúra meghatározása és fejlesztése azért is kiemelkedően fontos, ugyanis meghatározó alapja egy szervezet működésének, mivel a stratégiai tervezés önmagában nem képes a vállalat totális mozgósítására. Ahhoz szükség van a kultúrára is (Hax & Majluf, 1984). Számos modell született az évek során attól függően, hogy a kutatók milyen területeket tartottak fontosnak, illetve helyeztek a vizsgálat középpontjába (Balogh et al., 2011). Korábban úgy vélték, hogy a szervezeti kultúra a siker legfontosabb eleme (Lippert et al., 2015). Később ezt túlzónak ítélték, de abban továbbra is egyetértenek, hogy kulcsfontosságú szerepet játszik egy szervezet életében (Naranjo-Valencia et al., 2011). Formálja annak vezetőjét, aki önmaga is hatással van arra, hogy milyen kultúra alakul ki a kollektíván belül (Gaál et al., 2009). Kutatásunk során vizsgáltuk a *Handy-féle kultúramodellt,* mely az egyik leggyakrabban alkalmazott kultúratipizálás és hazánkban is igen népszerű. Abból indult ki, hogy az eltérő tevékenységeket végző szervezetek eltérő kulturális sajátosságok jellemzik. Figyelembe kell venni alkalmazása során, hogy létrejöhetnek szubkultúrák is, amelyek erősíthetik, de gyengíthetik is a szervezet teljesítőképességét. A Handy-féle modell esetében meghatározott kultúratípusok nem minden esetben alkalmazhatók, mivel a szervezet tagjai gyakran rugalmatlanok, azaz hisznek abban, hogy ha valami jól működik az egyik kultúrában az jól fog a másikban is (Cacciattolo, 2014). Kutatásunk során Handy megközelítésében a jövő vizsgálatának hiánya jelenti a legnagyobb korlátot, mivel így későbbiekben nem nyílik arra lehetőség, hogy a vágyott kultúra figyelembevétele megtörténhessen. *Hofstede* a nemzetek közötti különbségeket dolgozta fel és állapította meg, hogy adott kultúrajellemzők kombinációja bizonyos szervezeti formák gyakori előfordulásával jár együtt (Lippert et al., 2015; Hofstede, 2010). Jól használható ez a kultúramodell a telekommunikációs szektorban, azonban vannak korlátai alkalmazásának. Mint minden nemzetikultúra-vizsgálat a kultúra határait a nemzeti határokkal veszi egybeesőnek (Török, 2017), ami nem megfelelő kutatásunk során, ugyanis az általunk későbbiekben vizsgálni kívánt szektor és vállalatok döntő része leányvállalat, így pedig információk elvesztését eredményezheti ez a megközelítés. A modellel további hátránya, hogy technikailag bonyolult, így alkalmazása nehézkes (Mead, 1998). Célunk, hogy olyan módszerrel tudjuk vizsgálni a vállalatokat, amely könnyedén megismételhető, a felmérés folyamata pedig egyszerű. Vitatható pont továbbá, hogy az egyes dimenziókat az eltérő országok máshogy értelmezik, a modell nem határozza meg a kontextust, így pedig az eredmények is torzulhatnak (Török, 2017). A *Morgan-féle kultúramodell* az alapján határozza meg a kultúrát, hogy a vezetők milyen módon tekintenek szervezetükre. Mechanikus kultúrában a szervezetet gépként fogják fel, azaz megbízhatóan és hatékonyan kell működnie, előre lefektetett célokat lehessen általa elérni. Ezzel ellentétben az organikus kultúra esetében, mint egy élő szervezetre tekintenek (Morgan, 2007; Balogh et al., 2011). Morgan megközelítésének kritizálói (Jermier & Forbes, 2016; Kemp, 2016; Pinto, 2016) az empirikus megközelítésre támaszkodva javasolják további metaforákkal bővíteni a modellt. Bírálják a mechanikus és organikus definíciót, mivel megfigyelés révén ezek szervezet és nem ember irányultságúak, így pedig elsődlegességük vitatható (Örtenblad et al., 2016). Mivel az általánosságban megfogalmazott kritikák Morgannel szemben kiemelik a személyi aspektus hiányát, ezért kutatásunk során nehézkes lenne megteremteni a vezetői szerepekkel történő kapcsolatot. *Trompenaars* szintén a kétpólusú dimenzióktól történő eltávolodást képviseli. Kluckhohn és Strodtbeck kategóriáiból indult ki és állította fel dimenzióit, amik 6 alapvető kérdésre vonatkoznak. Így szintén eltávolodik a hofstedei kétpólusú dimenzióktól (Török, 2017). Négy szervezeti kultúratípust határozott meg, amelyek megmutatják a munkatársak véleményét a szervezet rendeltetéséről, céljairól és azon belül a saját szerepükről (Hampden-Turner & Trompenaars, 2006; Fekete & Berzsenyi, 2017). A Trompenaars modell kritikája, hogy nem ismeri fel a személyiség jellemzők hatását a viselkedésre. Valamint Trompenaars és mások, mint pl. Hofstede azt vallják, hogy a vállalatoknak el kell ismerniük a kulturális különbségeket, addig Ohmae (1999) és Levitt (2003) szerint a nemzeti határok csökkennek, és a világot egy egészként kell tekinteni nem külön országokként, eltérő kultúrával. Munkánk során kiemelten fontosnak tartjuk, hogy a kultúrákat, határok nélkül tudjuk vizsgálni. Ugyanis az általunk későbbiekben elemezni kívánt vállalatok többsége leány- vagy anyavállat. Így pedig határok nélküli, egy egészként működő szervezetre kell tekintenünk, amelyre Trompenaars modellje nem lenne alkalmas. *Cameron – Quinn versengő értékek keretrendszere* azt vizsgálja, hogy a szervezetek milyen értékek figyelembevétele mellett törekszenek hatékonyságuk növelésére hosszú távon. A kultúradimenziók beazonosítása és mérése elkerülhetetlen annak érdekében, hogy a vezetők képesek legyenek a kultúra fejlesztésére (Cameron & Quinn, 2011; Fekete & Berzsenyi, 2017). Cameron – Quinn munkája azért jelentős, mivel egyetlen modellbe vonja össze a szervezet hatékonyságát befolyásoló értéket. Ezt felhasználva határozza meg, hogy a vezetés milyen céloknak tulajdonít értéket (Lippert et al., 2015). Kutatásunk során e hatékonysági tényezők ismerete kiemelten fontos, mivel az IT-rendszerek működése szintén képes a hatékonyságot befolyásolni, így pedig a két terület együttes „mozgását" is képesek lehetünk feltárni. Ezen túlmenően a Cameron – Quinn modell lehetőséget biztosít nemcsak a jelenlegi, hanem a jövőben elérni kívánt állapot feltárására. *Wong megközelítésében* megjelenik a hatalmi távolság és az individualizmus – kollektivizmus dimenziója hasonlóan Hofstede modelljéhez, valamint a természet értelmezése megfeleltethető a Trompenaars-féle környezet belső-külső kontrolljának. Wong további hét dimenziót definiál, mint az idő, cselekvés, kommunikáció, tér, versenyszellem, szervezet, formalitás (Fekete & Berzsenyi, 2017; Gaál, 1999). Azonban gondolkodásával a nemzetikultúra-modellek közé tartozik, így pedig Trompenaarshoz hasonlóan azt vallja, hogy a válla-

latoknak el kell ismernie a kulturális különbözőségeket, ezáltal pedig nem alkalmas az általunk kívánt határok nélküli szemléletmód megvalósítására. Választásunk során azért került kizárása továbbá, mivel ez a modell hipotetikus, azaz empirikus tapasztalatok nem támasztják alá (Bognár & Gaál, 2013). *Hall* megközelítése teljesen eltér Hofstede és Trompenaarsétől. A cselekvésalapú vizsgálatot képviselte szemben az értékkutatással (Török, 2017). A modell figyelembe veszi az időt, a kommunikációt, valamint a teret egyaránt (Tolbert & Hall, 2008). A napjainkban kivitelezett kutatások a Hall-féle kultúradimenziókat nem egymástól elszigetelten, hanem egymást kiegészítve használják (Török, 2017). Azonban figyelembe kell venni, hogy nem jelenik meg benne olyan dimenzió, ami lehetőséget teremtene arra, hogy információbiztonság, valamint felhőalapú területekkel össze tudjuk kapcsolni. *Slevin* és *Covin* mechanikus és organikus kultúrákat különböztet meg. A mechanikus jellemzői a hierarchikusság és formalizáltság, de ezek a szervezetek nehezen alkalmazkodnak. Az organikus kultúra kevéssé formalizált, laza és az egyéni szaktudást helyezi előtérbe, mely alapja a sikerességének. Gyorsan változó, bizonytalan környezethez jól adaptálódnak az organikus vállalatok. A kultúrák ilyesfajta megkülönböztetése meghatározza az alkalmazkodás képességét (Covin & Slevin, 1990; Kiss & Csillag, 2014). Ez kutatásunk során hasznos, de a modellt vizsgálva megállapítható, hogy a kommunikációs csatornák, azaz az alkalmazott technológiák csupán kis részarányt képviselnek. Így pedig az általunk kívánt összekapcsolás más tudomány területekkel korlátozott vagy lehetetlen lenne. A *Harrison-féle kultúramodell* a strukturális, ellenőrzési, kapcsolódási és vezetői pontok alapján határozta meg a négy alap kultúratípust, melyek az erő-, a szerep-, az eredményen alapuló feladat- és személykultúrák (Caroll & Harrison, 2005; Matkó, 2016). Sajátossága a megközelítésnek, hogy nem ragadja ki a kultúrát a gazdasági környezetéből (Harrison, 1992), de ahogy Slevin – Covin nem alkalmas az összekapcsolásra, úgy Harrison modellnél sem lehet megvalósítani, így pedig nem alkalmas az általunk kívánt vizsgálatra. A *Henry Mintzberg-féle szervezeti konfigurációban* a szervezettervezés kulcsa a következetesség, valamint az összefüggés. A vállalat hatékony működése attól függ, hogy mennyire képes kapcsolatot kialakítani a szervezet kora, struktúrája, mérete és technológiája között. Ebből kiindulva olyan szervezeti alapformációkat különített el, amelyek egyrészt a környezet jellemzőivel, a technológiával, a szervezet nagyságával függenek össze. Másrészt belső "mozgató erőikben", ideológiai, szervezeti életmódbeli kultúrájukban különböznek (Mintzberg, 2010; Matkó, 2016). Mintzberg megközelítését számos kritika érte, mely szerint tervezési alapelvei hiányosak, megállapításai ellentmondanak a megfigyelhető tényeknek, valamint az előíró és leíró megfigyelések elemzése hiányzik. Nem definiálja továbbá saját modelljének kontextusát sem (Ansoff, 1991). Ezáltal pedig nem tudjuk alkalmazni, mivel elengedhetetlen, hogy egy olyan rendszert alkalmazzunk, ami kipróbált, bizonyított és hiányosságoktól mentes. *Kluckhohn* és *Strodtbeck* szerint a kultúra csak lassan változik és alapjaiban stabil. Ez a stabilitás teszi lehetővé, hogy vizsgálni lehessen a kulturális orientációkat. Hat dimenziót határoztak meg, melynek részeként vizsgálják az emberek természetét (jó, rossz, nem változtatható), az embereknek a természettel való viszonyát (uralkodó, harmonizáló, alázatos), az emberek egymás közti viszonyát (alárendelt, mellérendelt), az emberek aktivitását (tenni, létezni, kezdeményezni), az időt (múlt, jelen, jövő) és a teret (privát, közös, vegyes) (Kluckhohn & Strodtbeck, 1973; Matkó, 2016). Kluckhohn és Strodtbeck maguk is megállapították, hogy modelljük nem teljes, nem kezelik pl. a munka természetét, a tér meghatározását, valamint a nemek közti kapcsolatokat (Hills, 2002). Ezért nem alkalmas azon tudomány területekkel történő összekötésre, melyek esetünkben fontosak lennének, így munkánk során nem alkalmazható modelljük. A *Globe-kérdőív* eltávolodik a kétpólusú kultúradimenziós megközelítéstől, bár részben a Hofstede-modellre épül, hiszen a Hofstede-dimenziókat, azok továbbfejlesztett változatát, valamint más kutatóktól átvett és módosított kategóriákat tartalmazza. Azonban már nemcsak kvantitatív, hanem kvalitatív módszereket is használ Hofstede-vel ellentétben és a szervezeti kultúra vizsgálata során tapasztalt eredményeket külön-külön is kutatja (Török, 2017). Míg a korábbi a leíró dimenziók mentén mérik és értékelik a kultúrák egymástól való eltérését, addig a GLOBE ennél tovább megy és már nem csak azt vizsgálja, ahogy a dolgok vannak, hanem arra is kíváncsi, hogy miképp kellene lenniük. Így lehetőség van a kívánatos kultúrák mérésére is (Bakacsi, 2012), ami hosszú távon számunkra is cél. A modell részletes, szofisztikált vizsgálatra ad lehetőséget, de csak az emberi tevékenységre fókuszál, így nem léteznek olyan területek, amelyeket össze lehetne kötni az információbiztonsággal. Jelen esetben a humánbiztonsági kérdésektől tekintsünk el, mivel fontos, de csupán apró szeletei a biztonságnak.

A vizsgált modelleket az 1. táblázatban értékeltük az alapján, hogy alkalmasak-e az információbiztonsági és a felhőkutatásokkal történő kapcsolat megteremtésére, milyen vizsgált dimenziók/értékelési kritériumok jellemzik, továbbá a vállalati értékeket/cselekvés mintákat/fő fókuszt hogyan értékelik.

1. táblázat Vállalatikultúra-modellek

Kultúramodell	Kultúra összehasonlító modell	Lehetséges kapcsolat az információbiztonsági/felhő kutatásokkal	Vizsgált dimenziók/ értékelési kritériumok	Vállalati értékek/cselekvésminták/fő fókusz
Handy-féle kultúramodell (Handy, 1999)	x	Alkalmas - Figyelembe veszi az alkalmazott technológiákat.	Hogyan gyakoroljuk a hatalmat? A szabványok és eljárások fontosak, vagy az eredmények? A modell a szervezet múltját, tulajdonformáját, céljait, alkalmazott technológiát, környezetét és az embereket veszi figyelembe.	A szervezetek eltérő értékrenddel rendelkeznek. Így más a munkavégzés módja, ritmusa, más személyiségű embereket vonzanak, sokszor még a külső jegyek alapján is beazonosítható a kultúra.
Hofstede – nemzetikultúra-modell (Hofstede, 2010)	x	Nem alkalmas - Csak az ember - emberhez való viszonyát vizsgálja.	Bizonytalanságkerülés és a hatalmi távolság által létrehozott négy síknegyedhez különböző szervezeti struktúrákat rendelt.	Hatalmi távolság és az individualizmus/kollektivizmus határozzák meg a cselekvés mintát.
Morgan-féle kultúramodell (Morgan, 2007)		Nem alkalmas - Nem tér ki a technológiára, vagy a szervezetet kiszolgáló rendszerekre.	Vállalatvezetők szervezetszemléletét vizsgálta és annak alapján vont le a vállalati kultúrára vonatkozó következtetéseket.	A vezetők vagy úgy gondolnak a szervezetükre, mint egy adott művelet elvégzésére alkalmas, szakszerűen összeszerelt gépre (mechanikus), vagy úgy, mint egy élő szervezetre, amely életciklusa során folyamatosan alkalmazkodik környezetéhez (organikus).
Trompenaars kultúradimenziók (Hampden-Turner & Trompenaars, 2006)	x	Nem alkalmas - A kultúratípusokat a szervezeti struktúra vertikális és horizontális jellege, illetve a szervezet és beosztottja közötti feladat-, személyorientált hozzáállás dimenziói mentén állította fel.	Két tengely mentén csoportosítja a kultúrákat, az egyik tengely végpontjai a személy és a feladatorientált, a másiké pedig az egyenlőségre törekvő és a hierarchikus.	Hogyan gondolkodnak, tanulnak, motiválnak, jutalmaznak és oldják meg a konfliktusokat.
Cameron – Quinn – versengő értékek keretrendszere (Cameron et al., 2007)	x	Alkalmas - A modellben szerepet kapnak a sikerkritériumok, amelyek egyik eleme tud lenni a technológia, annak hatékonysága, valamint maga a biztonság is. Az adhokrácia kultúrában összetartó erőként jelenik meg az innováció. Értékteremtő elemként tekintenek az innovatív tevékenységekre, megoldásokra.	Az értékpreferenciák feltárásával jellemzi és hasonlítja össze a szervezeteket. A kultúratípusokat két tengely mentén, négy síknegyedben helyezi el.	Annak fényében azonosíthatók a minták, hogy a szervezet a stabilitás, rend, irányítás, rugalmasság, dinamizmus, önállóság, valamint a belső fókusz, integráció – külső fókusz, differenciálás mely tengelyén helyezkedik el.
Wong modell (Gaál, 1999)		Nem alkalmas - A használt dimenziók az emberi cselekvést, egymáshoz viszonyulást és annak tulajdonságait foglalják magukba, de sem a technológia, sem pedig az egyéb információs rendszer nem kap szerepet.	Tíz változóból álló vizsgálati modell. Természet, idő, cselekvés, kommunikáció, tér, hatalom, individualizmus, versenyszellem, szervezet, formalitás.	Egy önálló kultúradimenziót szentel a cselekvés témakörének. A modell megkülönböztet cselekvő kultúrákat, amelyekben a domináns viselkedésminta a haladni akarás, míg a létorientált kultúrákban a jelen és annak élvezete kerül előtérbe.
Hall modell (Tolbert & Hall, 2008)	x	Nem alkalmas - A technológia mint átadó közeg jelenik meg csupán.	Az elmélet a világ kommunikációjára építve készült el, melynek része a szavak, az üzleti, politikai és diplomáciai közeg, az anyagi dolgok, a státusz és a hatalom jellemzői. A viselkedés megmutatja, hogy hogyan éreznek az emberek és milyen technikákat alkalmaznak az összeütközés és a konfliktusok megelőzésére.	Az emberek a másoktól érkező szóbeli, írásbeli vagy egyéb jellegű üzeneteket közös tudásuk alapján értelmezik, amelynek szerves részét alkotják a kultúra beállítódásai, értékei és gondolkodásmintái.
Slevin – Covin modell (Covin & Slevin, 1990)		Nem alkalmas - Az infokommunikációs eszközök mint kommunikációs csatornák hangsúlya kicsi a teljes modellen belül.	Organikus és mechanikus szervezetikultúra-típusokat különböztet meg.	Szemlélteti, hogy a szervezet mennyire képes alkalmazkodni a változó környezethez.
Harrison-féle kultúramodell (Caroll & Harrison, 2005)		Nem alkalmas - A modell által a szervezet fő jellemzőiként azonosított elemek között nincsen technikai terület.	Négy alap-kultúratípust különböztet meg, melyek az alkalmazott strukturális, vezetői, ellenőrzési és kapcsolódási pontok alapján születtek meg.	A szervezet fő jellemzőiként tekinti a kontroll forrását, a kontroll eszközeit, a fő motivációforrást, központi értékeket, valamint a negatív jellemzőket/következményeket.
Henry Mintzberg - szervezeti konfiguráció (Mintzberg, 2010)		Alkalmas - A technostruktúra magába foglalja azokat a személyeket, akik a számítógépes és pénzügyi rendszereket működtetik, így lehetséges az információbiztonsággal való összekapcsolása.	Az egész szervezet koordinált irányítása a részek egymással való kölcsönhatásán keresztül valósul meg.	Öt alapvető szervezeti részt azonosít, melyek meghatározzák a szervezeti értékeket és működést. Ezek közé tartozik a működési mag, a stratégiai csúcs, a középvonal, a technostruktúra, valamint a segítő személyzet is.
Kluckhoh és Strodtbeck hat dimenziója (Kluckhohn & Strodtbeck, 1973)	x	Nem alkalmas - Csak az emberi tevékenységre fókuszál. Más tudományterületekkel való összeköttéshez hiányoznak a kapcsolódási pontok.	Hat területet vizsgál. Figyelembe veszi az emberek természetét, az embereknek a természettel való kapcsolatát, az emberek egymás közti viszonyát, az emberek aktivitását, az időt és a teret.	A vizsgált területek alapján állapítja meg, hogy az ember természete „Jó” (változtatható – nem változtatható), „Rossz” (változtatható – nem változtatható), valamint a „Jó és a Rossz” keveréke.
Globe-kérdőív kulturális dimenziói (House et al., 2004)	x	Nem alkalmas - Nem számol a szervezeten belül alkalmazott technológiákkal és azok befolyásoló hatásával.	A vizsgálat során meghatározott dimenziók: bizonytalanságkerülés, hatalmi távolság, individualizmus/ kollektivizmus, férfias/nőies értékek, jövőorientáció, teljesítményorientáció, humán orientáció, rámenősség.	Az értékek/kultúradimenziók szintjén ragadja meg a kultúrát. A kérdőív a kultúradimenziókat mind a szervezeti, mind pedig a társadalmi kultúrára vonatkoztatja.

A lehetséges kapcsolat megteremtése más kutatási területekkel azért kritikus, mivel ennek hiányában csak két egymástól független tudományág eredményeit igyekeznénk egyesíteni, azonban az egymásra hatások viszonyát nem lehetne feltárni. Azon modelleket nyilvánítottuk alkalmasnak a kapcsolat megteremtésére, ahol a dimenziók, vagy értékelési kritériumok között megjelentek olyan területek, melyek lehetőséget nyújtottak az összekötés létrehozására. E területeket a következők szerint csoportosítottuk:

- alkalmazott technológiák: azon rendszerek összessége, melyek szükségesek a szervezet működtetéséhez és az általa nyújtott szolgáltatások/termelés biztosításához, e területek esetében fontos kérdés az információbiztonság, az adatok kezelése és a felhőmegoldások alkalmazása,
- innováció: olyan szervezetek esetében, ahol az innovációra, mint értékteremtő elemre tekintenek elengedhetetlen, hogy az IT-rendszerek hatékonysága, biztonsága és stabilitása szavatolva legyen,
- üzemeltetés: az a szakértői csapat, aki az IT-rendszerek működtetéséért felelnek.

Ezek alapján a Handy-féle kultúramodell, Cameron - Quinn versengő értékek keretrendszere, valamint Henry Mintzberg szervezeti konfigurációja megfelelt az összekapcsolási kritériumoknak (Lásd: 1. táblázat).

Egy vállalat vezetése munkaadóként ügyel a jogi és szervezeti feltételekre, vezetőként fejleszti a munkavállalók képességeit, továbbá kultúraalakítóként támogatja az egyének igényeinek kifejezésre jutását (Szabó & Dancsecz, 2009). Számos dimenzió mentén közelíthető meg a vezetés, valamint a vezetők feladatai (Lippert et al., 2015). E dimenziók a vezetői funkciók, a vezetői problémamegoldási folyamat, a vezetési stílus, a vezetési rendszerek és a vezetői szerepek (Dobák & Antal, 2016). Mivel a vezetési szerepek jelentősége kiemelkedő egy szervezet formálásban, ezért azt feltételezzük, hogy szignifikáns hatással van az általunk vizsgált területekre is. Így munkánk során hangsúlyt fektettünk e terület bevonására. *Henry Mintzberg* arra keresi a választ, hogy a vezetők személyközi (nyilvános megjelenések, főnöki, kapcsolatteremtő és kapcsolatápoló), információs (információgyűjtő, információszétosztó, szóvívő) vagy döntési (vállalkozói, zavarelhárító, erőforrás-elosztó, tárgyaló, megegyező) szerepeket töltenek-e be (Lippert et al., 2015). Új megvilágításba helyezte a vezetői munkát azzal, hogy a mindennapos tevékenységüket vizsgálta. A modellt felső vezetők körében végzett empirikus vizsgálatokkal támasztották alá, így elsősorban erre a szintre igaz (Dobák & Antal, 2016). Ez azonban korlátot jelenthet számunkra, mivel nem minden esetben csak felső vezetők bevonása történik meg kutatásunk során. Kultúramodelljével történő összekapcsolás pozitív lehetőség, azonban tervezési alapelvi hiányosságok miatt alkalmazását elvetjük. *John Kotter* nem tekinti a menedzsment részének a vezetést (Bogdány, 2014). A vezetői feladatokat két szerepre osztja, manager és leader. A vezető manageri szerepében a szervezeti komplexitással birkózik meg. A leader szerepében ezzel szemben a szükséges változásokra koncentrál (Bakacsi, 2010). Ez a két szerepkör elkülönített alkalmazása és felmérése túlságosan bonyolulttá teszi a kutatásunkban történő használathoz. Ezzel ellentétben *Dian Hosking* nem bontja fel két külön területre a vezetést, hanem a menedzseri szerepet definiálja részletesebben, ahol a szervezeti erőforrások tervezése, szervezése, vezetése és ellenőrzése a feladata (Draft, 2012). A menedzser célja, hogy azzá váljon, amit a vállalat elvár tőle. Jól bevált technikákat alkalmaz, túl elfoglalt ahhoz, hogy időt szánjon a nehéz dolgokra (Bogdány, 2014). Abraham Zaleznik hasonlóan Kotterhez a management – leader szemléletet képviseli. Szerinte a leader új lehetőségeket keresi, míg a menedzser korlátozza a választási lehetőségeket. Eltérés van a vállalati célok értelmezésében is a két kategória között, mivel míg a leader alakítja, addig a menedzser elfogadja azokat (Angyal, 2009). A kormányzói szerepkör, mint kiegészítő terület jelenik meg, mely a hatalmi struktúra irányítója. Így pedig leginkább azon tulajdonosokat foglalja magába, akik részt akarnak venni a szervezet életében, azonban nem kívánnak egy teljes leader vagy menedzser pozíciót betölteni (Angyal, 2009). Zaleznik megközelítése ezért Kotteréhez hasonlóan bonyolult, a kormányzói szerepkör pedig további komplexitást ad hozzá. Ilyen szintű diverzifikálás és lebontás esetünkben nem indokolt, így alkalmazása nem lenne megfelelő modellünkhöz. *Richard Boyatzis* a személyorientált megközelítést képviseli. A vezető belső adottságaival, tulajdonságaival foglalkozik, és ezeket tekinti a legfontosabb kompetenciáknak (Spencer & Spencer, 1993). Szerinte a kompetenciák egy személy meghatározó, alapvető jellemzői, melyek kapcsolatban állnak a teljesítményszinttel (Karoliny & Poór, 1994; Lippert et al., 2015). A megközelítés az egyéni hatékonyságot értékelni és fejleszteni akkor lehet, ha a legjobban teljesítők személyiségjegyeit vesszük alapul. Ez azonban megítélésünk szerint nem minden esetben vezet eredményre, mivel egy szervezetben kialakult „jól teljesítő" nem biztos, hogy az adott iparágban is jónak vagy kiválónak számít. Így torz képet adhat, és egy téves teljesítménymodellhez vezethet. A feladatorientált (Input) irányzat ezzel ellentétes megközelítést alkalmaz, azaz a kompetenciákat nem az egyéni adottságok határozzák meg, hanem a munkakörhöz tartozó feladatok hatékony teljesítése bizonyítja. Egy szervezet sikerességének szempontjából nem a személyiségjegyeket, hanem a munkaköri teljesítményt helyezi előtérbe (Karcsics, 2011). Quinn a feladatorientált (Outcome) megközelítést képviseli, és a vezetők hatékony működését abban látja, hogy az ellentmondásokat milyen sikerességgel képesek megoldani (Pató, 2006). Quinn szerint fontos kérdés, hogy a vezető szervezeten belüli dolgokra helyezi a hangsúlyt, vagy a külső relációk a fontosak, továbbá a feladatok végrehajtása, vagy az alkalmazkodóképesség a hangsúlyosabb (Szintay, 2003).

A vizsgált vezetői szerepekkel kapcsolatos megközelítéseket a 2. táblázatban értékeltük az alapján, hogy outcome vagy input megközelítéshez tartoznak-e, milyen dimenziók/értékelési kritériumok jellemzik, továbbá a vállalati cselekvésminták/fő fókuszt hogyan értékelik. Kutatásunk során az outcome megközelítést tartjuk megfelelőnek, mivel így nyílik lehetőség arra, hogy a vezetőket ne személyiségjegyeik, hanem tényleges munkahelyi teljesítményük alapján értékeljünk.

2. táblázat Vezetői szerepek

Vezetői modellek	Outcome megközelítés	Input megközelítés	Vizsgált dimenziók/ értékelési kritériumok	Cselekvésminták/fő fókusz
Henry Mintzberg (Mintzberg, 2010)		x	A vezetői szerepek hármas csoportosítását valósítja meg, így pedig személyközi, információs és döntési szerepeket azonosít.	Arra keresi a választ, hogy a vezetőnek milyen szerepeket kell betöltenie. A szerepelvárások függenek attól, hogy a vezető a hierarchia mely szintjén áll, vagy milyen szervezetben dolgozik.
John Kotter (Kotter, 2012)		x	Vezetést és menedzsmentet külön fogalomként kezeli, amelyek egymást kiegészítő tevékenységek.	Menedzser – jól csinálja a dolgokat Leader – jó dolgokat csinál
Dian Hosking (Hosking, 1988)		x	A leadership általánosított feladata az alkotás, termelés, újratermelés, átalakítás körforgásának biztosítása indirekt és direkt tevékenységek mentén.	A menedzsert a helyzet racionális értékelése, szisztematikus fejlesztése, a szükséges erőforrások összerendezése jellemzi.
Abraham Zaleznik (Zaleznik, 1992)	x		Menedzser – leader szereposztást követi.	A menedzser korlátozza a választási lehetőségek számát, míg a leader folyton új lehetőségeket, megközelítéseket keres. A vállalati célokat a menedzser elfogadja, de a leader alakítja őket. A menedzser kapcsolata kevésbé emocionális, a leader ennek az ellenkezője, személyközi kapcsolata érzelmekkel dúsított.
Richard Boyatzis (Goleman et al., 2003)		x	Menedzsmentmodelljében három dimenziót különített el: kompetenciacsoportok, menedzseri funkciók, szervezeti környezet elemei.	A kompetenciák egy személy alapvető, meghatározó jellemzői, melyek okozati kapcsolatban állnak a kritériumszintnek megfelelő kiváló és hatékony teljesítménnyel.
Quinn (Quinn et al., 2015)	x		Nem vagy-vagy típusú jellemzés, hanem a vezetőben mindegyik tulajdonság valamilyen mértékben jelen van. Négy elkülönített modellt határozott meg, mindegyik két vezetői szerepet tartalmaz.	Arra keresi a választ, hogy milyen irányultságú a vezető gondolkodása. Ez lehet a szervezeten belülre vagy a környezetre (partnerek, versenytársak) fókuszáló. Továbbá a nyitottság, az offenzív/adaptív stratégiák a jellemzők, vagy a koncentráltság, meghatározott irányok és projektek szisztematikus működtetése dominál (Szintay, 2003).

Elemzéseinket követően a Cameron – Quinn versengő értékek modellt választottuk, mivel lehetőséget biztosít nemcsak a szervezeti kultúra, hanem a vezetési stílus meghatározására is és a két terület összekapcsolása könnyen megvalósítható. További előnye, hogy funkcionális, megfelelően alkalmazható jelen kutatásunk céljait és az esettanulmányt figyelembe véve. A módszer többféle értékelési megközelítést biztosít és lehetőséget teremt a jelenlegi és a vágyott kultúra egyidejű beazonosítására is. Ez azért is fontos, mivel így a stratégiai gondolkodás elemzése is elvégezhető. A modell képes arra, hogy meghatározzuk a kultúratípusok erősségét és a szervezeti tulajdonságok közötti kongrueniát. A Cameron – Quinn által megteremtett keretrendszer és a vezetői szerepek vizsgálata jól egészíti ki a szervezeti kultúra felmérését, így pedig támogatva vizsgálatunk komplexitásának csökkentését. A vizsgált vezető az eredményekkel jól jellemezhető, annak minden fontos tulajdonságát feltárva. Segítségével a szervezetikultúra-felmérés rövid idő alatt végrehajtható, és képes mind kvantitatív, mind kvalitatív elemek feldolgozására.

A Cameron – Quinn által kidolgozott OCAI (Organizational Culture Assessment Instrument) kérdőív négy kultúratípusra vonatkozóan hat dimenzió szerint végzi a felmérést. Ezek magukba foglalják a szervezetre jellemző domináns karakterisztikát, az irányítást jellemző vezetési stílust, a szervezetet összetartó erőt, a stratégiai hangsúlyokat és siker kritériumokat (Cameron & Quinn, 2011). Az OCAI kérdőív azon túlmenően, hogy segítséget nyújt a domináns kultúra megállapításában, fontos kutatásunk későbbi fázisa szempontjából, hogy megmutatja, a szervezeten belül mennyire uralkodik összhang (Balogh et al., 2011).

Információbiztonság és a felhőalapú rendszerek

A vállalatok működését támogató informatikai rendszerek stabilitását és biztonságát, valamint a felhasználók által érzékelt elérhetőségét az üzemeltetésért és információbiztonságért felelős szervezetek közösen teremtik meg, melyeknek egymástól függetlennek kell lenniük annak érdekében, hogy a biztonsági kontroll megvalósulhasson. Azonban nagy szerepet kap a felhőalapú megoldások használata, mely egyik eszköze lehet a rendelkezésre állás és a skálázhatóság további javításának. A virtuális környezetek, melyek a felhőrendszerek alapját képezik, lehetőséget terem-

tenek, hogy a vállalatok az aktuális igényeknek, valamint az igénybevételnek megfelelő és azokat kiszolgálni képes infrastruktúrát tudjanak rendelkezésre bocsátani saját működésükhöz ügyfeleiknek, vagy igénybe venni külső szolgáltatótól (Grace, 2010). A felhőmegoldások azzal az ígérettel jelentek meg, hogy az infrastruktúrát, alkalmazásokat olyan formában teszik elérhetővé, mint amilyenre korábban nem volt példa (Sultan, 2010). Melynek lehetőségét az elosztott, felhasználásalapú erőforrás rendelkezésre bocsátása jelentette (Beloglazov, 2013). E szolgáltatások alapvetően új megközelítést és működési modellt tesznek lehetővé a szervezetek számára, ami akár magasabb rendelkezésre állást és/vagy csökkenő költségeket is eredményezhet a méretgazdaságosságból fakadóan (Educause, 2009). Ugyanis nincs szükség saját eszközök vásárlására, fenntartására, továbbá saját üzemeltetési csapat alkalmazása se indokolt, mivel a beruházásokat és működtetési feladatokat a felhőszolgáltató elvégzi. Az ügyfeleknek csupán azért a szolgáltatásért kell fizetniük, amit ténylegesen igénybe vesznek. A használat mértéke pedig rugalmasan (on-demand) változtatható, így alkalmazkodva az igényekhez. Ez óriási előnyt jelenthet, mivel az információtechnológiai beruházásokra szánt forrásokat a vállalatok profiljukhoz jobban illő és az ügyfelek elégedettséget növelő kezdeményezésekre fókuszálva tudják elkölteni (Spilák & Kosztyán, 2013). A felhőszolgáltatások képesek időt és költséget megtakarítani, valamint hatékonyabbá tenni a mindennapi működtetést (Rittinghouse & Ransome, 2009; Kavis, 2014). Négy fő csoportra bontjuk őket annak függvényében, hogy az erőforrásokat a közösség együttműködve biztosítja (közösségi felhő) (Zhao et al., 2014), egy harmadik fél nyújtja (publikus felhő), házon belül épült ki (privát felhő), vagy pedig ezek kombinációja valósul meg (hibrid felhő) (Goyal, 2014). Számos szakember és kutató (pl.: Wienman (2012), Botta (2016), Rittinghouse & Ransome (2009), Chawla & Sogani (2011), Buyya et al. (2013), Agrawal et al. (2012)) úgy véli, hogy az IT jövője a publikus felhő, függetlenül a szükséges kapacitásoktól és vállalati mérettől (Weinman , 2016). A privát és publikus felhőszolgáltatások közötti gazdasági különbség abban mutatkozik meg, hogy a felmerült költségek fixek vagy felhasználásalapúak-e (Weinman, 2015). A publikus felhőszolgáltatásoknak költséghatékonyabb működést kellene elérniük a privát megoldásoknál, azonban a valóságban ez a kérdés jóval komplexebb, mint hogy ezt egyértelműen ki lehessen jelenteni. A kis- és középvállalkozások, sőt akár néhány nagyobb szervezet számára a publikus felhő lehet a legjobb választás. Vannak azonban ellenpéldák is, amikor a nagyvállalatok publikus szolgáltatótól saját infrastruktúrára történő költözéssel megtakarítást értek el (pl.: Instagram felvásárlását követően a Facebook saját privát felhőjébe történő átmozgatása esetén). Azonban nem szabad figyelmen kívül hagyni a hibrid megközelítésben rejlő lehetőségeket, amely a publikus, a privát és közösségi felhőmodelljét ötvözi. A vállalatok így a felmerült kapacitás- és szolgáltatásigényeiket a stratégiai, biztonsági és bizalmassági kritériumokhoz igazítva tudják kiszolgálni különböző felhőszolgáltatások egyidejű igénybevétele mellett (Puthal et al., 2015; Chou, 2015; Weinman , 2016). Két kritikus kérdéskört azonban mindenképpen mérlegelni kell e megoldások alkalmazásakor. Egyrészt a felhőalapú szolgáltatások biztonságával, rendelkezésre állásával, integritásával kapcsolatos problémák figyelembevétele (Ali et al., 2015) (pl.: az 2017-ben az Amazonnál felmerült hiba még az Apple által üzemeltetett iCloudra is kihatással volt), valamint a szervezet adatainak felhőbe mozgatásakor szükséges kockázatelemzés elvégzése elengedhetetlen. A védelmi mechanizmusok és intézkedések ellenére a felhasználók továbbra is szkeptikusan tekintenek a felhőre (Mathur & Purohit, 2017). A szolgáltatók nem tudnak lépést tartani az új technológiákkal és kihívásokkal, így gyakoriak a biztonsági incidensek (Liveri & Skouloudi, 2016). Az információbiztonsági érettségi modelleket vizsgálva (pl.: ISM3, IBM-ISF, NIST CSEAT IT SMM, Gartner Security Maturity Model, SUNY ISI, SSE-CMM, INFOSYS IT Security Maturity Model, Cyber Security Model stb.) megállapítható, hogy a hangsúly a technikai alapú biztonsági kontrollokra helyeződik, míg a nem technikai megoldások háttérbe szorulnak (Karokola et al., 2011). Tehát a biztonsági szakemberek még mindig a védelmi eszközökben látják a megoldás kulcsát, és nem a szervezeti intézkedések, tudatosság kialakításában. A biztonsági incidensek felmerülésekor a bekövetkezés gyakoriságát, hatását és kiváltó okát vizsgálják még az előtt, hogy kidolgoznák a lehetséges jövőbeni védelmi intézkedéseket (Ransbotham et al., 2012). Azonban a vállalatok döntő részénél problémát jelent, hogy az incidenseket nem detektálják, illetve nem rendelkeznek részletes riportokkal (Dekker et al., 2013). Ennek kritikussága tovább növekszik annak függvényében, hogy az Európai Unió szorgalmazza a felhőmegoldások használatát a vállalati környezetben, felismerve annak pénzügyi és gazdasági előnyeit (Dekker et al., 2013). A 2013-as Cybersecurity Strategy of European Union tanulmány igyekszik választ adni a fenti problémákra, mivel számos kezdeményezés mellett komoly hangsúlyt fektet a tudatosságra, a biztonsági fenyegetettségek időbeni kommunikációjára és információmegosztásra (Cavelty, 2013). Barack Obama 2013. szeptember 12-én a létfontosságú infrastruktúrák információbiztonsági irányelvének részeként szintén a cyber biztonsági információmegosztás jelentőségét hangsúlyozza (Boukalas, 2014). De a teljes nyilvánosságra hozatallal akár ellentétes hatást lehet elérni, azaz képes felgyorsítani a támadás térnyerését a megcélzott populáción belül, valamint növeli a „first attack" lehetőségét a sérülékenység közzétételét követően (Mitra & Ransbotham, 2015).

A felhőkörnyezetek flexibilitása és skálázhatósága hátrány is lehet biztonsági szempontból, mivel az erőforrások és az adatok magas koncentrációja ígéretes célponttá teszi ezen szolgáltatásokat (Catteddu & Hogben, 2009). Ezért egy vállalat adatainak felhőbe történő vitele esetén nem kerülhető meg a kockázatelemzés annak ellenére, hogy 2009 óta a felhőmegoldások piaca nagyban megváltozott, a szolgáltatók érettebbé váltak, a felhasználók biztonság tudatossága javult (Dekker & Liveri, 2015). Az ENISA által kiadott Benefits, risks and recommendations for information security tanulmány szabályozási–szervezeti, technológiai, jogi, valamint nem felhőspecifikus kockázati kategóriák alapján vizsgálja a felhőrendszereket annak érdekében, hogy a vállalatok átfogó képet kapjanak e technológiák korlátjairól (Catteddu & Hogben, 2009). A kockázatok azonban vállalatonként eltér-

hetnek, mivel nagyban függnek a szolgáltatótól, a tárolt adatoktól, valamint folyamatoktól (Dekker & Liveri, 2015). A kötelező biztonsági standardok képesek elősegíteni/kikényszeríteni a minimális biztonsági kontrollt, ami kritikusan fontos, mivel a szervezeteknek nemcsak magukat, hanem a rájuk bízott adatokat is meg kell tudniuk védeni. Tisztában kell lenni azzal, hogy a standardok megalkotói nem tudnak mindenre kiterjedő és elég részletezettségű kontrollt létrehozni, mivel az információs technológiák gyorsan fejlődő, komplex tényezők és rengeteg környezeti sajátossággal rendelkeznek (Lee et al., 2016). A döntési és statikus játékteóriákat is alkalmazzák annak érdekében, hogy a szakemberek képesek legyenek felismerni és jellemezni a hackerek és a vállalatok stratégiáját. Azonban még így sem lehetséges a kockázati környezet dinamikáinak teljes kezelése, amely kiemelt eleme az olyan modern és elosztott informatikai rendszereknek, mint a felhőmegoldások (Gao et al., 2013). A biztonsági incidens gyanúja, vagy bekövetkezése esetén lefolytatott forensics vizsgálatok segítenek abban, hogy az események körét, az ügyfelek érintettségét meg lehessen határozni. A felhőrendszerek esetén e vizsgálatok bonyolultabbak, mint a nem elosztott megoldásoknál (Liveri & Skouloudi, 2016). A vizsgálat komplexitása függ a szolgáltatási modelltől (Infrastructure as a Service, Platform as a Service, Software as a Service, Storage, Database, Information, Process, Application, Integration, Security, Management, Testing-as-a-service), továbbá az igénybevétel módjától (privát, publikus, hibrid vagy közösségi felhő) (Liveri & Skouloudi, 2016). Mindezért indokoltnak tartjuk, hogy a szervezeti, informatikai és biztonsági területeket együttesen vizsgáljuk. Korábbi kutatásunk rámutatott arra, hogy a szervezetek döntő része rendelkezik minimális információbiztonsággal, valamint a szervezeti kultúra és információbiztonság között kapcsolat fedezhető fel (Spilák & Kosztyán, 2013). A terület mélyebb vizsgálata azonban képes további hasznos kapcsolatokra rávilágítani, valamint segíteni azok megértését.

A vizsgálat során alkalmazott modell és kapcsolatok

A kutatás során arra törekedtünk, hogy a szervezeti kultúra, vezetői szerepek, információbiztonsági kiválóság és felhőalapú megoldások közötti relációk meghatározását egy olyan modell segítségével végezzük el, mely képes a területek közötti kölcsönhatások feltárására. A modell szervezeti kultúra és vezetői szerepek részét a korábban már említett Cameron – Quinn versengő értékek modellje adta. Az információbiztonsági kiválóság meghatározását olyan modellek pl. Buecker et al. (2014), Scholtz et al. (2016), Sjelin & White (2016), Bowen & Kissel (2017), Barrett (2018) értékelése előzte meg, melyek kiválasztásakor szempont volt, hogy ne csak egy specifikus területet vizsgáljanak az információbiztonságon belül, hanem szélesebb – akár a menedzsment – aspektust is figyelembe vegyék. Ezért értékelésünkkor (lásd 3. táblázat) öt tényezőre fókuszáltunk, mint az információbiztonsági területekre, fenyegetettségek felismerésére, felelősségek meghatározására, információbiztonság menedzsmentjére, valamint a fő kritériumok definiálására.

A 3. táblázatban összesített adatok alapján az elemzett kutatások mindegyike foglalkozik a fenyegetettségek felismerésével annak érdekében, hogy meg tudják határozni hatásukat és bekövetkezésük valószínűségét. Jól látható táblázatunkban, hogy csupán ennek a területnek a vizsgálata nem elég, ezért egyéb területeket is bevontak (pl. fizikai,

3. táblázat Információbiztonsági modellek dimenziói

Érettségi modell	Információbiztonsági kiválóság				Vizsgált dimenziók/Fő értékelési kritériumok
	Területek	Fenyegetettségek felismerése	Meghatározott felelősségek	Információbiztonság menedzsment	
INFOSYS IT Security Maturity Model (Narasimhalu et al., 2004)	x	x	x		Három dimenzió alapján vizsgálják a szervezeteket: infrastruktúra, IT biztonsági intelligencia és a folyamatok biztonsága. Ez alapján történik meg az egyes érettségi szintekbe való besorolás.
Towards An Information Security Maturity Model for Secure e-Government Services: A Stakeholders View (Karokola et al., 2011)	x	x			Több tényező vizsgálatának segítségével sorolja a szervezeteket az egyes érettségi szintekbe, így figyelembe veszi: adminisztratív és vezetői, tudatossági, etikai és kulturális, jogi és szerződéses folyamatok, szoftvermegoldások területeket.
Information Security Model (Saleh, 2011)	x	x	x	x	A biztonságot egy szervezetben a szervezet irányítása, a szervezet kultúrája, a rendszer architektúrája és a szolgáltatásmenedzsment befolyásolja.
Information Security Management Maturity Model (O-ISM3) (The Open Group, 2011)	x	x	x	x	Hangsúly a folyamat integráltságon. Az egyes érettségi szervezetek méretének, erőforrásainak, fenyegetettségeinek, ezek hatásainak, kockázatvállalási készségüknek, gazdasági szektornak megfelelően kell alakítani.
IBM Information Security Framework (IBM-ISF) (Buecker et al., 2014)	x	x		x	Alapját a Gap analízis adja. A középpontba a személyeket, adatokat, alkalmazásokat, az infrastruktúrát, a biztonsági intelligenciát és analízist helyezi. Ezen felül definiál egy érettségi modellt.
Cyber Security Capability Assessment (Hansen, 2016)		x		x	A szabályozottság és a cyber biztonság national aspektusú vetületét vizsgálja elsősorban.
Gartner: ITScore for Information Security (Scholtz et al., 2016)		x	x	x	Menedzsmenteszközök és megvalósított funkcionalitás mentén értékel.
Community Cyber Security Maturity Model (CSMM) (Sjelin & White, 2016)		x		x	A közösségi erőfeszítést és tudásmegosztást helyezi előtérbe.
Program Review for Information Security Management Assistance (PRISMA) (Bowen & Kissel, 2017)		x		x	Kiemelt hangsúlyt fektet a dokumentáltságra.
Framework for Improving Critical Infrastructure Cybersecurity (Barrett, 2018)		x		x	Elsődleges fókusz az azonosításon, védelmen, detektáláson, válaszadáson és visszaállításon van.

logikai, humán biztonság, felelősségek stb.). Itt azonban két táborra lehet osztani a feldolgozott tanulmányokat (lásd 3. táblázat), mivel egy részük pl. Narasimhalu et al. (2004), Karokola et al. (2011), Buecker et al. (2014) mélyebb informatikai vizsgálattal folytatta és kitért az egyes területekre, azok felépítésére és sajátosságaira. Mások pl. Saleh (2011), The Open Group (2011), Hansen (2016), Scholtz et al. (2016), Sjelin & White (2016), Bowen & Kissel (2017), Barrett (2018) azonban ehelyett inkább az információbiztonság tudatos menedzselésére helyezték a hangsúlyt és nem minden esetben merültek el a technikai részletekben. Az információmegosztás jelentősége az utóbbi évek kutatásaiban pl. Scholtz et al. (2016), Sjelin & White (2016), Bowen & Kissel (2017), Barrett (2018) jelenik meg hangsúlyosan, azonban ennek számos előnye mellett néhány negatív hatása is lehet, mint például felgyorsítja a támadás térnyerését a megcélzott populáción belül, valamint növeli a „first attack" lehetőségét. Megjelenik a szervezeti kultúra, illetve az irányítás mint befolyásoló tényező, de együttes vizsgálatuk csak részlegesen történt meg és nem foglalkoztak a szervezeti kultúra és vezetői szerepek pontos beazonosításával, a felhőalapú megoldások információbiztonságra gyakorolt hatásainak feltérképezésével. Az információbiztonsági kiválóságot a területek, fenyegetettségek felismerése, felelősségek meghatározása és az információbiztonság-menedzsment elemekre bontottuk fel, építve a korábbi kutatásokra, de bővítve azokat annak érdekében, hogy a korábban nem vizsgált kapcsolatokat képesek legyünk beazonosítani és értelmezni.

A felhőalapú megoldások alkalmazásának meghatározását olyan modellek értékelésére alapoztuk pl. Mattoon et al. (2011), Guangming et al. (2017), amelyek nem csupán technikai vagy technológiai aspektusból vizsgálták e szolgáltatásokat, hanem például információbiztonságra vagy az IT-szervezetre gyakorolt hatásaikat is értelmezték.

A vizsgált felhőmegoldásokkal kapcsolatos megközelítéseket a 4. táblázatban értékeltük öt tényező figyelembevételével, mint felhőmodell, üzemeltetés, szolgáltatásmodell, az információbiztonság-menedzsment, valamint a fő értékelési kritériumok definiálását.

A 4. táblázatban összesített modellek döntő többségének középpontjában a szervezet digitalizáltsága, az informatikai és a felhőképességek szerepelnek pl. Mattoon et al. (2011), Drogseth (2011), Conway & Curry (2012), Weiss et al. (2013). Az érettséget kritériumok kombinációjaként határozzák meg és sorolják be a szervezeteket érettségi

4. táblázat Felhőmegoldásokkal kapcsolatos modellek dimenziói

Érettségi modell	Felhőalapú megoldások alkalmazása				Vizsgálati dimenziók/fő értékelési kritériumok
	Felhőmodell	Üzemeltetés	Szolgáltatásmodell	Információbiztonság-menedzsment	
Oracle: Cloud Computing Maturity Model Guiding Success with Cloud Capabilities (Mattoon et al., 2011)	x	x	x	x	A szervezet érettségét a stratégia, architektúra, infrastruktúra, információk, üzemeltetésmenedzsment, projektportfólió, szervezet és irányítás értékelésével határozza meg.
The Road to The Responsible Cloud (Drogseth, 2011)	x	x	x		Az időszakos fejlődés és a menedzsment kettőse alapján értékeli az egyes érettségi szinteket.
Managing Cloud Computing: A Life Cycle Approach (Conway & Curry, 2012)	x	x		x	Life cycle management segítségével kívánja kontrollálni nemcsak a felhő szolgáltatások bevezetését, hanem a publikus felhő mindennapi működését is.
Towards a Consumer Cloud Computing Maturity Model - Proposition of Development Guidelines, Maturity Domains and Maturity Levels (Weiss et al., 2013)	x	x		x	A felhőmodellek domainjeit szervezeti és technikai csoportokra osztja. Kitér a szabályozásra, biztonságra, szervezeti készültségre, folyamatokra, infrastruktúrára és az üzemeltetés menedzsmentjére.
Cloud Maturity Model (Duarte & Mira da Silva, 2013)		x	x		Felhőérettségi modell alapját a kiszervezési életciklus és a CMMI (Capability Maturity Model Integration) képezi.
Cloud Computing With a Model Futuristic Maturity (Nagaraj & Sathish kumar, 2015)	x	x	x		Fázismegközelítést javasol, valamint öt kulcs komponenst határoz meg: konszolidáció, virtualizáció, automatizálás, felhasználás és felhő.
Cloud Data Governance Maturity Model (Guangming et al., 2017)	x	x	x	x	Az adatkezelés érettségének vizsgálatára összpontosít a felhőmegoldásokkal kapcsolatosan.
Enterprise Cloud Adoption - Cloud Maturity Assessment Model (Conway et al., 2017)		x		x	11 kulcskomponenst azonosít, mely hatással van a felhőmegoldások bevezetésére és használatára.
Maturity Level of Cloud Computing at HCT (Alqassemi et al., 2017)	x	x			Szolgáltatásorientált architektúramegközelítést alkalmaz az érettségi modell mérésében.
FHNW Maturity Models for Cloud and Enterprise IT (Grivas et al., 2018)	x	x	x	x	Nem a szokásos felhő érettségimodell-értékelést követi, azaz milyen felhőszolgáltatást használnak, vagy a bevezetés milyen szakaszában áll a cég. Hanem arra fókuszál, hogy miért használják a felhőmegoldásokat, és ez miképp változtatja meg az IT pozícióját és feladatait.

szintekbe (tanulmányonként négy-kilenc szint). A 4. táblázatban összegyűjtött adatok alapján arra a következtetésre jutottunk, hogy a legszignifikánsabb problémák nem a technológiai megvalósításban keresendők, hanem a vezetési és szervezeti kihívásokban rejlenek. 2017-től kerültek előtérbe az üzleti területeknek, az IT működésének, valamint a felhőmegoldások alkalmazásának összehangolására irányuló törekvések pl. Guangming et al. (2017), Conway et al. (2017), Alqassemi et al. (2017), Grivas et al. (2018). Így a modellek már képesek segítséget nyújtani a szervezetek számára a fenti területeket érintő döntések meghozatalában is. Ezáltal támogatják a felhőmegoldások jobb integrálhatóságát és a szervezetek digitális átalakítási folyamatát. Fontos kiemelni, hogy egyetlen modell sem képes megmondani, hogy miképpen használja egy szervezet e szolgáltatásokat, mivel alkalmazásuk formája és lehetőségei függenek a szervezet sajátosságaitól. Munkánk során elemzett kutatások eredményeit felhasználva a felhőalapú megoldásokat a felhőmodellek, üzemeltetés, szolgáltatások és információbiztonság-menedzsment elemekre bontottuk fel.

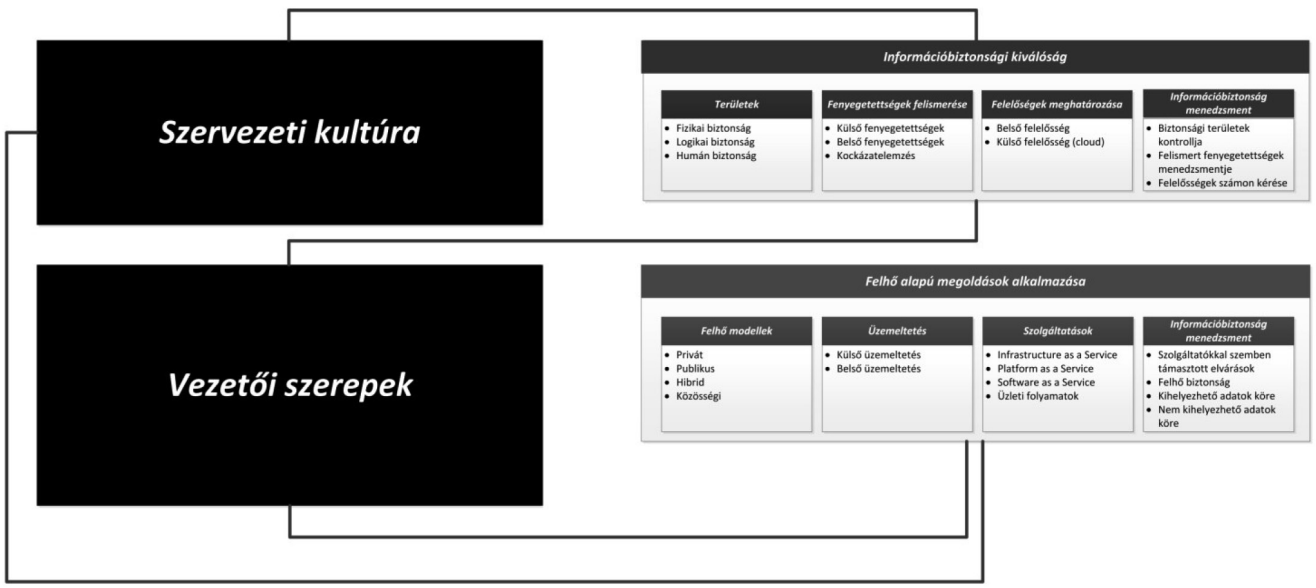
Az információbiztonsággal és a felhőmegoldások alkalmazásával foglalkozó modellek esetében is elmondható, hogy együttes feltérképezésük nem történt meg. Egyes tanulmányok pl. Buecker et al. (2014), Scholtz et al. (2016), Sjelin & White (2016), Bowen & Kissel (2017), Barrett (2018) már igyekeztek más tudományágakat (pl.: menedzsmenteszközök, tudásmegosztás, dokumentummenedzsment) is bevonni vizsgálatukba, de ez csupán apró részterületekre irányult. Kutatásunk során olyan modellt alkottunk, mely ezt a hiányzó kapcsolatot képes megteremteni a szervezeti kultúra, vezetői szerepek, információbiztonság és felhőmegoldások alkalmazása között. Azaz nemcsak egy kutatási szakmai terület kiegészítése, hanem három egymástól eddig függetlenül kezelt tudományág átfogása valósul meg. Az egyes területeket felépítő elemek ábrázolására létrehoztunk egy modellt (1. ábra), mely tartalmazza a szervezeti kultúra, vezetői szerepek, információbiztonsági kiválóság és felhőalapú megoldások alkalmazását.

Az 1. ábrán a szervezeti kultúrát, valamint a vezetői szerepeket nem bontottuk tovább részterületekre, mivel ennek részletezését már elvégezték helyettünk (Cameron & Quinn, 2011), így az általunk létrehozott új struktúrára, az az információbiztonsági kiválóságra és felhőalapú megoldások alkalmazására kívántunk koncentrálni. A biztonságot négy további területre osztottuk fel annak érdekében, hogy vizsgálni tudjuk a technikai területeket, a fenyegetettség-, a felelősség-, valamint a menedzsmentaspektust is. A felhő vizsgálatát szintén négy részegységre bontottuk fel, melyek kitérnek a felhő szolgáltatási modelljére, üzemeltetésre, az igénybevett szolgáltatás típusára és a menedzsmentre. Kutatásunk későbbi fázisában arra keressük majd a választ, hogy a kapcsolatok és hatások milyen irányúak, mivel azt feltételezzük, hogy nemcsak a kultúra és a vezetői szerepek hatnak az alkalmazott információbiztonsági megoldásokra, valamint a felhőszolgáltatások igénybevételére, hanem az információbiztonság és a felhő használata is szervezetet és vezetést formáló erejű.

Esettanulmány

Esettanulmányunkban egy magyarországi telekommunikációs vállalat működését vizsgáltuk, valamint dolgoztuk fel. Így egy olyan iparágba nyertünk betekintést, mely élen jár a modern technológiák alkalmazásában, valamint működése és nyújtott szolgáltatásai erősen építenek e megoldásokra. Célunk volt, hogy feltárjuk, milyen változásokat okoz a szervezet kultúrájában és vezetésében egy-egy információbiztonsági kérdés felmerülése és kezelése, valamint milyen hatással van a felhőalapú megoldások alkalmazása, különös tekintettel a privát és publikus felhő jelentette különbségekre. Természetesen nem mehetünk el amellett, hogy feltehetően a kultúrától és a vezetői szerepektől a biztonsági terület fejlettsége, az alkalmazott megoldások, továbbá a felhőszolgáltatásokra való nyitottság is függ. Tehát az egymásra hatás nem egyirányú, így a teljes reláció vizsgálata javasolt. A magyar piacon tevékenykedő, több mint 500 főt foglalkoztató telekommunikációs vállalatok száma

1. ábra A kutatási modell



alacsony, valamint a meghatározó szereplők mind leányvállalatok, így működésük és felépítésük mutat hasonlóságokat. Elmondható, hogy az esettanulmányunk megállapításai nem általánosíthatók teljes mértékben, azonban számos tekintetben igaznak bizonyulnak a szektor egészére.

A kutatási kérdések

- K1: Milyen biztonsági elvárásokat támasztanak a vállalatok a felhőalapú alkalmazásokkal szemben?
- K2: Hogyan hat a felhőalapú működés az információbiztonság menedzsmentjére?
- K3: Milyen változásokat okoz a szervezeti kultúrában és a vezetői szerepekben az információbiztonsági kérdés felmerülése és kezelése?
- K4: Milyen változásokat eredményez a szervezeti kultúrában és a vezetői szerepekben a felhőalapú megoldások alkalmazása?

A kutatási kérdésekkel kapcsolatos feltételezéseink

- A telekommunikációs szektor kiemelt hangsúlyt fektet az információbiztonságra, mivel az mindennapi működésük szerves részét képezi. Eszközeik fejlettsége és egyben sérülékenysége akár hozzáférést biztosíthat ügyfeleik adatvagyonához is, melynek bekövetkezte komoly negatív hatással lenne a szervezet piaci pozíciójára. Ezért feltételezzük, hogy az információbiztonsági kiválóság fejlett.
- A felhőalapú megoldások alkalmazása aktív, része a mindennapi működésnek, ezért jól elkülöníthető területekkel rendelkezik.
- A telekommunikációs vállalatok döntő többségénél nem tisztán publikus vagy privát felhőmegoldásokkal fogunk találkozni, hanem a két területet egyszerre alkalmazó hibrid felhővel.
- Az információbiztonság menedzseléséért felelős terület aktívan részt vesz a felhőmegoldások értékelésében, kiválasztásában és a szolgáltatások biztonságának folyamatos ellenőrzésében. Továbbá meghatározza azon adatok és alkalmazások körét, melyek kihelyezhetők publikus felhőbe, és melyek azok, amelyeket csak házon belülről lehet biztosítani.

Mintavétel a kvalitatív szakaszban

Az adatgyűjtés során kvalitatív módszert használtunk, mivel célunk volt, hogy az IT-szervezet gondolkodásmódját és várható reakcióit mélyebben megértsük. A strukturált interjúkat az IT és az információbiztonság menedzsmentjéért felelős területeket irányító összes menedzserrel és direkt riportjukkal (92 interjú alany) lefolytattuk annak érdekében, hogy teljes képet kapjunk a szervezet állapotáról. A vizsgálatot 2018. május – augusztus között végeztük el és megfigyelési egységnek az IT egyes részterületeit tekintettük. Az 5. táblázatban összefoglaltuk a vizsgálatba bevont területeket, azok felelősségi körét, valamint a csapat méretét.

Az interjúk során a pontos adatrögzítés érdekében hangfelvételt készítettünk az interjúalanyok jóváhagyásával annak érdekében, hogy későbbi adattisztítás során a pontos válaszokat tudjuk feldolgozni. Az összegyűjtött adatokat területi egységenként aggregáltuk, figyelembe véve az azonos tartalmú válaszok számosságát, így kialakítva az egyes csoportok véleményét.

Adatelőkészítés a kvalitatív szakaszban

Az interjúkat előre meghatározott vázlat alapján folytattuk le, mely kitért a következő területekre:

1. kultúra és vezetői szerepekkel kapcsolatos kérdésekre:
   a. Mik a szervezet főbb jellemzői?

5. táblázat A kvalitatív strukturált interjú mintajellemzői (N=92)

Azonosító	Terület	Felelősség	Terület mérete
VA1	Alkalmazás üzemeltetés	A vállalatnál működő alkalmazások üzemeltetése, támogatása mind belső, mind pedig külső erőforrások igénybevétele mellett. Alkalmazásokhoz kapcsolódó monitoringfeladatok ellátása, továbbá reaktív – proaktív hibaelhárítás.	15 fő + külső vendorok
VA2	Infrastruktúrafejlesztés és üzemeltetés	A vállalat hálózat, tűzfal, szerver, storage, adatbázis, middleware mentési rendszereinek üzemeltetése és bővítések, új rendszerek üzembe helyezése.	25 fő + külső vendorok
VA3	Alkalmazásfejlesztés	Üzleti területek és alkalmazás üzemeltetés által támasztott fejlesztési igények priorizálása és kiszolgálása.	25 fő + külső vendorok
VA4	Végfelhasználó támogatás	L1 helpdesk feladatok ellátása, beleértve a beérkező hibajegyek az érintett alkalmazás és infrastruktúra L2-L3 szintek felé történő továbbítása.	20 fő
VA5	Governance	Pénzügyi koordináció, szabályozási és auditfeladatok ellátása.	5 fő
VA6	Információbiztonság	Sérülékenységi vizsgálatok lefolytatása, feltárt hiányosságok menedzsmentje az alkalmazás és infrastruktúra csapatokkal közösen. Megjelenő biztonsági kockázatok vizsgálata, értékelése és indokoltság esetén az érintett területekkel védelmi megoldás kidolgozása, bevezetése.	2 fő

b. Milyen vezetési stílus és szemlélet hatja át az egész szervezetet?
c. Milyen módon bánnak az emberekkel?
d. Mi tartja össze a szervezetet?
e. Mely területek kiemeltek a szervezeti stratégiában?
f. Mik a sikerkritériumok?

2. alkalmazott felhőmegoldások modelljeire (privát, publikus, hibrid, közösségi),
3. az egyes információbiztonsági kérdések felmerülése esetén a szervezeti kultúrára és vezetésre gyakorolt hatására,
4. információbiztonság-menedzsment feladataira a felhőmegoldások kiválasztása és igénybevétele során,
5. a vállalaton kívülre helyezhető adatok meghatározására,
6. a felhőalapú működés információbiztonságára, mely szervezeti és vezetési szemszögből is számos kérdést vet fel.

A vállalati kultúra meghatározásához az OCAI kérdőív magyar nyelvű változatát vettük alapul. Azonban képessé kellett tennünk arra, hogy ne kérdőív formában alkalmazzuk, hanem egy strukturált interjú során is be tudjuk gyűjteni a szükséges információkat. A vezetési stílus meghatározása során a nyolc vezetői szerephez tartozó kérdéseket tettük fel, majd az ezekre adott válaszok alapján határoztuk meg a szervezetre jellemzőt vezetést.

A kvalitatív adatelemzés

A strukturált interjúk segítséget nyújtanak ahhoz, hogy az irodalmi feldolgozást követően létrehozott kérdéseinket megválaszoljuk, és átfogó képet kaphassunk a kutatási problémáról. A kiértékelés részeként figyelembe vettük, hogy az interjúkon begyűjtött adatok nehezebben operacionalizálhatóak, mint kérdőívvel történő lekérdezés alkalmával, azonban e vizsgálati forma olyan „puha" információkkal is képes szolgálni, melyek kutatásunk későbbi szakaszában is felhasználhatók. Az interjúanyagok tisztítást követően álltak rendelkezésre, mely így alapját képezte a kvalitatív elemzési fázisnak. Az adatelemzéshez szükséges kódok meghatározása nem csupán a szakirodalomra támaszkodott, hanem az interjúk során felmerült új elemek is bekerültek a kódkészletbe.

Felhőalapú megoldások információbiztonsági követelményei és szervezeti hatásai (K1, K2, K4)

A szakirodalomban fellelhető, a felhőmegoldások használatát alátámasztó előnyök, azaz a könnyű skálázhatóság, rugalmasság, jó automatizálhatóság, magas rendelkezésre állás fontossága a kvalitatív eredményeinkben is megjelennek. A költséghatékonyságot azonban nem emelték ki a válaszadók, ami arra enged következtetni, hogy a rugalmasság és a stabilitás iránti igény elsődleges szempontot képvisel.

„A könnyebb működtetés, egyszerűbb számonkérés, rugalmas skálázhatóság és számos automatizálási lehetőség olyan előnyök, melyek szervezetünk számára kritikusak. A felhőmegoldások lehetőséget biztosítanak a homogén működésre és működtetésre." (VA2)

„Központilag egyszerűbb menedzselésük és elosztott kialakításukból fakadóan stabilitásuk is kimagasló tud lenni." (VA1)

Az előnyök mellett kritikus kérdés volt számukra a megfelelő felhőmodell (privát, publikus, hibrid, közösségi), a szolgáltatástípus (IaaS, PaaS, SaaS stb.), a szolgáltató kiválasztása, továbbá az üzemeltetési modell tisztázása (külső, belső).

„A piacon rengeteg megvalósulással találkozni attól függően, hogy a felhőt házon belül építik fel, vagy pedig külső szolgáltatótól vásárolják meg. Mi ennek ötvözését biztosító hibrid megoldásban látjuk az IT jövőjét." (VA2)

„Így lehetőség nyílik arra, hogy a kritikus adatokat házon belül tartsuk, de a szabadon hozzáférhető, rugalmas kapacitások elérésében rejlő előnyöket is kihasználhassuk." (VA6)

Az információbiztonság menedzseléséért felelős terület feladatai azonban átalakultak, amikor a felhő alkalmazásának lehetőségét kezdték el vizsgálni. Már nem volt ugyanis elég egy belső ellenőrző szervezetként való megjelenésük. Ehelyett tanácsadó, ellenőrző, jogi megfelelésben aktívan részt vevő és folyamatos kontrollt gyakorló szervezetté kellett válnia egy olyan környezetben, ahol nem minden esetben képes hatni a külső szolgáltatókra. A korábbi kontrollszerep tehát egy használható megoldást javasló működés felé kezdett elmozdulni, de természetesen korábbi funkciójuk sem tűnt el.

„Az információbiztonság fókusza arra irányult a külső felhőszolgáltatók megjelenése előtt, hogy rendszereinket a külvilágtól a lehető legjobb módon elzárjuk és megvédjük." (VA6)

„A menedzsment és üzemeltetés által generált új igények azonban rákényszerítettek minket a változásra, mivel a publikus felhőből kiszolgált megoldások használata számos előnyt hordozott magában, így használatuk elkerülhetetlenné vált." (VA5)

„Ahhoz, hogy meg tudjunk felelni az új szervezeti igényeknek, merőben új kompetenciák felépítésére volt szükség. Belső ügyfeleink számára segítséget kellett nyújtanunk, hogy melyek azok a felhőalkalmazások, amiket használhatnak, és melyek azok, amelyek problémát jelenthetnek hosszú távon. Ennek meghatározása önmagában azonban nem elég. Definiálni kellett ugyanis azon adatköröket, amelyek a publikus felhőbe ideiglenesen vagy véglegesen „kihelyezhetők" és azokat, amelyek csak a belső privát megoldásban tárolhatók." (VA6)

A megjelenő új feladatok ellátása azonban indokolttá tette a létszám növelését az információbiztonság területén. Ehhez a folyamathoz azonban időre volt szükség, mivel a menedzsment nem minden esetben látta, vagy fogadta el ennek szükségességét.

„Csapatunk létszámát csak azután tudtuk növeli, hogy a belső üzleti ügyfelek önállóan olyan felhőmegoldásokat kezdtek el használni mindennapi munkájukhoz, melyekről nem volt tudomásunk. Nem gyakoroltunk kontrollt, valamint üzletileg kritikus adatok kerültek ki szervezeten kívülre. Ezen esetek egyre gyakoribb felbukkanása ösztönözte arra a vezetőket, hogy újra pozícionáljak az

információbiztonság területét és annak szerepét a vállalati struktúrában." (VA6)

A külső felhőszolgáltatás igénybevételének feltétele volt, hogy megfeleljen a belső biztonsági elvárásoknak, jogi és szabályozási környezetnek. Nehézséget jelentett, hogy ez csak a belső szolgáltatásokra állt korábban rendelkezésre. Ezért ki kellett dolgozni azon feltételeket, standardokat, biztonsági elvárásokat, amelyek mellett használhatók a publikus megoldások. Fontos figyelembe venni, hogy e szolgáltatások esetében Európai Unión kívüli és belüli adattárolás GDPR szempontjából jelentősen eltérhet. A meghatározott elvárások között szerepelt:

- biztosítson egy elkülönített, a vállalat számára fenntartott felhőszeletet (tenant),
- történjen meg mikroszegmentáció,
- lehessen meghatározni és korlátozni az adatok tárolásának földrajzi helyét,
- legyen lehetőség arra, hogy a felhőben futó saját alkalmazások biztonsági tesztelése megvalósulhasson, kitérve a felhőszolgáltatási rétegre is.

Az ENISA 2016-os Exploring Cloud Incidents tanulmánya a standardok jelentőségét hangsúlyozta, amire való törekvés a vizsgált szervezetnél is megjelenik. Definiálták az ún. „building block"-okat, biztonsági ajánlásokat és elvárásokat, melyek használata kötelező a saját privát felhő építése, bővítése során. Az információbiztonság menedzseléséért felelős terület számára minden publikus felhőalapú szolgáltatás igénybevétele előtt kötelező ellenőrizni azok megfelelőségét, és jóváhagyásuk nélkül alkalmazásuk nem lehetséges. Annak érdekében, hogy ne csak a szabályozási szint valósuljon meg, ezért a belső hálózatból minden, korábban még nem engedélyezett felhőalapú megoldás elérése tiltott, így biztosítva a kontroll meglétét.

„Meghatároztunk három biztonsági szintet az üzemeltetési, információbiztonsági, jogi területekkel együttműködve, annak érdekében, hogy adatainkat bizalmasságuknak megfelelő rendszerben tudjuk kezelni:

1. Magyarországról kiszolgált, privát felhő: ebben az esetben az adatok nem hagyják el a vállalat adatközpontjait,
2. nemzetközi privát felhő: a kiszolgáló infrastruktúra több országban (pl.: Magyarország, Hollandia, Németország, Anglia) található, de a vállalat adatközpontjaiban,
3. nemzetközi hibrid felhő: a belső erőforrásokon túl külső publikus felhőszolgáltatókat használ a terhelés és igények függvényében." (VA5, VA6)

„Olyan korlátozásokat építettünk a belső rendszereinkbe, melyek megakadályozzák belső ügyfeleinket abban, hogy publikusan működő szolgáltatásokat vegyenek igénybe jóváhagyásunk nélkül. Erre azért volt szükség, mivel az üzleti területek esetében számos esetben tapasztaltuk, hogy a belső szabályozást megszegve használnak külső szolgáltatásokat (p.: Google Drive, Slack stb.)." (VA2)

Az interjúk során kiemelték, hogy Magyarország csak korlátozottan vesz igénybe publikus felhőszolgáltatásokat, mivel azt biztonsági és jogi oldalról aggályosnak tartják, azonban a nemzetközi privát felhő felhasználásában, valamint kiszolgálásában nagy lehetőségeket látnak.

„A GDPR-nak való megfelelésre történő felkészülésünk része, hogy megvizsgáljuk mélyebben a publikus megoldások használatának lehetőségét, de jelenleg az a döntés született, hogy nem képezik részét a magyarországi szervezet 2019-es céljainak. Azonban a nemzetközi privát felhő számos előnyt képes jelenteni számunkra. Az üzemeltetési csapatunk a nemzetközi rendszer építésének második fázisába már aktívan bekapcsolódott és stratégiailag is fontos lépést tett, mivel a bővítés részeként Magyarország biztosítja a már működő rendszer erőforrás kiterjesztésének egyik színhelyét." (VA2)

A felhőmegoldások egyértelmű hatást gyakorolnak nemcsak az információbiztonsági szervezetre, hanem megváltoztatják az üzemeltetési csapatok feladatkörét. Az on-site infrastruktúra biztosítása során szükség van a rendszerek fizikai üzemeltetését ellátó személyzet fenntartására, valamint saját adatközpontok és az azokhoz tartozó kiszolgáló szolgáltatások biztosítására (pl. áramellátás, UPS, hűtés stb.). Erre egy publikus felhő esetében – legyen az akár IaaS, PaaS, SaaS stb. – nincs szükség. Így pedig terjedésükkel negatívan fognak hatni az üzemeltetési létszámra. Az, hogy ez csupán az adatközpont, az infrastruktúra, vagy az alkalmazásüzemeltetőkre gyakorol hatást, szoros kapcsolatban van az igénybevett szolgáltatással. Az IaaS esetében az adatközponti, a PaaS során az infrastruktúra, míg a SaaS már az alkalmazásüzemeltetőket is képes érinteni.

„Be kell látnunk, hogy a publikus felhőszolgáltatások használata negatívan fog hatni a belső IT feladataira. Sok közülük feleslegessé fog válni, mivel a külső szolgáltató fogja elvégezni." (VA1)

„Nem gondolom, hogy a belső IT teljes mértékben megszűnne, mivel a felhőszolgáltatások igénybevételének számos feltétele van. Ezért abban hiszek, hogy a hibrid megoldásoké a jövő, amikor van helye egy belső szakértői csapatnak is. Azonban azt el kell fogadni, hogy az újonnan kialakult helyzethez a szakembereknek is alkalmazkodniuk kell, ha versenyképességüket fenn akarják tartani." (VA2)

Olyan munkakörök fognak felértékelődni, amelyek már sok szervezetben jelen vannak, de eddig a belső folyamatokra fókuszáltak (pl. szolgáltatásmenedzserek). Így a vezetői szint biztosan nem fog eltűnni, azonban szerepe átalakul. Azon túl, hogy számon kérni és ellenőrizni fogja a külső szolgáltatókat, koordináló szerepet is el fog látni a belső ügyfelek és a külső szolgáltatók között.

„Az igénybevett SaaS megoldásokat azonos módon kezeljük, mintha belső csapat biztosítaná, annyi különbséggel, hogy nem minden esetben tartoznak közvetlen az üzemeltetési vezetők alá, hanem ún. szolgáltatásmenedzser felel értük. Annak meghatározása, hogy mely vezetőhöz kerül a felelősség, függ

attól, hogy IaaS, PaaS vagy SaaS modellt veszünk igénybe. De a hibakezelés és KPI-ok követése azonos azzal, amit jelenleg is alkalmazunk." (VA5)

Az OCAI kérdőív segítségével összegyűjtött adatok és értékelést követően megállapítható, hogy a szervezetben adhokrácia a domináns kultúra, mely előny egy, a telekommunikációs szektorban működő vállalat esetében. Sikeréhez elengedhetetlen ugyanis a dinamikus és kreatív munkakörnyezet. Tapasztalataink alapján az alkalmazottak bátran vállalnak kockázatot annak érdekében, hogy kiemelkedő eredményeket érjenek el, valamint az innováció és kísérletezés lehetősége fontos számukra. A felhőmegoldások alkalmazásának egyik alappillére a vállalatnál tapasztalt jellemzők, azonban kutatásunk jelen szakaszában még nem mondható ki, hogy biztosan előnye van e szervezeti kultúrának az új technológiák alkalmazása terén.

A kapott eredmények (N=92) alapján kimondható, hogy egy, a telekommunikációs szektorban működő meghatározó vállalatnál a felhőalapú megoldásokat aktívan használják. Vállalatonként és működési környezetenként eltérő lehet azonban, hogy publikus, privát, hibrid vagy közösségi megoldást választanak a szervezetek. Az információbiztonság menedzseléséért felelős területeknek – annak érdekében, hogy meg tudjanak felelni a felhő által támasztott új kihívásoknak – változáson kell keresztülmenniük, melyhez hozzá tartozik funkciójuk újradefiniálása is.

Szervezeti információbiztonság (K3)

Az interjúk eredményei alapján kimondható, hogy az IT-szervezet tudatában van, valamint körültekintően tervezi a biztonsági intézkedéseket, de számos hiányosság tapasztalható vezetői és kulturális szempontból a vállalat egészét tekintve.

„Egy telekommunikációs vállalat számára elengedhetetlen, hogy ne csak saját rendszereit, hanem ügyfelei otthoni hálózatát is legyen képes megvédeni." (VA5)

„Nem engedhetjük meg azt, hogy mint internetszolgáltató veszélyeztessük előfizetőink saját gépeit és adatait, ezért a fejlesztés során minden elkövetünk azért, hogy a kihelyezett eszközeinket folyamatosan biztonsági aspektusból teszteljük, és a feltárt réseket azonnal befoltozzuk." (VA3)

„De be kell ismernünk azt is, hogy a felső vezetés és az üzleti területek nem minden esetben partnerek a biztonsági kérdésekben. Nem érzik annak jelentőségét és a versenyképességet befolyásolni képes hatásait." (VA4)

A szervezet erős a fizikai biztonság területén és ehhez kapcsolódó intézkedéseket proaktívan végzi. Logikai biztonság témakörében számos védelmi megoldást vezettek be (tűzfalak, szeparált hálózati szegmensek, IPS, IDS-eszközök). Az intézkedések egy része nem proaktív módon történik, hanem audit megfelelés céljából, vagy az audit során feltárt hiányosságok kezeléseként. A humán biztonsági oktatások vannak, de a szervezet egyes területeinek a biztonság tudatossága ennek ellenére elmarad az elvárt szinttől.

„Számos beruházást eszközöltünk az elmúlt években annak érdekében, hogy megújítsuk határvédelmünket. Ezt indokolta, hogy egyes audit vizsgálatok megállapították, hogy a korábbi megoldásaink esetében számos olyan kockázattal rendelkeztünk, amelyek nem voltak felvállalhatók." (VA2)

„Készítünk belső oktatási anyagokat, melyek célja, hogy felhasználóink biztonsági tudatosságát fejlesszék és segítsenek számukra kiszűrni a feléjük irányuló vagy rajtuk keresztül végrehajtani kívánt támadásokat. Ez egy nem könnyű folyamat, mivel a tudatosságot kiépíteni energiaigényes, azonban a megfelelő szint fenntartása még ennél is több energia befektetését követeli meg." (VA6)

A válaszadók a tervezett és rendszeresen lefolytatott, biztonsági vizsgálatokat elengedhetetlennek tartják annak érdekében, hogy a meglévő védelmi szintet fenn lehessen tartani, illetve javítása megtörténhessen. Kiemelték, hogy több alkalmazás esetében tapasztalták, hogy már nem képesek működni a támogatás alatt levő operációs rendszereken, így rákényszerítve az üzemeltetési csapatokat a nem biztonságos, elavult környezetek fenntartására.

„Alkalmazásaink egy része elavult és támogatással már nem rendelkező rendszereken képesek csak futni (pl: Windows Server 2003)." (VA2)

„Ez olyan üzemeltetési kockázatokat rejt magában, amely akár egy kritikus alkalmazás megállásához is vezethet. Ezzel a felső vezetés tisztában van, azonban az új fejlesztések, új szolgáltatások bevezetése minden esetben elsőbbséget élveznek a „karbantartó" fejlesztésekkel szemben." (VA3)

A felmérés során kiderült, hogy a szervezet végez saját vizsgálatokat, bevon külső cégeket, valamint az auditok során is történnek biztonsági tesztelések. Megkülönböztetett figyelmet fordítanak az újonnan bevezetendő alkalmazások biztonsági tesztelésére, ami nélkül nem kerülhetnek éles üzembe.

„Elengedhetetlen, hogy rendszereinket folyamatosan teszteljük, külsős, független szervezetek bevonásával annak érdekében, hogy a belső kollégák által fel nem tárt hiányosságokat, biztonsági réseket fel tudjuk ismerni és kidolgozzuk rájuk a megfelelő válaszlépéseket." (VA6)

Kiemelték, hogy tapasztalatuk alapján a szervezet akkor veszi komolyan a biztonsági fenyegetettségeket, ha korábban már átesett valamilyen krízishelyzeten (biztonsági incidensen, pl. SONY). Addig a biztonsági intézkedések és kezdeményezések alacsony prioritással rendelkeznek. Ezt a viselkedésmintát már az irodalmi áttekintés során is megerősíteni láttuk. Természetesen ez a megállapítás nem általánosítható minden szervezetre, mivel vannak kiemelkedő biztonságtudatossággal rendelkezők, de a hozzáállást nagyban befolyásolja a vezetés.

„Az információbiztonsággal kapcsolatos fejlesztésekre és intézkedésekre mindig korlátozott keretösszeggel rendelkezünk. A költések szintjét a korábbi

évekkel azonos szinten kell tartanunk annak ellenére, hogy a kihívások és fenyegetettségek nem minden évben azonosak ezen a területen." (VA1, VA2)

„Olyan esetben, mikor egy támadás, vagy tényleges incidens történt, mindenkit aktívan érdekelni kezd a Senior Vezetői szinten, hogy javítsunk a kialakult helyzeten, akár extra erőforrások (emberi, anyagi) bevonásával." (VA5)

Az információbiztonság-menedzsment az üzemeltetési csapatoktól független, önálló szervezet kell, hogy legyen az interjúalanyok elmondása szerint, amely egybevág az irodalmi kutatásunk során tapasztaltakkal.

„A kontrollt és ellenőrzést gyakorló szervezet minden esetben teljes függetlenséggel kell, hogy rendelkezzen az üzemeltetést és fejlesztést végző csapatoktól. Ellenkező esetben nem valósulna meg az őszinte és megbízható kontroll." (VA5)

Az elmúlt két évben számos szervezeti átalakuláson ment át a vizsgált vállalat, melynek egyik fókusza volt a biztonsági kihívásokra történő hangsúly helyezése. Egyértelművé vált, hogy lokálisan nincs elég erőforrás a napjainkban felmerülő biztonsági kihívások felismerésére és a szervezet időben való felkészítésére. Ezért az új fenyegetettségek azonosítását, annak követését központosították egy nemzetközi csapat formájában, és az ezzel foglalkozó személyek számát növelték.

„Nem tudtuk megvalósítani az összes rendszerünkkel kapcsolatosan felmerült új biztonsági hibák követését, monitorozását, a szervezeten belüli kommunikációját, és ami a legfontosabb, az ellenőrzését. Ennek egyrészt oka volt a kis létszámú biztonsági és governance csapat, másrészt a lokális vezetés ez irányú érdeklődésének hiánya." (VA5)

„Az információbiztonsági kérdések kezelése korábban mindig másodlagos volt. A felső vezetésen nehéz volt átvinni azokat az intézkedéseket, amelyek a belső felhasználókat korlátozták a biztonság fenntartásának érdekében." (VA4)

A vizsgált szervezetnél az átalakítással elérték, hogy a kontroll elvételével a korábban ellenállást tanúsító felsővezetői réteg már csak végrehajtó szintre került. Nem volt joguk módosítani a biztonsági elvárásokat és intézkedéseket, amelyet korábban lokális szinten meg tudtak tenni. Ellentétben a korábbi gyakorlattal, amikor az igazgatósági egyeztetéseken ebben a kérdésben az IT-vezető mindig egyedül maradt. Ez merőben új megközelítést jelentett, így lehetőség nyílt arra, hogy egységes biztonsági elvárásokat lehessen támasztani egy több országban működő nemzetközi szervezeten belül.

„A biztonsági kérdéseknek központosítása merőben új helyzetet teremtett a vezetés számára. A korábban „mi megmondjuk, mit nem lehet megcsinálni" attitűdből a „hogyan tudjuk ezt megoldani" felfogásba fordultunk át." (VA6)

A szervezeti kultúra lassan tud csak változni, de az elmúlt két évben a válaszadók elmondása alapján észlelhetővé vált az információbiztonsággal kapcsolatosan, hogy a korábbi adhokrácia típusú működésből elindult a hierarchikus irányba a központosított vezetést követően. Azt feltételezzük, hogy az információbiztonsági intézkedések a változás egyik generálói voltak. Természetesen a szervezet teljes egészét tekintve nem történt szignifikáns változás a kultúra szemszögéből, azonban biztonsági kérdésekben szabályozottabbá és kiszámíthatóbbá vált a vállalat.

„Alkalmazkodnia kellett a szervezetnek az újonnan kialakult működési formához. Ez nemcsak az emberekre, hanem a szervezetünk viselkedésére is hatott. Voltak azonban olyanok, akik nem tudtak azonosulni ezzel az új megközelítéssel, mivel számukra elfogadhatatlan volt, hogy a döntéseket a jövőben központilag és nem az országban hozzák meg." (VA2)

A feltárt eredmények igazolják azt a feltételezésünket, hogy egy, a telekommunikációs szektorban működő vállalat esetében kiemelt hangsúlyt fektetnek az információbiztonságra és aktívan tesznek azért, hogy szavatolják és fejlesszék, azonban lehetőségeik nagyban függenek a felső vezetés biztonság iránti elhivatottságától.

Következtetések

A kutatásunk eredményeképpen megállapítható, hogy az információbiztonság csak akkor kap kellő hangsúlyt, ha korábban valamilyen szignifikáns biztonsági esemény következett be. Ez alól a vizsgált telekommunikációs vállalat sem kivétel, azonban azt tapasztaltuk, hogy működése során már megjelent az információbiztonság javítása iránti igény és elvárás. Azonban ennek tényleges megvalósulására hatással van a felső vezetés biztonság iránti elkötelezettsége (K3). Az információbiztonság menedzseléséért felelős szervezet független a fejlesztést és üzemeltetést biztosító csapatoktól, az interjúalanyok elmondása szerint ez alapvető feltétele, hogy a valós kontroll megvalósulhasson (K3). A biztonsági szervezet hatékonyságának feltérképezése során érdekes meglátás volt, hogy amíg lokális szervezeti egységként működött, nem volt meg a kellő ereje ahhoz, hogy a szükséges lépéseket kikényszerítse és betartassa. Ezt felismerve a funkciót központosították, így pedig megváltoztak a korábbi vezetői szerepek, mivel már nem a helyi irányítás határozta meg a biztonsággal kapcsolatos irányokat, hanem azokat mint elvárás kapták (K3). Munkánk rávilágított, hogy a szervezet adhokrácia típusú kultúrája elengedhetetlen ahhoz, hogy a kiélezett piaci versenyben képes legyen helytállni. Az eredményorientáltság, valamint a komparatív előnyök megszerzésének vágya arra ösztönzik a vállalatot, hogy a legújabb, innovatív, hatékonyságot javítani képes, vagy költség csökkentésére alkalmas megoldásokat mint „early adapter" igyekezzen bevezetni (pl. felhőalapú szolgáltatások) (K4). De az elmúlt években érezhetővé vált a kultúra változása is annak ellenére, hogy ez egy hosszú folyamat. Az adhokrácia típusú kultúrából a hierarchikus irányba mozdult el a szervezet, mely az információbiztonság jelentőségének felértékelődésére vezethető vissza (K3). Az információbiztonság menedzseléséért felelős terület feladatai nagyban átalakultak, aktívan részt kell venniük a felhőmegoldások értékelésében, kiválasztá-

sában és a szolgáltatások biztonságának folyamatos ellenőrzésében, valamint a felhőbe kihelyezendő adatok körének meghatározásában (K2). Ez egybevág az irodalmi feldolgozás alapján meghatározott hipotézisünkkel is. A felhőrendszerekkel szemben támasztott biztonsági elvárások meghatározása megtörtént (K1) a vizsgált szervezetnél, továbbá definiáltak olyan standardokat, amik ahhoz szükségesek, hogy saját privát felhőmegoldásuk egységes és biztonságos legyen. A felhőmegoldások hatást gyakorolnak a belső üzemeltetési feladatkörökre (K4). Néhányuk eltűnik, mások át fognak alakulni, mely folyamatban az alkalmazkodás és az új feladatok ellátásának képessége fogja meghatározni, hogy mely szakemberek és vezetők lesznek alkalmasak az új környezetben is működni (K4). Természetesen lesznek olyan feladatkörök, amelyek ezért akár teljesen eltűnhetnek egy-egy vállalat esetében, míg másikaknál (felhőszolgáltatók) koncentrálódni fognak (K4).

Összefoglalás

Kutatásunk is megerősítette, hogy az információbiztonság kiemelten fontos napjainkban. Mára egyetlen, sikeresen működő vállalat sem engedheti meg magának, hogy rendszerei kompromittálódjanak, ezáltal pedig ügyfeleit negatív hatások érhessék. Ugyanakkor dilemmát jelent számukra, hogy a hatékonyság, a biztonság, a stabilitás, valamint a felhőmegoldások alkalmazásának figyelembevétele mellett miképpen képesek megtalálni a szükséges egyensúlyt. Ebben a feladatban nagy szerepet kap az információbiztonság menedzseléséért felelős szervezet a jövőben.

Munkánk következő lépéseként a vizsgálatot kiterjesztjük annak érdekében, hogy feltételezéseinket és az esettanulmányból levont következtetéseket nagyobb mintán is ellenőrizni tudjuk. Ennek érdekében elkészítjük a kutatási kérdéseket vizsgálni képes kérdőívünket, mivel a strukturált interjú módszere mély, azonban nehezen összehasonlítható válaszokat eredményez. Az így begyűjtött adatokat kvantitatív kiértékelési módszerek és SPSS segítségével fogjuk értékelni.

Felhasznált irodalom

Agrawal, D., Das, S. & Abbadi, A. E. (2012). *Data Management in the Cloud: Challenges and Opportunities (Synthesis Lectures on Data Management).* London, UK: Morgan & Claypool Publishers.

Ali, M., Khan, S. U. & Vasilakos, A. V. (2015). *Security in cloud computing: Opportunities and challenges.* North Dakota State: Information Sciences.

Alqassemi, S., Ever, Y. K. & Rajan, A. V. (2017). *Maturity Level of Cloud Computing at HCT.* Dubai: Institute of Electrical and Electronics Engineers .

Angyal, Á. (2009). *Vállalatok társadalmi felelőssége, felelős társaságirányítás.* Budapest, Magyarország: Kossuth Kiadó.

Ansoff, I. H. (1991). Critique of Henry Mintzberg's 'The design school: Reconsidering the basic premises of strategic management. *Strategic Management Journal, 12*(6), 449-461.

Bakacsi, G. (2010). *A szervezeti magatartás alapjai.* Budapest, Magyarország: Aula.

Bakacsi, G. (2012). A GLOBE-kutatás kultúraváltozóinak vizsgálata faktoranalízis segítségével. *Vezetéstudomány, 43*(4), 12-22.

Balogh, Á., Gaál, Z. & Szabó, L. (2011). Relationship between organizational culture and cultural intelligence. *Management & Marketing Challenges for the Knowledge Society, 6*(1), 95-110.

Barrett, M.P. (2018). *Framework for Improving Critical Infrastructure Cybersecurity.* Gaithersburg: National Institute of Standards and Technology.

Bayer, J. (1995). *Vezetési modellek - vezetési stílusok*. Budapest, Magyarország: Vinton Kft.

Beloglazov, A. (2013). *Computing, energy-efficient management of virtual machines in data centers for cloud*. Melbourne, Australia: Department of Computing and Information Systems The University of Melbourne.

Bogdány, E. (2014). *Átadni tudni kell! Vezetői szerep átadás a hazai kis- és középvállalkozásokban.,* Veszprém, Magyarország: Pannon Egyetem, Gazdálkodás- és Szervezéstudományok Doktori Iskola.

Bognár, F. & Gaál, Z. (2013). A beszállítói kapcsolatok megbízhatósági és karbantartási konzekvenciái. *Vezetéstudomány, 44*(6), 14-21.

Botta, A. (2016). Integration of Cloud computing and Internet of Things: A survey. *Future Generation Computer Systems, 56*(3), 684–700.

Boukalas, C. (2014). *Homeland security, its law and its state: A design of power for the 21st century.* New York, USA: Routledge.

Bowen, P. & Kissel, R. (2017). *Program review for information security management assistance (PRISMA),* Gaithersburg: National Institute of Standards and Technology.

Brătianu, C., Vasilache, S. & Jianu, I. (2006). In Search of Inelligent Organizations. *Management & Marketing, 1*(4), 71-82.

Buecker, A. et al. (2014). *Using the IBM Security Framework and IBM Security Blueprint to Realize Business-Driven Security.* hely nélk.:IBM.

Buyya, R., Broberg, J. & Goscinski, A. (2013). *Cloud computing: Principles and Paradigms.* Hoboken, USA: Wiley.

Cacciattolo, K. (2014). Understanding organisational cultures. *European Scientific Journal, 2(*Nov), 1-7.

Cameron, K.S. & Quinn, R.E. (2011). *Diagnosing and changing organizational culture: based on the competing values framework.* San Francisco: Jossey-Bass.

Cameron, K.S., Quinn, R.E., DeGraff, J. & Thakor, A.V. (2007). *Competing values leadership: Creating value in organizations*. Northampton: Edward Elgar Publishing.

Caroll, G. & Harrison, R. J. (2005). Organizational demography and culture: Insights from a formal model and simulation. *Administrative Science Quarterly, 43*(3), 637-667.

Catteddu, D. & Hogben, G. (2009). *Benefits, risks and recommendations for information security,* Heraklion: ENISA - European Union Agency for Network and Information Security.

Cavelty, M.D. (2013). *Cybersecurity strategy of the European Union: An open, safe and secure cyberspace,* Zurich: The Swedish Institute Of International Affairs.

Chawla, V. & Sogani, P. (2011). *Cloud Computing – The Future.* India, Springer, 113-118.

Chou, D. C. (2015). Cloud computing: A value creation model. *Computer Standards & Interfaces,* 72–77.

Conway, G. & Curry, E. (2012). *Managing Cloud Computing: A Life Cycle Approach*. Porto, Springer.

Conway, G., Doherty, D. E., Carcary, D. M. & Crowley, C. (2017). *Enterprise Cloud Adoption - Cloud Maturity Assessment Model.* Maynooth, Innovation Value Institute.

Covin, J. G. & Slevin, D. P. (1990). Juggling enterpreneurial and organizational structure. How to act together. *Sloan Management Review,* 43-53.

Dekker, M. & Liveri, D. (2015). *Cloud Security Guide for SMEs.* Heraklion: ENISA - European Union Agency for Network and Information Security.

Dekker, M., Liveri, D. & Matina, L. (2013). *Cloud Security Incident Reporting.* Heraklion: European Union Agency for Network and Information Security.

Dobák, M. & Antal, Z. (2016). *Vezetés és szervezés.* Budapest: Akadémia Kiadó Kft..

Draft, R. L. (2012). *Management*. Mason: South-Western.

Drogseth, D. (2011). *The Road to the Responsible Cloud*. Boulder: EMA - IT & Data Management Research , Industry Analysis & Consulting.

Duarte, A.́. & Mira da Silva, M. (2013). *Cloud Maturity Model*. Santa Clara, IEEE Xplore.

Early, C. & Ang, S. (2003). *Cultural Intelligence: Individual Interactions Across Cultures.* Stanford: Stanford University Press.

Educause (2009). *7 things you should know about cloud computing.* hely nélk.: Educause.

Fehér, P., Kő, A. & Szabó, Z. (2016). Kapacitásmodellezés és az IT-architektúratervezés kihívásainak vizsgálata statisztikai és prediktív analitikai eszközökkel. *Statisztikai Szemle*, 1149-1164.

Fekete-Berzsenyi, H. (2017). *Erre tart a hajó?: A szervezeti stratégia, a struktúra és a kultúra hatásainak vizsgálata a vállalati teljesítményre II. kötet*. Riga: GlobeEdit.

Gaál, Z. & Szabó, L. (2008). S*egédlet a stratégiai menedzsmenthez.* Veszprém: Pannon Egyetmi Kiadó.

Gaál, Z. (1999). Emberi tőke – szervezeti kultúra. *Harvard Business Manager,* 69-76.

Gaál, Z., Szabó, L. & Obermayer-Kovács, N. (2009). „Tudásmenedzsment-profil" érettségi modell. *Vezetéstudomány.*

Gao, X., Zhong, W., & Mei, S. (2013). Information security investment when hackers disseminate knowledge. *Decision Analysis*, 352-368.

Goleman, D., Boyatzis, R. & McKee, A. (2003). *Primal leadership: Realizing the power of emotional intelligence*. Boston: Harvard Business Review Press.

Goyal, S. (2014). Public vs private vs hybrid vs community - cloud computing: A critical review. *I.J. Computer Network and Information Security,* 20-29.

Grace, L. (2010). *Basics about cloud computing.* Pittsburgh: Software Engineering Institute Carniege Mellon University.

Grivas, S. G., Peter, M., Giovanoli, C., & Hubli, K. (2018). FHNW Maturity Models for Cloud and Enterprise IT. *Business Information Systems and Technology 4.0,* 133-146.

Guangming , C., Yao , L., Zhiwei , G. & Xiaoyin , L. (2017). *Cloud data governance maturity model.* Beijing, IEEE Press.

Hampden-Turner , C., & Trompenaars, F. (2006). Cultural intelligence: Is such a capacity credible?. *Group & Organization Management,* 56-63.

Handy, C. B. (1999). *Understanding Organisations.* Harmondsworth: Penguin.

Hansen, R. (2016). *Cyber security capability assessment.* Tallinn: Tallin University of Technology.

Harrison, R. L. (1992). Toward a theory of inter-refuge corridor design. *Conservation Biology,* 293-295.

Hax, A. C., & Majluf, N. S. (1984). *Strategic management: An integrative perspective.* New Jersey: Prentice Hall; Facsimile edition.

Hills, M. D. (2002). *Kluckhohn and Strodtbeck's Values Orientation Theory.* Melbourne: International Association for Cross-Cultural Psychology.

Hofstede, G. (2010). *Cultures and Organisations: Software for the Mind.* London: McGraw-Hill.

Hosking, D. M. (1988). Organising, leadership and skilful process. *Journal of Management Studies,* 147-166.

House, R. J. et al. (2004). *Culture, Leadership, and Organizations: The GLOBE Study of 62 Societies.* California: Culture, Leadership, and Organizations: The GLOBE Study of 62 Societies.

Jermier, J. & Forbes, R. (2016). Metaphors, organizations and water: Generating new images for environmental sustainability. *Human Relations*, 1001–1027.

Karcsics, É. (2011). *Menedzseri kompetencia-elvárások a munkaerőpiacon. Doktori értekezés.* Budapest: Budapesti Műszaki- és Gazdaságtudományi Egyetem, Gazdálkodás- és Szervezéstudományi Doktori Iskola.

Karokola, G., Kowalski, S., & Yngström, L. (2011). *Towards an information security maturity model for secure e-government services: A stackeholders view.* London, University of Plymouth.

Karoliny, M. & Poór, J. (1994). *Személyzeti/ emberierőforrásmenedzsment kézikönyv.* Budapest: Közgazdasági és Jogi Könyvkiadó.

Kavis, M. J. (2014). *Architecting the Cloud*. New Jersey: John Wiley & Sons Inc.

Kemp, L. (2016). 'Trapped' by metaphors for organizations: Thinking and seeing women's equality and inequality. *Human Relations,* 975–1000.

Kiss, C., & Csillag, S. (2014). *Szervezeti kultúra*. Budapest: NKE.

Kluckhohn, F., & Strodtbeck, F. L. (1973). *Variations in Value Orientations*. London: Greenwood Press.

Kollman T., Stöckmann, C., Linstaedt, J. & Kensbock, J. (2015). *European Startup Monitor,* hely nélk.: KPMG.

Kotter, J. P. (2012). *Leading change. Boston:* Harvard Business School Press.

Kroeber, A. L., & Kluckhohn, C. (1978). *Culture: A Critical Review of Concepts and Definitions*. hely nélk.:Kraus Reprint Company.

Lee, C. H., Geng, X. & Raghunathan, S. (2016). Mandatory standards and organizational information security. *Information Systems Research,* 70-86.

Levitt, T. (2003). The globalization of markets. *Harvard NOM Working Paper* , 92-102.

Lippert, R., Gaál, Z. & Kovács, T. (2015). A vezetői szerepek és a szervezeti kultúra hatása a klasztersiker érettségi modelljére. *Vezetéstudomány*, 2-13.

Liveri, D. & Skouloudi, C. (2016). *Exploring Cloud Incidents,* Heraklion: ENISA - European Union Agency for Network and Information Security.

Marchese, K., Crane, J. & Haley, C. (2015). 3D opportunity for the supply chain: Additive manufacturing delivers. *Deloitte University Press.*

Mathur, N. & Purohit, R. (2017). Issues and challenges in convergence of big data, cloud and data science. *International Journal of Computer Applications,* 160(9), 7-12.

Matkó, A. (2016). Versenyképesség és szervezeti kultúra vizsgálata az észak-alföldi régió önkormányzatainál. Taylor: *Gazdálkodás- és szervezéstudományi folyóirat,* (8)5, 87-97.

Mattoon, S., Hensle, B., & Baty, J. (2011). *Cloud computing maturity model guiding success with cloud capabilities.* California: Oracle.

Mead, R. (1998). *International management. Cross cultural dimensions*. Massachussets: Blackwell Publisher Inc..

Metzler, A. (2009). *The Mandate to Implement Unified Performance management.* [Online].

Mintzberg, H. (2010). *A menedzsment művészete.* Budapest: Alinea Kiadó.

Mitra, S., & Ransbotham, S. (2015). Information Disclosure and the Diffusion of Information Security Attacks. *Information Systems Research*, 565-584.

Morgan, G. (2007). *Images of Organization*. London: SAGE Publications, Inc.

Nagaraj, C., & Sathish Kumar, N. M. (2015). Cloud computing with a model futuristic maturity. I*nternational Journal of Advance Research in Science and Engineering.*

Naranjo-Valencia, J. C., Jimenez-Jimenez, D., & Sanz Valle, R. (2011). Innovation or imitation? The role of organizational culture. *Management Decision.*

Narasimhalu, A. D., Dayasindhu, N., & Subramanian, R. (2004). *INFOSeMM: Infosys IT Security Maturity Model: A Report,* Singapore: Singapore Management University.

Ohmae, K. (1999). *The Borderless World*. New York: HarperBusiness.

Oju, O. (2009). Impact Assessment of Corporate Culture on Employee Job Performance. *Business Intelligence Journal,* 2. kötet, 388-397.

Oju, O. (2010). Organisational Culture and Corporate Performance: Empirical Evidence from Nigeria. *Journal of Business Systems, Governance and Ethics,* 5(2), 88-100.

Örtenblad, A., Putnam, L. L., & Trehan, K. (2016). Beyond Morgan's eight metaphors: Adding to and developing organization theory. *Human Relations,* 875–889.

Pató, G. (2006). *Kompetenciák, feladatok logisztikai rendszerekben. Doktori értekezés.* Veszprém: Pannon Egyetem, Gazdálkodás- és Szervezéstudományok Doktori Iskola.

Pekgünk, P. M., Griffin, P. & Keskinocak, P., (2016). Centralized vs. Decentralized competition for Price and Lead-Time Sensitive Demand. *Decision Science.*

Pinto, J. (2016). 'Wow! That's so cool!': The Icehotel as organizational trope. *Human Relations*, 891–914.

Pisoni, A. & Onetti, A. (2018). When startups exit: comparing strategies in Europe and the USA. *Journal of Business Strategy,* 26-33.

Posey, C., Roberts, T., Lowry, P., & Hightower, R. (2014). Bridging the divide: A qualitative comparison of information security thought patterns between information security professionals and ordinary organizational insiders. *Information & Management, 51*(5), 551-564.

Puthal, D., Sahoo, B. P. S., Mishra, S. & Swain, S. (2015). *Cloud Computing Features, Issues and Challenges: A Big Picture*. India, IEEE.

Quinn, R. E. et al. (2015). *Becoming a Master Manager: A Competing Values Approach.* New Jersey: WILEY.

Ransbotham, S., Mitra, S., & Ramsey, J. (2012). Are markets for vulnerabilities effective?. *MIS Quarterly*, 43-64.

Rittinghouse, J. W., & Ransome, J. F. (2009). *Cloud Computing - Implementation, Management and Security.* Boca RAton: CRC Press.

Roberts, N., & Varun, G. (2014). Leveraging Information Technology Infrastructure to Facilitate a Firm's Customer Agility and Competitive Activity: An Empirical Investigation. *Journal of Management Information Systems,* 231-270.

Saleh, M. F. (2011). Information Security Maturity Model. *International Journal of Computer Science and Security (IJCSS).*

Schein, E. H. (2010). *Organizational Culture and Leadership.* San Francisco: Jossey-Bass.

Scholtz, T., Byrnes , F. C., & Wheatman, J. (2016). *ITScore for Information Security*, Stamford: Gartner.

Shaul, O., Vakola, M. & Armenakis, A. (2011). Change Recipients' Reactions to Organisational Change: A 60-Year Review of Quantitative Studies. *The Journal of Applied Behavioral Science,* 461-524.

Sjelin, N. & White, G. (2016). The Community Cyber Security Maturity Model. *Cyber-Physical Security,* 161-183.

Spencer, L. M., & Spencer, S. M. (1993). *Competence at work: Models for superior performance.* New York: John Wiley & Sons.

Spilák, V. & Kosztyán, Z. T. (2013). *A szervezeti kultúra és vezetési stílusok hatása az információbiztonsági kiválóságra.* Győr: Neumann János Számítógép-tudományi Társaság.

Sultan, N. (2010). Cloud computing for education: A new dawn. *International Journal of Information Management, 30*(2), pp., 109-116.

Szabó, L., & Dancsecz, G. (2009). A nemzetközi sportrendezvényszervezési projektek sikerténye zői és a siker megítélésenk kritériumai. *Vezetéstudomány*, 30-31.

Szintay, I. (2003). *Vezetéstudomány.* Miskolc: Bíbor Kiadó.

The Open Group (2011). *Open Information Security Management Maturity Model (O-ISM3).* Zaltbommel: Van Haren Publishing.

Tolbert, P.S., & Hall, R.H. (2008). *Organizations: Structures, Processes and Outcomes*. London: Routledge.

Török, J. (2017). Kultúra összehasonlító (cross-cultural) és interkulturális (intercultural) kutatási modellek: összehasonlító elemzés. *Szakmai Füzetek Budapesti Gazdasági Főiskola,* 11-16.

Weinman, J. (2016). Hybrid Cloud Economics. *IEEE Cloud Computing,* 18-22.

Weinman, J. (2015). The Strategic Value of the Cloud. *IEEE Cloud Computing,* 66-70.

Weiss, D., Repschlaeger, J., Zarnekow, R., & Schroedl, H. (2013). *Towards a Consumer Cloud Computing Maturity Model - Proposition of Development Guidelines, Maturity Domains and Maturity Levels.* Jeju Island, PACIS.

Wienman, J. (2012). *Cloudonomics*. Hoboken: Wiley.

Yang, C. et al. (2015). IT capabilities and product innovation performance: The roles of corporate entrepreneurship and competitive intensity. *Information & Management,* 643-657.

Zaleznik, A. (1992). Managers and Leaders: Are They Different?. *Harvard Business Review.*

Zhao, H., Liu, X. & Li, X. (2014). Towards efficient and fair resource trading in community-based cloud computing. *Journal of Parallel and Distributed Computing,* 3087-3097.