Óbudai Egyetem

Doktori (PhD) értekezés

A felhasználók biztonságtudatosságának jelentősége a publikus felhőszolgáltatások nagyvállalatoknál történő bevezetésekor

Rubóczki Edit Szilvia

PhD hallgató

Prof. Dr. Rajnai Zoltán

Egyetemi tanár

Témavezető

Biztonságtudományi Doktori Iskola

Budapest, 2019

Szigorlati Bizottság:

Elnök:

Prof. Dr. Berek Lajos egyetemi tanár, ÓE

Tagok:

Dr. habil. Lazányi Kornélia egyetemi docens, ÓE

Dr. habil. Farkas Tibor egyetemi docens, külső - NKE

Nyilvános védés bizottsága:

Elnök:

Prof. Dr. Szlivka Ferenc egyetemi tanár, ÓE

Titkár:

Bakosné Dr. Diószegi Mónika adjunktus, ÓE

Tagok:

Dr. Fregán Beatrix egyetemi oktató, külső - NKE

Dr. habil. Michelberger Pál egyetemi docens, ÓE

Dr. habil. Lazányi Kornélia egyetemi docens, ÓE

Bírálók:

Dr. Szűcs Endre adjunktus, ÓE

Dr. Puskás Béla, külső

Nyilvános védés időpontja

……

TARTALOMJEGYZÉK

BEVEZETÉS

A *nagyvállalati felhasználók információbiztonságának tudatosítása napjainkban az egyik legfontosabb teendő. Különösen abban az esetben, ha a nagyvállalat infrastruktúrájában megjelenik a számítási felhő. Az információbiztonság oktatott és ezzel együtt annak betartása egy elvárt követelmény a vállalat részéről a saját munkavállalóival szemben. Az utóbbi években a vállalat informatikai határai elmosódnak, aminek egyik legfőbb oka a mobil eszközök, az internet és az internethez szorosan kapcsolódó informatikai eszközök használatának terjedése. Az internet és az internetképes eszközök teszik lehetővé a munkavállalók számára, hogy olyan egyéb informatikai rendszerekhez is hozzáférjenek, melyek nem részei a vállalati informatikai infrastruktúrának. Lehet technológiailag tiltani tartalmak vagy portok elérését, és erős falat húzni a vállalat és az internet „vadnyugata" között, ma már azonban bizonyos munkakörök elengedhetetlen része a világháló szabad használata.*

A vállalatok főbb célja tehát az, hogy technológiailag biztonságos környezetet hozzon létre, melyben a felhasználók egymástól egyértelműen megkülönböztethetők, a felhasználók tevékenysége a vállalati informatikai környezetben nyomon követhetők, az adatok rendelkezésre állása, sértetlensége és integritása pedig megvalósítható.

Kutatásomban azért választottam a nagyvállalati környezet vizsgálatát, mert ezekben az informatikai hálózatokban többé-kevésbé megoldott a technológia biztonságának megvalósítása. Kiépített és évek vagy évtizedek üzemeltetési és felügyeleti tapasztalata alapján a fenti követelményekkel az általam vizsgált magyarországi nagyvállalatok rendelkeznek. Dolgozatomhoz három magyar székhellyel rendelkező, multinacionális céget vizsgáltam, melyek mindegyikével titoktartási szerződést kötöttem, hogy személyes interjúimban és kérdőívemben is használhassak a vállalat gyenge pontjaira is irányuló kérdéseket. Dolgozatomban ezért a három nagyvállalatot nem nevezem meg. Kutatásom során tehát ebben a nagyvállalati szegmensben vizsgálom a felhasználók biztonságtudatosságát. Ugyanakkor egy új technológia, a felhőszolgáltatások megjelenése és a felhasználók döntése alapján való használata valóban fejfájást okozott a vállalatok életében. A felhasználó nemcsak munkája során használhat egy felhőszolgáltatást a rendelkezésére bocsátott vállalati eszközön, hanem magánfelhasználásra is. Ekkor válik a vállalat számára valódi kockázattá a felhasználó tevékenysége. A vállalat által biztosított eszközön ezáltal két különböző felhasználású, biztonsági besorolású és célú adatcsoport jelenik meg, a magán és az üzleti.

A felhasználó biztonságtudatossága ezért egy központi kérdés minden vállalat életében, ugyanakkor az általam vizsgált vállalatok esetében kiemelten fontos a biztonságtudatos felhasználó. Ezek a vállalatok nem félnek új, tudatosító módszerek bevezetésétől, és külön oktatási-, képzési programot alakítanak ki munkatársaik számára ebben a témában.

Dolgozatomban arra keresem a választ, hogy a vizsgált nagyvállalatok esetében milyen módszert használnak a munkatársak tudatosításának érdekében, valamint milyen eredményeket érnek el ezen a téren. Az elért eredményekre milyen hatással van az oktatás rendszeressége, felépítése, módszertana, illetve a biztonságtudatos viselkedést hogyan várja el a vállalat a felhasználótól.

A kutatásom során arra kerestem választ, milyen eszközökkel tehető elkötelezetté a felhasználó, mennyire érzi magát felelősnek az információbiztonság megőrzésében.

Kutatásom során vizsgálom a nagyvállalatok információbiztonságra vonatkozó oktatási módszereit, vizsgálom a vállalatok által alkotott információbiztonságra vonatkozó szabályegyüttest, és vizsgálom az oktatási folyamatban résztvevő felhasználók ismereteit a fenti témakörben. Dolgozatomban a nagyvállalati szegmens egy szeletét kutatom, ahol három azonos tevékenységű nagyvállalat munkatársainak biztonságtudatosságát vizsgálom. Azért választottam hasonló tevékenységű és folyamatú vállalatokat, hogy az összehasonlításukat minél pontosabban tudjam elvégezni. A szerzett információk pontosabb elhelyezése és feldolgozása érdekében vizsgálom a felhőtechnológiákra vonatkozó hazai és nemzetközi szabályozási kört és ajánlásokat. Vizsgálom, az akaratlanul, de az ember hibájából, tudatlanságából bekövetkező problémák milyen hatással vannak a vállalat életére, és melyek azok a pontok a rendszerben, amikor a humán faktor nem várt kockázatot jelent az információ szempontjából. Ugyanakkor nem vizsgálom azokat a helyzeteket, amikor a felhasználó vagy a felhasználó segítségével egy külső személy, saját érdekek mentén szándékosan sérti a vállalati rendszer biztonságát.

Vizsgálom azonban, mennyire szabályozható az ember viselkedése az adat védelme érdekében, milyen tényezők befolyásolják a munkavállalót a nem szabályszerű viselkedésre.

Dolgozatom nem terjed ki a teljes hazai nagyvállalati szegmens vizsgálatára. Továbbá nem terjed ki a kis- és középvállalkozások vizsgálatára sem. Bár az eredmények használhatók más vállalatok esetében is, pontos képet csak a vizsgált nagyvállalatok jelenlegi állapotáról adhatok.

A tudományos probléma megfogalmazása

Dolgozatomban a felhőrendszereket használók biztonságtudatosságával és annak fejlesztésével foglalkozom. A felhőrendszerek technológiáját biztonságosnak tekintve, a szolgáltatási lánc legkritikusabb elemét, az emberi tényezőt és annak fejlesztését tűztem ki célul. Vizsgálom az emberi tényező magatartását befolyásoló tényezőket, különösen a nagyvállalati szektor munkatársait vizsgálva.

Vizsgálom, jelenleg milyen szinten áll a felhőt privát célra is használó munkatársak biztonságtudatossága. Valóban kapnak teljeskörű információt arra vonatkozóan, hogyan használják a vállalati és a magáncélú eszközöket és alkalmazásokat? Mennyire relevánsak és beépíthetők számukra a kapott információk? Megfelelő-e az az oktatási keret és módszer, amivel a munkatársak képzése történik? Létezik-e olyan eszköz, amivel az információátadás hatásfoka növelhető? Hatással van-e a vállalati oktatások során megszerzett ismerethalmaz a privát felhasználásra is? Erősebb-e a biztonságtudatosság abban az esetben, ha a vállalati szabályzat megsértésével az okozott kár szankcionálásra kerül?

Kutatásomban arra keresem a választ, hogy a nagyvállalati szektorban a felhasználók vállalati képzése során a biztonságtudatosság növelését milyen eszközökkel lehet hatékonyabban elérni, valamint ahol megjelenik az oktatást követően a monitorozás, számonkérés és szankcionálás, ott lehet-e komoly eredményt elérni a biztonságtudatosság növelése területén.

A témaválasztás indoklása

A felhőtechnológiák elterjedése során a szolgáltatók törekednek a lehető legbiztonságosabb és leginkább felhasználóbarát rendszereket kialakítani. Igyekeznek az általános felhasználó számára a rendszert úgy biztonságossá tenni, hogy az adat- és információvédelem ne sérüljön. A legtöbb olyan esetben, amikor mégis nem kívánt adatok nyilvánosságra kerülnek, kiderül, hogy az nem a szolgáltató, hanem a felhasználó hibájából történt.

Véleményem szerint a felhasználók tudatosításával csökkenthetők a biztonságot kockára tevő helyzetek előfordulása. Nagyvállalati környezetben a felhasználók részt vesznek információbiztonsági képzéseken, ugyanakkor éles helyzetben, vagy magánéletben a biztonságtudatosság mértéke még mindig nem megfelelő. Szükség van egy olyan rendszerszintű gondolkodásmódra, ami a felhasználók ismereteibe beépül, és minden

helyzetben előhívható. Szükséges továbbá egy olyan módszer, amivel a folyamatosan változó technológiai környezet által generált tudáshalmaz érdekessé, szerethetővé válik, amivel a tudatosításban résztvevő motivációja szinten tartható, a téma fontossága pedig megérthetővé válik.

Kutatási célkitűzések

1. Célként fogalmaztam meg, hogy bizonyítom, a felhőtechnológiák biztonságának mértéke, és a szolgáltatási lánc másik eleme, az emberi tényező biztonságának mértéke bár összefügg, mindenképpen külön kockázati tényezőként érdemes kezelni.

2. Célként fogalmaztam meg, hogy feltérképezem és elemzem néhány hazai távközlési piacon résztvevő nagyvállalat felhasználóinak információbiztonság-tudatossági szintjét.

3. Célul tűztem ki, hogy a vizsgált nagyvállalati környezetekben összevetem az elvárt és a tapasztalt biztonsági állapotokat. Megvizsgálom, hogy a leírt, a vezetők vagy a HR által felállított követelményrendszer érthetők, elfogadhatók és betarthatók-e a különböző vállalatok munkatársi szintjén.

4. Célként fogalmaztam meg, hogy kimutassam az oktatásban használható módszerek közül az a hatékonyabb, melyiknél a résztvevők a témához kapcsolódó személyes viszonya szorosabb, bevonódása mélyebb. Ezért az átadni kívánt információ is jobban rögzül.

A téma kutatásának hipotézisei

H1: Feltételezem, hogy a felhőszolgáltatás technológiája képes alacsony kockázati szinten kezelni az adattárolást és -hozzáférést minősített szolgáltató igénybevétele esetén, de ennek együtt kell járnia a humán faktor megfelelő, biztonságtudatos munkavégzésre történő felkészítésével.

H2: Bizonyítható, hogy a számítási felhő –> kommunikációs hálózat –> vállalati informatikai rendszer –> felhasználó láncnak az utolsó és leggyengébb láncszeme a felhasználó

H3: Bizonyítható, hogy a biztonságtudatosság, a humán fejlesztés, valamint a vállalati szabályozás szoros kapcsolatban állnak. Igazolható ezek összefüggése, és együttesen hatásuk van a vállalat információbiztonságára.

H4: A személyes élményeken keresztül fokozható a biztonságtudatos viselkedés és ennek tapasztalatai az oktatási programokba is beépíthetők.

Kutatási módszerek

Kutatásom során a számítási felhők biztonságának technológiai kérdésein túl vizsgáltam a felhőtechnológiák szabályozási kérdéseit is. Megvizsgáltam a jelenleg számottevő felhőt minősítő és szabályozási szervezetek érvényben lévő dokumentumait, melyeket hasonló szempontok alapján hasonlítottam össze. Ennek érdekében a rendelkezésre álló nemzetközi angol nyelvű irodalmat dolgoztam fel, és törekedtem az elméleti összefüggések és a gyakorlati alkalmazás komplex vizsgálatára.

A felhőtechnológiák biztonságos nagyvállalati bevezetéséhez a szakirodalomban található kockázati tényezők és az elméleti kockázatmenedzsment segítségével alkottam meg a téma kockázatkezelési mátrixát. Ennek segítségével könnyebben mérlegelhetők és a különböző döntési szinteken könnyebben érthetővé tehetők a felhőtechnológiák bevezetése során felmerülő kockázatok. A kockázatkezelési mátrix felállításához szükségem volt a rendelkezésre álló információk szintetizálására, összevetésére és összehasonlítására, valamint kutattam felmerülésük gyakoriságát és súlyosságát.

Vizsgáltam a nagyvállalati környezetet, mint a technológiát bevezetni kívánó és használó közeget. Vizsgálatom során hazai és nemzetközi irodalmat, esettanulmányokat, vállalati beszámolókat és stratégiákat kutattam, különös tekintettel a vállalati kultúra, a vállalati oktatáspolitika, valamint a vállalatoknál található adatkezelési megoldásokat elemeztem.

A dokumentum- és kutatáselemzéseket minden esetben saját kutatási témámhoz kapcsolódóan végeztem.

A feltérképezett technológiai, vállalati és humán elméleti tényezőket a gyakorlatban is vizsgáltam, ehhez személyes interjúkat folytattam 3 különböző nagyvállalat HR és informatikai vezetőivel és beosztottjaival. Tanulmányoztam a vizsgált vállalatok informatikai biztonsági kézikönyveit – két vállalat rendelkezett ilyen dokumentummal. A teljesebb kép érdekében személyes kérdőívezést végeztem a munkatársak bevonásával ezeknél a vállalatoknál. Az elvárt és a mért eredmények összevetésével kaptam pontosabb információt, mely információ a vizsgált nagyvállalatok számára is érdekes és fontos visszajelzést ad.

Ahhoz, hogy egy kiválasztott felhőtechnológia bevezetése során a humán tényezőből eredő kockázatok csökkenthetők legyenek, nagy hangsúlyt kell fektetni a munkatársak időben történő bevonására, tájékoztatására és oktatására. Részt vettem az egyik vizsgált hazai nagyvállalat bevezetési projektjében, mint a munkatársak felkészítéséért felelős oktató. Dolgozatom szempontjából mérhetetlenül értékes információt kaptam a munkatársi biztonságtudatosság szintjéről, valamint azt ezt befolyásoló hozzáállásról, motivációról, az oktatások során nyújtott aktivitásokról. Oktatási tevékenységem során alkalmaztam a játékosítás eszközeit, így annak hatékonyságát elsőkézből tapasztaltam meg. Ezeket az eredményeket gyűjtöttem össze és elemeztem kutatásom során, melyek karakterisztikáját folyamatosan illesztettem a játékosítás hazai és nemzetközi elméleti eredményeihez.

A kutatás lezárásra került 2019. január 15-én.

1 A SZÁMÍTÁSI FELHŐK BIZTONSÁGOS BEVEZETÉSÉT TECHNOLÓGIAI SZEMPONTBÓL BEFOLYÁSOLÓ TÉNYEZŐK

A számítási felhő hatékony, rugalmas és egyszerűbb munkavégzést nyújt. Korunk elvárásainak megfelelve, egyszerre nyújtja a mobilitást, az eszközfüggetlenséget és a széles tartalom- vagy alkalmazásválasztékot. A felhőtechnológia a 2010-es évek egyik legnépszerűbb technológiája, mellyel mind a magán-, mind az üzleti életben találkozunk. Azzal, hogy kommunikációs eszközeink mobilak, hordozhatók lettek, az eszközökön lévő funkcióktól is elvárjuk, hogy ne csak az irodában vagy az otthonunkban használhassuk, hanem bármikor, amikor szükségünk lehet rá. Az igényelt funkciókat egy készülékbe emeltük, így az eredetileg telefonálásra szánt készülék ma már e-mailt küld és fogad, híreket jelenít meg, videót vagy fotót rögzít, munkaterületet valósít meg, zenét játszik le, és játékokat kínál, miközben telefonálni is képes. Minden egyes alkalmazás mögött ott áll egy szolgáltató, aki biztosítja ezen funkciók szünetmentes, biztonságos és távoli elérését, tárolja a fényképeinket, leveleinket, egyéb gyűjtött vagy mért adatainkat. Egy egyszerű felhasználó, egy okostelefon megvásárlásával és használatával ma már több felhőszolgáltatóval állhat kapcsolatban, mint közműszolgáltatóval. Minden helyzetre találhat olyan alkalmazást, ami segíti a mindennapi életét hatékonyabbá, gyorsabbá, átláthatóbbá tenni.

Ugyanezek az igények az üzleti világban is megfogalmazódnak, és a számítási felhők használata ma már megtalálhatók a nagyvállalatok rövidtávú informatikai stratégiájában. Nem kérdés, hogy ezek a vállalatok a jövőben mindenképpen használni fogják a felhőtechnológiákat, a mértékben, módban és kialakításban találkozunk majd eltérő megoldásokkal. Ez a fajta technológia egyrészt nagy rugalmasságot és szabadságot lesz képes adni a vállalatok számára, ugyanakkor sokkal körültekintőbben, megfontoltabban kell a szakembereiknek megtervezni a jövőbeli informatikai infrastruktúrát az elvárt kiszolgálási szint mértékét figyelembe véve.

Az első fejezetben vizsgálom a felhőtechnológia szabályozási környezetét, ami mind a nemzetközi mind a hazai szolgáltatásbevezetéseket befolyásolják. Összehasonlítom a különböző, felhőtechnológiával a kezdetektől foglalkozó szervezetek ajánlásait, szabályozásait. Javaslatot teszek arra vonatkozóan, melyik szervezet ajánlása alkalmazható leginkább egy nagyvállalati környezetben. Összefoglalom a technológia

előnyeit, illetve megvizsgálom a publikus felhők, üzleti alkalmazásra szánt szolgáltatásainak biztonságát. Dolgozatomban a publikus felhők nagyvállalati használatát vizsgálom, és mutatom be annak környezetét, hátterét, kockázatait. Ahhoz, hogy megértsük, miért kap egyre nagyobb szerepet a felhő egy infrastruktúra tervezés vagy újratervezés során, megvizsgálom, mik azok az előnyök és hátrányok, melyeket kockázatkezelési szempontból figyelembe kell vennünk. A kockázatok megfelelő értékelése szempontjából a rendelkezésemre álló szakirodalom alapján állítom fel a kockázatkezelési mátrixot.

Mindezeken felül azonban a felhőben tárolt adat bizalmassága, sértetlensége és rendelkezésre állása a legfontosabb követelmény nemcsak a privát felhasználó, hanem a vállalat részéről is. Amennyiben a felhőtechnológia képes megfelelő szintű (az esetek többségében ez a szint magasabb, mint amit saját maguk biztosítani tudnak) biztonságot nyújtani, válik olyan szolgáltatóvá, akire egy cég rábízza a vállalati adatvagyonát, vagy annak egy részét. A felhőbe költözés során így a megfelelő szolgáltató kiválasztását, az általa nyújtott biztonságot megerősítő tevékenységek és technológiák együttes eszközrendszere határozza meg.

Hazai és nemzetközi szakcikkek és kutatások feldolgozásával és elemzésével vizsgáltam meg a számítási felhők technológiájának biztonságosságát. Fontos megismernünk azokat a tényezőket, melyeket adottnak vehetünk a technológia használata során, és a vállalati kockázatelemzési kézikönyvben konkrétan számolhatunk az esetleges kockázatokkal. A fejezetben leírtakkal az a célom, hogy a kutatásom során a felhőbiztonság technológiájának tényezőjét adottnak vehessem. A leírtakat figyelembe véve és betartva az ebből eredő kockázat tervezhető, ezáltal csökkenthetővé váljon.

1.1 Számítási felhő

A felhő elnevezést először Eric Schmidt, a Google vezérigazgatója használta a 2006-os Google Konferencián San Jose-ban, és alkotta meg a „Cloud Computing” vagyis a Számítási felhő fogalmat. Ugyanebben az évben, még a konferenciát megelőzően vitték piacra a Google Docs alkalmazásukat, ami később meghatározó mérföldköve lett az irodai alkalmazások felhőben való elhelyezésének. [1]

A felhőszolgáltatás egy speciális módon kialakított szolgáltatásrendszer, amely szolgáltatásait meghatározott feltételekkel, megadott SLA-val, rendelkezésre állással, mérhető és elszámoltatható módon kínálja. A felhőszolgáltatásokat a felhasználók internetkapcsolaton keresztül érik el.

A számítási felhő definíciói közül ma leginkább a NIST meghatározását használjuk:

„A felhőalapú számítástechnika egy olyan modell, amelynek segítségével bárhonnan, kényelmesen és igény szerint hozzáférhetünk a testreszabott informatikai erőforrások megosztott halmazához (pl. hálózat, szerver, tárhely, alkalmazás, szolgáltatás), miközben a rendelkezésre bocsátás minimális adminisztrációs tevékenységet és szolgáltatói beavatkozást igényel.” [2]

A hat alapkritériummal rendelkező rendszereket nevezhetjük felhőszolgáltatásnak:

1. Adatkapcsolaton keresztül érhető el (internet)
2. Az előfizető önkiszolgáló portálfelületet használ
3. Skálázható: a felhasználó annyit vesz igénybe, amennyire szüksége van.
4. Az árazása felhasználás-alapú: a felhasználók mindig csak annyi kapacitás után fizetnek, amennyit igénybe vesznek
5. Automatizált folyamatok működtetik a szolgáltatást
6. Egységesített szolgáltatáselemekből kialakított csomagolt megoldást nyújt [2]

A felhőtechnológiák megjelenése az üzleti életben gyorsabb és szabadabb mozgásteret adott a vállalatok számára. A technológia igénybevételével egy új üzleti vállalkozás akár 24 óra alatt fejlett, a nagyvállalatokhoz hasonló infrastruktúrával rendelkezhet, melyet használat és felhasználószám alapján fizet, ugyanakkor testre szabhatja a saját vállalkozására. Az előfizető nem szoftvert vagy hardvert vesz, hanem szolgáltatást, annak minden előnyével együtt. Beruházási költség, üzemeltetési díj, és várakozási idő nélkül.

A felhőalapú szolgáltatások a magánéletben hamarabb okoztak technológiai robbanást. Bár a rendszer alapjai a nagyvállalati informatikai szolgáltatások mobilizálása során alakultak ki, az áttörést mégis a privát szektor hozta a technológia számára. [1]A bárki által elérhető informatikai szolgáltatások, az internetképes mobileszközök segítségével hódították meg a magánfelhasználókat. Az alap kommunikációs szolgáltatásoktól kezdve a szűk rétegeket érintő speciális alkalmazásokig ma már az ezeken az eszközökön megtalálható alkalmazások mind felhőtechnológiát használnak. Ugyanakkor a biztonsági,

folyamatbeli és a hosszabb döntési idő, valamint az alkalmazások komolysága miatt a felhőtechnológia nagyon lassan hódított teret az üzleti életben. Bőgel György szerint az utóbbi évtizedben komoly és reális igényként merült fel a felhőalapú számítástechnika komplex üzleti rendszerekben történő felhasználása. [3] A korábbi vállalati technológiáktól eltérően a felhő elterjedése lentről felfelé terjedt el (bottom-up). Amíg a mikro- és kisvállalatok szinte gondolkodás nélkül vették igénybe az újonnan elérhető publikus szolgáltatásokat, addig a nagyvállalatok óvatosan kezelték ezt a kérdést, és maradtak a privát- vagy hibridfelhő kialakítások mellett, vállalva azok magasabb költségeit a magasabb biztonság és rendelkezésreállás érdekében.

1.2 A hazai nagyvállalatok érdeke, elvárásai

A nagyvállalatok rendelkeznek saját, testreszabott, egyéni igényeket kielégítő informatikai infrastruktúrával vagy ehhez tartozó szigorú biztonsági folyamatokkal, szabályozásokkal. Az utóbbi években egyre több nagyvállalat dönt [4] a felhőszolgáltatás teljes vagy részleges bevezetése mellett. Ez ma még több szinten megvalósulhat, vannak vállalatok, akik saját maguk építenek ki és üzemeltetnek privát felhőrendszereket, ugyanakkor egyre több érv szól a publikus, üzleti szolgáltatások igénybevétele mellett.

A vállalati döntést elsősorban a pénz és az idő határozza meg. Ma már üzleti szempontból egy terméknek vagy szolgáltatásnak a megfelelő időben történő piacra lépése legalább annyira fontos üzleti szempont, mint a költséghatékony megoldás. A felhőtechnológiák mindkettő feltételnek képesek egyszerre eleget tenni, hiszen a felhőben található szolgáltatásegyüttesek olyan kész vagy gyorsan testreszabható megoldásokat nyújtanak pay-as-you-grow alapon, melyeket a vállalat több hónapos vagy éves fejlesztéssel lenne képes kialakítani, mire a piaci igények már mást diktálnak.

A három legnagyobb felhőszolgáltató, az Amazon, a Microsoft és a Google [5], [6], [7], [8], [9], húzzák a piacot, és diktálnak újabb és újabb feltételeket a technológia, a szabályozás, valamint a szolgáltatási paletta területein.

Az ISACA ROI számítása alapján elmondható, hogy felhőszolgáltatások megtérülése 5 évre számolva 50% is lehet [10]. Bár a ROI csak egy gazdasági számítás és ok arra, hogy a nagyvállalati döntéshozók financiálisan is elgondolkozzanak egy új rendszer bevezetése előtt a számítási felhők igénybevételéről.

A vállalati informatikától tehát elvárt, hogy naprakész, könnyen használható, könnyen hozzáférhető, könnyen bevezethető és integrálható rendszert nyújtson a társosztályok

számára. Ez sok esetben olyan magas követelményszintet feltételez, aminek nem minden szolgáltató képes eleget tenni. Egy bevezetni kívánt „idegen” szolgáltatás bevizsgálása is hónapokat vehet igénybe, egy nagyvállalat amúgy is nehezen hoz gyors döntést, a mamuthoz hasonlóan lassan, komótosan halad előre.

A legfontosabb igények a bevezetendő rendszerrel szemben nagyvállalati oldalról:

- Legyen kiemelkedően biztonságos
- A meglévő rendszerekhez illeszthető legyen
- Elérhető legyen egy megfelelő, hazai nyelvű támogatás (e-mail, telefon vagy személyes)
- A külső szolgáltató vállalja a felhasználói oktatások levezénylését
- Oldja meg a teljes problémát, ami miatt a bevezetés elindul, de ne generáljon újakat

1.3 A publikus felhők szolgáltatási lánca

A publikus felhők szolgáltatási lánca az a halmaz, ahol az adat keletkezési helye és a végleges tárolási helye közötti minden, a láncban aktívan szereplő informatikai elem részt vesz.

A technológia annyira lehet biztonságos, amennyire a leggyengébb láncszeme az. [11] Ezért a felhőtechnológia biztonságának felmérése során a szolgáltatási lánc egyes láncszemeinek erősségeit, gyengeségeit kell megvizsgálnom.

A jelenlegi vizsgálat során is csak a vállalati alkalmazást vizsgálom.

A szolgáltatási lánc összetétele az adat keletkezési helyétől viszonyítva a következő:

1. **Felhasználói eszköz(ök):** ez az eszköz képes a vállalati infrastruktúrában működni, a vállalati informatikai rendszer része, mellyel a felhasználó adatot hoz létre, kezel vagy megjelenít. Az eszköz a vállalat által üzemeltetett – jó esetben – tehát az eszköz fölött adminisztratív joggal maga a vállalat rendelkezik. A vállalati informatikai biztonsági szabályzatban ezen eszközök használatát szabályozni kell, hogy a vállalati adatvagyon és a személyes adat ne keveredjen egymással.

2. **Vállalati informatikai infrastruktúra:** a vállalat vagy egy külső partner által üzemeltetett informatikai rendszer, mely a vállalat informatikai szolgáltatásait nyújtja a vállalat külső és/vagy belső ügyfelei számára. A vállalati infrastruktúra lehet helyi üzemeltetésű, ekkor fizikailag is minden rendszerelem a vállalat telephelyén található meg. Lehet hibrid, amikor külső partnerek szolgáltatásai és a vállalat által üzemeltetett szolgáltatások együttesen nyújtják az informatikai szolgáltatásokat. Vagy lehet teljesen külső üzemeltető által biztosított. Az infrastruktúra bizalmassága, rendelkezésre állása és sértetlensége a legfontosabb kritériumok. Az informatikai szolgáltatásokat a nagyvállalat minden egyes osztálya használja, és elvárja azok folyamatos rendelkezésre állását, a nap 24 órájában, az általuk használt és a vállalat által felügyelt végfelhasználói eszközökön.

   A felhőszolgáltatásoknak ebbe a vállalati informatikai infrastruktúrába kell illeszkednie hibrid megoldások esetén, a meglévő szolgáltatási szinteket tartva, vagy javítva.

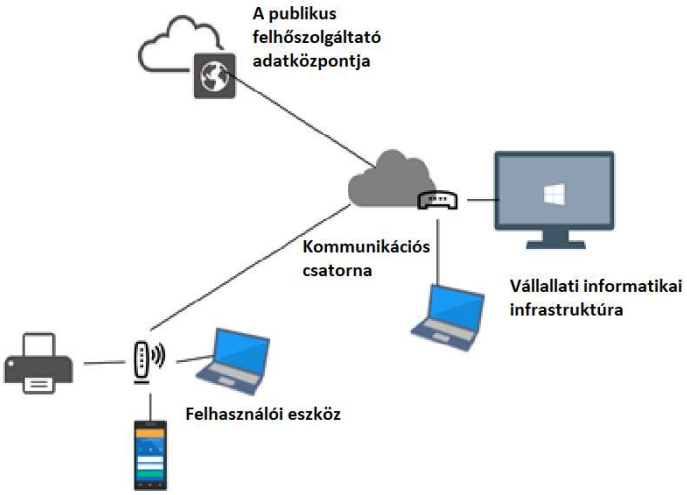
   Teljes vállalati infrastruktúra kiváltására nagyvállalati környezetben eddig a Graphisoft esetében volt példa 2017-ben, ahol kizárólag publikus felhőszolgáltatások igénybevételével valósítják meg az informatikai kiszolgálást, a Microsoft Azure szolgáltatások igénybevételével [13], [14].

3. **Kommunikációs csatorna:** a vállalat és a felhőszolgáltató közötti kommunikációs csatorna. Ezen a csatornán keresztül jut el az adat a keletkezési helytől a végleges tárolás helyéig, a felhőszolgáltató adatközpontjába. A kommunikációs csatornát távközlési szolgáltató biztosítja, Európán belül megfelelő szinten, legalább 99,5-ös SLA-val [15].

4. **A publikus felhőszolgáltató adatközpontja**: az adat végleges tárolási helye, amit a felhőszolgáltató tárol. Az adat a vállalat tulajdona marad, ugyanakkor az infrastruktúráért a felhőszolgáltató a felelős. Az adat védelme, tárolása, mentése, biztonsági mentése és szükség esetén visszaállítása is a felhőszolgáltató feladata.

A minősített publikus felhőszolgáltatóknak technikailag rendelkezniük [16], [17] kell:

- Biztonságos adatközponttal (adatközpontokkal)
- Fizikai védelemmel ellátott adatközponttal
- Belső policy-val, melynek fókuszában a biztonság áll
- Folyamatos adatmentéssel, hogy szükség esetén képesek legyenek az adatok visszaállítására
- Kezelik a felhasználókat és a kezelésre az ügyfeleik adminisztrátori joggal rendelkező munkatárainak is lehetőséget biztosítanak
- Szabványos interfészeket, API-kat használnak
- Szabványoknak, ellenőrzéseknek, auditoknak megfelelnek, ezeket rendszeresen elvégzik (pl. PCI DSS, ISO)
- Törekednek, hogy ügyfeleik meglévő infrastruktúrájához a legtökéletesebben illeszkedjenek, akár több platformra is kiterjesztik a szolgáltatásaikat
- Megfelelő SLA-t nyújtanak
- Regionális vagy helyi táogatást nyújtanak több csatornán keresztül (weboldal, chat, e-mail, telefon, személyes)
- Virtualizációt kínálnak [18]
- Skálázhatóságot tesznek lehetővé, mellyel pontosabb és testreszabottabb szolgáltatást képesek adni
- Image Library-t nyújtanak
- Komplex alkalmazásokat és azok folyamatos fejlesztését, javítását vagy kivezetését kínálják ügyfeleik részére.



1.ábra: A publikus felhő szolgáltatási lánca (saját szerkesztés [12] alapján)

1.4 A három vezető szolgáltatóplatform

A felhőszolgáltatók közül a három nagy óriást, a piacvezetőket emelem ki. Mindhárom felhőszolgáltató, a Microsoft, a Google és az Amazon megoldásai rendelkeznek azokkal a szigorú feltételekkel, melyekkel képesek a nagyvállalatok biztonsági követelményeinek megfelelni. Ehhez üzemeltetik a megfelelő számú adatközpontokat, amivel az egész világon redundánsan képesek a szolgáltatásaikat nyújtani. Az adatközpontok biztonságát ma már közös szempontok alapján értékelik. A globális adatközpont minősítési rendszert az Uptime Institute dolgozta ki még 1993-ban. Az ő besorolásaik alapján beszélünk TIER I-IV-ig minősített adatközpontokról. Az általuk végzett audit vizsgálja az adatközpontok elektronikus, mechanikus, monitoring- és automatizációs alrendszereit is. Természetesen az egyes szinteken az elvárt rendelkezésre állás is növekszik, 99,67%-tól egészen 99,995%-ig. A TIER IV minősítéssel rendelkező adatközpontoknak abszolút hibatűrőnek kell lenniük. (Pl. Magyarországon az Invitech rendelkezik TIER III-as minősítéssel).

Mindhárom szolgáltató különböző platformokon is elérhető, és mind rendelkezik mobil applikációval is, mellyel a szolgáltatásaik nagy része elérhető. A piacvezetők élen járnak a termékfejlesztésben, és nagy erőkkel fókuszálnak minden olyan új technológiai trendre, ami valamilyen módon kapcsolható a saját platformjukhoz. Ezáltal nemcsak az IT világában szereznek vezető szerepet, hanem megrendelőként hatnak a hozzájuk köthető iparágakhoz is (energiaellátás és -tárolás, zöld energiák alkalmazása, robotika, automatizálás, önvezető autók stb.).

Ami a dolgozatom szempontjából kiemelkedő ennél a három nagyvállalatnál, az az utánpótlás kinevelése és a felhasználók oktatása. Mindhárman elkötelezettek az inkubátorok kialakításában és a jövő technológiáin gondolkozó és dolgozó kutatók, startupok támogatásában. Nemcsak Észak-Amerikában, hanem Európában és Ázsiában is több inkubátorházat nyitottak, ahol várják és segítik az innovátorokat. Ezen felül ingyenes képzéseket – természetesen a saját termékeik bemutatásával – tudatosító videókat vagy webinárokat tartanak ingyenesen vagy fizetős formában. Ezeket sok esetben lokalizálják – tehát hazánkban magyar nyelven is nagyon sok oktató videóval, tananyaggal találkozunk.

1.4.1 Microsoft Azure Platform

A Microsoft felhő alapú megoldásait 2008-ban jelentette be Steve Ballmer, azzal a céllal, hogy konkurenciát építsenek fel a Google web alapú irodai alkalmazásaihoz. Akkor ezekkel a szavakkal indította útnak a szolgáltatást: „egy internetközpontú, az összekapcsolt rendszerekre koncentráló technológia lesz, mely igyekszik felszámolni a helyi gépeken futó alkalmazások és az operációs rendszer közötti elvi különbséget, s a függőségek megszüntetését vették célba. A virtualizációs technológiák eredményeit felhasználva egy olyan rendszer kidolgozásán fáradoznak, mely a minimálisra igyekszik redukálni a felhasználó gépén futó operációs rendszert, illetve az alkalmazások szükségességét, vagyis egyre nagyobb mértékben a hálózat biztosítaná ezek lehetőségeit az egyedi PC-k számára.”

A Microsoft korábban leginkább a nagy üzleti partnerekre fókuszált, ma már a Google térhódítása miatt nemcsak a KKV, hanem az otthoni felhasználók felé is professzionális szolgáltatást nyújt.

Mára a szolgáltatások széles palettáját kínálja, több, mint 600 féle szolgáltatása elérhető, melyek a jelenleg felkapott technológiák további fejlesztésének támogatását tűzték ki célul (pl. Machine Learning és Internet of Things). Szolgáltatásait georedundánsan nyújtja világszerte, adatközpontjai 42 + 12 (2018 végéig kerülnek átadásra) régióban vannak. Az Azure is rendelkezik európai adatközpontokkal (Dublin és Amszterdam). [19]

1.4.2 Google

A Google céget 1998-ban alapították, eleinte online hirdetések céljára. A Microsoft Office termékek Google megfelelőit (Google Docs) kínálták felhő alapon – elsőként az összes óriás között. Ezzel a lépéssel nagyot löktek a piacon, a Google Docs hatására lépett

a Microsoft is nagyobbat, és tette felhő alapon is elérhetővé a ma már töretlen népszerűségnek örvendő Office termékeket.

A Google gyors fejlődésnek indult, és az elmúlt 20 év során ma már kevés az a terület, ami az internethez kötődik, és amivel ne foglalkozna. A Google minden elérhető platformra fejleszt, és rengeteg alkalmazást tesz elérhetővé a felhasználói számára, amely alkalmazások ma már a mindennapjaink része (google maps, google translate, google analytics, AdWords stb.).

A Google felhő adatközpontjai Észak-Amerikában, Ázsiában és Európában találhatók, összesen 6 régióban, 18 zónában, de pontos számukat nem ismerjük. 2013 óta az adatközpontok közötti kommunikáció titkosított, valamint 2017 óta az adatközpontok teljes energiaellátása megújuló energiákkal történik. A Google progresszív biztonsági rétegeket alkalmaz a fizikai helyszínek, hardver és szoftver, a vállalati és fogyasztói számítástechnikai folyamatok és adatok vizsgálatában. A rétegelt védelem segítségével a Google adatközpontjai is vállalati szempontból biztonságosnak tekinthetők, rendelkezik ISO 27001, 27017 és 27018-as minősítéssel. [20], [21]

Dolgozatom szempontjából azért érdekes, mert nagyvállalati szolgáltatásokat nyújt (G-Suite), melyek biztonsági szempontból megfelelőek ennek a felhasználói körnek. Ezen az üzletágon olyan nagy mamutokkal dolgozik együtt, mint a Salesforce, az Oracle, az Adobe vagy az IBM.

1.4.3 Amazon Web Services

Az Amazon Web Services (AWS) 2006 óta elérhető, eleinte kliens oldali webszolgáltatások nyújtásával lépett piacra. 8 adatközponttal rendelkezett, melyek közül egy, az írországi adatközpont található Európában. A szolgáltatások REST és SOAP üzenetekkel érhetők el, HTTP protokollon keresztül. Az összes szolgáltatásért használat alapján (pay-as-you-grow) számláz az Amazon.com.

Két fő termékkel indult, az Amazon EC2-vel (virtuális szerver) és az Amazon S3-mal (tárolómegoldások). Ma már minden felkapott információtechnológiai termék megtalálható a palettáján, úgymint a Maching Learning, az Internet of Things, adatbázismegoldások stb.

Jelenleg 17 + 6 (beindításuk folyamatban) földrajzi régióban találhatók meg. Az AWS garantálja, hogy minden régióban keletkezett adat a régión belül marad. Minden régió

több rendelkezésre állási zónával rendelkezik, amelyek egy vagy több különálló adatközpontból állnak, amelyek mindegyike redundáns áramellátással, tárolókapacitással és összeköttetéssel rendelkezik, külön-külön létesítményekben.

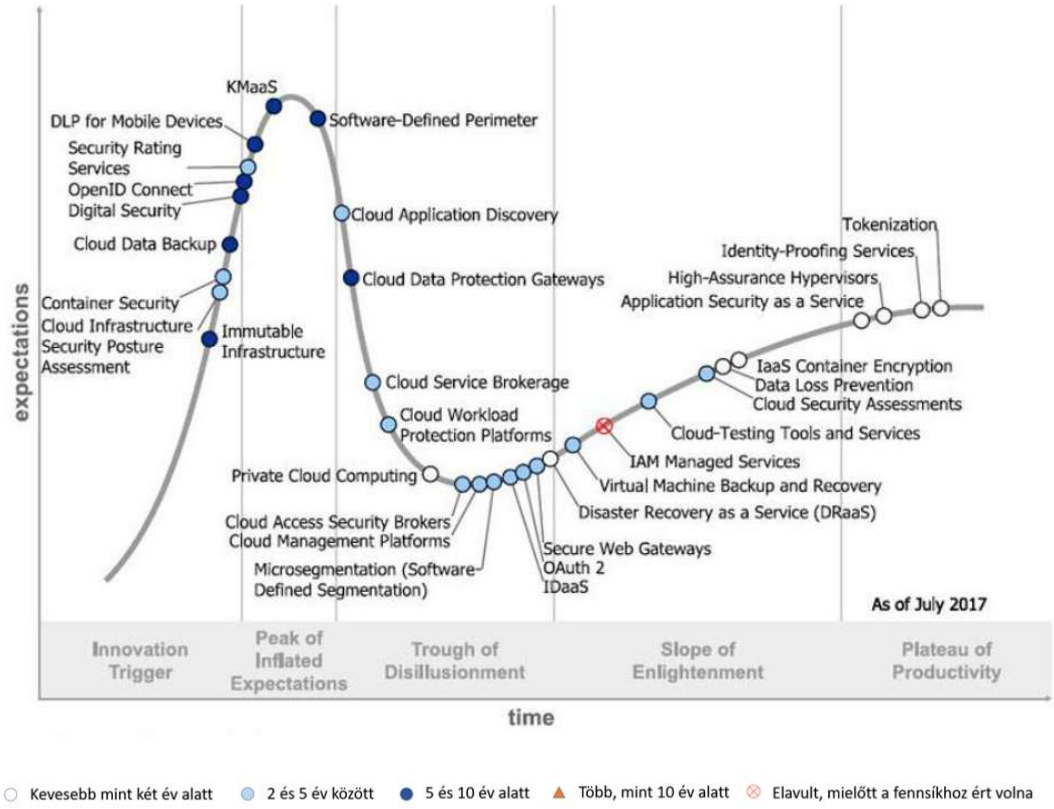
A 2011-től üzemeltett GovCloud mellett 2014 óta szigorúan zárt, kormányzati megoldások nyújtását indította el, amit kimondottan az amerikai titkosszolgálat kiszolgálására épített ki. Ennek neve „Secret Region", a GovCloud mellett, attól elkülönítve szolgáltat, ugyanakkor ugyanannak a célcsoportnak.

Az AWS a nagyvállalatok további motiválása érdekében hibrid felhős megoldást kezdett kínálni 2018 második felétől a Dell segítségével. Ennek alapja egy Dell fizikai szerver, mely összekapcsolható az Amazon felhős tárolószolgáltatásával, gyorsítva a lokális adatelérést. A rendszert biztonsági mentéshez, archiváláshoz, katasztrófa utáni helyreállításhoz, felhős adatfeldolgozáshoz, tárolórétegzéshez, illetve migrációhoz egyaránt ajánlja az Amazon. Fő előnye, hogy a fizikai szerver megoldást a saját felhőszolgáltatásához kapcsolja. [22], [23]

1.5 A felhőtechnológiák jövője

Az évtized legforradalmibb és talán legnépszerűbb IT infrastruktúra megoldása a felhő technológia. Ahogy az a korábbi technológiai újítások során is megfigyelhető volt, ez a fajta lelkesedés egy idő után alább hagy, és jogosan merül fel az alkalmazhatóság és a hatékonyság kérdése. A Gartner minden évben közzéteszi az úgynevezett hype cycle grafikont, vagyis az új technológiák körüli felfokozott várakozásokat és kijózanodás fázisait mutató görbéjét. A görbe öt szakaszból áll – a technológia megjelenése, a túlzott elvárások csúcsa, a csalódás verme, a kijózanodás emelkedője és a termelékenység fennsíkja -, számba veszi a különböző technológiákat, és azokat érettségi szintjük alapján értékeli, osztályozza. Minden egyes technológia végigmegy az innovációs robbanás, a felfokozott várakozások és a kijózanodás vagy csalódás fázisain, majd eljut a valódi hatékonyságig. A 2017-es hype cycle grafikon szerint a felhőtechnológiák túl vannak a csúcson, és tartanak a görbe legmélyebb pontja felé. Lassan, várhatóan 2-5 éven belül érik el a valódi hatékonyság szintjét. [24]

Így a hype cycle a vállalatoknak egyféle iránytűként működik, melyik technológiákba érdemes időt, pénzt fektetni és melyek érésére érdemes még várni.



2.ábra: A Gartner Felhőszolgáltatásokra vonatkozó hype-cycle ábrája, 2017 [24]

Akár magánszemélyként, akár nagyvállalati döntéshozóként találunk kiforrott felhő megoldásokat. Ezek a szolgáltatások biztonságban, elérhetőségben, rugalmasságban, szolgáltatási színvonalban is kiemelkedők, ugyanakkor tisztában kell lennünk a friss technológiák használatának előnyeivel, hátrányaival és kockázataival.

Már jócskán ott tartunk, amikor a vállalatok kezdik megérteni, kitalálni, pontosan mire is használható a felhőtechnológia. A korai felhasználók mindennapjainak már részese a technológia, az innovatív cégek is bevezették vagy tervezik bevezetését.

Továbbá a nagyvállalatok is elkezdhetnek a gazdasági megtérülésben gondolkodni, hiszen a felhő lassan az ötödik fázisba ér, kiforrott technológiává válik, ami a termelékenység szempontjából a legkedvezőbb.

1.6 Szabályozási környezet

A technológia szabályozási köre a felhőtechnológiák esetében folyamatosan változik. Egy új, folyamatosan fejlődő és folyamatos növekedésben lévő technológia esetén nehéz egy viszonylag állandó szabályozási szempontrendszert meghatározni. Nemzetközi és hazai ajánlásokkal találkozunk, melyek közül választani nehéz egyetlen egyet.

Figyelembe kell venni az adott ország törvényeit és szabályozásait az adatra, adatkezelésre és adatvagyonra vonatkozóan, valamint az adott iparágra vonatkozó esetlegesen szigorúbb szabályozási rendszert. Ezt a csokrot befolyásolhatja az adott vállalat tulajdonosi szerkezete, valamint az üzemeltetésért felelős csapat földrajzi elhelyezkedése, mely hozhat szigorúbb vagy megengedőbb adatkezelési politikát a vállalat életébe.

A felhőre nemcsak a használt technológiából eredő szabályozások vonatkoznak. Mivel a felhő esetében az adat tárolása, kezelése, mentése, vagy helyreállítása harmadik fél által történik - tehát az adat kikerül a vállalat (vagy magánszemély) tulajdonából – az adatra vonatkozó helyi vagy régiós jogi szabályozások vonatkoznak a felhőre is.

1.6.1 Az információbiztonságot, adatkezelést érintő érvényben lévő, Magyarországra vonatkozó jogszabályok, rendeletek, ajánlások

A fejezetben felsorolt törvény, illetve rendelet jogi szempontból ugyan, de befolyásolja a felhő használatát országunkban. Bár közvetett módon, nem a technológiáról szól, mégis meghatározza az adat kezelésére vonatkozó körülményeket, elvárásokat.

GDPR

A 2018. május 25-étől érvénybe lépő rendelet nagy port kavar. A rendelet javaslata 2016. áprilisában került elfogadásra, és egy igencsak rövid felkészülési időt követően bevezetésre. A rendelet minden uniós tagállamra vonatkozik, és nem betartás, nem megfelelés esetén komoly pénzbüntetést von maga után.

A rendelet, amely a nemzeti jogszabályokat felülírva egységesíti az uniós tagállamok adatkezelési szabályait, a természetes személyeknek a személyes adatok kezelése tekintetében történő védelmére és a személyes adatok szabad áramlására vonatkozó szabályokat állapít meg.

Ezen felül pedig a természetes személyek alapvető jogait és szabadságait és különösen a személyes adatok védelméhez való jogukat védi, a magánszemélyeknek nagyobb betekintést és jogokat ad az adataik kezelésével kapcsolatban, ezzel párhuzamosan pedig a cégek ez irányú kötelezettségeit növeli, a mulasztásokat pedig pénzbüntetéssel sújtja.

Többek között kitér a személyi adatok kezelésére, az adatkezelés jogszerűségére, a helyesbítés és a törléshez való jogra, a gyermekek személyes adatainak kezelésére, valamint az adathordozhatóság jogára is. A rendelet továbbá kimondja, hogy az európai

adatok tárolási helyének Európán belül kell lennie. Ezzel felügyelve az európai adatok felügyeletét, és biztosítva az adatok sértetlenségét, rendelkezésre állását és bizalmasságát. [25], [26]

MSZ ISO/IEC 27000

Az MSZ ISO/IEC 27000-es szabványcsalád a nemzetközi ISO szabványcsalád magyar megfelelője, mely az informatika, a biztonságtechnika és az információbiztonság-irányítási rendszereket szabályozza. A nemzetközi ISO/IEC követelmények magyar nyelvű változatát a Magyar Szabványügyi Testület teszi közzé. [27]

A Magyar Nemzeti Bank 2/2017. (I.12.) számú ajánlása a közösségi és publikus felhőszolgáltatások igénybevételéről

Az elérhető szabványokon, törvényeken kívül a Magyar Nemzeti Bank (MNB) ajánlását tartom kimagaslónak ebben a témában. [28]

Az ajánlás kimondottan pénzügyi szervezetek számára készült, akik a 2013. évi CXXXIX. törvény 39. §-ában meghatározott jogszabályok hatálya alá tartoznak. Az ajánlás kimondja, hogy a jogszabályi megfelelősséget biztosítani kell. Továbbá kimondja, hogy a pénzügyi szervezetnek el kell készítenie még a felhőszolgáltatás bevezetését megelőzően a kockázatelemzését, és kockázatcsökkentő intézkedési tervet kell készítenie. Kitér a szerződéskötésre, a bevezetésre, az üzemeltetésre és a kivezetésre is. Külön fejezetben tárgyalja a biztonságra vonatkozó elvárásait, úgymint adatbiztonság, az informatikai folyamatok biztonsága, az erőforrások védelme, az üzemeltetés és fejlesztés biztonsága, a felhasználók jogosultság-kezelése és a biztonságmenedzsment. A dokumentum teljes körű, és sokkal szigorúbb feltételeket szab egy felhőszolgáltatóval szemben, mint egy hazai nagyvállalat.

A fentiek közül a GDPR betartása kötelező, ugyanakkor azok a vállalatok, ahol az informatikai rendszerek biztonsága kiemelkedően fontos, ott érdemes az MNB követelményspecifikációját tanulmányozni. Az I.12-es ajánlás használható és gyakorlati leírást ad, mely mind a döntéshozók, mind a szakértők számára érthető, tehát segíti őket a közös megoldás megtalálásában is.

1.6.2 A felhőtechnológiákra vonatkozó nemzetközi szervezetek

A szabályozói kör egyes szereplőit egy táblázat segítségével a funkcióik mentén csoportosítottam. Dolgozatomban azokkal a szervezetekkel – és a hozzájuk köthető

ajánlásokkal – dolgozom, melyek a legfrissebb eredményt adják, melyek jelenleg érvényben vannak, és Európán belül, illetve azon belül Magyarországon is használatban vannak. [29]

A számítási felhőhöz kapcsolható fontosabb szervezetek, bizottságok, szabványosítók csoportosítása		
Cloud szervezetek	**Biztonsággal foglalkozó szervezetek**	**Üzemeltetéssel, felügyelettel foglalkozó szervezetek módszertanai vagy ajánlásai**
NIST	**CSA**	**ITIL**
ISO	**ENISA**	**ISO 270xx**
IEEE	**OWASP**	**COBIT 5**
OCC	**ISO**	**Togaf 9**
CSCC	**COBIT**	**FitSM**
DMTF	**GDPR**	
ETSI		
GICTF		
SNIA		

1.táblázat: A felhőszolgáltatáshoz köthető szabályozó testületek, egyesületek, fórumok (saját készítésű táblázat [29] alapján)

Ahogy a fenti táblázatból látszik, a piacon több, a témával foglalkozó szervezet, bizottság, fórum működik, melyek munkája csak részben összehangolt. Az érvényben lévő ajánlások közül azokat emelem ki, melyek a hazai piacon is alkalmazhatók, és olyan útmutatást, irányt adnak, melyeket felhőbiztonsági aspektusból fontos ismerni, és érdemes megfontolni.

Felhőtechnológiával foglalkozó szervezetek

Ebből a csoportból két szervezetet tartok jelentősnek, melyeket a dolgozatom céljainak elérése szempontjából is vizsgáltam. A fenti táblázat alapján látható, hogy több szervezet is foglalkozik a számítási felhővel, és készítenek ajánlásokat, útmutatásokat, meghatározásokat a bevezetésre, használatra vonatkozóan. Azonban most csak azokkal a szervezetekkel foglalkozom, melyek eredménye a hazai nagyvállalatok számára is elfogadott érvényű lehet. Mivel a legtöbb számítási felhőszolgáltató az Egyesült Államok területén működik, ezért a rájuk vonatkozó törvények és szabályozások ismerete és

valamilyen mértékű alkalmazása a szolgáltatás használata során elkerülhetetlen – például az NSA felé történő adatszolgáltatási kötelezettsége számos amerikai nagyvállalatnak.

Érdemes azokat a szolgáltatókat megvizsgálni egy esetleges bevezetés során, melyeknek európai vonatkozásai is vannak, európai szabvánnyal, minősítéssel és nem utolsó sorban adatközponttal rendelkeznek, ez utóbbi követelmény a GDPR szempontjából is fontos. A magyar nagyvállalatok jelentős többsége rendelkezik ISO tanúsítvánnyal, és rendszeresen végeznek informatikai auditot. Ezért az a felhőszolgáltató, aki maga is ISO tanúsítvánnyal rendelkezik, és az általa nyújtott szolgáltatást is minősíti tanúsító szervezet által, megbízhatóbb partnernek minősül az amúgy igencsak nagy felhőszolgáltatói piacon. [29]

A felhőtechnológia nem nevezhető még kiforrott technológiának, de az utóbbi években sokat fejlődött, így a nagyvállalatok számára is elfogadható szolgáltatási szintet képesek biztosítani ügyfeleik számára.

1. **NIST**

A NIST, az amerikai szabványügyi hivatal által a 2011-ben létrehozott 800-145-ös dokumentum volt az első, ami a ma is érvényben lévő felhő meghatározást adta (1.2 fejezet). Peter Mell és Timothy Grance szerzőpáros definíciója szerint a számítási felhő egy működési modell, amely bárhol használható, kényelmes, igény szerinti hálózati hozzáférést biztosít a konfigurálható, közös blokkokból álló számítási erőforrásokhoz, amely erőforrások azonnal kiadhatók minimális felügyeleti erőfeszítéssel vagy szolgáltatói közreműködéssel. A NIST ezen felül meghatározza a számítási felhők öt alaptulajdonságát (essential characteristics), melyek a 1.2.1 fejezetben kifejtésre kerültek. [2]

- Igény szerinti önkiszolgálást biztosítanak (On-demand self service)
- Jó hálózati hozzáféréssel rendelkeznek (Broad network access)
- Erőforrás készletekre épülnek (Resource pool)
- Teljes rugalmasságot biztosítanak (Rapid elasticity)
- Mért szolgáltatások (Measured Service)

2. **ISO és IEC**

Az információk és informatikai rendszerek rendelkezésre állásának, bizalmas jellegének és sértetlenségének biztosítására a Nemzetközi Szabványügyi Szervezet (ISO) és a

Nemzetközi Elektrotechnikai Bizottság (IEC) közös műszaki bizottsága dolgozta ki az ISO/IEC 27000-es szabványsorozatot. [27] A 27000-es szabványcsalád az információbiztonsággal, üzemeltetéssel, kockázatmenedzsmenttel foglalkozik, és határoz meg alapvető kritériumokat.

A 27000-es szabványcsaládból az ISO/IEC 27017-es szabványt emelem ki, ami kimondottan a számítási felhő felhasználói szabványa lett.

ISO/IEC 27017:2015

A szabvány [30] az ISO/IEC 27002:2013 szabványon [31] alapul, és olyan szervezetek számára tervezték, melyek a felhőszolgáltatásokat – vagy szolgáltatókat - információbiztonsági szempontok alapján kívánják vizsgálni, kiválasztani. A szabványt a felhőszolgáltatók is használhatják útmutatóként az ügyfeleikkel közösen elfogadott védelmi ellenőrzések végrehajtásához. A szabványban szerepel a 27002-es szabványban lefektetett 37 vezérelv, melyeket a 27017-ben további 7 új alapelvvel egészítették ki, melyek kimondottal a felhőre vonatkoznak:

1. Megosztott szerepek és felelősségek a számítási felhőben
2. Felhőszolgáltatás ügyféleszközök eltávolítása és visszaszolgáltatása a szerződés megszűnésekor
3. Az ügyfelek virtuális környezetének védelme és elválasztása a többi ügyféltől
4. A virtuális gép alapkövetelményei az üzleti igények kielégítésére
5. Felhőalapú számítástechnikai környezet adminisztratív műveletei
6. Lehetővé teszi az ügyfelek számára, hogy figyelemmel kísérjék a megfelelő tevékenységeket a számítási felhőben
7. A virtuális és fizikai hálózatok biztonsági menedzsmentjének összehangolása

A NIST, mint az amerikai szabványokért felelős szervezet foglalkozott először a felhőtechnológiák szabványosításával. Bár maga a technológia is erről a kontinensről indult el, ma már világméretekben is hódít. Nemcsak az amerikai szabványoknak, jogi környezetnek és amerikai adatvédelmi törvényeknek kell megfelelnie a technológiának, hanem most már a világ szinte bármely pontján, a helyi szabályozásnak megfelelő

környezetbe kell illeszkedni. A NIST fektette le az alapokat, de véleményem szerint túl általános megfogalmazású.

Európán belül az ISO kimondottan a felhőszolgáltatásokra írt szabványai (27017 és 27018) alkalmazhatók, de ezek a szabványok kötöttek és nem sok mozgásteret hagynak a felhőszolgáltatás üzemeltetőinek.

Amennyiben a vállalat felhőszolgáltatás bevezetése előtt áll, a szolgáltató ISO minősítése már jelezhet valamit. Azok a szolgáltatók, akik az európai üzleti piacot komolyan gondolják, már jóval korábban gondot fordítottak arra, hogy a helyi szabályozásoknak is megfeleljenek. Nem utolsó sorban a szabvány kialakításában is részt vettek.

Cloud Biztonsággal foglalkozó szervezetek

1. **ENISA**

Az ENISA információbiztonsággal foglalkozó európai szervezet, mely 2009-ben adta közzé a felhő biztonságot és kockázatokat tartalmazó tanulmányát, melynek elkészítésében számos, a felhőtechnológiával foglalkozó nemzetközi vállalat és szervezet szakértői vettek részt. [32]

A tanulmány megállapítja, hogy a felhő méretgazdaságossága és rugalmassága egyaránt barátságos és ellenséges biztonsági szempontból. Az erőforrások és az adatok tömeges koncentrációja vonzóbb célpontot jelent a támadók számára, de a felhőalapú védelem erősebb lehet, skálázható és mindemellett költséghatékony. A tanulmány lehetővé teszi a számítási felhők számítástechnikai biztonsági kockázatok és előnyök tájékozott értékelését - biztonsági útmutatást nyújtva a felhőalapú számítógépek potenciális és meglévő felhasználói számára. A tanulmányban 35 kockázattípust határoztak meg, mellyel segítséget kívánnak nyújtani a leendő felhasználók számára.

A tanulmány kitér arra a tényre is, hogy mind a kormányok, mind a KKV-k szembesülnek azzal a valósággal, hogy munkatársaik nagy része felhőalapú szolgáltatásokat fog használni, függetlenül attól, hogy ezt a vállalati belső szabályozás megengedi-e számukra.

A vállalatok támogatása érdekében az ENISA közzétett egy ellenőrző listát, mellyel a jövőbeli, még szolgáltatásválasztás előtt álló ügyfeleknek kíván segíteni, miszerint:

1. Mérjék fel a felhőszolgáltatások kockázatait

2. Hasonlítsák össze a különböző felhőszolgáltatók ajánlatait

3. Szerezzenek biztosítékot a biztonságra vonatkozóan a kiválasztott felhőszolgáltatókról

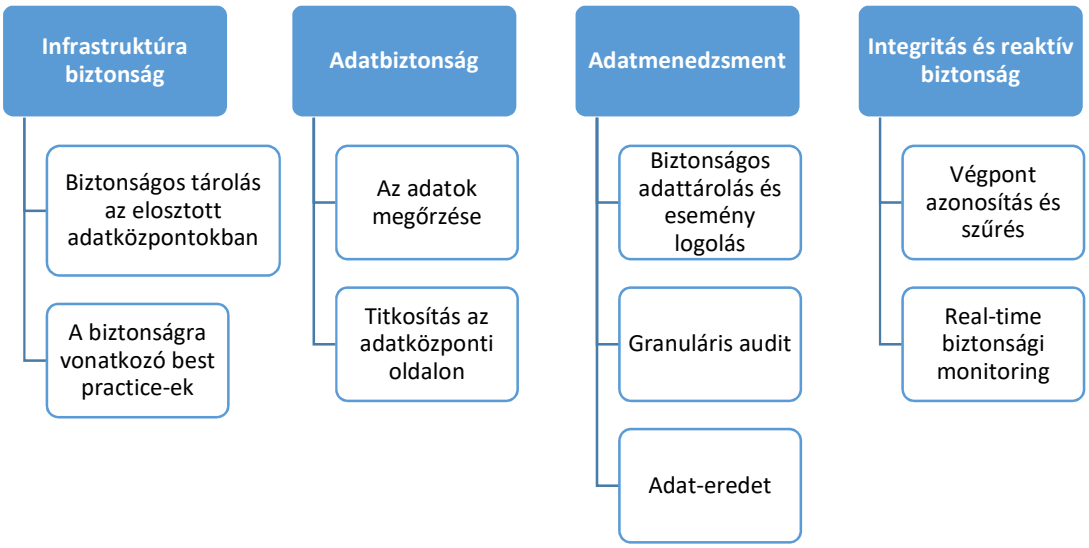
4. Csökkentsék a felhőszolgáltatókra háruló biztonsági terheket

A biztonsági ellenőrző lista tartalmazza a biztonsági követelmények valamennyi aspektusát, beleértve a jogi kérdéseket, a fizikai biztonságot, a szakpolitikai kérdéseket és a technikai kérdéseket is.

Az ENISA európai szinten foglalkozik a kormányzati felhő kérdésével és kialakításával, és dolgozik az Európai Felhő Stratégián. [33]

2. CSA

A szövetség a Security Guidance For Critical Areas of Focus in Cloud Computing v4.0 dokumentumban [34] átfogóan és minden piaci szereplő számára használható módon mutatja be a felhőtechnológiákat. A CSA a felhőtechnológiákat használó piaci szereplők számára gyűjtötte össze és csoportosította a felhő technológiájából származtatható kockázatokat.



3.ábra: A felhőtechnológiából eredő főbb kockázatok csoportosítása a CSA alapján [34]

[35] Ez a fajta megközelítés segíti a döntéshozókat abban, hogy a felhőszolgáltatás technológiai kockázatait csoportosítva a lehetséges kockázatokra felkészülve, azok befolyását csökkenteni tudják. Azokat a technológiai szempontokat vizsgálja, amiket mindenképpen érdemes megfontolni egy infrastruktúra fejlesztésénél, bővítésénél vagy tervezésénél. Az adatállomány méretének növekedése olyan menedzsmentet, adatkezelést, tárolókapacitást és keresőkapacitást igényel, amit nagyvállalati környezetben kiépíteni is hatalmas költséggel jár, ezért ezen a szinten is érdemes a felhőbe való költözés lehetőségeit megvizsgálni.

A felhőszolgáltatás kockázatainak vizsgálatakor tulajdonképpen a CSA-féle csoportosítás négy fő területe ad releváns információt, és segít abban, hogy az ISACA által felsorolt kockázatokat strukturálva értelmezni lehessen, és akár a megfelelő felelősök bevonásával legyen összegyűjtve a vállalatot érintő kihívások és kockázatok csoportja. A CSA négy olyan csoportot alkot meg, ami a hálózati szinttől a menedzsment szintig érinti a vállalati adatvagyont, tehát az összes megjelenési forma megvizsgálható abból a szempontból, hogy a felhő használatát képes-e az adott nagyvállalat biztonsági szempontból menedzselni minden platformon. Sokan abba a hibába esnek, hogy csak gazdasági döntésként gondolnak a felhőre, mint költségcsökkentő megoldásra, ugyanakkor azok olyan kockázati elemeket hozhatnak a vállalat életében, aminek kezelésére nincsenek felkészülve.

3. OWASP

Az OWASP szervezet [36] egy nyílt társaság, mely nemzetközi szinten fogadja a tagokat soraiba. Elsősorban gyakorlati megközelítésből foglalkozik minden felkapott technológiával és mindenki előtt igyekszik a lehető legtöbb és legértékelhetőbb esettanulmányokat összeszedni.

A felhővel kapcsolatban az esettanulmányokat elemezve alkotta meg a legfőbb 10 kockázati tényezőt (lsd. részletesen a függelékben), mellyel a bevezetés előtt állókat kívánja segíteni. Tanulmányai főként a legelterjedtebb, legtöbbször előforduló eseteket gyűjti össze és elemzi.

Dolgozatomban a gyakorlatiassága és tapasztalata miatt foglalkozom velük. Elemzéseik a szakemberek számára adnak gyakorlati útmutatót a várható kockázatokra és az azt megelőző felkészülésre. Mivel gyakorlati oldalról közelít, számomra az OWASP adja a

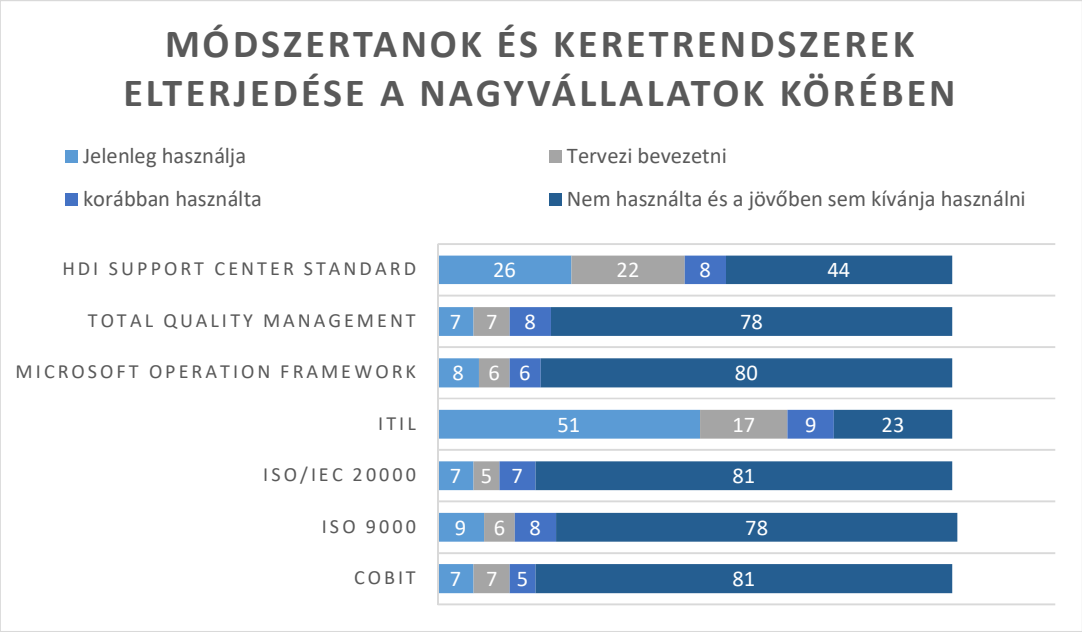
legnagyobb hozzáadott értéket, mindamellett, hogy felhőmegoldásokra általános megoldásokat kínál.

Mindamellett felmérve a felhő kihívásait, a biztonságra jelentős hangsúlyt fektettek. [37] Számomra a legnagyobb kihívást a felhasználók okozta biztonsági rés okozza, az OWASP ajánlásai és megoldási javaslatai között találtam használható ötleteket. Az OWASP ajánlások alapja a felhőt is először meghatározó NIST dokumentumok. [38]

Üzemeltetéssel, felügyelettel foglalkozó szervezetek módszertanai

1. **ITIL**

Informatikai rendszerek üzemeltetésére és fejlesztésére szolgáló módszertan, illetve ajánlás gyűjtemény. Az ITIL egy felhőszolgáltatás bevezetése és kezelése során is képes segítséget adni a vállalat számára, bár alapvetően nem erre a technológiára fejlesztették. A módszertan segítségével hatékonyabban és sikeresebben vezethető be a vállalat IT infrastruktúrájába a felhőszolgáltatás, melynek eredménye egy fenntartható és átlátható szolgáltatáscsoportot eredményez. A nagyvállalatok többsége az ITIL módszertant használja. [39], [40]



4.ábra: Módszertanok és keretrendszerek elterjedése a nagyvállalatok körében (saját készítésű táblázat a [39] alapján

Az ITIL 5 fő fejezetből áll, melyek a következők:

Szolgáltatásstratégia (Service Strategy): segíti a vezetőket abban, hogy megértsék, hogyan fog különbözni a szervezetük a konkurens megoldásoktól, és ennek megfelelően hogyan elégíti ki mind a külső, illetve a belső ügyfeleket. Ebben a fázisban egy stratégiai

dokumentum készül el, melynek legfontosabb részei a Szolgáltatás-portfólió kezelés és a Pénzügyi menedzsment.

Szolgáltatástervezés (Service Design): Ebben a szakaszban a stratégia megvalósítására projekt-terv készül. A terv részletezi az új szolgáltatás bevezetésének minden vonatkozását, a bevezetéshez és üzemeltetéshez szükséges támogató folyamatokkal együtt. A kötet legfontosabb fejezetei az Üzemeltetés és üzemvitel biztosítása, Kapacitástervezés valamint az Informatikai- és üzembiztonság.

Szolgáltatás bevezetés (Service Transition): A megtervezett szolgáltatás létesítéséhez és a környezet módosításához szükséges folyamatok leírása. Fontos fejezetek a Változás- és verziókezelés, Konfigurációmenedzsment és Dokumentációkezelés.

Szolgáltatásüzemeltetés (Service Operation): Az előzővel szorosan összefüggő kötet tárgyalja a szolgáltatás folyamatos és hibamentes üzemeltetéséhez szükséges folyamatokat és szervezési kérdéseket. A folyamatok garantálják a szolgáltatási megállapodásokban (SLA) vállalt szolgáltatásminőséget. Legfontosabb fejezetek a Hiba- és igény- és incidenskezelés.

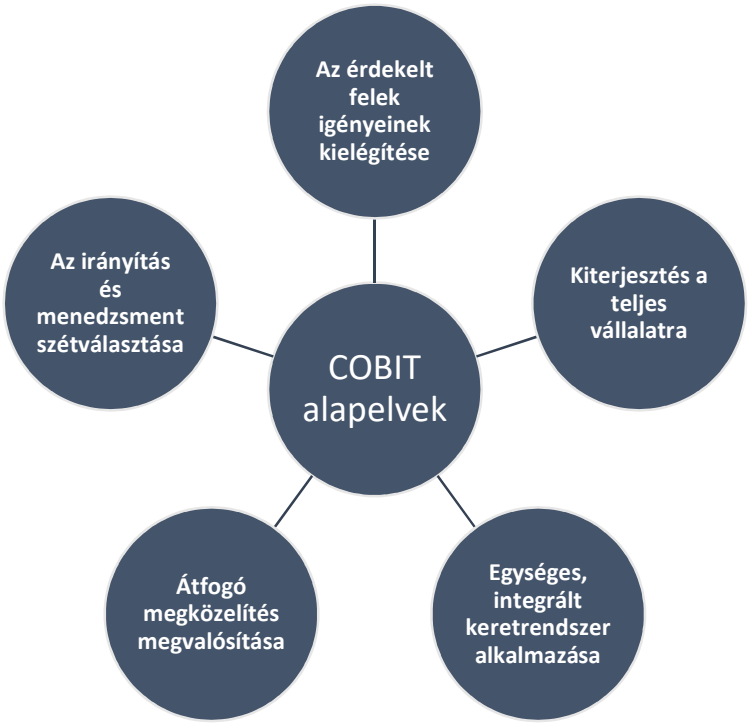
Folyamatos szolgáltatásfejlesztés (Continual Service Improvement)**:** ebben a fejezetben találhatók azok a szempontok, melyek segítségével a kívánt szolgáltatást folyamatosan fejlesztik és bocsátják a belső ügyfelek részére. Cél, hogy ne egy állandó minőségi szintet nyújtsanak, hanem folyamatosan magasabb minőségi szintet érjenek el – mellyel az ügyfeleik (jelen esetben belső ügyfelek) elégedettségét is elérik. Kiemelt fejezetek a Szolgáltatási szint mérése, riportolása (jelentése) és menedzsmentje.

2. COBIT 5

Az ISACA [41] az információrendszerek biztonságával, a vállalati IT felelős irányításával és menedzselésével foglalkozik, valamint az IT-val összefüggő kockázatok és törvényi megfelelőséggel kapcsolatos tudás, képesítések, közösség, szakmai képviselet és oktatás vezető globális szolgáltatója.

Az ISACA alakította ki és folyamatosan fejleszti a COBIT keretrendszert, amely segít az IT szakembereknek és vállalatvezetőknek, hogy megfelelhessenek az IT irányítással és menedzseléssel kapcsolatos felelősségeiknek a biztonság, a kockázatok és a kontrollok terén, hogy értéket teremthessenek az üzleti oldal számára.

A jelenleg érvényben lévő COBIT 5 átfogó keretrendszert nyújt a szervezeteknek a vállalati IT irányításával és menedzselésével kapcsolatos céljaik eléréséhez. A COBIT 5 abban segíti a vállalatokat, hogy a legnagyobb hasznot hajtsák az IT-ból azáltal, hogy egyensúlyt teremtenek az eredmények megvalósítása, a kockázatok mértékének optimalizálása és az erőforrások felhasználása között. A COBIT 5 lehetővé teszi az IT átfogó szemléletű irányítását és menedzselését az egész szervezetre vonatkozóan, kiterjed az üzleti és IT szakterületek minden felelősségi körére, és figyelembe veszi a belső és külső érdekelt felek IT-val kapcsolatos elvárásait is. A COBIT 5 általános érvényű és hasznos bármilyen méretű szervezet számára, az üzleti, a nonprofit és az állami szektorban egyaránt. A COBIT 5 a vállalati IT irányítás és menedzselés öt alapelvén nyugszik:



5.ábra: A COBIT 5 öt alapelve (saját szerkesztés a [42] alapján)

A COBIT a felhőszolgáltatások bevezetése során is döntő szerepet kaphat. Mivel a keretrendszer az eredmények megvalósítása, a kockázatok mértékének optimalizálása és az erőforrások felhasználása között teremt egyensúlyt, a felhőszolgáltatás bevezetésének vizsgálatakor kiválóan alkalmazható. Másik nagy előnye, hogy nemcsak nagyvállalati körben nyújt megoldást, hanem a piac valamennyi szereplője számára értelmezhető és használható.

Gyakorlati tapasztalatom leginkább nagyvállalati környezetből szereztem. Minden nagyvállalat, ahol megfordultam, használta az ITIL-t valamilyen szinten. Sajnos azt tapasztaltam, hogy az ITIL bevezetése/használata/megfeleltetése egész embert, sokszor egész szervezetet kíván. Alapvetően nagyon jók az elvei, a felépítése, de annyira bonyolult, és a meglévő vállalati folyamatokhoz nem illeszkedő, hogy hatalmas erőforrásokat vesz igénybe vállalaton belül úgy, hogy használata sosem lesz 100%. Minden változásra reagáltatni kell az ITIL-t, és mindenről „értesíteni" kell, ami a vállalaton belül informatikai szempontból történik. Egy olyan vállalatban, ahol a folyamatok nagy része automatizált, a rendszerek felügyelete naprakész, a riportok automatikusan elérhetőek az ITIL olajozottan képes működni, sőt, együttműködni a vállalati IT-val. A gyakorlat azonban azt mutatja, hogy bizony vannak „elfelejtett" szerverek, rég nem használt alkalmazások jelenleg is érvényes adatokkal feltöltve, manuális áthidalások rendszerek között. Amíg ezek a helyzetek fennállnak, sajnos az ITIL egy megerőszakolt választás lesz a vállalatok életében, és nem lesz képes kielégíteni azokat az elvárásokat, amikre a módszertant fejlesztették.

1.7 A publikus felhőszolgáltatás bevezetése során a technológiából származtatott kockázati tényezők

A felhő alapú megoldásokkal szemben felmerülő leggyakoribb ellenérvek az átláthatóság és az adatok feletti kontroll hiányával kapcsolatosak. Való igaz, hogy az adatok felhőben való tárolásával a vállalat számtalan olyan lehetőségről lemond, amelyek a hagyományos megoldásoknál adottak. Így a felhő használata során nehézségbe ütközik az adatok fizikai tárolási helyének, valamint a kontroll környezet (védelmi intézkedések) felmérése is. A felhőszolgáltató ugyan szerződésben vállalja a rá bízott adatok védelmét, azonban a legtöbb vásárlónak nincsen lehetősége megbizonyosodni arról, hogy ezt a védelmet pontosan hogyan valósítja meg. A felhő infrastrukturális alapjait a világon elszórt hatalmas adatközpontok biztosítják, amelyek azonban nem homogének sem felépítésükben, sem védelmüket tekintve.

A globális információs hálózat korában nehezen elképzelhető, milyen lenne a világ az internet nélkül. A felhőtechnológia talán legegyértelműbb hátránya a megoldások függősége mind a szolgáltató mind a vásárló internetkapcsolatától. Ennek az érvnek azonban – főként itt, Európában – egyre kevesebb a létjogosultsága, mivel a szolgáltatási színvonal messze meghaladja a biztonságos mértéket (egy vállalati internet szolgáltatás esetén a szolgáltató által vállalt SLA szint legtöbbször legalább 99,5%-os [20]). [43]

A felhő alapú technológia megjelenésének egyik legérdekesebb hozadéka az a folyamat, ahogyan az új tényezők átrajzolják a hagyományos kockázati térképeket. Az informatika kezdete óta az üzleti élet számára a kockázatok köre néhány bővülést leszámítva (közösségi média megjelenése, számítógépes bűncselekmények megjelenése stb.) többé-kevésbé állandó volt. A felhő megjelenésével és széles körű terjedésével egy vállalat hagyományos adattárolóit akár teljes mértékben felválthatják a felhő megoldások, amellyel az adattárolásból fakadó kockázatok (adatvesztés, lopás, illetéktelen hozzáférés) kikerülnek a cég közvetlen ellenőrzése alól. Az üzleti életben most először állhat elő az a helyzet, hogy a cég számára kritikus adatok legnagyobb része egy külső fél őrizete alatt áll. Ezzel együtt a felhő használatának legnagyobb kockázata az adatkezeléssel kapcsolatos. A közeljövő egyik nagy kihívása az lesz, hogy ezeket az adatkezelési kockázatokat hogyan tudjuk majd megfelelő keretek között tartani. Ugyanakkor a felhő is csak egy szolgáltatás, amelyet a vállalat igénybe vesz. Minden újdonsága ellenére kockázati szempontból nem sokban különbözik más szolgáltatásoktól, amelyeket külső partnerek bevonásával valósít meg az adott vállalat.

1.7.1 A felhőszolgáltatási lánc egyes elemeinek kockázatai

Nem elég a felhőszolgáltatások bevezetésekor csak a technológiai kockázatokat sorra venni. Fontos, hogy a teljes szolgáltatási lánc minden egyes pontjának kockázata adja a teljes eredményt. Ennek a teljes kockázati mátrixnak azonban a kezelési módja sokszorosan összetett feladat, ennek feladata több szakterület közös munkájából áll. Különösen fontos lesz a megváltozott környezetben ezen szakterületek együttműködése, és a közös cél érdekében egy közös, a teljes láncra vonatkozó kockázatmenedzsment kialakítása.

Az adatközpontok kockázati tényezői

A felhőszolgáltatások bevezetése ellen érvelve a legtöbbször a biztonsági kockázatokat említik a nagyvállalatok vezető szakemberei [48]. Mivel a felhőszolgáltatás igénybevétele miatt az adott szolgáltatáselem üzemeltetése vagy az üzemeltetés egy része már nem a vállalati IT feladata lesz, ezért a legnagyobb kockázatot az jelenti, hogy a külső szolgáltató hogyan nyújtja a kívánt szolgáltatást, rendelkezésre áll-e a vállalati adatvagyon a szükséges pillanatban, illetve ez az adatvagyon nem kerül-e illetéktelenek kezébe.

Ezen felül pedig a szolgáltató képes-e megőrizni az adatok sértetlenségét, integritását és rendelkezésre állását.

Ugyanakkor az üzleti szolgáltatást nyújtó számítási felhő adatközpontjai erősebb biztonsággal rendelkeznek az alábbi területeken. Ha azt vesszük alapul, hogy egy felhőszolgáltató egyszer fizeti meg a fentiek költségét, érezhető az, hogy erre sokkal több energiát, időt és pénzt áldozhat, ugyanakkor a fajlagos költsége mégis nagyságrendekkel alacsonyabb lesz.

Az adatközpontok védelme többrétegű, általában három rétegben alakítják ki, melynek mélysége minden egyes szolgáltatónál változik. Ez a fajta védelmi rendszer biztosítja azt, hogy a felhasználók adatai több szintű védelmet élvezve akkor is biztonságban legyenek, ha egy adott ponton az illetéktelen hozzáférést keresők sikerrel járnának. A minősített, üzleti szolgáltatást nyújtó felhőszolgáltatók adatközpontjaiban futó szolgáltatásoknak része az esetleges támadások, behatolási kísérletek folyamatos figyelése is, a szakemberek és automatizált rendszerek képesek észlelni, megelőzni és semlegesíteni a biztonsági fenyegetéseket, általában már azelőtt, hogy bármiféle gondot okozhatnának.

Három rétegű védelem:

1. **Fizikai védelem:** az ügyfelek adatait a szolgáltatások működtetésére dedikált adatközpontokban tárolják, amelyek földrajzilag redundánsak, vagyis egymástól távoli pontokon épültek fel. Ez csökkenti annak esélyét, hogy valamilyen lokális esemény (természeti katasztrófa, az energiahálózat hibája stb.) megzavarja a szolgáltatást, mivel szükség esetén egy másik távoli létesítmény képes átvenni az érintett adatközpont munkáját.

   Az adatközpontokat természetesen eleve úgy tervezték meg, hogy a természeti behatásoknak és a (fizikai) behatolási kísérleteknek is ellenálljanak. Az illetéktelen behatolók elleni intézkedéseknek része egy igen komoly, folyamatosan működő beléptetési rendszer, melyben az engedélyeket mindig csak az adott napra és munkára adják ki, és a hozzáférési szinteket az abszolút szükségesre korlátozzák.

   Mindenkinek, aki be akar jutni az adatközpontba egy többlépcsős beléptető-rendszeren kell átjutnia melyben az okos belépőkártyák mellett a biometrikus azonosítás is szerephez jut, a helyszínen biztonsági szolgálat tartja szemmel a

látogatókat, az adatközpont területét pedig folyamatosan kamerákkal, mozgásérzékelőkkel figyelik és riasztórendszerekkel biztosítják.

A különféle természeti katasztrófák esetére is különféle automatizált rendszereket telepítenek az adatközpontokban, így például tűzoltórendszereket, amelyek a lehető legjobban kímélik a hardvereket. Emellett olyan rackeket használnak, amelyek egy földrengés esetén képesek megvédeni az érzékeny eszközöket a sérüléstől.

A hálózatot annak peremén és a hálózatban elhelyezett eszközök segítségével védik. Az alapelv az, hogy csakis azokat a kapcsolatokat, csak olyan kommunikációt engedjenek át, amely a rendszer működéséhez feltétlenül szükséges, minden más portot, protokollt és kapcsolatot blokkolva.

A rendszer routerein hozzáférés-jogosultsági listákat (ACL) használnak, amelyek tartalmazzák az információkat arról, hogy milyen kapcsolatok férhetnek hozzá egy-egy objektumhoz a rendszeren belül, illetve, hogy milyen jogosultságokkal bírnak, mit tehetnek az adott objektumokkal. A hosztokon IPsec protokollcsomagok biztosítanak védelmet, és természetesen a hálózatot több szinten működő tűzfalak is védik a támadásoktól. A routereken működő biztonsági rendszer lehetővé teszi, hogy a behatolási kísérleteket, illetve a különféle sebezhetőségeket hálózati szinten észleljék.

Az adatközpontokon belüli hálózatokat fizikailag is szegmentálják, a kritikus back-end szervereket és tárolókat, valamint a publikusan elérhető interfészeket egymástól független rendszerek védik.

2. **Logikai védelem:** számos kontroll és folyamat védelmezi a hoszt gépeket, a rajtuk futó applikációkat, illetve mindazokat a felhasználókat, akik ezeket a gépeket és alkalmazásokat használják.

   A hosztokon és applikációkban végzett műveletek többsége automatizált, az emberi beavatkozás minimális – így igyekeznek a következetlen konfigurációból eredő hibákat kizárni, illetve a káros tevékenységeket kiszűrni.

   Az adminisztrátori hozzáférést szigorúan ellenőrzik, minden személynek a lehető legminimálisabb szintű hozzáférést adják az adatokhoz, hogy adott műveleteket el tudjanak végezni. A rendszerben végzett tevékenységeket, illetve a

hozzáféréssel rendelkezőket folyamatosan monitorozzák (legyenek jelen akár fizikailag az adatközpontban, akár távoli kapcsolat révén).

Security Development Lifecycle (SDL): egy szoftverfejlesztési folyamat, amelyet a Microsoft alkalmazott és javasolt a szoftver karbantartási költségeinek csökkentése és a szoftverbiztonsággal kapcsolatos szoftverek megbízhatóságának növelése érdekében. [49] A klasszikus spirális fejlesztési modellen alapul. A szolgáltató a szoftverek és szolgáltatások tervezése, fejlesztése és telepítése során folyamatosan ellenőrzi, hogy megfelelően érvényesülnek-e a biztonsági szempontok. Az SDL segítségével igyekeznek még az egyes szolgáltatások elindítása előtt azonosítani a lehetséges sebezhetőségeket, támadható felületeket és fenyegetéseket, és kiiktatni ezeket a rendszerből.

Az adatokat természetesen antimalware szoftverek is védik, amelyek a káros programokat akadályozzák meg abban, hogy hozzáférjenek bármihez a rendszeren belül, vírussal fertőzzék meg azt vagy férgeket juttassanak be. A szoftverek feladata az is, hogy a fertőzött állományokat karanténba zárják, megelőzve a további károkat.

3. **Adatvédelem:** a publikus felhőszolgáltatások általában több bérlős, nagymértékben skálázható szolgáltatások, ami azt jelenti, hogy adataink sokszor más ügyfelek adataival osztoznak a fizikai hardveren.

   A modern adatközpontokban azt az adatvédelmi problémát, amit ez jelenthet, már korábban sikerült feloldani. Az adattárolás és -feldolgozás olyan, speciálisan a szolgáltatás számára fejlesztett megoldásokon keresztül történik, amelyeknek célja a több bérlős környezetek kiépítése, kezelése és biztonságossá tétele. Az így kialakított rendszernek köszönhetően adatainkhoz más ügyfelek nem férhetnek hozzá és nem módosíthatják azokat.

   Mindezek mellett a felhőalapú szolgáltatásokban számos titkosítási megoldás is található, amelyek akkor is védik az adatokat, ha azokhoz a többszintű védelmen keresztül eljutna egy illetéktelen behatoló. [50]

A kommunikációs útvonal során fellépő kockázati tényezők

Az adatok titkosítása:

Az üzleti felhőszolgáltatók kiválasztásakor nem utolsó szempont, hogy milyen titkosítást használnak az ügyfelek adatainak megőrzésére. Az adatok titkosítása jogosulatlan személyek számára olvashatatlan, még akkor is, ha áttöri a tűzfalat, átszivárog a hálózaton, fizikai hozzáférést biztosít a készülékeihez, vagy megkerüli a helyi gépen található engedélyeket. A titkosítás az adatokat átalakítja, így csak a titkosítási kulcsokkal rendelkező személy férhet hozzá. [51]

A felhőszolgáltatók akkor tekinthetők üzletileg minősített szolgáltatónak, ha a titkosításkor az iparági szabványú biztonságos adatátviteli protokollokat használják az adatok átadása során - akár a felhasználói eszközök és az adatközpontok között, akár az egyes adatközpontok között. [52]

Például a Microsoft felhőszolgáltatás [53] során többféle titkosítási módszert, protokollt és algoritmust használ termékein és szolgáltatásain keresztül, hogy segítse az adatok biztonságos elérési útját és elősegítse az infrastruktúrában tárolt adatok titkosságának védelmét. A Microsoft az iparág egyik legerősebb, legbiztonságosabb titkosítási protokollját használja az adatokhoz való jogosulatlan hozzáférés ellen.

Az alkalmazott protokollok és a technológiák közé tartoznak a következők:

A **Transport Layer Security / Secure Sockets Layer (TLS / SSL)**, titkosítási protokollok, melyek az Interneten keresztüli kommunikációhoz biztosítanak védelmet. A TLS és SSL protokollok titkosítják a hálózati kapcsolatok szegmenseit a szállítási réteg felett.

Az **Internetes protokollbiztonság (IPsec),** iparági szabvány protokollkészlet, amely az IP csomagok szintjén biztosítja a hitelesítést, az integritást és az adatok titkosságát, amik átvitele a hálózaton keresztül történik.

Advanced Encryption Standard (AES)-256 (a NIST által kialakított) szimmetrikus kulcsadat-titkosítás, melyet az Egyesült Államok kormánya fogadott el a **(DES) és az RSA 2048** nyilvános kulcs titkosítási technológia helyettesítésére.

BitLocker titkosítás, amely az AES-t használja a Windows szerver és kliens gépek teljes kötetének titkosítására, amely virtuális Trusted Platform Module (TPM) hozzáadásakor

használható Hyper-V virtuális gépek titkosítására. A BitLocker a Windows Server 2016-ban is titkosítja az árnyékolt VM-eket annak biztosítása érdekében, hogy a rendszergazdák ne férjenek hozzá a virtuális gépen belüli információkhoz.

A vállalati infrastruktúrából adódó kockázatok

Érdemes egybevetni a felhő által nyújtott, a szolgáltatási szintre vonatkozó vállalásokat a belső IT elvárásaival, képes lesz-e a leendő felhőszolgáltatás ugyanazokat – vagy jobb – paramétereket nyújtani, mint a belső üzemeltetés. Szintén meg kell határozni a kérdését annak, ki lesz a felelős a saját infrastruktúra-környezet üzemeltetéséért, illetve a felhőben lévő adatok menedzsmentjéért. Azoknál a szolgáltatásoknál, amelyeknél a felhőelemek megjelennek, az egyik legfontosabb felhasználói elvárás az adatbiztonságot követően, hogy a szolgáltatást úgy lehessen használni, mintha az házon belül lenne. Tehát biztosítani kell azt az adatkapcsolatot, mintha a szolgáltatás a nagyobb sávszélességgel rendelkező belső hálózatot használná. És hasonlóan biztosítani kell tudni akkor is, ha ez az elem egy földi szolgáltatáselemmel áll adatkapcsolatban (tehát a két elem között adatkapcsolat van).

A felhasználói végeszközök műszaki paramétereiből adódó kockázatok

Ebben a fejezetben csak a felhasználói eszközök kockázatait gyűjtöm össze, a humán faktorból eredő mindennemű kockázatok elemzésével a 2. fejezetben foglalkozom.

A felhasználói eszközök legfontosabb feladata az adatok létrehozása, megjelenítése, kezelése vagy módosítása. A vállalati IT szempontjából azok a legbiztonságosabb eszközök, melyek működését a lehető legjobban kontroll alatt tudják tartani, vagy legalább a rajta futó eseményeket monitorozni képesek. Bármilyen olyan eszköz, amin vállalati adat úgy jeleníthető meg, hogy az eszköz a vállalati infrastruktúrához kapcsolódik, de magát az eszközt a vállalat nem tudja menedzselni, kockázatossá válik. Ma már számos olyan megoldás létezik, amivel szegregálható egy adott eszközön a személyes adat a vállalati adattól. A szakemberek elsődleges célja a technológia használata minden olyan helyzetre, ami biztonsági kockázatot jelent a vállalatra nézve.

A felhasználói végeszközök kockázatának jelentős részét a mobileszközök eltérő platformja és a platformok gyengeségei okozzák. A legtöbb olyan esetben, amikor a technológia tehető felelőssé az adatvesztésért, adatlopásért, annak oka a nem megfelelően tesztelt, vagy a nem kellően biztonságos mobil platform. A gyártók igyekeznek a lehető

legbiztonságosabb mobil operációs rendszereket megalkotni, sokszor azonban a széles körű menedzselhetőség igénye miatt a biztonsági szinten kell áldozatot hozni. Több nagyvállalat elvárt igénye, hogy a felhasználói végeszközöket menedzselni tudja, ezáltal kontrollja legyen ezen eszközök felett.

Eugene Kaspersky szerint [54] a mobil platformok jelentősége is megnőtt és elsődleges céljaivá váltak a hackereknek, mert szinte mindenki használ okostelefont. Véleménye szerint a három vezető mobil operációs rendszer közül a Microsoft operációs rendszere a legbiztonságosabb, a cég az utóbbi években nagy erőfeszítést tett a biztonság javításának érdekében. A legbiztonságosabb platform címnek oka lehet az is, hogy ebből a mobil operációs rendszerből van a legkevesebb a piacon. Ez lehet az oka annak, hogy az Android rendszert használók vannak a legnagyobb veszélyben, hiszen számosságukat tekintve a piac nagy részét ők uralják.

1.7.2 A legelterjedtebb kockázatok, hatásuk és kezelési módjuk publikus felhőszolgáltatások használata esetén

Ma leginkább gazdasági és biztonsági oldalról nézik meg a bevezetés lehetőségeit, és többnyire az egyik, illetve a másik oldalhoz tartozó szakemberek nem beszélnek közös nyelvet. Az informatikai szerepek, feladatok változásai mindenképpen megkövetelik a felhasználók széleskörű kiszolgálását, ugyanakkor az informatikai biztonságért felelős szakemberekre ma sokkal több feladat hárul, mint korábban bármikor. A technológia fejlődése, a vállalati infrastruktúra határainak elmosódása, vagy a kisfogyasztói (konzumer) piacon elérhető eszközök és applikációk hatalmas választéka hozhat olyan kockázatokat egy eddig zárt környezetbe, ami megváltoztatja a rendszer biztonságáért felelős szakemberek mindennapi feladatait, és új kompetenciák megszerzésére kényszeríti őket.

A felhőtechnológiából eredő kockázatok egy része a felhőszolgáltatótól öröklődik, a másik részét a szolgáltatást igénybe vevő generálja. De mindkettő kezelését megelőzi a felhőbe való költözés kockázata, amikor adatok a migráció során sérülhetnek [45], [47]. Több szolgáltató a szabályozói kör nyomására adott ki útmutatókat, amik a döntésben, a migrációban és az azt követő felhővel való együttélésben segítenek. Az ENISA 2009-ben kiadott közleményében 35 kockázattípust határozott meg, amiből kiemelt 8 olyan kockázatot, melyet priorizált bekövetkezési valószínűségük és hatásaik mértéke szerint. Az ezt követő évben az ENISA mellett a CSA is megjelentette azt a top 7 felhőt fenyegető

veszélyforrást, amit a CSA szakmai tagjai állítottak össze meglévő tapasztalataik alapján. A két szervezet eredményeit az OWASP kockázati listával [44], [46] hasonlítom össze, hogy egy átfogó képet adjak a több szervezet által meghatározott felhőtechnológiákra vonatkozó kockázatokról. (lsd. Függelék). [32]

A függelék és az OWASP kockázati lista alapján készítettem el a fenyegetettség-hatás-megelőzés táblázatot, melynek segítségével a várható és eddig tapasztalt kockázati tényezők és azok megelőzési módjai szerepelnek.

Fenyegetettség	Hatás	Megelőzés
Szoftverhibák	Alkalmazások hibás funkcionalitása	Szoftverfejlesztési ciklusok és tesztelési előírások betartása
Szoftverfrissítés és verzióváltás	Operációs rendszerek, adatbáziskezelők és alkalmazások hibás funkcionalitása	Frissítések tesztelése éles üzleti környezetben történő használat előtt. Visszaállási terv megléte.
Adatvesztés	Szolgáltatás sérülés	Redundáns adattárolás, mentési és visszaállítási terv
Infrastruktúra biztonság	Nincs kiépítve többszörös fizikai biztonsági zóna	Szükség esetén lehessen személyi támogatást igényelni a szolgáltatótól.
Az admin hozzáférések nem szerepkör alapúak		Különböző admin jogosultság kiosztására legyen lehetőség, a bevezetés során a vállalat kapjon egyértelmű leírást a felhőszolgáltatótól a biztonságos beállításokra vonatkozóan
Internetszolgáltató kiesése	A felhőszolgáltató elérhetetlenné válik	Redundáns internetszolgáltató választása
Illetéktelen hozzáférés	Információk szivárgása	Erős felhasználóazonosító eszközök alkalmazása
Multitenancy és Fizikai biztonság	Egy másik bérlő befolyásolhatja a többi bérlő biztonságát	Lehessen kérni dedikált szervert, amin csak az adott vállalat adatai vannak.
Incidenskezelés	Az elosztott adatközpontok miatt a naplózás is elosztott, szükség estén nem elérhetők a naplófájlok	A szolgáltató biztosítson lokalizált információt, mely a vállalat elvárásainak megfelel
Szabályozói megfelelés	A vállalat szigorúbb szabályozási megfelelés alá esik, mint amit a felhőszolgáltató nyújtani tud.	A szolgáltató rendelkezzen megfelelő minősítésekkel, lokalizált szabályrendszerrel és régiós adatközponttal
Üzleti folytonosság és rugalmasság	Adatvesztés léphet fel Katasztrófahelyzetben nem működik a szolgáltatás	Rendelkezzen a felhőszolgáltató a vállalat számára megfelelő SLA-val, és legyen a szerződésben rögzítve a szolgáltatás

Fenyegetettség	Hatás	Megelőzés
(Nem az ügyfél igényei szerint van kialakítva)		folyamatosságának megoldása, valamint a szolgáltatásminőség
Beragadni egy szolgáltatási környezetbe	Nehéz vagy nem megoldható a szolgáltatásváltás	Az adat költöztetése ne ütközzön akadályokba, legyen rá megfelelő esettanulmány (egyszer már valaki sikeresen meg tudta csinálni). Kompatibilis legyen más felhőszolgáltatók alkalmazási protokolljaival, nyelvével.
Szolgáltatás és adatintegráció/védelem	Adatátvitel során sérül az adatvédelem (a végfelhasználó és az adatközpont vagy az adatközpontok között)	A szolgáltató nyújtson SLA-t, biztosítsa az adatkapcsolat titkosítását, az adattovábbítás során használjon adatszeletelést.
Felhasználói identitás federációja	Hibrid megoldás esetén, nem minden esetben megoldható a felhasználók federációja	Hibatűrő, robosztus, magas rendelkezésre állású rendszert érdemes választan; tartsa a jelszavakat a saját földi rendszerén
Az adat tulajdonjoga és az elszámoltathatóság kockázata	Adatszivárgás vagy adatvesztés	Szerződésben rögzíteni kell, milyen adatvisszaállítási garanciát vállal a szolgáltató adatvesztés esetén, valamint milyen backup rendszerrel dolgozik
Felhasználói adatvédelem és másodlagos adatfelhasználás	Adatvesztés	A szerződésben szerepelni kell, a szolgáltató milyen adatokat használhat vagy nem használhat fel másodlagos célokra. Minden adatra vonatkozik, a közvetlen és közvetett módon (pl., kattintások, kimenő URL-ek stb.) generált adatokra is.

2.táblázat: A publikus felhőszolgáltatások ismert technikai kockázatai és megelőzési módjuk

Összefoglalás

A fejezetben bemutattam a felhőtechnológiák szolgáltatási láncát. Részletesen kitértem a nevesebb szabályozói testületek ajánlásaira és tanulmányaira. Bemutattam azokat a kockázati tényezőket, melyek leginkább foglalkoztatják a nagyvállalatokat, és felsorakoztattam azokat a szempontokat, melyeket a felhőtechnológia választása esetén mindenképpen megfontolandónak tartok.

A felhőtechnológia – minden más informatikai technológiához hasonlóan – hordoz magában biztonsági kockázatokat. Mára azonban ezen kockázatok nagy része feltárásra került, a várható kockázatokat nemcsak a felhőszolgáltatók, hanem a szabályozói kör, és

a felhasználók is ismerik, megismerhetik. Ezért gondolom úgy, hogy a technológiából származtatott kockázatokra fel lehet készülni vállalati szinten. Megfelelő körültekintéssel kiválasztható egy felhőszolgáltató, és biztonságosan üzemeltethető egy olyan nagyvállalati IT infrastruktúra, melynek egy része felhőbe költözött.

A kockázatok megfelelő értékeléséhez a szolgáltatási lánc elemi kockázatai, valamint a három nagy szervezet (ENISA, OWASP, CSA) kockázati rangsorai alapján alkottam meg a kockázati mátrixot. Leginkább azokat a kockázati elemeket illesztettem a mátrixba, melyek hazai nagyvállalatok működésében is felléphetnek, ezáltal kockázatot jelentenek. Ez a mátrix útmutatást adhat a nagyvállalati szektornak, melynek segítségével a bevezetésre szánt technológia kockázatkezelési szempontból értékelhetővé válik.

Az első hipotézisem, miszerint „Feltételezem, hogy a felhőszolgáltatás technológiája képes alacsony kockázati szinten kezelni az adattárolást és -hozzáférést minősített szolgáltató igénybevétele esetén, de ennek együtt kell járnia a humán faktor megfelelő, biztonságtudatos munkavégzésre történő felkészítésével", nem csökkenthetők nullára a felmerülő kockázatok, de maga a rendszer – így a szolgáltatási lánc egyes elemeinek kockázata mérhető, a kockázati mátrixban elhelyezhető, tehát a technológia kockázataira a vállalat felkészíthető.

A fejezethez korábbi kutatási tevékenységem során a publikációim jelentek meg, „How to Develop Cloud Security" (IX.), és a „Biztonság a felhőben. A publikus felhők biztonsági kérdései" (VII).

2 A SZÁMÍTÁSI FELHŐ SZOLGÁLTATÁSI LÁNCÁNAK LEGGYENGÉBB ELEME, AZ EMBERI TÉNYEZŐ

Bevezetés

A fejezetben a korábbi, a technológiával foglalkozó részt egészítem ki a humán faktorral. Az ember az a láncszem a kommunikációs folyamatban, mely az információ minőségét, besorolását, tartalmát és értékét befolyásolni, módosítani képes. Ezt a módosítást vállalati környezetben elfogadott szabályok mentén teszi, mégis azt tapasztaljuk, hogy az előírt – és általa is elfogadott – vállalati szabályokat nem minden esetben tartja be. Az előző fejezet tárgyalásában a hálózati-, kommunikációs- és biztonsági protokollok meghatározták az informatikai rendszer működését az emberi tényező nélkül. Az informatikai rendszer kockázatai nem csökkenthetők nullára, de bekövetkezési valószínűségük számítható, a várható eseményekre fel lehet készíteni a vállalatot. Ebben a fejezetben azt vizsgálom, hogy az emberi tényező bevonásával a további kockázatok mérhetők-e, ahol csak azokkal a kockázatokkal foglalkozom, ahol az ember nem szándékos károkozást tesz. Vizsgálom, hogy az akaratlanul, de az ember hibájából, tudatlanságából bekövetkező problémák milyen hatással vannak a vállalat életére, és melyek azok a pontok a rendszerben, amikor a humán faktor nem várt kockázatot jelent az információ szempontjából. Továbbá vizsgálom, mennyire szabályozható az ember viselkedése az adat védelme érdekében, milyen tényezők befolyásolják a munkavállalót a nem szabályszerű viselkedésre.

A legtöbb leírt szabállyal és szabályozással – mind a rendszer, mind pedig a munkavállalóra nézve – a katonai, a kormányzati és a nagyvállalati szektorban találkozunk. Kutatásom során azért választottam a nagyvállalati környezetet, mert ez a fajta vállalattípus jól szervezett, nemzetközi módszertanokat követ, oktatási, minősítési (auditálás), üzemeltetési és folyamatmodellezési gyakorlattal rendelkezik. A magyarországi nagyvállalatok nagy része multinacionális vállalat, ezért az anyavállalat működését követve, több évtizedes múlttal és tapasztalattal rendelkeznek a fent említett területeken.

Választásom másik oka, hogy a nagyvállalatokban van elég tőke és erőforrás a piacon megtalálható újdonságok és új technológiák kipróbálására. Bár biztonsági szempontból a döntések meghozatala nagy körültekintést igényel, ami önmagában is sok időt vesz igénybe. Ehhez adódik az adott technológia bevizsgálása, tesztelése, kipróbálása, majd a

bevezetéshez kapcsolódó feladatok megszervezése. Kutatásom kezdetekor a nagyvállalatok nem voltak nyitottak a publikus felhőszolgáltatások használatára. Az eltelt négy év során ez a trend gyökeresen megváltozott, ma már több publikus felhőszolgáltatást vesznek igénybe és továbbiak bevezetését tervezik. A privát megoldások költségszintje magas, és a szolgáltatások színes palettája sem éri el a publikus szolgáltatások szintjét. Ezért egyre több nagyvállalat esetében látjuk, hogy publikus felhőszolgáltatást vezet be, melyet illeszt meglévő infrastruktúrája mellé. Sok esetben az így keletkezett informatikai kiszolgáló környezet hibrid megoldássá válik, ami okozhatja az előző fejezetben tárgyalt kockázatokat. Azonban a piac gyorsasága, az ügyfelek és a munkatársak megtartása érekében a nagyvállalatok meghozták azt a döntést, amivel a fenti hármas egységet egyensúlyban képesek tartani.

Mindemellett a biztonság kérdése már nemcsak ezen szakemberek feladata lesz, hanem a vállalaton belül minden egyes felhasználónak érdeke és kötelessége a vállalati adatvagyon megóvása. Korábban nem volt elvárás, hogy a munkavállaló körültekintően járjon el, ha a vállalati informatikai rendszerben dolgozik, mert egyszerűen nem tudott bármihez bármikor hozzáférni, az általa használt eszközök pedig folyamatos felügyelet alatt álltak. Ma már a belső hálózati eszközöket elérve munkát végezni, bárhonnan és bármikor nem okoz problémát. Sajnos azonban a munkaidő és a szabadidő összemosásával a vállalati és a magánfelhasználás összemosása jár együtt. Érdekes azonban megfigyelni azt, hogy a felhasználók szempontjából a vállalati „benti” munka és a felhős munka között nagyobb különbség mutatkozik, mint a technológiák illesztésekor.

Választásom harmadik oka pedig a nagyvállalatoknál dolgozó munkatársak munkafeltétele, környezetük tulajdonságai. A vizsgált nagyvállalatok munkatársai vállalati laptoppal és csúcskategóriás vállalati mobilkészülékkel rendelkeznek. A vizsgálatom során ezeket a tulajdonságokat adottnak vettem. A munkatársak a rendelkezésükre bocsátott eszközöket személyes célokra is használják, ugyanakkor az eszközök biztonságáért, védelméért a vállalat felelős. Továbbá a vállalati oktatásokat sem szüntették meg a válság idején, mint ahogyan az a KKV szektorban tapasztalható volt. Így a nagyvállalatok munkatársai megkapják a folyamatos fejlődés lehetőségét, hogy lépést tartsanak a technológiai változásokkal.

Nagyvállalati szinten jellemző, hogy fejlett IT üzemeltetés áll rendelkezésre, akik a korábbi incidenseket képesek voltak kezelni, keretek között tartani. A felhő

bevezetésének tervezésekor felmerül a kérdés, hogy ugyanez a csapat képes lesz-e a felhő használatából eredő incidensek kezelésére, a problémák elhárítására. Rendelkeznek-e megfelelő kompetenciával és erőforrással az új feladatkör elvégzéséhez. Amikor a számítási felhő mellett érvelünk, elsődlegesen a rendelkezésre állása (sokszor 99,9%), a skálázhatósága, az alacsony környezeti terhelése, a költségek csökkentése és tervezhetősége merül fel. Amit véleményem szerint fontos még megemlíteni, hogy a felhőrendszerekben kialakított szabályok mindenkire egyformán érvényesek. Tehát egy vállalkozás tulajdonosára, vezetőjére, informatikusára és az asszisztenciájára egyformán – ellentétben egy saját tulajdonban lévő informatikai környezettel, ahol a biztonsági rést legtöbbször maga a vezető vagy az informatikus nyitja meg azzal, hogy számukra több mindent lehet megtenni a vállalati hálózaton belül.

2.1 Nagyvállalati sajátosságok

A nagyvállalatok működése eltérő a piacon található egyéb szereplők működésétől. Speciális, mert a szabályok betartása és betartatása rájuk nézve kötelező [26], [27], [40], [41], és minden esetben mért, vizsgált és felügyelt. Ugyanakkor a nagyvállalati szektor adja a hazai GDP több, mint felét, [42] ezért különösen nagy figyelem övezi szabályszerű működésüket, bevételüket. A hazai GDP 53%-át az 500 legnagyobb vállalat adta Magyarországon 2012-ben. [55]

A nagyvállalatok külső (a piacon lévő auditálható szabályok, szabványok, törvények) és belső (Informatikai Stratégia, BCP, DRP, Informatikai Biztonsági Kézikönyv, Katasztrófaterv stb.) szabályozása is erősebb, mint a piacon lévő kisebb vállalatok esetében. A folyamatos profit érdekében a folyamataik, a belső szabályozásuk, a biztonságuk, az üzletmenet folytonosságuk is folyamatos auditoknak van kitéve. Ennek megfelelően ismerik a legújabb szabványokat, szabályokat, szabályozásokat és törvényeket a saját iparágukra vonatkozóan, melyeknek minden körülmények között igyekeznek megfelelni.

Ugyanakkor a szabályozói körnek időnként maguk is tervezői és tanácsadói, ipari szakértőként részt vesznek az ajánlások, szabályozások kialakításában. Lehetőséget nyújtanak arra, hogy a tervezeteket technológiai, ipari környezetben is tesztelhessék, sokszor a hatályba lépést megelőzően. A nagyvállalatok támogatják az innovatív megoldásokat, és erőforrást nyújtanak az innováció kisebb, de kompetensebb – vagy merészebb – résztvevői számára. Több nagyvállalat épített ki tervező vagy fejlesztő

laboratóriumokat [56], [57], [58], [59], [60], [61], [62], [63], [64], [65], [66], [67], [68], ahol startupokat, kis cégeket, egyetemeket vagy egyetemi hallgatókat, kutatókat engednek közelebb a technológiához úgy, hogy erőforrást biztosítanak számukra. A nagyvállalatok mindig is nagy gonddal támogatták a tudományt, természetesen mindenképpen figyelembe véve a gazdaságosság szempontjait.

Mivel a nagyvállalatoknak folyamatosan meg kell felelniük a kereteknek, a pontos és jól dokumentált munkavégzést a munkatársaiktól is elvárják. Ehhez rendszeresen tartanak vállalati oktatást és képzést, ahol minden olyan új információt, ami a munkavállaló munkájára hatással lehet, igyekeznek bemutatni. Erre megfelelő időt, energiát és pénzt áldoznak, hiszen a megfelelő ismeretekkel rendelkező munkatárs képes egyedül, strukturáltan, a vállalati szabályoknak megfelelően dolgozni.

2.1.1 A nagyvállalati kultúra, a felhasználó és az informatika kapcsolata

A vállalati kultúrát a cég vezetői, tulajdonosai és munkatársai alakítják ki. Egy multinacionális nagyvállalat esetében a vállalati kultúra egy része az anyacégből érkezik és egészül ki a hazai kulturális mintákkal. A kultúrát meghatározza a szektor, ahol a vállalat tevékenységet végez, meghatározza az ott dolgozók életkora, neme, az elvárt feladatok mennyisége, minősége, a vállalati folyamatok, a leadási határidők, a teljesítmény mérése, a hazai vezetőség és a munkatársak kapcsolata. A vállalati kultúra írott és íratlan szabályokból áll.

A vállalati kultúra hat [68], [69], [70], [71], [72], [73], [74], [75], a vállalat biztonságára. Amennyiben az írott és íratlan szabályok megengedők, a várható kockázatok száma is magasabb. Ha a kultúra zárt, folyamataik tiszták, a szabályok megszegése érthető és következetes szankciókat von maga után, melyek a vállalat minden tagjára egyformán érvényesek, a humán faktorból eredő kockázatok száma is alacsonyabb lesz. Fontos, hogy a vállalat a céljainak megfelelően, tudatosan építse fel a saját vállalati kultúráját.

Az informatikai biztonsági szabályok használatánál is hasonló eredményeket tapasztalhatunk. Találkozunk írott szabályokkal, a felhasználó mit tehet és mit nem tehet a vállalati informatikai környezetben. És ugyanúgy megtaláljuk az íratlan szabályokat, melyek a biztonságot fenyegetik, de a felhasználók élnek ezekkel a megoldásokkal is. Fontos tényező lesz a precedensre való hivatkozás, ami a rendszerben megtehető, azt a munkatárs meg fogja tenni.

Ugyanakkor az informatika használata a meglévő vállalati kultúrát is megváltoztatja, hatással lesz rá. Hiszen változik a kommunikáció a felek között, a visszacsatolás sebessége és a kommunikáció minősége, tartalma, ideje, összetétele [76], [77], [78] is. Az informatikai rendszereknek köszönhetően az elküldött adat megmarad, visszakereshetővé, másolhatóvá, idézhetővé válik. Mindennek nyoma marad. Másoldalról pedig az informatika segítségével szervezhetőbbé válik a munkavégzés, egyszerűsödnek a mindennapi feladatok, átláthatóbbá válik az időbeosztás. Fontos, hogy az informatikában valóban mindennek nyoma maradjon, a keletkezett adatok, új információk a megfelelő helyre kerüljenek az informatikai rendszerben, és a folyamatnak megfelelően továbbíthatók legyenek a következő folyamati szintre. Vagy, egy esetleges betegség, személyi változás, vagy a munkakörök átcsoportosítása során a feladatok egyértelműen átadhatók legyenek. Az adminisztrációs tevékenység része lett a mindennapoknak, hogy a vállalati feladatokat folyamatokat és szabályokat – vagyis bizonyos értelemben a biztonságot könnyebb legyen megtartani.

A felhasználónak ennek megfelelően ismernie kell azt az informatikai környezetet, amiben elvárt a részéről a pontos munkavégzés, az adatok pontos kezelése. Ismernie kell, hogy az informatikai rendszer sérülékeny, és az általa kezelt adatok különböző biztonsági besorolásúak. Fontos, hogy körültekintően, és az adat biztonsági szintjének megfelelően járjon el munkája során. Az informatikai rendszert minden felhasználónak védenie kell. A vállalat felelőssége tehát, hogy megfelelő informatikai rendszert, vállalati szabályokat, belső folyamatokat és tudatos munkavállalót hozzon létre. Ehhez pedig mindezeket folyamatosan fejlesztenie kell. Csak a folyamatos fejlesztéssel lehet megfelelő, az információbiztonságot támogató környezetet kialakítani.

2.1.2 A nagyvállalati információs és informatikai biztonsági szabályok humán vonatkozásai

Ahhoz, hogy minden egyes rendszer, munkaállomás és a különböző jogosultságokkal rendelkező felhasználók együtt tudjanak dolgozni a közös rendszerekben, szükség van szabályokra. A szabályok feladata támogatni a megfelelő működést. A szabályok azonban nem sokat érnek, ha azokat nem, vagy csak alkalmanként tartják be. A vállalat feladata tehát betartatni az általa megalkotott vagy bevezetett szabályokat, a munkatárs feladata pedig betartani azokat.

A vállalat sikerességét befolyásolják a vállalati szabályrendszerek. Ma már nem elég csak a technológiára vonatkozóan szabályokat alkotni [79], hanem a legtöbb szabályrendszer a felhasználás módjára és a felhasználó személyére (kompetenciáira, feladataira) is kitér.

Az információvédelem, ahogy azt a bevezetőben is kifejtettem, több biztonsági szint biztonságából áll össze. Ji - Yeu Park szerint ezek a következők: [80]

1. **Információtechnológiai infrastruktúra** (hardver-, szoftver- és hálózatvédelem) – erről a szintről a felhő vonatkozásában írtam az első fejezetben. Ebben a fejezetben a humán faktorból eredő kockázatokra térek ki, azon belül is azokat a helyzeteket vizsgálom, melyekben az emberi tényező nem szándékosan okoz kárt.

2. **Információkezelés** (adatfelvétel, -módosítás, -törlés, informálódás, ill. lekérdezés) – ez a pont kapcsolódik szorosan a humán faktorhoz, hiszen az információkezelés minden pontján munkatárs áll, aki a fenti adatkezelési műveleteket hajthatja végre. Ezeken a különböző pontokon fér hozzá az információhoz és annak tartalmát, minőségét változtatni képes.

3. **Üzleti folyamatok** (folyamatszabályozás, workflow) – a folyamatok egyes pontjai szintén a munkatársakra vonatkoznak. A munkafolyamatok határozzák meg egy poszt tevékenységét, hatáskörét, a kapott feladat és a továbbadandó feladat minőségi paramétereit, időkorlátját, szabályait (pl. az eszkalációs folyamatot), elvégzésének körülményeit.

4. **Szervezet** (információbiztonsági stratégia, kockázatkezelés) – a stratégiaalkotás és a kockázatkezelés nem a munkatárs feladata, de mindkét tervezést az első három szint határozza meg.

A fentiek értelmében az első három szintet vizsgálom, ahol a munkatárs közvetlenül kapcsolódik a vállalati információhoz, információs rendszerhez. Ahhoz, hogy a szervezet ezeken a szinteken megfelelő biztonsággal rendelkezzen, a hozzáféréseket az alábbiak mentén érdemes beállítani:

- **IT szint** – felhasználó azonosításán és a felhasználó tevékenységének monitorozásán van a legnagyobb hangsúly. A rendszerben sem azonosítatlan felhasználót, sem pedig alkalmazást nem szabad beengedni. A felhasználó minden olyan eszközének, mellyel a vállalat rendszereihez hozzáfér, a vállalati IT által menedzselhetőnek kell lennie.

- **Információkezelési szint** – csak a munka elvégzéséhez minimálisan szükséges adathozzáféréseket szabad kiosztani, felesleges hozzáférést a felhasználók számára nem érdemes adni. A munkavállalók hozzáféréseit folyamatosan aktualizálni kell, és egy rendszerben kell kezelni. Amennyiben egy munkatárs jogosultságaiban változás lép fel (elmegy a cégtől, más beosztást kap, tartós szabadságra megy stb.), a jogosultságait annak függvényében változtatni szükséges. Amennyiben ez nem egy rendszerben szerepel, a jogosultságkezelés átláthatatlanná válik.
- **Üzleti folyamat szint** – érdemes a kritikus folyamatokat a felhasználók között megosztani, így minden egyes jogosult felhasználó a kritikus folyamatnak csak egy részét kezeli, és látja. Ezzel a módszerrel helyhez és személyhez kötött jogosultságrendszer alakítható ki.
- **Szervezeti szint** – a stratégiaalkotás és a kockázatkezelésen felül a jogosultsági csoportok kialakítása és a jogosultsági rendszer állandó felügyeletének szabályozása a feladata.

Az információs rendszerek üzemszerű működésének fenntartása érdekében a szervezetek a kockázatokkal összhangban írásos dokumentumokat, forgatókönyveket állítanak össze. Váratlan események bekövetkezésekor ezek alapján állítják helyre az informatikai rendszer normál működését. Ennek értelmében két fontos, az üzlet szempontjából elengedhetetlen dokumentumot emelek ki, melyek a legtöbb nagyvállalatnál megtalálhatók:

Üzletmenet Folytonossági Terv (Business Continuity Plan - BCP)

A vállalat életében a folyamatos működés fenntartása erősen függ az üzleti folyamatokat támogató IT infrastruktúra rendelkezésre állásától.

Egy jól kialakított, átfogó BCP-vel nagy mértékben csökkenthetők az ismert kockázatok (pl. hacker-támadás vagy lopás) nagy része, e mellett a nem várt kockázatok (pl. terrortámadás vagy földrengés) következményeire is képes felkészíteni a vállalatot. A jól elkészített BCP segíti a vállalatot abban, hogy a lehető legrövidebb idő alatt visszaállhasson az üzemszerű működésre, fókuszban azzal az elvárással, hogy a lehető legkisebb költségen tartható az üzemszerű állapot visszaállítása. Szükséges a

dokumentumban számba venni az egyes folyamatok lehetséges fenyegetettségeit, ezek bekövetkezési valószínűségét, a folyamat kieséséből származó esetleges károkat. [81]

Az üzletmenet folytonossági terv kialakításának a legfontosabb célja és várt eredménye, hogy a vállalat képes legyen gyorsabban reagálni a felmerülő fennakadásokra, rövidebb legyen a kríziskezelésre fordított idő, ezáltal az erre fordítandó összeg is alacsonyabb szinten maradjon. Védje a kritikus folyamatokat – egyáltalán a vállalat felismerje, mik a kritikus folyamatai és a kríziskezelésben résztvevők ismerjék saját feladatukat – majd hatásosan tudjanak fellépni egy esetleges akció során.

Katasztrófa Visszaállítási Terv (Disaster Recovery Plan - DRP)

A katasztrófa visszaállítási terv tartalmazza, hogy egy üzleti folyamatot hogyan kell visszaállítani egy nem kívánt esemény után. Szemben a BCP-vel, nem mondja meg, hogy a vészhelyzet alatt hogyan biztosítsuk a folytonosságot.

Természetesen a vállalatok nagy része törekszik a kritikus rendszereinek működését biztosítani, de fel kell készülnie azon esetekre is ha ez belső vagy külső körülmény hatására mégsem tartható fenn a normál munkamenet szerint.

Az ilyen jellegű katasztrófa események két folyamatot kell, hogy elindítsanak. Egyrészről a kiesett erőforrások visszaállítását (DRP), másrészről a kiesett erőforrások nélküli minimális funkcionalitást biztosító üzleti működést. [82] [83]

A külső szabályozások vizsgálatakor több hasznos módszertannal találkozunk. Az első fejezet tárgyalásakor kitértem azokra az információbiztonsági szabályokra, melyeket egy nagyvállalati működés során érdemes figyelembe venni. Most azzal egészíteném ki, hogy a technológián kívül érdemes megvizsgálni, mely módszertanok foglalkoznak az emberi tényezővel. Amennyiben a humán faktor edukálása egy részcél a vállalati stratégiában, akkor képes a vállalat biztonságosabb rendszert felépíteni, hiszen ma már az információs, a kommunikációs lánc elválaszthatatlan részét képezi az ember.

Az emberi tényezőt is figyelembe vevő szabályok vagy módszertanok:

ISO 27001 és 27002

Az ISO más tanulmányok eredményei alapján, miszerint az ember a leggyengébb láncszem az informatikai hálózatban, alkotta meg a 27001:2013-at, aminek segítségével tudatos programot alakít ki a humán faktor képzésére. Ezt három lépcsőben, az alkalmazást megelőzően, az alkalmazás során és bármilyen személyi változás esetén tesz meg. A legfontosabb célja, hogy megvédje a vállalatot, a vállalat ügyfeleit, és a munkatársakat. Célja, hogy a vállalat munkatársai ne csak ismerjék, hanem alkalmazzák a vállalat belső házirendjét, és annak megfelelően viselkedjenek a vállalati eszközök használatakor. Elvárja, hogy minden munkatárs – beleértve a kontraktorokat is – betartsa a vállalat információbiztonsági szabályzatát, és azt a belépéskor megismerje – ez a munkaköri leírás része is lehet - elsajátítsa, amit a vállalat ezt követően vizsgával ellenőriz. Ahhoz, hogy a munkatársak érezzék a felelősségét annak, hogy a rendszerek és adatbázisok, amiket elérnek komoly adatvagyont jelentenek a vállalat számára, az incidenseket megosztják a munkatársakkal is, akár azok megoldásaival együtt, hogy a vállalat egésze ismerje meg a veszélyforrásokat és azok elhárítási módszereit. [84]

COBIT 5

Az ISACA nagy hangsúlyt fektet a humán erőforrás megfelelő kiválasztására és képzésére. Álláspontjuk szerint nem elég csak a technológiai környezet korszerűsítése, legalább annyira fontos a kompetens munkaerő megszerzése és fejlesztése is. Ezt a munkaerő toborzásával, képzésével, teljesítményének értékelésével, elfogadott gyakorlatok követésével érik el, illetve adnak erre vonatkozóan útmutatást. Mind a vállalatvezetés, mind pedig a biztonság nagymértékben függ a munkatársak motivációjától és kompetenciáitól. Tehát ezek folyamatos fejlesztésével a munkatársak szabálykövetése és tudatossága is fenntartható.

A COBIT 5 – ami 2012-től van érvényben - hét különböző Enabler-t tett közzé, mely tényezők önállóan és együttesen is befolyásolják a vállalatirányítás sikerességét [85], [86]:

1. **Belső szabályozások, policy-k:** olyan eszközök, amelyekkel a kívánt viselkedés gyakorlati útmutatássá válik a napi irányítás számára.
2. **Folyamatok:** olyan gyakorlatokat és tevékenységeket írnak le, amelyek bizonyos célok elérését és a teljes informatikai célok elérését támogató kimeneteket eredményeznek.
3. **A szervezeti struktúrák:** a vállalat legfontosabb döntéshozó egységei.
4. **Az egyének és a vállalat kultúrája, etikája és viselkedése:** ez a kérdéskör gyakran alul értékelt, ugyanakkor a szabályok betartása és betartatása szempontjából mérhetetlenül fontos tényező.
5. **Információ:** az összes olyan információ, amelyet a vállalat készített és használt. Operatív szinten az információ gyakran a vállalat legfontosabb vagyona.
6. **A szolgáltatások, az infrastruktúra és az alkalmazások:** ide tartozik az infrastruktúra, a technológia és az alkalmazások köre is, amelyek a vállalatot informatikai folyamatokkal és szolgáltatásokkal látják el.
7. **Az emberek, készségek és kompetenciák:** ezek a területek szorosabban kapcsolódnak a felhasználókhoz, ugyanakkor meglétük az összes tevékenység sikeres elvégzéséhez is hozzájárulnak.

Részletesen a humán erőforrás kiválasztásával, képzésével, személyes motivációival, kompetenciáival foglalkozik a COBIT P07 [87], [88], a felhasználói tréningekkel, képzésekkel pedig a DS7 [89].

Dolgozatom szempontjából a COBIT ajánlásait tudtam leginkább alkalmazni. Számomra könnyen átlátható, logikailag jól felépített, az egyes területek pedig egymástól függetlenül értelmezhetőek, ugyanakkor rendszerben is átláthatók. Az egyes területek könnyen elválaszthatók egymástól, ami a bevezetés során mindenképpen egy előnyös tulajdonsága a COBIT 5-nek. Az ISO rendszerek keretet adnak, melyek a nagyvállalati környezetben már bevezetésre kerültek. Tehát a beléptetéssel, a monitorozással és az információbiztonsági szabályzattal az általam vizsgált nagyvállalatoknál találkoztam. Azonban a COBIT P07 és a DS7 tud nagyvállalati szinten is támogatást nyújtani a folyamatos képzések kialakítására és irányára vonatkozóan. Továbbá a COBIT kimondja, hogy a motiváció fenntartása hatással van a tudatosság szintjére, amit dolgozatomban a 3. fejezet során vizsgálok.

2.1.3 Informatikai biztonsági oktatások

Nagyvállalati szinten az informatikai és információbiztonsági oktatások fontossága miatt a legtöbb esetben azokat az új belépő kolléga kezdeti oktatási csomagjába illesztik. A biztonsághoz köthető oktatások megoldásai lehetnek személyesek a közvetlen vezető által, tantermiek a biztonsági felelős által, vagy egy erre a célra kiválasztott belső vagy külső munkatárs által megtartottak. Nagyobb részben lehetnek E-Learning alapúak, melyet egy szintén elektronikus vizsga követ, vagy előfordulhat a szöveg alapú, önálló feldolgozásra szánt, szintén vizsgához kötött önálló feldolgozás, mint tanulási forma.

Az E-Learning olyan képzési forma mely a tanítási-tanulási folyamatot hatékony, optimális ismeretátadási, tanulási módszerek birtokában megszervezve mind a tananyagot és a tanulói forrásokat, mind az oktató-tanuló kommunikációt, mind pedig az interaktív számítógépes oktatószoftvert egységes keretrendszerbe foglalva hozzáférhetővé teszi a tanuló számára. [90] E-Learningnek nevezhető minden olyan tanítási és tanulási forma, amiben a tananyag feldolgozásához, szemléltetéséhez vagy akár a kommunikációhoz digitális médiumokat használunk.

Az oktatások tartalma leginkább az alábbi felsorolás mentén képzelhetők el:

- Információbiztonsági alapfogalmak
- Törvényi kötelezettségek, vonatkozó jogszabályok
- A vállalat saját, az információbiztonságra vonatkozó szabályai, szankciói
- Kockázatelemzés
- Kockázatmenedzsment
- Adatok és osztályozásuk, a vállalati adatvagyon
- Támadások, vírusok és emberi kártevők – mit tegyél, ha baj van
- Hozzáférés és jelszavak – a hozzáférés mire jogosít fel, hogyan őrizd a jelszavad
- „Tiszta asztal, tiszta képernyő” policy
- Mobil eszközök és Internet használata a vállalaton belül
- Social Hacking – mire érdemes odafigyelni

2.1.4 A felhőszolgáltatások hatása a vállalati kultúrára

A technológia fejlődése az egyik oldalon ad, a másikon elvesz. Könnyítette a munkatársak, de a vállalat életét is, hogy a cég informatikai rendszerét távolról is, akár mobileszközről is könnyedén elérik. Bárhol, akár külföldön is, bármikor, akár éjszaka is, elérik a rendszert, elérik őket is. Ez egyik oldalról szabadságot biztosított, hiszen a munkát tényleg bárhonnan el lehet végezni, ugyanakkor jelenti azt is, hogy valóban, bármikor lehet munkát végezni. Elmosódott a munkaidő eleje és vége, és a feladatokat sokszor hazaviszik a munkatársak.

Ezzel a fajta szabadsággal új lehetőségek is nyíltak. Az anyacéggel vagy egy külföldi partnerrel való közös munka ma már nem jelent hatalmas költségeket, minden résztvevő a saját országából végezheti a feladatait. Egy külföldi projektben való részvétel is könnyebben megoldható, ami a munkavállaló motivációjára is hatással van. Lehetőséget biztosít a rugalmas munkavégzésre, a home office-ra. Ma már a legtöbb nagyvállalat engedi a heti egy nap otthonról való munkát [91], [92] felismerve a nyugodt körülmények között készült produktívabb, hatékonyabb, összeszedettebb feladatmegoldásokat.

A kommunikációs alkalmazások segítségével gyorsabban találják meg egymást a kollégák. A kommunikáció ideje és tartalma is rövidebb lett, a chat funkciókkal bíró alkalmazások esetében tényleg csak egy kérdés és a válasz utazik a csatornán keresztül. A reakcióidő függ attól is, a munkatárs melyik csatornán küldi a feladatot kollégája számára. A 6-os ábrán látható, attól függően érdemes kiválasztani a legmegfelelőbb vállalati alkalmazást, hogy az információt hány résztvevő felé szükséges eljuttatni, valamint mennyire gyorsan érkezzen válasz. A fenti alkalmazások szinte kivétel nélkül megtalálhatók a nagyvállalatoknál, használatuk azonban nem mindenhol ennyire egyértelmű. Érdemes a kommunikáció céljának és címzettjének megfelelő alkalmazást kiválasztani. Ha gyors választ várunk a kérdésünkre, érdemes azt nem e-mail formájában megfogalmazni, hanem egy azonnali megoldást választani – ahol meggyőződhetünk arról, hogy a címzett gép előtt ül (online) és gyorsan választ is képes adni. Viszont, ha több személynek szeretnénk eljuttatni egy információt – érdemes azt a vállalati közösségi portálra helyezni.

6.ábra: Milyen kommunikációs eszköz használata javasolt az válaszidő függvényében (saját szerkesztés Microsoft alapján)

A nagyvállalatnál dolgozó munkavállalónak, aki munkaidejének nagy részét számítógép előtt tölti, nagyon tudatosan kell a munkaidejét beosztania. A legtöbb esetben a munkahelyen a munkaidő elúszik, a határidős feladat pedig nem készül el a munkaidő alatt, a munkahelyen. Ilyenkor hasznos, ha a munkatárs a feladatokat az otthonában be tudja fejezni, de a napi 10-12 órás munkavégzés egyéb, nem kívánt hatásokat von maga után. Fontos, hogy rendelkezésére álljanak olyan technikai megoldások, melyekkel a saját erőforrásait jobban kihasználva képes jobban szervezni idejét, vagy hatékonyabbá tenni a munkával töltött órákat. Egy üzleti, minősített felhőalkalmazásban több ilyen megoldást is talál. A nagyvállalatok nehézkes ügyvitelkezelése, vagy folyamatai mellett felüdülés olyan alkalmazásokat használni, melyekkel azonnal megoldás vagy válasz érkezik egy adott kérdésre.

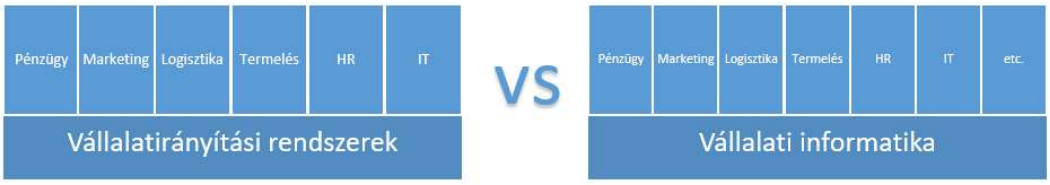
2.2 Az informatikai szervezet szerepe a nagyvállalatoknál

Az informatika az ezredfordulót megelőzően még egy önálló vállalati egységként élt a vállalat életében. Ma már sokkal inkább egy mindent átfogó és kiszolgáló – vagy uraló – ágazatot és ezzel együtt feladatkört jelent, aminek ügyfele a vállalat bármely más területén dolgozó felhasználó. Az vállalaton belül az Informatikai Stratégiát is úgy kell megalkotni, hogy ügyfelei részére – tehát társosztályai és munkavállalói számára - nyújthassa azokat a szolgáltatásokat, ami az adott szervezeti egység számára hasznos, többletbevételt képes termelni, a felhasználók munkáját megkönnyíti – és nem utolsó sorban illeszthető az Informatikai Biztonsági Rendszerhez, és a már kialakított IT Infrastruktúrához.

Korábban az informatika egy külön ágazatként, (lásd 7. ábra bal oldala) hasonlóan a többi társszervezethez élt a vállalatban. Szerepe az volt, hogy a társosztályok munkavállalóit

kiszolgálják, és rendelkezésreállást biztosítsanak a vállalat minden egyes munkaállomása számára.

Az ezredforduló környékén megjelentek azok a vállalatirányítási rendszerek, a vállalatok működését átfogó informatikai megoldások, melyek segítségével a társosztályok által elkészített adatokat, eredményeket együtt lehetett működtetni. Az informatika így minden egyes osztály kiszolgálójává vált (lásd 7. ábra jobb oldala). Ma már nem tudunk olyan



területet vagy ágazatot mondani, ami ne használná az informatikai megoldásokat, ne lenne része a teljes vállalati rendszernek.

7.ábra: Az Informatika szerepe az ezredforduló előtt és ma (saját ábra)

2.2.1 A Felhőszolgáltatások elterjedésének hatása a vállalati informatikára

A 2000-es éveket megelőzően jellemző volt az informatikai trendekre, hogy a vállalatnál használt alkalmazások, rendszerek és eszközök megjelentek a kisfogyasztói piacokon is. A vállalat alkalmazottainak igénye volt arra, hogy a céges környezetben jól megszokott rendszerekhez hasonlókat otthon is elérhessen és használhasson, tehát legyen privát levelezése, naptára, tárhelye, telefonkönyve, kommunikációs (Internet alapú) eszköze. Ugyanazt az integritást és fejlettségi szintet szerette volna elérni, mint amit munkahelyén az IT szervezet nyújtott a számára.

Ugyanezek a lehetőségek az okostelefonok megjelenése előtt a magánfelhasználók számára nem, vagy csak nagyon alacsony funkcionalitással voltak elérhetők otthoni használatra. Szigetszerűen otthon is használhatta az irodai alkalmazásokat, de azok szállítása, megosztása, az azokon való közös munka lehetősége nem volt adott. Az okostelefonok megjelenésével találkoztunk először olyan konzumer megoldásokkal, amik egyszerűbb, gyorsabb, vagy olcsóbb megoldást kínáltak, mint az üzleti párjuk (pl. chat alkalmazások). Az internet, majd a szélessávú internet elterjedésével már elérhették egymást azok is, akik nem feltétlenül egy cégen belül dolgoztak (pl. Skype). Rosszabb szolgáltatásminőséggel, alacsonyabb rendelkezésreállással, mint egy üzleti videókonferenciarendszer, de az ingyenes alkalmazás és a több millió forintos berendezés közötti választáskor az átlagfelhasználó elégedett volt akkor is, ha néha megszakadt a beszélgetés. Nem fizetett érte.

Az okostelefonok fejlődésével egyre több konzumer alkalmazás készült el, és ma már gyakorlatilag nem találunk olyan élethelyzetet, amit ne lehetne okostelefonnal támogatni (napi vízfogyasztás, napi kalóriaszámlálás, nyelvtanulás, utazás stb.). Az ingyenesen, vagy megfizethető áron elérhető szolgáltatások ellepték a különböző platformokat, és egész sereg szolgáltatót neveltek ki, akik mind olyan megoldásokat hoztak, amik akár az üzleti életben is használhatók.

A felfelé terjeszkedés elvét követve az okostelefonok használatával elindultak a felhőszolgáltatók az üzleti élet meghódítására. A kis- és középvállalkozások vezetői ezen alkalmazások használatával gyorsabban és hatékonyabban tudtak reagálni az üzleti helyzetekre. Nem feltétlenül rendelkeztek szakértő informatikai csapattal, az alkalmazások egyszerűsége könnyen értelmezhető volt számukra.

Nem meglepő fordulat, hogy a változásokat sok esetben előidéző, ámde a piaci változásokra nehezen reagáló nagyvállalatok belső informatikai kiszolgálórendszere egy idő után elavultnak számított az újdonságokkal szemben. A felhasználók titokban, de használtak publikus felhőalkalmazásokat. Sokszor a cég által rendelkezésre bocsátott mobileszközök nem voltak olyan „okosak”, mint amivel a felhasználó rendelkezett, így a vállalati SIM kártya inkább a saját készülékben dolgozott, mert azt több mindenre lehetett használni.

Ha a nagyvállalat pontosan meghatározza azokat a feltételeket, hogyan lehet az általa rendelkezésre bocsátott eszközöket használni, valószínűleg akkor is előfordul ugyanez a szituáció. A felhasználók szeretnek hatékonyabban, kényelmesebben és gyorsabban dolgozni, annak érdekében, hogy több idejük maradjon bármi másra. Ha azt tapasztalják, hogy a vállalati rendszerek lassúak, nyakatekertek, a folyamatok nehézkesek, a kommunikáció többlépcsős, ki fogják kerülni ezeket. Nem arra gondol, hogy az általa használt rendszer biztonságos-e vagy sem. Sokszor hallottam azt az érvet, gyorsabb és ingyen van. Mindenki tudja használni. Egy átlagos felhasználó számára ennyi elég.

Így egyes vállalatok egyes projektjein megjelentek piaci alkalmazások is, amivel a beosztást, a kommunikációt vagy a közös munkát támogatták. A kezdeményezésük sem a vállalat vezetése, sem az IT támogatását nem élvezte, a munka „hatékonyabb” elvégzéséért vállalták annak használatát, biztonsági rést ütve ezáltal a nagyvállalati tűzbiztos falakon.

A North Bridge 2016-os kutatásában 1351 válaszadó vett részt a felhasználói és beszállítói oldalról összesen. A válaszadók 53 vezető nagyvállalattól érkeztek, és a kutatás arra világít rá, hogy ezen nagyvállalatok 90%-a valamilyen formában használ cloud szolgáltatást. Ezt a mérést alátámasztja a Felhőszolgáltatók éves bevételének növekedése, ami 2015-höz képest 19%-kal nőtt (75Mrd USD-ről 90 Mrd USD-re). [93]

2.2.2 A vállalati informatika megváltozott kompetenciái

A vállalati informatikától elvárjuk, hogy a felmerülő problémát a lehető leggyorsabban, a legkisebb károkozással oldja meg. Azonnal álljon rendelkezésre, és a jelentett probléma megoldásához azonnal fogjon hozzá. A vállalati működés során az informatika egy nagyon kritikus pontot ér el, ha nem tudja biztosítani az üzemszerű működést, a munkatársak nem tudnak dolgozni. Az informatika biztosítása olyan kritikus ponttá vált a vállalatok életében, hogy működésképtelensége esetén a vállalat működése is leáll. Ezért az IT szakemberek munkája egyrészt a mindennapos problémák megoldásából, másrészt a rendszer biztonságos működésének fenntartásából áll. Mivel a vállalat minden egyes osztálya különböző rendszereket használ, mindnek a támogatásához szakértő kolléga szükséges.

A felhőszolgáltatások bevezetésével azonban a támogató szakemberek feladatköre megváltozik. Korábban félelmet keltett, hogy a külső szolgáltató által üzemeltetett rendszerek mellett szükség lesz-e a belső üzemeltetésre. Ma már látszik, hogy az IT feladatköre tágult, ami a meglévő kompetenciák mellé újabbakat kíván. Az adatelemzés, adatbányászat, a riportkészítés előkészítéséhez olyan rendszerek kialakítására van szükség, amik nem napra képes, hanem „perce képes” adatokkal szolgálnak. Ezek megvalósítása és összekapcsolása a felhőmegoldásokkal szintén kihívást jelentő feladatok, amik az IT új hatáskörébe tartoznak.

A felhőmegoldások használatával az IT support megítélése is változik. A felhőben való munkának egyik nagy előnye az eszközfüggetlenség. Egy vállalati gép meghibásodása esetén – amikor a munkatárs éppen felhőben dolgozott – a kiesett munkaidő annyi, amíg a munkatárs megkeresi az IT-t, és kicserélik a gépét arra az időtartamra, amíg az övé szerelés alatt áll. A munkát pedig folytatja ott, ahol abbahagyta. Az üzleti felhő magas rendelkezésre állása miatt kevesebb a munkatársi [94], [95], [96] panasz, bejelentés, így csökken a hibaelhárítások száma. A kiválasztott felhőszolgáltatások az IT számára is hozhatnak előnyt, hiszen az üzemeltetéssel, a mentésekkel, frissítésekkel töltött időt

fordíthatja más, magasabb szintű tevékenységekre. E mellett az IT szervezetben való elfogadtatása sem okoz gondot, hiszen "más" szolgáltató nyújt egy olyan szolgáltatást, aminek a rendelkezésre állása, az elérhetősége, a biztonsága és a stabilitása adott és jól működő. Az IT-nak nem panaszt kell kezelnie, vagy hibát elhárítania, hanem valós igényeket kielégítenie – amivel a szerepe és az elfogadottsága is jobb, fontosabb, pozitívabb lehet, a már átalakult (lsd. 7. ábra) vállalati hierarchiában.

2.2.3 A vállalati társosztályok elvárásai az informatikai kiszolgálással szemben

A vállalat működéséért a különböző osztályok felelősek. Működésüknek megfelelően eltérő támogatásra és kiszolgálásra van szükségük. A vállalati informatika szerepe, hogy a vállalatot felkészítse az informatikai kihívásokra, az üzletmenet érdekében bevezetni kívánt informatikai termékeket a már meglévő infrastruktúrába vagy rendszerbe illessze, a vállalati informatikát tudatossá tegye. Ennek a tudatosságnak lenne a legnagyobb szerepe az Informatikai Stratégia kialakításakor, hogy az abban megfogalmazott igények konkrét célok megvalósítását szolgálják és segítsék elő.

A konzumer piacon megtalálható alkalmazások fejlettségét követelik a helyi vagy céges IT-tól – és nehezen látható be, miért nem lehet egy új adatbázisrendszert, vagy egy új CRM-et kattintásra letölteni és használni. Fejlettebbé vált a felhasználó, ezáltal magasabbak lettek az elvárásai, mert privát életében eléri, használja, letölti és kidobja, amint arra nincsen szüksége. Minden egyes igényére legalább 3 ingyenes megoldást tud és talál meg – és ugyanezt a termékbőséget és kiszolgálást várja a vállalati IT-tól is.

Felmerül az igény – jogosan és érdekes módon a felhasználó oldaláról – miért nem oldja meg a céges problémákat ingyenesen elérhető, „otthon kipróbált" eszközökkel – amik felhasználói szempontból azonnali megoldást nyújtanak.

Az IT szerepe azonban a felhőszolgáltatások kiválasztásában lesz döntő. Mivel ezt a terméket a már meglévő IT infrastruktúra mentén a földi rendszerekhez kell illeszteni, a kiválasztás során a kompatibilitásnak és az együttműködésnek is meg kell felelnie a felhőszolgáltatásnak. Elsősorban ezek a megfelelőségek köthetők szabványokhoz (ISO 2700x, PCI-DSS, COBIT stb.), ajánlásokhoz és belső házirendekhez (BCP, DRP), amik szigorúbb feltételeket szabnak meg a felhőterméket szolgáltatók felé. Nagyon nem mindegy, milyen az a felhőszolgáltatás, amit a nagyvállalat bevezetni kíván – hiszen már működő infrastruktúrába illeszti, ami sok esetben auditált, tehát szabványnak megfelelően működik.

2.2.4 Ami nem a vállalati informatika felügyelete alá tartozik, a Shadow IT

Ahogy a 2.2.3 fejezetben utaltam rá, ha egy munkacsoport talál a piacon egy gyorsabb, hatékonyabb, ingyenes megoldást, ami a feladataik elérésében támogatja őket, használni fogják. Akár a vállalati IT beleegyezése nélkül is.

A Shadow IT olyan rendszert és megoldásokat foglal magában, amelyek kívül esnek a szervezeti hozzájáruláson vagy a megfelelésre vonatkozó előírásokon. Az erre való igény akkor merül fel, ha az egyik társosztály által elérni kívánt célok elérése a biztosított rendszerekkel nem megoldható. Ez arra készteti az alkalmazottakat, hogy olyan technikai döntéseket hozzanak, amelyek rövid távú előnyökkel járnak, de mindemellett negatív hatást is gyakorolhatnak a biztonságra. [97]

Az így használt rendszerek nagy kockázatokat hoznak a vállalat életébe. Vállalati adatok kerülnek ki egy, az IT által nem jóváhagyott rendszerbe, melyek használata a csoport által felügyelt. A csoport vagy a csoport erre kijelölt felelőse dönt a felhasználók hozzáféréséről, az esetleges külső partnerek felvételéről, a jogosultságok kezeléséről, kiosztásáról, megszüntetéséről. A rendszerben használt jogosultságok nem kerülnek be a vállalati jogosultsági rendszerbe, az ott bekövetkezett változások nem lesznek szinkronban egymással. A csoport által használt alkalmazáshoz az IT-nak nincs hozzáférése, tehát az ebben keletkezett adat nem lesz része a vállalati adatvagyonnak. Amint a csoport befejezi működését, sokszor nem törlik az alkalmazást, vagy a vállalati adatokat a felhőszolgáltatónál. előfordulhat, hogy a csoport tagjai között változás történik, új tagok jönnek, akik hozzáférést kapnak az IT által nem támogatott rendszerhez, de tagok távozhatnak is a csoportból, és nem minden esetben törlik a hozzáférésüket, hiszen „nem ez a dolguk”, vagy „soha nem volt ez a dolguk”, sokszor nem is gondolnak arra, hogy a konkurens céghez távozó kolléga hozzáfér a legújabb marketing tervekhez.

A felhőalapú megoldások terjedésével, valamint az informatika erőteljes használata csak felgyorsította a Shadow IT használatát. A 2014-es PMG által végzett felmérés szerint [97] az informatikai szakemberek 53%-a állítja, hogy a vállalaton belüli szervezeti egységek a jogosulatlan technológiák különböző formáira támaszkodnak.

Fontos, hogy a vállalat megkeresse és megértse, miért dolgoznak az alkalmazottak alternatív megoldásokkal. Legtöbbször nincs semmi rosszindulat a használat mögött, csupán megoldást keresnek, a használhatóság, a jobb támogatás, a több szolgáltatás vagy a hatékonyság növelése céljából. Ez azt bizonyítja, hogy a vállalati IT-megoldások nem

elég jók a munkatársak számára. Ennek megoldása nem az IT Shadow rendszerek kiirtása, hanem a vállalati rendszerek fejlesztése – akár üzleti minősített felhőszolgáltatással. Ugyanezt vallja Mark McDonald, a Gartner [94] egykori GVP-je: “Restructure rather than restrict shadow IT.” (Ne írtsd ki a shadow IT-t, inkább építkezz belőle!)

Az Shadow IT legnagyobb kockázata, hogy elsődleges célpontja a hackerek támadásainak. Például egy, a vállalat által meghatározott erős jelszó-biztonsági házirend még nem jelenti a jelszavak biztonságosságát. A jelszó-frissítések egyszerűsítése érdekében a felhasználók könnyebben megjegyezhető és könnyebben feltörhető jelszavakat hozhatnak létre. Vagy csak ugyanazt a jelszót használja mindkét helyen. Ha nem kapnak képzést jelszókezelő rendszer használatáról, akkor a felhasználók papírra írhatják őket, és biztonságban tarthatják őket, például az asztaluknál.

Tulajdonképpen a Shadow IT technológiai feladatok végrehajtására irányul, anélkül, hogy figyelembe venné a biztonságra gyakorolt hatásukat. Ennek a helyzetnek pedig magas kockázatai lesznek. Ennek csökkentésére a következő ötleteket dolgozta ki Travis Wilkins [98].

1. **Egy megfelelő vezető kiválasztása** - akinek feladata a biztonsági feladatok vezetése. Fontos, hogy minden kommunikáció és a biztonsággal kapcsolatos ügyekben hozott döntésekről ez a vezető tájékoztatva legyen.

2. **Kommunikáció** – minden esetben legyen meg a kapcsolat a társosztályok és az IT között. A munkatársaknak legyen lehetőségük az igényeiket megfogalmazni, az IT pedig próbáljon azokra megbízható, vállalati megoldást nyújtani.

3. **Folyamatok** – a sikeres biztonsági szervezet mágikus kombinációja, az emberek, a folyamatok és a technológia hármasa. Ha a sorból bármelyik kilóg, a rendszer nem tud megfelelően működni. Érdemes a folyamatokat egyszerűsíteni, lehetőség szerint automatizálni. A kommunikációval és az oktatással meg kell fogni a munkatársakat, a technológiának pedig illeszkedni kell a vállalati folyamatokhoz, valamint ki kell tudnia elégíteni a munkatársak igényeit.

4. **Biztonságos szoftverek/megoldások felhasználása** – a legfontosabb szempont a vállalati rendszerek átláthatósága.

A kommunikáció hiánya áll leginkább a Shadow IT elterjedése mögött. Egy felhatalmazott biztonsági vezető megkönnyítheti a megfelelő kommunikációt az egyes

csapatok között annak biztosítása érdekében, hogy kialakulhasson a mindenki számára elfogadható megoldás. A közös célok kitűzésével a munkatársak nagyobb valószínűséggel osztják meg az ötleteiket és elvárásaikat, és kevésbé fordulnak olyan megoldások felé, mint a shadow IT, ami veszélyezteti a vállalat biztonságát.

2.3 Az adatok minősítése, besorolása

Dolgozatomban, a felhőtechnológiákat szem előtt tartva, csak az elektronikus adatok kezelésével, minősítésével, besorolásával foglalkozom.

A dokumentumok osztályozása az azokban szereplő információval áll páthuzamban. A védendő vállalati adat ezek alapján lehet:

Nyilvános: külső ügyfelek által elérhető, pl. a honlapon közzé tehető, éves eredmény, pénzügyi jelentés stb.

Csak belső felhasználású: a vállalat minden belső dolgozója számára elérhető, a mindennapi munkavégzéssel kapcsolatos, a vállalatot nem hagyhatja el, pl. belső szabályozások, utasítások, belső policy stb.

Bizalmas információ: általában osztályon belüli, vagy csak egy adott csoportra vonatkozó (pl. projekt) információkat tartalmazza, pl. marketing terv, HR információk, pénzügyi adatok

Szigorúan bizalmas információk: csak az arra jogosultak számára elérhető adatok, pl. fizetési kimutatások, céges banki adatok, ügyféladatok, szerződések stb. Olyan speciálisan védendő adatok, melyek illetéktelenek által való megismerése komoly üzleti károkat okozhatnak.

Titkos információk: melyek kitudódása esetén a vállalat piaci szerepe, pozíciója is veszélybe kerülhet

Több vállalatnál is ezt az osztályozási rendszert alkalmazzák. Az általam vizsgált vállalatok is hasonlóan osztályozzák az adataikat. Mind az öt kategória megtalálható ezeknél a vállalatoknál, a besorolás módjában van minimális eltérés. Az osztályozás mellett a vállalatoknak pontosan meg kell határoznia az egyes kategóriák definícióját, a kategóriákhoz tartozó szabályokat, a kezelés módját és az esetleges szankciókat is. A folyamat csak akkor lesz használható, ha a fenti kategóriák mellé meghatározzuk a megfelelő eljárásrendet is. [99]

Az adatok mellé meg kell adni a(z):

- hozzáférési jogosultságot
- használat körülményeit
- adat szállításának módját
- tárolás módját
- megsemmisítés idejét, állapotát, körülményeit
- adatok formai követelményét

2.3.1 Vállalati adatok a felhőben

A felhő kellő biztonságától félve, de a felhőben rejlő potenciál kihasználására több vállalat is azt a politikát követi, miszerint az adatok osztályozása szerint használja a felhőszolgáltatásokat. Ennek elsődleges kritériuma, hogy a vállalatnál megfelelően, pontosan és minden adatra kiterjedően legyenek az adatok minősítve. Ezt követően hoz olyan döntést a cégvezetés, melyek azok a kategóriák, melyeket a felhőbe költöztetnek. Általában, nagyvállalatoknál a szigorúan bizalmas és a titkos adatok azok, melyek nem hagyhatják el a földi vagy privát környezetet. Sok vállalat kezdi a felhő használatát egyes projektek felhőbe való kihelyezésével. A projektek számára – főként abban az esetben, ha a projekt informatikai erőforrásokat is erősen igényel (pl. szerver, CPU, szoftver licence stb.) – egy minősített üzleti felhőben alakítanak ki olyan környezetet, melyet a résztvevők a projekt időtartama alatt használhatnak. Ez különösen előnyös a földi rendszerrel szemben is, hiszen a projekt eredménye, esetleges hibái nem befolyásolják az éles környezetet.

Más esetben egyes osztályok kérik, hogy izolálva, vagy párhuzamosítva használhassanak olyan felhőszolgáltatásokat, melyek kimondottan egy bizonyos feladat elvégzésére specializáltak, és sok esetben több és magasabb szintű szolgáltatást tudnak nyújtani, mint amit a vállalati IT biztosítani tud, ugyanazon költségek mentén. Ilyen rendszer lehet pl. a kommunikációs rendszer (Skype for Business), vagy a közös munkaterület használata (pl. SharePoint Online), vagy az ügyfelek adatainak kezelése egy felhős CRM (Customer Relationship Management) segítségével (pl. SalesForce). Ahogy a felsorolásból is látszik az adatok minősítése szempontjából a társosztályok kérése nem feltétlenül fedi a vállalati felhőpolitikát, az ügyféladatok és szerződések magasabb minősítési kategóriába esnek. Ebben az esetben az IT-nak meg kell tudnia határozni és szétválasztani azokat az

adatokat, mik kerülhetnek egy felhős CRM-be, mi maradjon feltétlenül saját üzemeltetés alatt.

Nem mindegy ugyanakkor, hogy a vállalat milyen tulajdonosi szemlélettel rendelkezik. Az innovatívabb vezetők, akik bíznak a külső szolgáltatókban, és több külső partnerrel tanácsadóval dolgoznak együtt, nyitottabbak a felhőtechnológiák kipróbálására [100], [101], [102], [103]. Hamarabb határozzák el magukat a költözést illetően, és pontosabban képesek definiálni, a vállalati informatikai rendszerek mely pontjai azok, melyek bátran a felhőszolgáltatóhoz kerülhetnek. Mérlegelik azokat az erőforrás/költség számításokat, amiket felhőben vagy földi környezetben lennének képesek kialakítani. Ahol az üzlet megkívánja a költségcsökkentést és a magas rendelkezésreállást, nagyobb erőforrás biztosítását, ott a minősített felhőszolgáltatók palettájából fognak választani.

Másik oldalról azonban meg kell vizsgálnunk azokat a szempontokat is, mely iparágból érkezik a vizsgált vállalat. A húzó technológiák, a szolgáltató vállalatok vagy az informatikai cégek esetében nagyobb a nyitottság a felhők iránt. A gyártó- vagy banki szektor a mai napig zártabb, ezért vagy a földi saját környezetet, vagy a privátfelhő megoldásokat választja [104].

2.3.2 A felhő, mint backup

A felhőrendszerek másik elterjedt használata az archiválás. Az információbiztonsági szabályzat, vagy a külső szabálycsokrok is előírják egy mentési politika kialakítását a vállalaton belül. Az egyre nagyobb mértékben keletkező adatmennyiség tárolása és visszaállítása komoly erőforrásokat igényel. Ennél azonban sokkal nehezebb feladat az archív állományokban való keresés, és az adatok többszöröződésének kiszűrése. Ezen utóbbi problémákra tudnak már nagyon jó megoldásokat adni egyes felhőszolgáltatók. [105]

A kockázata ennek a megoldásnak nemcsak az, hogy vajon a kívánt pillanatban rendelkezésre áll-e az az adat, amire éppen szükség van, hanem az is, hogy a felhőszolgáltató által tárolt vállalati adat vajon fizikailag hol helyezkedik el, és a módosítás/törlés valóban minden egyes helyen, ahol az adat a rendelkezésreállás miatt tárolva van (georedundancia), megtörténik-e.

Az előrejelzések alapján a Back-upként használt felhőmegoldások 2023-ig 21%-kal nőnek, ami 5,6 Mrd USD többletbevételt jelent majd a felhőszolgáltatóknak. Az

előrejelzés alapján nemcsak a KKV szektor használja ki a felhőmegoldások előnyeit, 2023-ra egyre több nagyvállalat költözik a felhőbe. [106]

2.3.3 A felhő, mint nagyobb erőforrás

A harmadik nagy előnye a felhőszolgáltatásoknak a nagyobb erőforrás azonnali elérhetősége. Egy fejlesztési projekt szempontjából sokkal tervezhetőbb és kifizetődőbb megoldás a környezetet felhőben kialakítani, és mind a szoftvereket, mind a hardvereket virtuálisan használni a projekt időtartama alatt. A projekt fázisaihoz méretezhetők a szükséges erőforrások, mely a felhők skálázható tulajdonsága miatt bármikor növelhető vagy csökkenthető. Ugyanez igaz a rendelkezésreállásra is, hiszen nem kell hónapokat várni a beszerzésre és a szállításra, a vezetői jóváhagyással az erőforrások elérhetővé válnak.

További előnye, hogy a projekt lezárását követően az erőforrások „visszaadhatók”, valamint a tesztelés is nagyobb volumenű skálán hajtható végre. A fejlesztői környezet ugyanúgy szigetszerű tud maradni, azonban könnyebben kipróbálhatók az illesztési megoldások is.

2.4 A publikus felhőszolgáltatás bevezetése során az emberi tényezőből származtatott kockázati tényezők

Az emberi tényezőből fakadó kockázatok száma nagy, természete kiszámíthatatlan, ezért az informatikai rendszerre gyakorolt hatása hektikus. A rendszerhez hozzáféréssel rendelkező személyek jogosultságaikban, a hozzáférések számában vagy mélységében eltérnek egymástól. Az emberi tényezőből eredő kockázatokat két nagy részre oszthatjuk. Az egyik, mikor szándékos károkozásról beszélünk. A kockázatok ezen területével dolgozatomban nem foglalkozom, a tézisekkel összhangban csak azt vizsgálom, hogy az emberi tényezőből fakadó akaratlan kockázatok hogyan, milyen eszközökkel csökkenthetők. Ehhez ebben a fejezetben vizsgálom, milyen nem szándékos emberi tevékenységből származó kockázattípusokkal találkozunk a nagyvállalati környezetben.

Az emberi tényező a kommunikációs lánc minden egyes pontján képes számottevő kockázatot hozni a rendszerbe. Maga a rendszer nem zárt, tehát a lánc minden egyes pontján találunk olyan elemeket, amiket az emberi viselkedés befolyásolni képes. Dolgozatomban az adatközpontban történő emberi hibákat kizártam, ezek kereteken belüli tartását az első fejezet alapján adottnak veszem. Valamint felhőszolgáltatás igénybevétele esetén nagyon szépen különválasztható a két terület, hiszen az

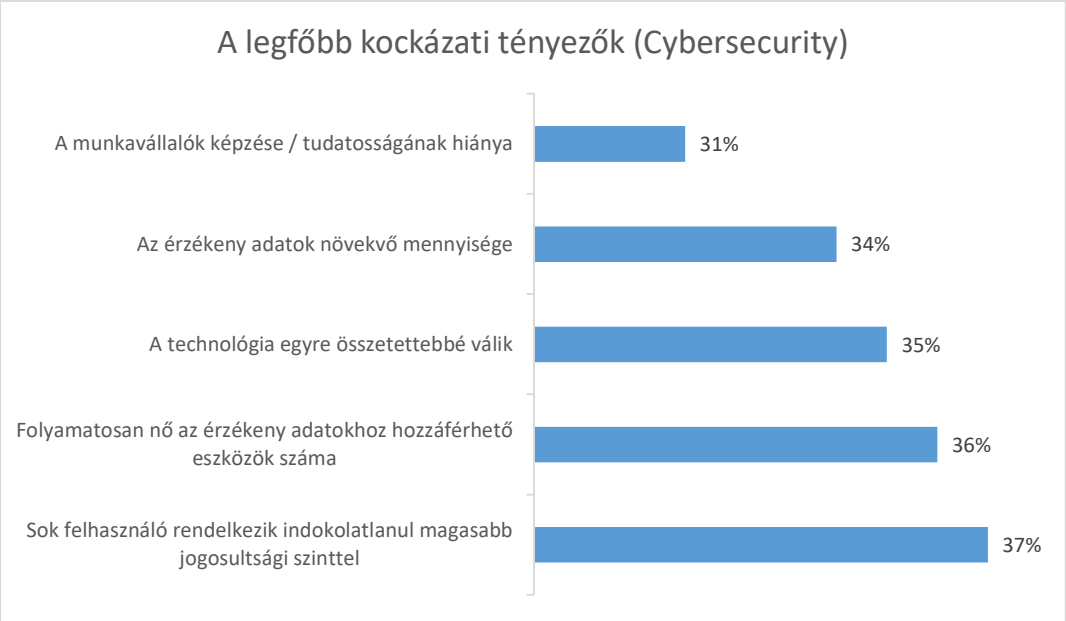
adatközpontok biztonságáért maga a felhőszolgáltató felel. Célom a kutatásom során, a nagyvállalatnál dolgozó munkatársak viselkedésének és azon keresztül befolyásának vizsgálata, és az általuk létrejöhető kockázatok csökkentése. A lánc kommunikációs útvonala szintén függhet a felhasználótól, a felhasználó választja meg, milyen csatornán keresztül (mobilinternet, nyilvános wifi hálózat, biztonságos, esetleg otthoni zárt wifi, vezetékes internet, VPN, vállalati belső hálózat) és a szolgáltató által kínált titkosításon felül használ-e további titkosító algoritmusokat az adat biztonsága érdekében.

Bár a külső támadások által okozott károk a leggyakoribbak, ez után a következő dobogós helyen az adatvesztés, adatszivárgás áll. A Cybersecurity 2018-as Insider Threats riportja szerint [107] a belső adatvesztések 47%-a még mmindig szándékos, de nagyobb fele, 51%-a véletlenszerű, nem szándékos károkozásból ered. A riport alapján ezt az 51%-ot a felhasználók tevékenysége teszi ki, és leginkább gondatlanságból, figyelmetlenségből vagy az érzékeny adatok nem megfelelő kezelése miatt követik el. Érdekes megfigyelni a riport alapján, hogy a vállalati átlagfelhasználók (56%) és az adminjogokkal rendelkező felhasználók/üzemeltetők (55%) ugyanolyan arányban okozhatnak kockázatot. Ugyanakkor a vállalat külső munkatársai, tanácsadói a felmérés alapján kisebb (42%) fenyegetést jelentenek a vállalati informatikai rendszerre.

A vállalati felhasználók legtöbbször „ellkövetett” biztonsági hibái:

1. A jelszavak nem megfelelő kezelése, tárolása, gyakori cseréje (ez utóbbi rendszerszinten kikövetelhető a felhasználóktól)
2. A nem lezárt eszközök felügyelet nélkül „felejtése”
3. A-jelszavak egymás közötti megosztása (pl. szabadságolás idején, vagy egy csoport egy hozzáféréssel rendelkezik egy felülethez, fájlszerverhez, adatbázishoz stb.)
4. A vállalat wifi hálózata nem biztonságos

A Cybersecurity felmérése rávilágít arra, hogy a kiberbiztonsági szakemberek véleménye alapján a munkavállalók képzése és tudatosítása előkelő helyen áll, amivel fékezhető lenne a vállalatot fenyegető kockázatok egy része. A technológiát érintő fenyegetéseket DLP-vel, titkosítással, IAM-mel, végponti- és mobileszközvédelemmel, valamint CASB-vel kezelik, ezért kimondottan ajánlják a munkavállalók megfelelő felkészítését, és folyamatos tudatosítását.



8. ábra: A Cybersecurity szerint rangsorolt legfontosabb vállalati informatikát fenyegető kockázati tényezők

Az informatikai rendszereket, hálózatokat, számítógépeket érő támadások során korábban nem látott mértékben játszanak szerepet azok a technikák, amelyek az emberi kíváncsiságra, hiszékenységre építkeznek. [108], [109], [110]

Az Egyesült Királyságban működő WinMagic felmérése szerint [111] mind a felhasználók, mind pedig a vállalatok számára nem egyértelmű, hogyan kezeljék a felhőben tárolt adatokat.

A megkérdezettek:

- 35% -a használja a munkáltató által szankcionált szolgáltatást
- 50% -a hetente legalább egyszer használ saját eszközöket az üzleti adatok és szolgáltatások elérésére
- A munkavállalók 65% -a nem hallott vagy nem ismeri a vállalati politikát a felhő tárolására vonatkozóan
- 5% felhőszolgáltatásokat használ, tudva, hogy a szolgáltatást a vállalat korlátozta

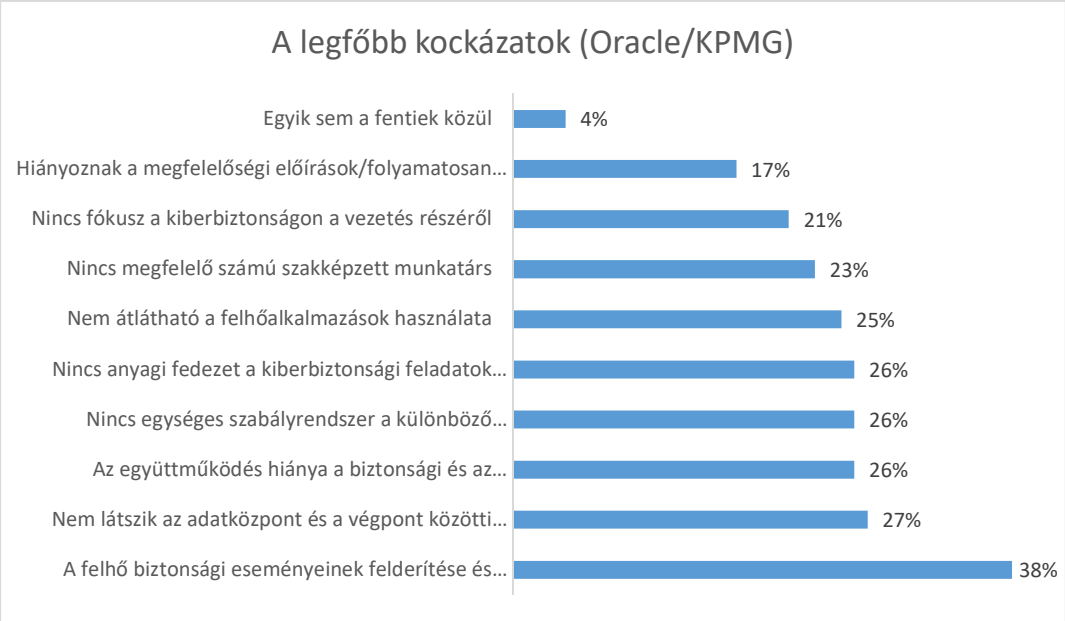
A tanulmány nemcsak azt mutatja, hogy a munkatársak nem ismerik a vállalati információbiztonságra vonatkozó szabályzatot, hanem azt is, hogy nincsenek tudatában annak, hogy mekkora felelősségük van a vállalati adatvagyon megőrzésében. Egy nagyvállalat esetében a vállalati értékek megtartása csak a tudatosítással, a közös érdekek

hangsúlyozásával, a közös kultúra kialakításával alapozhatók meg. Amíg egy kisvállalkozás esetén a dolgozók minden egyes tagja féltve őrzi egy közösen megalkotott termék minden titkát – legfeljebb szándékosan adja azt ki – addig egy nagyvállalatnál a közös szellemi termék megőrzése valahogy nem minden esetben része a munkatársak mindennapjainak.

Az Oracle és a KPMG által közösen megjelentetett 2018-as „Cloud Threat" riportban [112] további humán kockázati tényezőket elemez:

1. A technológia nem minden: egy felhőszolgáltatás bevezetése során nem elég az adatok megfelelő mozgatása, fontos, hogy a meglévő folyamatokat illesszék a megváltozott körülményekhez, valamint erről a felhasználókat is időben értesítsék, készítsék fel
2. A biztonságot befolyásolja a munkavállalók megváltozott kommunikációs szokásai: előtérbe kerül a mobileszközök használata – így a munkahelyi biztonsági oktatásoknak nem elég a vállalati hálózatra fókuszálni, fontos, hogy integrált tudást nyújtsanak, aminek a mobileszközök (akár saját eszköz esetén is, ha azon elérhető vállalati adat) is szerves részei
3. A felhőszolgáltatás lehet biztonságosabb, mint a meglévő rendszer: ugyanakkor ez nem kizárólag a felhőszolgáltatón múlik. A vállalatvezetésnek tudatosítania kell a saját felelősségét és kockázatait a szolgáltatás igénybevételét megelőzően.
4. „Cloud Security Architect" pozíció kialakítása vállalaton belül: A vállalatban legyen egy olyan szaktudással rendelkező mérnök, aki képes a felhőbiztonságot átlátni, kialakítani és felkészíteni a szervezetet az incidensek megfelelő kezelésére. Mivel a felhőszolgáltatások biztonsága amellett, hogy évről évre erősebb, az összetettsége miatt szükséges, hogy minden vállalat kezelje az ezzel kapcsolatos feladatait. A riport felmérésében résztvevő nagyvállalatok 41%-nál már működik ez a pozíció.

Az Oracle/KPMG riport alapján a legfőbb kockázatok, a felmérésben 450 válaszadó vett részt, és minden válaszadó 3 választ jelölhetett meg felsoroltak közül (lásd 9. ábra).



9. ábra: az Oracle/KPMG felmérése alapján felállított legfőbb humán erőforráshoz köthető kockázatok

A felsorolt kockázatok közül nem ad minden pontra megoldást a felhasználók, a szakemberek vagy a vezetőség oktatása, de a kockázatok nagy mértékben csökkenthetők a megfelelő képzés kialakításával. Ebben az esetben nem elég a folyamati lépések, vagy a vállalati biztonság ismertetése – fontos megértetni a munkatársakkal, hogy mindez miért fontos, mi múlik az ő tudásukon, hozzáállásukon, tehát elkötelezett biztonságtudatos felhasználóvá kell tennünk őket.

2.4.1 Felhasználói oldal

A felhőalapú számítástechnika új kockázatokat jelent a vállalati információ biztonsága szempontjából. Nehezebben lehet nyomon követni azt a munkavállalót, aki a vállalati interneten keresztül használ egy általa használt privát felhőalkalmazást, ahová nyugodt szívvel másolhat ki vállalati adatokat is.

Azoknál a vállalatoknál, amelyek egy felhőalapú rendszerre áttérnek, létfontosságú, hogy ne csak technológiailag készüljenek fel a változásra. A HR feladatai közé kell tartozzon a munkatársak kellő felkészítése, ami nem csupán az új technológia használatára terjed ki, hanem arra is, milyen új biztonsági környezetet alakítanak ki ezzel a technológiai váltással, és ebben a megváltozott környezetben mit vár el a vállalat a munkatárstól. Fontos, hogy már ezen a szinten tudatosítsák a munkatársakat – esetleg a migrációs projekttel párhuzamosan – és éreztessék, hogy a biztonság megőrzése mindenkin múlik,

nemcsak az üzemeltető csapaton. Ismertessék meg a munkatársakkal a várható kockázatokat és azok leghatékonyabb elkerülési módjait.

A felhasználói oldal a rendszerbe nem várt és nem várt mértékű kockázatokat képes behozni. Ennek elkerülése érdekében alkottak meg olyan alap biztonsági intézkedéseket, melyek mind a nagyvállalatot, mind a munkavállalót védik. Ezek közül az alábbiakat emelem ki:

1. **Gép hozzáférhetősége:** mely meghatározza, hogy az adott eszközhöz ki, mikor és milyen jogosultsággal férhet hozzá. Ezek a belépések és az eszközről indított rendszerkapcsolatok mentésre kerülnek.

2. **Tiszta asztal, tiszta képernyő politika:** a munkatársi gépeket az irodában is lezárják arra az időre, amíg a felhasználó nincs fizikailag az eszköznél. Nem hagy „nyitva” számítógépet, laptopot, nem hagy elöl az asztalán bizalmas vállalati vagy személyes adatokat sem.

3. **Felhasználó eszközei:** a felhasználó minden olyan vállalat által rendelkezésére bocsátott eszközét, amivel vállalati alkalmazásokhoz, rendszerekhez fér hozzá, a vállalat által (távolról is) menedzselhetővé kell tenni. Amennyiben megoldható, a személyes és az üzleti alkalmazásokat fizikailag vagy logikailag el kell választani egymástól.

4. **Mobileszközök használata és védelme:** A mobil eszközökre is érvényes a távolról menedzselés kialakításának lehetősége. A mai okoseszközök akkora számítási kapacitással és funkcionalitással rendelkeznek, melyekkel könnyen kár tehető egy informatikai rendszerben. A mobileszközökre ma már korszerű logikai védelmet lehet építeni, mindamellett itt is fontos szempont az üzleti és a privát felhasználása szétválasztása.

5. **A felhasználó által használt, de a vállalat által nem hitelesített eszközök használata:** célszerű ezen eszközöket csak személyes célokra korlátozni. Nagyvállalati szinten is előfordul, hogy a privát eszköz korszerűbb, mint amit a vállalat nyújt a munkatárs számára. A vállalatnak érdeke kell legyen, hogy a munkatárs ne használjon általa nem hitelesített eszközöket, és ne tegye lehetővé, hogy ezen eszközöket bármilyen módon a vállalati rendszerhez kapcsolhassa.

6. **A felhasználó által használt alkalmazások:** ez a terület félelmetes tempóban fejlődik. A piacon lévő alkalmazások nagyobb része nincs minősítve, nemcsak üzleti, hanem privát felhasználás esetében sem. Az interneten vagy a mobiláruházakon keresztül olyan alkalmazásokhoz férhetnek hozzá a felhasználók, amik nemcsak az adott eszköznek és használójának, hanem azon keresztül minden olyan eszközre kockázatot jelentenek, amelyekkel kapcsolatban állnak. A felhasználó vállalati eszközeit menedzselve érdemes egy olyan vállalati, belső alkalmazásáruházat kialakítani, ahová a már bevizsgált, jóváhagyott applikációkat gyűjtik, amik a felhasználók számára szabadon elérhetők.

A fenti példákból is jól látszik, hogy a biztonság megtartása a szabadság egy részének elveszítésével jár együtt. A szabályok nemcsak az üzemeltetésre rónak terheket, a feladatok mellett korlátozásokat is hoz a felhasználók számára. A felhasználókkal azt kell tudni megértetni, hogy ezek a korlátozások milyen célból lettek bevezetve, és ezek nélkül milyen kockázatok és veszélyek leselkednének a vállaltra.

2.4.2 A humán erőforrás okozta kockázatok a felhőtechnológiák használatakor

A humán faktor kockázatértékeléséhez összegyűjtöttem és megvizsgáltam az előforduló leggyakoribb kockázatokat, melyeket felhasználók követnek el. Meghatároztam, mik azok a felkészülési elemek, melyekkel a kockázat bekövetkeztét megelőzően is módunkban áll fellépni az esetleges károk ellen. A kezelési mód normál üzemtartományban csökkenti a kockázat kialakulásának lehetőségét. A munkatársak fejlesztésével részben csökkenthetők a táblázatban összefoglalt kockázattípusok. [113]

Kockázat típusa	Kockázat csökkentésének módja	Csökkentheti-e a kockázatot a felhasználó tudatosítása
Shadow IT használata	Kommunikáció az IT és a társosztályok között Korszerű informatikai rendszerek, alkalmazások Fejlett IT biztonsági politika A felhasználói igények megértése és kielégítése	Igen
Kulcsemberek kiesése		Nem
Szakképzetlenség		Igen
Illegális szoftverek használata		Igen

Kockázat típusa	Kockázat csökkentésének módja	Csökkentheti-e a kockázatot a felhasználó tudatosítása
Dokumentálatlanság		Igen
Szakszerütlen IT tervezés és üzemeltetés		Igen
Felhasználói hozzáférésekből adódó compliance kockázat	Többféle jogosultsági szint használata A felhasználó csak ahhoz az adathoz férjen hozzá, amelyikhez feltétlenül szükséges Szegregáció	Nem
Jelszókezelés	Többféle jelszó kikényszerítése Többszöri jelszómódosítási házirend A korábbi jelszavakat ne használhassa újra A jelszavak biztonságos tárolása a felhasználó részéről	Igen
A privát és az üzleti információk közös kezelése	Ne használhasson vállalati eszközön privát alkalmazásokat, privát eszközön vállalati adatokat	Közvetve
Nem saját eszközre való belépés	A cégen belül más eszközének használatához házirendet használjon, melynek betartását maga az eszköz követeli meg.	Igen
Vállalati mobileszköz magáncélra való használata	Megfelelő BYOD házirenddel Megfelelő MDM-mel Vállalati korlátozások bevezetése	Közvetve
Titkos vagy szigorúan bizalmas adatok felhőben való használata	Adatok osztályozása Adatok mozgatásának monitorozása A titkos vagy szigorúan bizalmas adatok kezelési körének meghatározása	Közvetve
A vállalat által nem hitelesített mobilalkalmazások, vagy felhőszolgáltatások használata magán célra (Pl. Dropbox, GoogleDrive) vállalati eszközön	Ezen alkalmazások letiltása az eszközön A vállalati adatokhoz való mobilhozzáférés korlátozása	Igen

Kockázat típusa	Kockázat csökkentésének módja	Csökkentheti-e a kockázatot a felhasználó tudatosítása
	Hasonló megoldásokat kínáló, de minősített, üzleti alkalmazások kínálata vállalaton belül	
Nyilvános wifi használata vállalati mobileszközzel	Korlátlan adatcsomag biztosítása a munkatársak részére	
Saját mobilinternet megosztása idegen eszközökkel	Csomagkorlátozás (ne tudja megosztani az internetet csak regisztrált eszközzel)	Részben igen
E-mail-ek helytelen kezelése (idegen helyről érkező csatolmány megnyitása, az e-mail cím ellenőrzése nélkül)	Anti-malware védelem Levélkarantén kialakítása Spamszűrés	Igen
Kapott linkek helytelen használata (a link elolvasása vagy értelmezése nélküli kattintás)		Igen
Felhőszolgáltatás használata - nem https kapcsolaton keresztül érik el	Minősített, üzleti felhőszolgáltatás használata	Igen

3. táblázat: A humán erőforrás okozta kockázatok a felhőtechnológiák használatakor (saját munka)

Összefoglalás

Mint minden rendszer, aminek az ember is része, kockázatokat hordoz magával. A megoldás semmi esetre sem a felhőtechnológiák elkerülése. A technológiai trendek abszolút a közös tárolás, a felhő irányába vezetnek. Célratörőbb megoldás, ha a vállalatot és a munkatársakat készítjük fel arra, hogy az általuk kezelt vagy hozzáférhető adatokat hogyan kezeljék a megváltozott környezetben. Nem az a cél, hogy elriasszuk a felhasználókat a szolgáltatás használatától, hanem hogy tudatos felhasználókká tegyük őket. Ehhez mindenképpen ismeretátadásra van szükség. Az általam bemutatott humánerőforrás okozta kockázatok egy része közvetett, nagyobb része pedig mindenképpen csökkenthetők a felhasználók és/vagy üzemeltetők megfelelő képzésével.

A felhőszolgáltatás bevezetését megelőzően a vállalaton belül legyen egy konkrét és egységes IT stratégia, amiben szerepel, hogy az infrastruktúra mely részét kívánják felhőből megoldani. A szolgáltató legyen minősített, vállaljon garanciát az adatvesztésre, legyen szankcionálható és eleve adjon megoldásokat a kockázatok nagy részének elhárítására.

A hasznos és biztonságos felhőszolgáltatások egyensúlya, a felelősségteljes felhasználást elősegítő egyértelmű szabályok és a kockázatokat felügyelő és mérséklő eszközök javítják a vállalatnak nemcsak a biztonsági profilját, hanem a hatékonyságát is, mint üzleti tevékenységet.

A humán erőforrás felkészítése pedig ugyanolyan fontos szerepet kell kapjon a vállalat életében, mint a technológiai rész monitorozása, üzemeltetése, kezelése. Az emberi tényező nem kiküszöbölhető, de tanítható, és megfelelő biztonsági szabályokkal, és a keretek egyértelmű megfogalmazásával a belső, nem szándékos károkozás számottevő mértékben csökkenthető.

A második hipotézisem során állítom, hogy bizonyítható, a számítási felhő, kommunikációs hálózat, vállalati informatikai rendszer és a felhasználó szolgáltatási láncnak az utolsó és leggyengébb láncszeme a felhasználó. Amennyiben a mobileszközök használatát – mivel ez a tevékenység szorosan köthető a felhasználóhoz – még a humánerőforrás szokásaihoz, biztonságtudatosságához kötjük, a hipotézisben megfogalmazottak bizonyíthatók.

Kutatási tevékenységem során ennek alátámasztásául a következő publikációim jelentek meg: „Moving towards cloud security” (V.), valamint a „Comprehensive Implementation of Cloud Services in Enterprise Environment” (VIII.)

3 A NAGYVÁLLALATI FELHASZNÁLÓK FELHŐ ISMERETÉNEK FELMÉRÉSE

Bevezetés

Kutatásom során azt vizsgáltam, hogy az elméleti módszereket hogyan használják az egyes magyarországi nagyvállalatok. Vizsgálatom során három magyarországi nagyvállalattal dolgoztam, egyazon szektorból. Ezt a módszert azért alkalmaztam, hogy homogénebb vizsgálati kört kapjak, ahol a tartalom, a módszertan, a rendelkezésekre álló eszközök, de még a munkavállalók egyenszilárdsága is közel azonos.

Az esettanulmányt három részre osztottam. Az első részben személyes interjúkat folytattam a vállalat információbiztonsággal kapcsolatban álló vezetőivel és munkatársaival. Az interjúk során képet szerettem volna kapni a vállalati környezetről, hogyan kezelik az információbiztonsági szabályokat, hogyan készítik fel a munkavállalóikat annak betartására. A második szakaszban személyes kérdőívezéssel a vállalat munkavállalóit kerestem fel. Ennek a szakasznak az volt a jelentősége, hogy összehasonlíthassam a valós képet a személyes interjúk alatt kapott válaszokkal. Ebben a fejezetben a személyes interjúk és a személyes kérdőívek eredményeit dolgozom fel.

3.1 Személyes interjúk

Kutatásom során személyes interjúkat folytattam a vizsgált nagyvállalatok IT és HR vezetőivel, és az informatikai üzemeltetésért felelős munkatársaival, valamint HR munkatársakkal. A beszélgetéseket 4 blokkra osztottam, ahol az első blokkban megkérdeztem a szervezet által biztosított oktatások gyakoriságát, folyamatát és eredményeit. A második blokkban a szubjektív véleményüket kérdeztem, ahol a hatékonyságra, a minőségre, és az oktatás módszertanára kérdeztem rá.

A harmadik blokk a vállalat belső szabálygyűjteményéről szólt, szintén mérhető, objektív szemszögből, a negyedik pedig az általuk érzékelt információs biztonságról, tehát szintén egy szubjektív megközelítést alkalmaztam.

	Objektív kérdések	Szubjektív kérdések
Oktatás	**Oktatás** • Van-e IB oktatás a cégnél? • Milyen gyakran vannak ilyen képzések? • Hogyan épül fel az oktatás? • Milyen oktatási módszerrel találkoznak a munkatársak? (E-Learning, Személyes kiscsoportos, előadás, videóüzenet, workshop, esettanulmány, ethical hacking) • Szükséges-e vizsgát tenniük valamelyik oktatási formát követően? • Ha igen, milyen időközönként? • Milyen gyakran újul meg az oktatások tartalma? • A vállalaton belül kinek a felelőssége az oktatások kezelése?	**A megkérdezettek véleménye az oktatásról** • Miről szól ez a képzés? • Mi a véleménye az oktatásról? • Milyen fajta oktatást tartana hatékonynak? • Mikor vett részt utoljára biztonsággal kapcsolatos oktatáson? • Mikor vizsgázott utoljára információbiztonsági témában? • Milyen gyakran vesz részt vállalaton kívüli oktatáson, tanfolyamon, konferencián ebben a témában? • Önt kérték fel belső vállalati képzés/előadás megtartására a vállalaton belül?
Belső Policy	**Belső policy** • Milyen szabályozást követnek? • Van saját, belső IB policy? • Része ennek a publikus felhőszolgáltatások használatának szabályai is? • Van-e Információbiztonsággal foglalkozó részleg vagy személy? • Az IT felügyelet mit monitoroz a felhasználókról? • Tudnak-e erről a felhasználók? • A munkatárs közvetlen vezetőjének van-e feladata, felelőssége a munkatárs információs biztonság-tudatosságával kapcsolatban?	**A vállalat saját információbiztonságának szubjektív megközelítése** • Milyen az IB-gal foglalkozók hatékonysága? • Mi a véleménye a kollégák IB ismereteiről? • Mit gondol, a munkatársak mennyire veszik komolyan az IB szabályokat? • Vannak szabályszegések? • Általában mik ezek? • Mekkora volt a legnagyobb szankció? Mi a legnagyobb szankció? • Mi volt a legnagyobb informatikai zavar/támadás/probléma, amit alkalmazott követett el, és amiről tudomása van? • Ha megtehetné, mi lenne az a 3 dolog, amit tiltana a felhasználók számára informatikailag?

4. táblázat: A személyes interjúk kérdései csoportosítva (saját munka)

A megkérdezettek köre:

Dolgozatomban az interjúban résztvevők kóddal szerepelnek. A megkérdezetteknél fontosnak tartottam, hogy az interjúalany legalább egy éve a vállalatnál az adott pozícióban dolgozzon, hogy kellő rálátása és ismerete legyen az általam kérdezettekről.

Szervezeti egység	Beosztás	Hány éve dolgozik a vállalatnál	Azonosító az értekezésben
IT üzemeltetés	Vezető	2	ITMA
IT üzemeltetés	munkatárs	8	ITEB
IT üzemeltetés	munkatárs	5	ITEC
HR	munkatárs	6	HREA
HR	munkatárs	4	HREB
HR	vezető	4	HRMC

5. táblázat: A személyes interjúkban résztvevők adatai (saját szerkesztésű táblázat)

Ezt a két területet azért kérdeztem, mert az IT felelős az IB szabályrendszer előállításáért és annak tartalmáért, a HR feladata az oktatás megszervezése a témában a teljes vállalatra nézve. A válaszok elemzésénél eleve szétválasztottam az objektíven mérhető és a szubjektív válaszokat.

3.1.1 Első blokk – Oktatás objektív megközelítésből

Mindhárom nagyvállalatnál elérhető az Információbiztonsági (továbbiakban IB) oktatás. Mindhárom vállalatnál elektronikus (E-Learninges) tananyag segíti a munkatársakat, és mindenhol vizsgát is tesznek az elvégzett tanfolyamot követően. Általában az elektronikus tananyagot követi a vizsga, időben nem válik ketté az oktatás és a számonkérés. A vizsgák eredményét ’megfelelt’ és ’nem megfelelt’ -ként minősítik, a megfelelt szint vállalatonként eltérő (50% vagy 60% feletti eredmény számít megfeleltnek). A ’nem megfelelt’ eredményt elért kollégáknak a tanfolyamot (a vizsgával együtt) újra el kell végeznie, egy új időpontban. Arra a kérdésemre, hogy vállalati szinten átlagosan milyen a vizsgák eredménye, nem kaptam választ.

Elsősorban a tananyag azért elektronikus, mert mindenkinek el kell végeznie a tanfolyamot, és ebben a formában eljuttatható mindenki számára, akár különböző kezdési időpontokban is, valamint ez a megoldás a leginkább költséghatékony. A munkatársak a tanfolyamot egyedül végzik, a vállalati hordozható eszközön (laptop vagy tablet), és az általuk meghatározott időben, ami akár munkaidőn kívülre is eshet.

A tananyag technikai eszközei azonban eltérőek. Az egyik vállalat esetében videóval, fotóval, példával ellátott, a vállalatra testreszabott megoldással rendelkeznek, míg a másik két vállalatnál ennek az egyszerűbb E-Learninges változata található meg. Ezek közül az egyiknél az elektronikus tananyagot személyes oktatással is ötvözik – aminek ritmusa nem mindig esik egybe az elektronikus tanfolyam elvégzésével (Egy új belépő esetében az elektronikus tanfolyamot a belépéskor végzi el, a személyes oktatásra van, hogy 6-7 hónap múlva kerül sor).

A tananyagot általában 2-3 évre készítik el, ezalatt az idő alatt változatlan tartalommal érhető el a felhasználók számára. A tananyagot minden belépőnek el kell végeznie, de a már régebb óta a vállalatnál dolgozóknak is 1-2 évente meg kell ismételnie a képzést és az azt követő vizsgát is, ami alól a felsővezetés sem kivétel. Mindhárom vállalatnál a képzésekért a HR vagy a HR-hez tartozó képzési részleg felel.

Az online képzésen kívül alkalmanként van lehetőség arra, hogy a vállalat IT szakemberei előadást tartsanak a témában a vállalat munkatársai számára. Sajnos ezen előadások ritkán és alkalomszerűen – leginkább egy-egy nagyobb incidenst követően – szerveződnek két vállalat esetében is, a harmadik cégnél ütemezve, de szintén ritkán, 8-12 havonta tartanak személyesen előadást a témában munkatársi szinten. Ezen fórumoknak nagy előnyét abban látják, hogy személyesebben tudnak bemutatni egy adott témát, valamint az előadó szakembert is megismerik a kollégák – és felkereshetik őt hasonló kérdésekben. Így teret adnak a vállalaton belüli informális csatornák kialakulásának.

3.1.2 Második blokk – Oktatás szubjektív megközelítésből

A képzés tartalmára vonatkozó kérdésre az IT területen dolgozók részletesen adtak választ, a HR területről érkező megkérdezettek csak nagy vonalakban tudtak válaszolni. A hatékonyságára vonatkozó kérdésemnél is eltérés volt a két terület válaszadói között, az IT munkatársak nem tartották kellően hatékonynak az online oktatásokat, sem a tartalmukat, sem az elektronikus módszert, míg a HR-ről érkezők kimondottan pozitívan értékelték a módszertant és a képzési tartalmat.

A kérdésemre, miszerint milyen oktatást tartana hatékonynak a témában, olyan válaszokat kaptam, mint hogy ’Aminek nagyobb tétje van’, ’Felnyitja a munkatársak szemét’, ’Gyakorlatiasabb’ vagy éppen ’Ami egészséges paranoiát alakít ki bennük’. A többi válaszadó megfelelőnek, kimondottan jónak találta a képzési anyagot.

Az interjúm során rákérdeztem, mikor végezték el a megkérdezettek a tanfolyamot, és mikor vizsgáztak utoljára a témából. A válaszadóknál vegyes válaszokat kaptam, de két évnél régebben senki nem végzett tanfolyamot. Vizsgát pedig minden esetben a tanfolyamot követően tettek.

A témában az IT szakterületről érkezőknek van lehetősége ebben a témában külső oktatáson, konferencián részt venni, a HR területről megkérdezettek ebben a témában nem voltak még külső rendezvényen. És ugyanezt a választ kaptam arra a kérdésemre is, hogy tartottak-e előadást ebben a témában.

Az egyik vezető beosztású válaszadó véleménye szerint a legfőbb probléma az oktatással az, hogy mindenki számára egyforma. Pedig a munkavállalóik sem azonos generációból érkeznek. Jelenleg négy generáció van a munkaerőpiacon, mindannyian másképpen viszonyulnak az informatikához. Az 55+ korosztály soha nem fogja készségszinten használni az informatikai rendszereket. A 35-55 évesek tudatosan megtanulták az informatikai rendszereket alkalmazni, de csak munkaeszközként használják, az ő kommunikációs eszközük legfőképpen az E-mail. A 35 év alattiak, nagyon kötődnek a social megoldásokhoz, minden a digitális térben történik náluk, a munka és a magánélet is. Csak félig vannak jelen a munkahelyen, és leginkább a social csatornákon keresztül kommunikálnak. A 25 év alattiaknak szinte minden őskövület a vállalati informatikában, ők leginkább chat alapú kommunikációt folytatnak (chatbase).

Ehhez a felosztáshoz képest a jelenlegi nagyvállalati IT az X generációt (35-55 évesek) szolgálja ki. Mindenkinek ad E-mail címet xMB-os postafiókkal. Amíg ez az X generációnak elég, a nála fiatalabbaknak kevés, és nem elégíti ki a kommunikációs igényeiket. Az Y generáció kiszolgálója pedig a számítási felhő lenne. Véleménye szerint ezért kell a vállalatoknak – ebbe beleérti a nagyvállalatokat is – a felhőmegoldások felé nyitni, hogy megtarthassa és kielégíthesse az Y generáció IT-tól elvárt igényeit is. Jelenleg a vállalat, ahol vezetőként dolgozik nagy hangsúlyt fektet az ügyfélélmény javítására (customer journey), ahol minden esetben a vállalat előfizetőire gondolnak. Hiányolja ugyanezt a módszertant az IT oldaláról, az IT is egy szolgáltatóként működik a vállalaton belül, és fontos lenne kialakítani egy olyan rendszert, ahol pontosan látják, és mérhetik a felhasználók, mint ügyfelek élményútját. Ezzel olyan információhoz jutnának, amivel a Shadow IT mértéke csökkenthető lenne, mert pontosan látnák, mi

nehézkes a jelenlegi megoldásokban és milyen egyéb alkalmazásokat részesítenek előnyben a felhasználók.

3.1.3 Harmadik blokk – A Belső Policy objektív megközelítésből

Belső szabályozással, belső Információbiztonsági Szabályzattal a megkérdezett három nagyvállalat rendelkezik. A vállalati Információbiztonsági Szabályzat (IBSZ) mellett a hazai szabályozásokat és a jogi irányelveket is be kell tartaniuk. Az IBSZ meglétéért az IT vagy az IT egy részlege felelős, sajnos az IBSZ-szel kapcsolatos kérdésekre csak ők tudtak helyes választ adni. Minden vállalatnál van olyan csoport vagy osztály, akinek a mindennapi feladata az IB felügyelete. Sajnos a publikus felhőhasználatra egyik vállalatnak sincs megfelelő szabályozása. A három vállalat három eltérő módon monitorozza a belső hálózatán történt eseményeket, valamint dolgozza fel az így nyert információt. A mérhető információk érkezhetnek a belső hálózatról, figyelik az internetforgalmat, az E-mail forgalmat, ahol az E-mail fejlécet nézik, szoftver meteringet, login-logout eseményeket figyelnek, és vizsgálják a fájlszerverek hozzáféréseit, lekérdezéseit is. A rendszerüzemeltetők munkájából többet látnak, de ezek a kollégák tudnak is a megfigyelésükről – náluk véletlenszerűen nézik a képernyőképet. Ezen felül a biztonsági eseményeket gyűjtik, ezek leginkább szerveradatokat jelentenek.

A második vállalat biztonsági kialakítása példaértékű volt hazánkban. Kialakítottak egy a CEO-nak jelentő biztonsági igazgatói pozíciót, akihez elsősorban a fizikai biztonság (beléptetés, létesítmény biztonság stb.) tartozott, valamint a logikai biztonság szabályozási része: ők állították össze a vállalati szintű IT biztonsági dokumentumokat. Az IT szervezethez tartozott az IT biztonsági központ, akinek a feladata pedig a logikai biztonság végrehajtása volt. A két szervezet egymást is kontrollálta. Ezt a megoldást utána több hazai nagyvállalat is követte.

A felhőtechnológiák ekkora mértékű felhasználógyarapodására ezek a nagyvállalatok nem tudtak előzetesen felkészülni, így azok szabályozása egyik vállalat szabályrendszerében sem szerepel. Tiltani, amit lehet, és ezt meg is teszik, munkavállalóiknak publikus felhőrendszerek vállalati alkalmazása nem engedélyezett. Ugyanakkor az üzemeltetési oldal azt tapasztalja, hogy a munkatársak használják a felhőt, olyan helyzetekben, amire a vállalati infrastruktúra nem kínál egyszerű megoldást. A tiltás megszegését nem szankcionálják – mivel nagyon monitorozni sem tudják – a felhasználók „érzik”, mely esetekben nyúlhatnak a felhős megoldások felé. Kimondatlan

szabály a dokumentumok besorolása szerinti döntés tehát a szigorúan bizalmas és titkos dokumentumok a nyilvános felhőrendszerekbe semmi esetre sem kerülhetnek.

Az IT üzemeltetés és felügyelet számára a Shadow IT jelent nagy kihívást. Például a munkavállalók okostelefonon keresztül használják a Viber szolgáltatást, mert ügyfeleik igénylik ezen a csatornán a kapcsolattartást. Mivel ez a szolgáltatás nem része a vállalati informatikai infrastruktúrának, ezért nemhogy monitorozva nincs ez a csatorna, de az ezen keresztül történő chat üzenetek sem kerülnek központilag rögzítésre. Egy vitás esetben (ügyfél és vállalat között) nincs bizonyítéka a vállalatnak egy pl. megrendelt/letiltott szolgáltatáselemről, ami későbbi compliance problémákat vethet fel. Vagy egy ügyfélátadás során értékes információk maradnak az átadó birtokában, amit nem fog tudni kollégájával megosztani.

Ugyanilyen probléma, ha egy csoport vagy egy projekt publikus felhőtárhelyet használ a közös dokumentumaik tárolására vagy közös szerkesztésére. Az ott elhelyezett dokumentumok nem a vállalaton belül helyezkednek el, tehát olyanok a vállalat többi munkavállalója számára, mintha nem léteznének. Egy esetleges átadás vagy zárás, egy személycsere komoly problémákat okozhat az így kialakult Shadow IT és vállalati IT infrastruktúrában. Az egyik megkérdezett vállalat a 2017-es évben végzett egy felmérést, hogy mennyi, a vállalat által nem engedélyezett informatikai megoldást találnak házon belül. Az eredmény őket is megijesztette, több, mint 20 alkalmazást találtak, amit kollégáik rendszeresen használnak, és kezelnek (tehát ők viszik az admin feladatokat is). A kérdés nagyon idekívánkozik, mi a folyamat abban az esetben, ha a Shadow IT rendszert használó egyik kolléga a konkurenciánál folytatja tevékenységét? Az IT a saját rendszereiből kivezeti a felhasználót, de vajon kivezetik- e a Shadow IT rendszerekből is? Ez kinek a feladata lenne? És számonkérhető-e ez a feladat bárkin, hiszen egyik folyamatban és egyik vállalati rendszerben sem szerepel? És mi történik abban az esetben, ha a Shadow IT adminja távozik a konkurenciához?

Az IT a felhőmegoldásokkal kapcsolatban azt a szabályt hozza, hogy csak olyan felhőszolgáltatást vehetnek igénybe, ahol szerződés köthető a vállalat és a felhőszolgáltató között, valamint az adminisztratív jogokat megkapja a vállalati üzemeltetés. (Ez a két igény hazánkban KKV oldalról nem minden esetben elvárt). Ezen felül pedig el kell fogadniuk, hogy a cloud egy feketedoboz, és adataikat csak a szerződéssel tudják védeni, semmi más eszközük nincs.

A harmadik megkérdezett vállalat is hasonlóan áll a Shadow IT jelenségéhez. Náluk is megtalálható, és szintén nehezen küzdenek meg a felszámolásával. A Shadow IT-ban azt tartják a legveszélyesebbnek, hogy ezeket a rendszereket az IT nem támogatja, nem integrálja a saját rendszereibe, nem monitorozza, nem ad hozzá frontLine supportot, és nincs adatintegrációs része sem. A kollégák által így kialakított rendszer szigetként működik a vállalaton belül. Az ő esetükben van olyan megoldás, amiről tudnak, és vállaltan nem támogatják informatikailag, de jobb rendszert nem tudnak nyújtani helyette, így el kell fogadniuk a terület döntését, akiknek a munkájukhoz elengedhetetlen az adott felhőszolgáltató termékének használata. Itt azonban egy üzleti döntés támogatja a rendszer használatát, és az előbb említett support, adatintegráció és rendszertámogatás a felhőszolgáltatónál maradt, tehát a vállalat és az üzleti felhőszolgáltató szerződéses jogviszonyban állnak egymással.

Amit mindannyian nehéznek tartanak az az, hogyan értessék meg kollégáikkal azt, hogy azok a szolgáltatók, akik nem állnak szerződéses kapcsolatban a vállalattal, non compliant megoldást tudnak csak nyújtani, ami a jelenlegi szabályozási és jogi megfelelősségi körbe semmilyen módon nem illeszthető.

3.1.4 Negyedik blokk - A Belső Policy szubjektív megközelítésből

A vállalatnál dolgozó, az IB-ért felelős emberek munkáját egy válaszadón kívül mindenki hatékonynak, eredményesnek tartja. Volt, aki kifejezetten jónak tartja kollégái munkáját, vagy iparági szinten is kiemelkedőnek. A HR-től érkezett válaszadóknak nincs rálátásuk az IT mindennapi munkájára, ezért az ő tapasztalataik inkább szubjektívek, és az éves teljesítményértékelést követően kapnak részletesebb képet kollégáikról. Az IT részlegen dolgozók munkájukat általában a konkurenciával hasonlítják össze – abszolút ismert előttük, hogy miben jobbak vagy gyengébbek az konkurenciához képest. A velük nem egyetértő válaszadó véleménye szerint felesleges munkát végeznek, hiszen szolgáltatásként is meg lehetne venni a piacról. Az adatvagyonra fordított költségek magasak, ugyanakkor a hatékonyságuk alacsony. Véleménye szerint a jelenlegi megoldásnál egy vállalati cloud szolgáltatás is jobb lenne.

Az IT terület válaszadói munkatársaik IB tudásáról nincsenek megelégedve, véleményük szerint a felhasználók nem veszik elég komolyan a leselkedő veszélyeket, sem a munkahelyen, az otthonukban pedig különösképpen nem. Az egyik válaszadó elismerte, hogy saját magát kifejezetten paranoiásnak tartja a témában, és fontosnak tartja, hogy

kollégáiban is kifejlődjön egy egészséges félelemszint, véleménye szerint „az óvatosság alapja a félelem” és „addig nem veszik komolyan a témát amíg nem ijedtek meg”. A HR ugyanakkor megemlítette, hogy a kollégák részt vesznek különböző tudatosító programokban, amiket leginkább diákok részére szerveznek. Ezeket a feladatokat cégen belül hirdetik, és bárki jelentkezhet rá. A HR véleménye szerint nagyon népszerűek ezek a programok a gyerekek körében – és a munkatársakat is motiválja.

Minden válaszadó igennel válaszolt arra a kérdésre, hogy van-e a vállalatuknák szabályszegés. Ez a legtöbb esetben adatlopás, amit a kolléga követ el. A második helyen a helytelen jelszókezelés áll, ezt pedig szorosan követi az eszközök elvesztése. A véletlenszerű, vagy nem tudatos károkozást a vállalat nem szankcionálja, ami alól az eszköz elvesztése kivétel, ott az új eszközt a munkatársnak ki kell fizetnie – az azon tárolt adatok ilyenkor nem kerülnek értékbecslés alá. Az elsővel dolgozatomban nem foglalkozom, mivel szándékos cselekedetről van szó. A jelszókezelés tudatosító programokkal javítható lenne, az eszközök elvesztése elleni védelem pedig részben informatikailag megoldható. Eddig a legnagyobb szankció az érintett kolléga elbocsátása volt. Szabályszegésről a HR részleg akkor szerez tudomást, ha a szankcionálási folyamatnak része a HR is (pl. elbocsátás, Compliance vizsgálat, fegyelmi eljárás stb.).

Mindhárom vállalat rendelkezik MDM (Mobile Device Management – Mobileszköz Menedzsment) megoldással (a piacon ügyfeleik számára kínálják szolgáltatásként is). Ezért a felhasználók nagy része „biztonságban” érzi magát, hiszen az IT figyel minden olyan kockázatra, ami őt érintheti. És szükség esetén közbe is lép. Sajnos ezek a rendszerek sem elegek minden esetben, az elmúlt évben két vállalatnál is történt olyan eset, amikor a vállalati MDM már kevés volt.

A legérdekesebb válaszokat az utolsó kérdésemre kaptam az IT részéről: „Ha megtehetné, mi lenne az a 3 dolog, amit tiltana a felhasználók számára informatikailag?” Erre a kérdésre már a publikus felhőkkel kapcsolatos válaszok is érkeztek:

1. Külső eszközök csatlakoztatása, gmail vagy egyéb ingyenes felhő használata, és a gyereknek ne adják oda a telefonjukat
2. Azért a rendszerek úgy vannak kialakítva, hogy nagy bajt a felhasználó ne okozhasson. A legtöbb probléma az adatok nem megfelelő besorolásából vagy hozzáféréséből adódik. Szükséges lenne a jogosultságokat szigorúbban kezelni. E

mellett több felhasználó használ dropbox-ot, vibert a céges telefonján – ezt semmiképpen nem engedném.

3. Amit tudunk, azt tiltjuk. Nem engedném, hogy a céges mobillal fotózzon, fizessen, felhős rendszerekhez és app-okhoz férjen hozzá. Azt sem engedném, hogy saját tulajdonú okostelefonnal a vállalati wifire csatlakozzon.

4. Nem kapcsolhatja ki a tűzfalat, a vállalati vírusírtót nem szedheti le, valamint ami tilos, azt ki kell kényszerítenie az IT-nak

5. A felhőben szigorúan bizalmas dokumentum nem tárolható. A telefon és notebook mindig jelszóvédett legyen megfelelően erős jelszóval. Megfelelően erős jelszó legalább 8 karakter számokat és speciális karaktert is tartalmazzon.

6. Kikényszeríttetném, hogy a vállalati és a magánfelhasználást minden munkavállaló szétválassza egymástól. A legtöbb bajt az okozza.

A HR válaszadói nem érezték magukat kellően kompetensnek a kérdés megválaszolásához. Egyikük megjegyezte, hogy korábban nem volt ennyi probléma a céges adatok körül, amióta a munkatársak okostelefonnal és folyamatos adateléréssel rendelkeznek, azóta van számottevően több incidens.

Összefoglalva a válaszadók nem tartják egyértelműen rossznak a vállalat és a munkatársak felkészültségét IB-i témában. Az IT szakemberek igyekeznek objektíven figyelni a cégnél kialakult helyzetet és összehasonlítani más nagyvállalatokkal. Többször jutnak arra a – néha hibás – következtetésre, hogy a többi szereplőhöz képest jól állnak. Bár időt és energiát fordítanak a kollégák képzésére, a tananyag gyakorlatba való ültetését nem mérik, csak a kötelező képzéshez tartozó vizsga sikeres letételét várják munkatársaiktól. Véleményem szerint probléma lehet az is, hogy a kollégák szerint az IB még mindig valamilyen informatikai dolog, amitől jobb elhatárolódni, mert úgysem értik.

3.1.5 A személyes interjúk tapasztalata

Mind a három vizsgált nagyvállalatnál van ütemezett, minden munkatársa kiterjedő IB képzés. Ezek a vállalatok rendelkeznek Információbiztonsági Szabályzattal. Fontos számukra a kollégák megfelelő tájékoztatása, és fontosnak tartják azt is, hogy a vállalati informatikai rendszereket megfelelő hozzáértéssel kezeljék a munkatársak. Ennek érdekében a képzési anyagokat frissítik, valamint alkalmanként tudatosító előadásokat

tartanak. A szándékos károkozást mind a három helyen szankcionálják, a legerősebb büntetésnek az elbocsátást ítélik meg.

A vizsgált vállalatok nemcsak a munkatársaikra, hanem a felhasználóikra, lakossági ügyfeleikre is gondolnak, és önkéntesként részt vesznek különböző szervezetek tudatosító rendezvényein, kampányaiban, valamint ők is szerveznek hasonló rendezvényeket.

Az IT és HR szakemberek információi és adott válaszai nem azonosak a témában. Ennek egyik oka a szakterületek eltérése, a kérdezett téma az IT-hoz tartozik, szakmailag ő a kompetens a megválaszolásában. A HR ugyanúgy ügyfele az IT-nak, mint minden más munkatárs – a vizsgálatom szempontjából a kiszolgálóval és a felhasználóval folytattam kutatást. A HR ugyanakkor a képzésekért vagy azok megszervezéséért felelős, az IT-val össze kéne dolgoznia, hogy együtt találják meg a megfelelő tartalmat és a módszertant a képzésekhez. A válaszok alapján a személyes oktatásokra felkérik a kollégákat, de sokszor nem moderálják ezeket az eseményeket, és ez a közérthetőség rovására mehet.

A tananyagok formája mindhárom esetben elektronikus, hogy minél szélesebb körben, automatizálva juthasson el a munkatársakhoz. Ennek a megoldásnak a kezdési ideje, az időtartama és a feldolgozás sebessége is a tanuló képességeitől függ, ami véleményük szerint segíti az egyéni megértést. A vizsga is elektronikus úton történik. Az egyik interjúalany szerint a vizsgáztatásnak lehetne nagyobb tétje, véleményem szerint pedig legalább a vizsgát lenne szükséges személyessé tenni, hogy pontosabb képet kapjanak a munkatársak tudásáról, valamint megerősítsék őket abban, hogy a téma fontos, és fontos, hogy naprakész és pontos ismereteik legyenek az információbiztonságról.

Ezen felül javaslom, hogy a képzésekért felelős, oktatástechnológiához értő kolléga és az információbiztonságért felelős kolléga közötti kommunikáció szorosabb legyen, és közösen dolgozzák ki a megfelelő tartalmat és találják meg a mai kor felhasználója számára a megfelelő módszertant a téma oktatásához.

3.2 Személyes kérdőívek

A személyes kérdőíveket megelőzően tanulmányoztam az általam vizsgált nagyvállalatok információbiztonsági oktatási tananyagait. Az oktatási anyagok alapján összegyűjtöttem a közös pontokat, és a kérdőívben csak azokat használtam, ahol az oktatás tartalma mindhárom vállalatnál azonos volt. Ennek az volt az oka, hogy a lehető leghasonlóbb kutatási környezetet biztosítsam a kutatásban résztvevők számára.

A kérdőív összesen 4 nagy blokkból és összesen 35 kérdésből áll.

A személyes kérdőívet az interjúkhoz hasonlóan négy nagy területre bontottam:

1. Demográfiai adatok
2. Technológiára vonatkozó kérdések
3. Az információ- és adatbiztonságra vonatkozó kérdések
4. A biztonságtudatosság oktatására vonatkozó kérdések

A teljes kérdőív a Függelékben található.

A kérdőívben a résztvevők információbiztonsági tudását vizsgálom elsősorban, csak egy-egy pontban vizsgálom a felhőszolgáltatások használatát és a magánfelhasználási szokásokat. Ennek legfőbb oka az, hogy a vállalati környezetben a publikus felhőszolgáltatások használata vagy nem engedélyezett (tehát a Shadow IT részeként találkozunk vele), vagy használatát most vezetik be – tehát az ehhez kapcsolódó oktatások elsősorban funkcionálisak, nem biztonsági jellegűek. A publikus felhőszolgáltatások használata feltételez egy alapfokú biztonságtudatos viselkedést a felhasználók részéről, amit a szervezett és rendszeres vállalati oktatások hivatottak kialakítani. Amennyiben a felhasználók rendelkeznek ezzel a tudással, erre az alapra építhető a felhő biztonságtudatosságának kialakítása is. A kérdőívemben arra keresem a választ, hogy ez a tudás létezik-e, mennyire alapos és rendszeres, milyen a résztvevők hozzáállása a témához, valamint milyen vállalati folyamatok, szabályok, vezetői attitűdök befolyásolják a biztonságtudatosságot.

A kérdőívet 53 fő töltötte ki, ezek több, mint 90%-án személyesen vettem részt. Ennek egyik legfőbb oka az volt, hogy a kitöltés során a megkérdezettek pontosan válaszoljanak, valamint egyes kérdéseket szükség esetén kiegészíthettem, újrafogalmazhattam.

A kérdőív összesen 35 kérdésből áll, a kitöltési idő átlagosan 30 perc volt. A kérdőív harmadik része a kutatás megkezdésekor tartalmilag más volt, mint a jelenlegi, végleges kérdőív. Az első néhány alany kitöltése után a kérdőíven módosítottam, mert kitöltése túl nehéznek bizonyult a résztvevők számára, és több kérdésre nem, vagy nem értékelhető választ kaptam. A kérdőív összeállításánál arra számítottam, hogy a megkérdezettek emlékeznek a vállalati információbiztonsági szabályokra– hiszen a képzést mindannyian elvégezték -, és azokat készségszinten ismerik, használják és betartják. A szabályok közül

néhány valóban közismert, de a megkérdezettek számára könnyebb volt a felismerés – tehát leírva a kérdőíven szereplő minták közül felismeri a rá vonatkozót, – mint a felidézés. Ez a tény mindenképpen igazolja, hogy a jelenlegi információ- és adatbiztonsági oktatások hatékonysága nem megfelelő. A tudás inkább passzív, néhány esetben használt, de semmi esetre sem tudatos viselkedést tükröz.

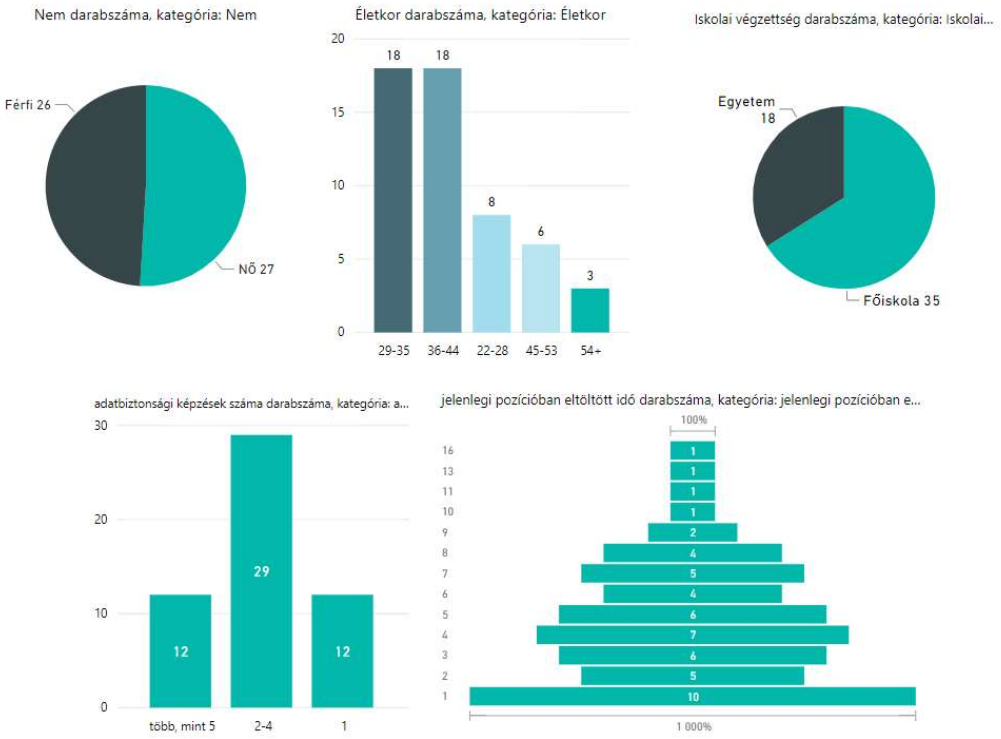
A kérdőív jelenlegi tartalma sem könnyű, a válaszadók többször nehezebben értékelték, mint az online vizsgát követő tesztet. A kérdőív harmadik blokkját tartották a legnehezebben kitölthetőnek – ez a rész vonatkozik a megkérdezettek IB tudására, és több esetben a meglévő, szintetizált tudásukra kérdeztem rá.

A kérdőív felépítése komplex, és a kapott válaszok között is kutathatók összefüggések.

A kérdőívben a válaszadókat kóddal láttam el. Az első vizsgált nagyvállalatnál 17 résztvevővel töltettem ki a kérdőívet, az elemzés során ők kapták az A1-A17-ig kódokat. A második nagyvállalatnál 25 fővel tudtam kérdőívet kitölteni, az ő kódjaik a B1-B25-ig található. A harmadik vállalatnál 11 főt értem el személyesen, ők a C1-C11 kódokat kapták. Az elemzés során a vállalatok nevének az egyéni kódok alapján A, B és C vállalatot választottam. A kérdőív kiértékelésénél a válaszokat vállalatonként és összesítve is vizsgálom.

3.2.1 1.Blokk – Demográfiai adatok

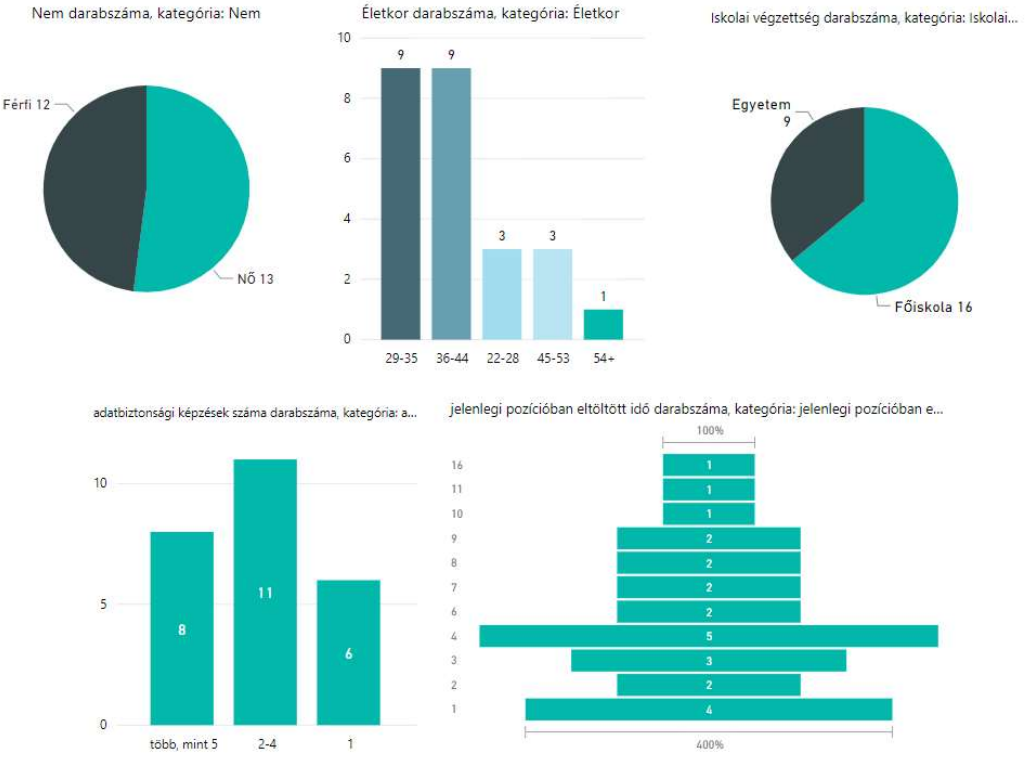
Az első blokk 5 kérdésből áll. A résztvevők közül 27 nő és 26 férfi. Életkorukat tekintve korcsoportokra bontottam őket, ahol a 29-44 éves korosztályt értem el nagyobb százalékban. Végzettségüket tekintve 66%-uk főiskolai, 34%-uk egyetemi végzettséggel rendelkezik. 54,7%-uk (29 fő) egynél többször (2-4 alkalom) vett részt információbiztonsági képzésen. A megkérdezettek 20%-a 1 éve van a jelenlegi pozíciójában, és viszonylag ritka, hogy 10+ évig egy pozícióban dolgozzanak (1 fő 16, 1 fő 13, 1 fő 11 és egy fő 10 éve van a jelenlegi pozíciójában is – aminek a neve változhatott ezalatt az idő alatt, de tevékenységében ugyanaz a feladata).



10.ábra: Összesítő ábra a kérdőív demográfiai eredményeiről (saját készítésű ábra)

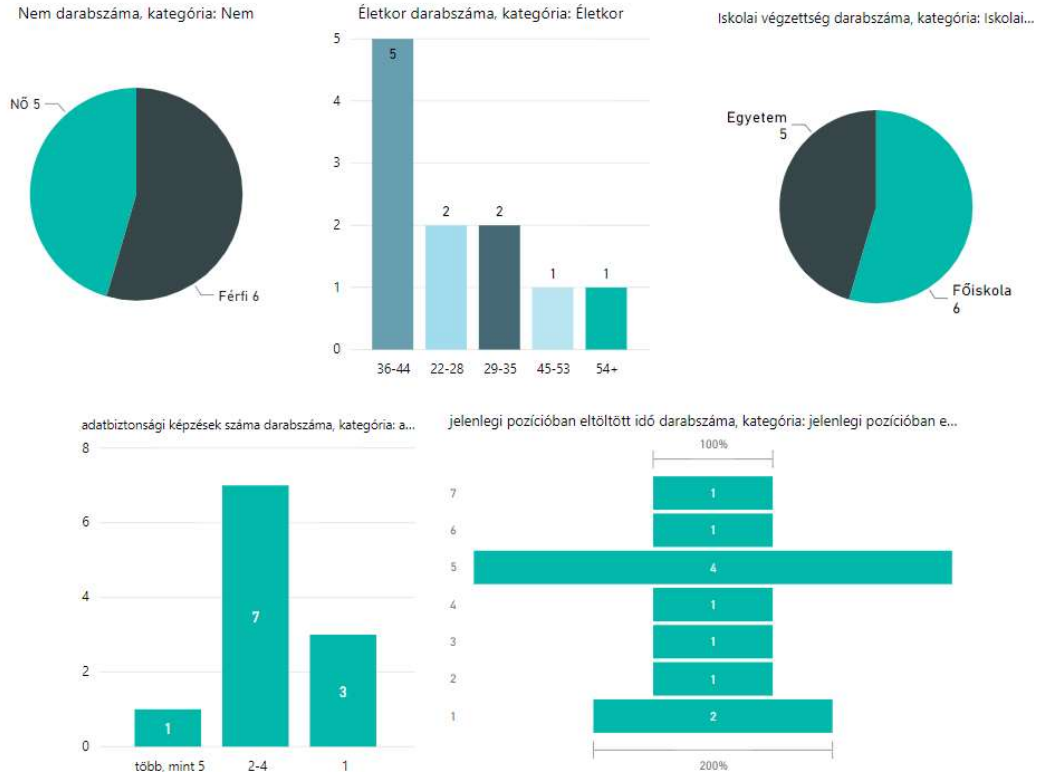
Az A és B vállalat vizsgálatakor az összesítéshez viszonyítva a nemek aránya és a végzettségük, valamint az IB-i képzések száma azonos, viszont az életkorukat tekintve fiatalabb résztvevőket értem el a kérdőívvel.

11.ábra: Demográfiai adatok az A vállalat válaszai alapján (saját készítésű ábra)



12.ábra: Demográfiai adatok a B vállalat válaszai alapján (saját készítésű ábra)

A C vállalat esetében magasabb a férfiak és az egyetemi végzettséggel rendelkezők aránya is. Életkorukat tekintve inkább középkorúak, viszont jelenlegi pozíciójukban több éve stabilan dolgoznak.



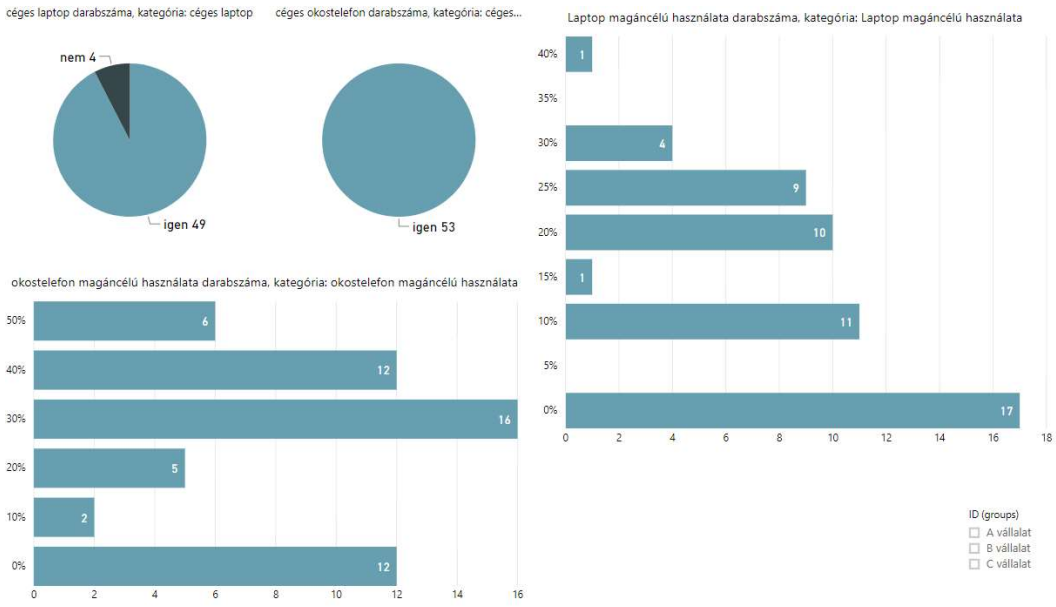
13.ábra: Demográfiai adatok a C vállalat válaszai alapján (saját készítésű ábra)

A demográfiai adatokat összesítve a résztvevőkre elmondható, hogy minden megkérdezett legalább felsőfokú végzettséggel rendelkezik, és legalább egyszer már vett részt információbiztonsági képzésen.

3.2.2 2.Blokk – Technológiai adatok

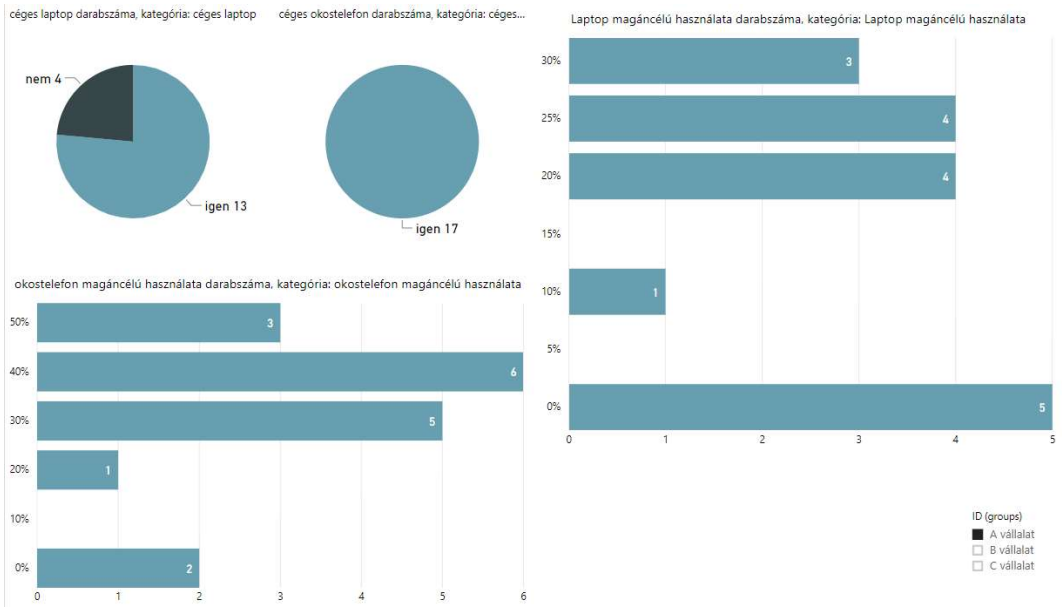
A résztvevők technikai felszereltségére vonatkozó kérdésekből összesen 4 szerepel a 2. blokkban. A résztvevők az iparágból adódóan csúcsminőségű vállalati eszközökkel rendelkeznek, aminek magánfelhasználását a vállalat nem tiltja. Tehát az okostelefont használhatják magán célra is hanghívásokra, ezen felül korlátlan adatforgalommal rendelkeznek. A vállalati laptopok esetében a böngésző szintén használható, a gépeken azonban nem rendelkeznek admin jogokkal, azokra telepíteni nem tudnak semmilyen alkalmazást. Az eszközök vállalati és magánfelhasználásának arányát kérdeztem, amire a válaszadók egy általuk becsült értéket adtak. Az értékek a vállalati laptop és a vállalati okostelefon felhasználás között eltérést mutattak. Nem minden megkérdezett rendelkezik

vállalati laptoppal (4 főnek még nincsen, ők mindannyian 1 éve dolgoznak a vállalatnál), vállalati okostelefonja azonban mindenkinek van. A laptopok esetében az átlagos magánfelhasználás aránya: 13,3%, míg ugyanez az érték az okostelefonok esetében: 26%. A jóval magasabb értéket a mobiltelefonok szélesebb körű használata okozhatja, ezeken az eszközökön használja a privát célra használt informatikai eszközök nagy részét is.



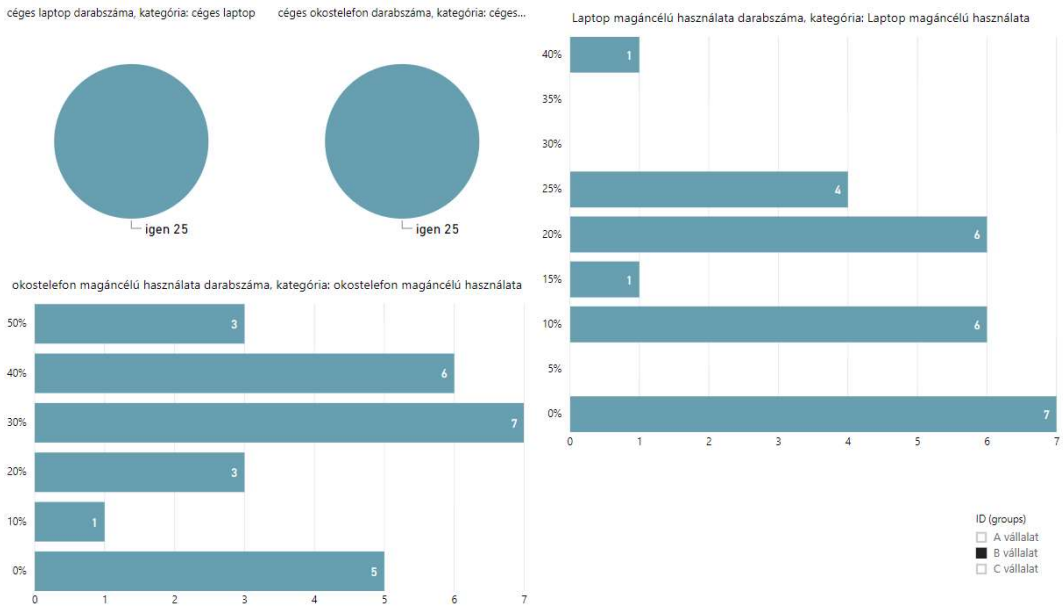
14.ábra: Összesített technológiai adatok a kutatásban résztvevőkről (saját készítésű ábra)

A lenti összesítő ábrán jól látszik, hogy csak az A vállalat szerepeltet olyan munkatársat, aki nem rendelkezik vállalati laptoppal, ők jellemzően pályakezdők és átlagosan 1 éve dolgoznak jelenlegi pozíciójukban, munkahelyükön, asztali gépen dolgoznak. Azonban az összesített eredményekhez viszonyítva az A vállalat esetében a legmagasabb a vállalati eszközök magáncélú használata, a laptopok esetében ez 14,7%, a mobiltelefonok esetében pedig 32,9%.



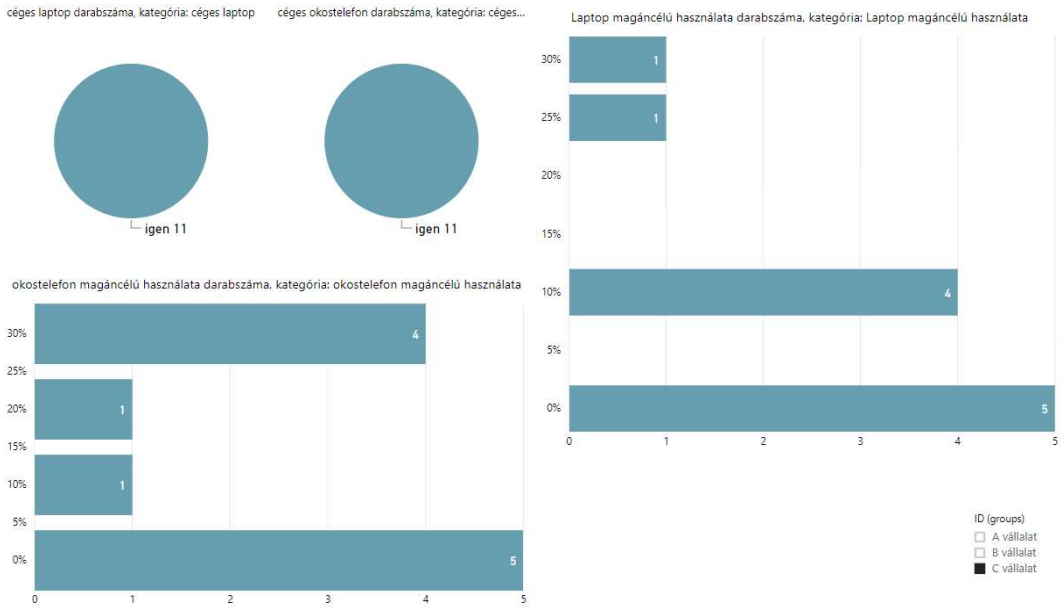
15.ábra: Technológiai adatok az A vállalat válaszai alapján (saját készítésű ábra)

A B vállalatnál minden megkérdezett rendelkezik laptoppal és okostelefonnal. Mind a mobilhasználat (26,8%), mind a laptopok (13,8%) magáncélú használatának aránya megegyezik az összesített átlaggal.



16.ábra: Technológiai adatok a B vállalat válaszai alapján (saját készítésű ábra)

A C vállalat megkérdezett munkatársai hozzák a legalacsonyabb eredményeket, ők használják a legkevesebbet magáncélra a vállalattól kapott eszközöket. A céges laptopok magáncélú használata 8,6%, a céges mobiloké pedig 13,6%.



17.ábra: Technológiai adatok a B vállalat válaszai alapján (saját készítésű ábra)

3.2.3 3.Blokk, Az információ- és az adatvédelem ismeretének felmérése

A kérdőív harmadik blokkja 18 kérdést tartalmaz. A visszajelzések alapján ennek a blokknak a legnehezebb a kitöltése, és sokszor többet kérdezek, mint ami az elektronikus tananyag vizsgájában szerepel. Ebben a blokkban konkrét tudásra, ismeretre kérdezek rá, aminek felidézése nem volt egyszerű a megkérdezettek számára, a kitöltési idő 50-60%-át erre a részre fordították. A 19 kérdésből 11 kérdés feleletválasztós, a maradék 8 kérdés esetén szabadszöveges választ vártam a résztvevőktől. Ebből a 8 kérdésből 3 esetben konkrét vállalati IB-i szabályra voltam kíváncsi, ahol az egyik esetben valóban mértem, hogy helyes-e a kérdésre adott válasz.

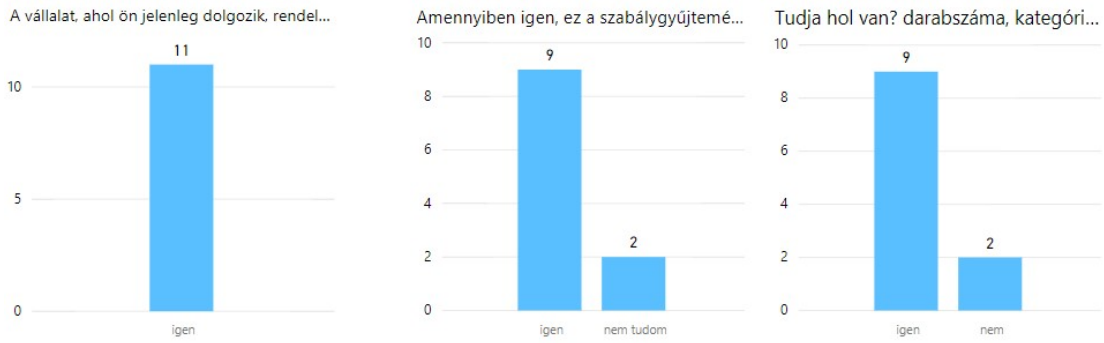
A kérdőívben leginkább IB-i kérdéseket szerepeltettem, az első három kérdés során az ehhez kapcsolható tudásra kérdeztem rá. A megkérdezettek közül 43 válaszolt igennel arra a kérdésre, hogy a cége rendelkezik-e IB Szabályzattal. Az erre a kérdésre igennel válaszolók közül 38-an tudták, hogy ezt a szabályzatot ők is elérik, és csupán 36-an (68%-uk) voltak tisztában azzal, hogy ezt hol találják.

Az A, B és C vállalatok közül a C vállalat szerepelt a legjobban, ott 81,8%-ot értek el, míg az A vállalat 53%-kal, a B vállalat pedig 72%-kal szerepelt.

18.ábra: A vállalati Információbiztonsági szabályzat helyének ismerete, összesítve minden megkérdezett

19.ábra: A vállalati Információbiztonsági szabályzat helyének ismerete az A vállalatnál

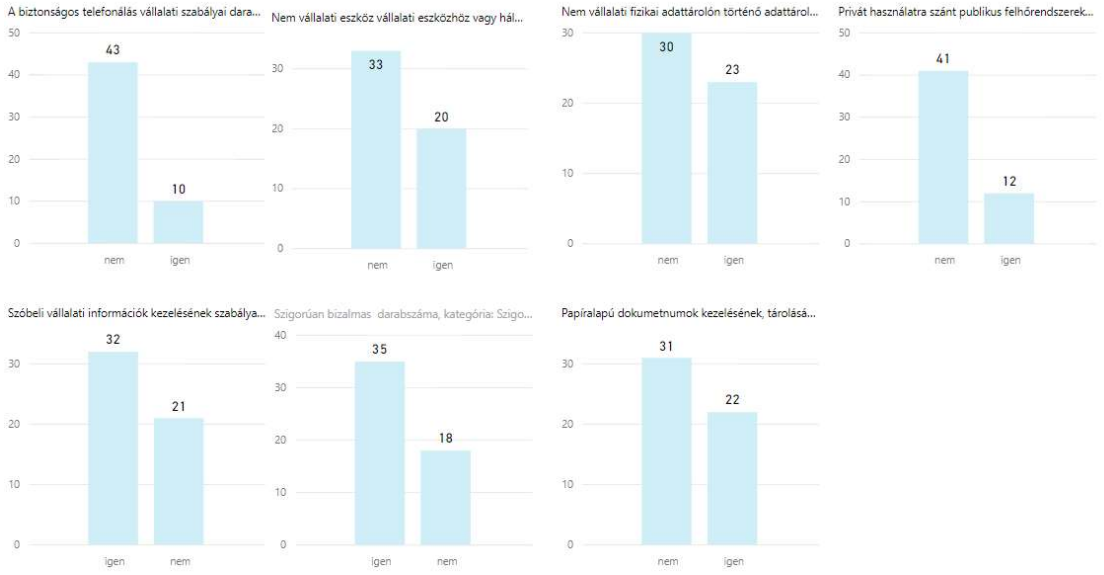
20.ábra: A vállalati Információbiztonsági szabályzat helyének ismerete a B vállalatnál



21.ábra: A vállalati Információbiztonsági szabályzat helyének ismerete a C vállalatnál

A következőkben arra kértem a résztvevőket, hogy az IBSZ-ben található szabály közül hármat idézzenek fel. A legnépszerűbb helyesen felidézett szabály a jelszókezelés volt, milyen a jó jelszó, és az ő felelőssége annak megóvása. A második helyen a vállalati adatvagyon megőrzése, a harmadik helyen pedig tiszta képernyő szabályai álltak.

A 3.5 kérdésben 10 szabályt soroltam fel. Arra kértem a válaszadókat, hogy jelöljék meg azokat, amik a saját vállalati IBSZ-ükben szerepel. A 10 kérdés közül 6 valóban, mind a három nagyvállalat tananyagában is benne van, 4 pedig nem része a szabályzatnak.



22.ábra: A 3.5 kérdés szabályai (4.-10. rangsorral)

A 3.6 kérdés az előző pontban megjelölt szabályokhoz kapcsolódik, itt arra kértem a résztvevőket, hogy rangsorolják az általuk bejelölt szabályokat, melyiket tartják a legfontosabbnak. Az első három helyezett:

1. A vállalat informatikai rendszereinek használatához kapcsolódó biztonsági szabályok
2. Jelszókezelés szabályai (jelszó védelme, változtatása, megőrzése, felelőssége)
3. Vállalati szabályok a biztonságos E-mail használatra vonatkozóan

23.ábra: Rangsorban az első három szabály összesített eredményei

A 3.7 kérdésben a szabályok felidézését kértem a válaszadóktól. Itt azt vizsgáltam, hogy fel tudja-e idézni a témához tartozó szabályt, mennyire pontos a tudása, hibás választ ad, vagy egyáltalán nem tud választ adni. A szabályok felidézését csak akkor kértem, amennyiben a 3.5 kérdésre igen választ adott. A 3.6-os kérdéshez hasonlóan azt tapasztaltam, hogy a népszerű (a ranglistán az első három szabály) szabályok felidézése pontosan történik, a kevésbé ismertek (Papíralapú dokumentumkezelés vagy a Szóbeli vállalati információk kezelésének szabályai) pontos felidézése csak 13 illetve 15 résztvevőnek sikerült.

Mivel egyik vállalat sem rendelkezik konkrét publikus felhőszolgáltatásról szóló irányelvvel (csak tiltják a használatát vállalati adatokra vonatkozóan), így ezen szabályok számokérése is csak részben, közvetett módon tehetők meg. A felhős szolgáltatásokra nagy részben alkalmazhatók a vállalatnál megtanult informatikai alapelvek, ezért kerestem összefüggést a vállalatnál tanultak és a magánfelhasználás során alkalmazott biztonsági szabályok között (3.15). Úgy feltételezem, hogy a magánéletben használt szabályok már beépültek, azok betartása ösztönösen működik a résztvevőknél.

További feltételezésem, hogy a felhasználók szabálytartására hatással van az informatikai környezetben végzett munkájuk megfigyelésének (monitorozásának) ismerete. Amennyiben a felhasználó tisztában van azzal, hogy a munkája során figyelik milyen alkalmazásokat nyit meg, milyen oldalakat látogat, milyen gyakran, mikor és honnan lép be a vállalati rendszerekbe – szabálykövetőbbé teszi. Ezért ebben a blokkban a 3.14 és a 3.17-es kérdések során erre kérdeztem rá. A válaszok alapján egyértelműen látszik, hogy az a vállalat, ahol a legerősebb és a legtudatosabb a monitorozás (C vállalat), a válaszadók szabálykövetése is erősebben nyilvánul meg. A 3.5, 3.6 és 3.7 kérdéseknél is látható, hogy a C1-C11 válaszadók az IBSZ-ben nem szereplő szabályokat is többször értékelték szabálynak, és azok megfogalmazására is képesek voltak.

A magánfelhasználás során (3.16) szintén a szabályok közül rangsorolt első három szabály követődik. Ezeket a szabályokat otthoni környezetben is betartják, odafigyelnek rá. Szintén a C vállalat munkatársai a szabálykövetőbbek ezen a téren is, több óvintézkedést tesznek a saját tulajdonú eszközök és adatok védelme érdekében. A felhőszolgáltatásokat magáncélra is körültekintőbben veszik igénybe.

A 3.17 kérdés válaszaiban több nemzetközi példát hoztak, ahol az adatbiztonság, a felhőplatform sérült. A válaszok alapján látható, hogy a téma ismert számukra, a híreket figyelik, érintettnek érzik magukat.

A 3.18-as kérdésnél a válaszadók 78%-a elismeri, hogy lenne szerepe, ha a tevékenységük folyamatosan monitorozva lenne. Ez a válasz bizonyítja, hogy a kontroll szerepére nagy igény lenne, ugyanakkor mutatja azt is, hogy belső kontroll még nem alakult ki, a felhasználónak fontos, hogy a felelősség szerepén osztozzon a kiszolgálóval.

3.2.4 4.Blokk - Biztonságtudatosság oktatása

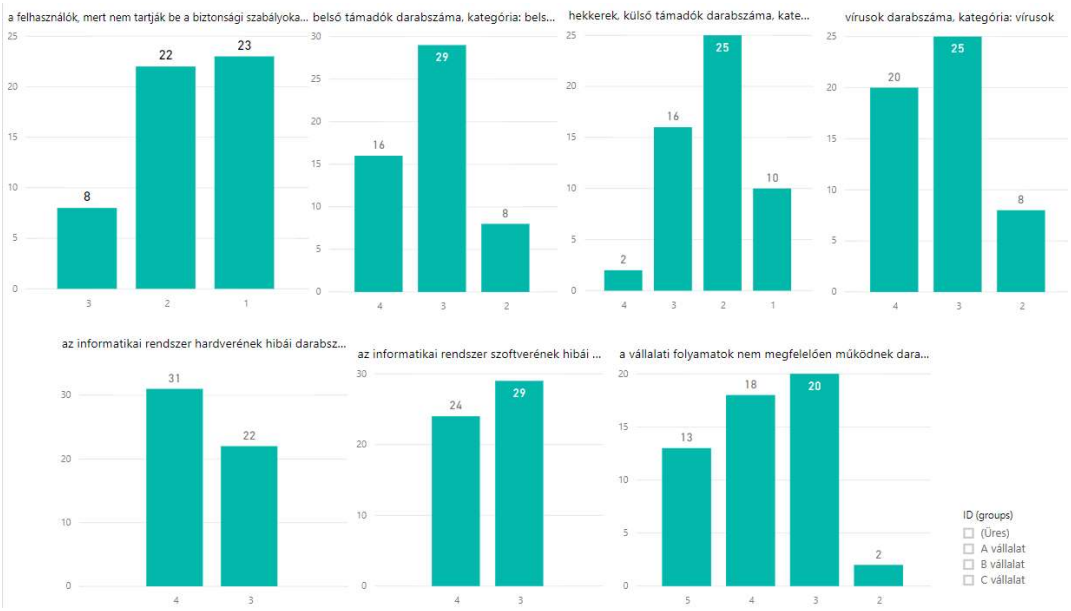
A kérdőív negyedik blokkja 7 kérdése a jelenlegi képzésről és a válaszadó képzéssel kapcsolatos ötleteiről szól. A jelenlegi képzést nem tartják hatékonynak, az elektronikusan elérhető tartalom nem azt a hatást váltja ki, ami az eredeti célja volt. Értékelik, hogy a tananyag online elérhető, azonban a tananyag évenkénti ismétlését ebben a formában nem támogatják. A személyes előadásokat jobban értik és személyre szabottnak érzik, ahol aktuális helyzeteket és kérdéseket közösen is megvitathatnak. Az elektronikus tananyagot egy kötelező elemnek tartják – ami a mindennapi munkájuk során nehezen adaptálható, ugyanakkor kötelező jellege miatt eleve ellenszenvet vált ki. (4.1, 4.2, 4.3, 4.4) kérdések. Az A vállalat videós anyagait a megkérdezett munkavállalók

nem értékelik, többen nem nézték végig. A videó véleményük szerint trivialitásokat tartalmaz – ugyanakkor ebben a kérdőívben is látszik, hogy a trivialitást visszaidézni nem olyan egyszerű.

A képzésekre évente szánnának időt, és leginkább interaktív módon, szituációba ültetve tudnák hatékonynak elképzelni. Vállalati példákra lenne szükségük a jobb megértéshez, valamint az egészséges félelemérzet kialakítására. (4.5)

Szívesen vennének részt hasonló tartalmú képzésen, meghatározott időkeretben. (4.6)

A 4.7 kérdés táblázata a felhőkockázatokat méri a válaszadók szubjektív megítélése szerint. Rangsorba tették kérésem szerint, ahol a legfontosabbnak ítélt kockázat az emberi tudatosság hiányára vezethető vissza, „a felhasználók, mert nem tartják be a biztonsági szabályokat”.



24.ábra: Összesített ábra a kockázatokról

3.3 A személyes interjúk és kérdőívek kapcsolatának elemzése

A HR és IT vezetőkkel, munkatársakkal folytatott személyes interjúk során a vállalat által elvárt munkatársi viselkedésre, a vállalati informatikai biztonságpolitikai háttérre, valamint a vállalati informatikai szabálygyűjteményekre kérdeztem rá. A személyes interjúk során tehát azt a területet térképeztem fel, amit a vállalat kialakított a munkatársai számára, megfelelő szabályokkal látott el, aminek ismeretét elvárja minden egyes munkavállalójától. Ehhez ismeretátadást szervez, belső- és külső oktatásokat tart vagy

tartat, helyenként szerződésben (titoktartási nyilatkozatban vagy munkavállalói munkaszerződésben) rögzíti ezen ismeretek nem tudásának szankcióit.

A HR és IT területeken dolgozók joggal várják el munkatársaiktól, hogy felkészültek legyenek ebben a témában is, és minden körülmények között tudják, mi a feladatuk, mit kell tenniük. Ismerjék fel azokat a körülményeket, amik veszélyt jelenthetnek a vállalatra nézve, és azokat a megfelelő csatornákon keresztül jelentsék be.

A személyes kérdőívek során pont ezt a célcsoportot kérdeztem arról, milyen elvárt viselkedést támaszt a vállalat velük szemben, hol találja a kérdéses dokumentumokat, milyen veszélyek leselkedhetnek rá, hogyan birkózik meg ezekkel.

A munkatári válaszokat elemezve sokkal árnyaltabb kép születik a vállalati felhasználók biztonságtudatosságát illetően. A kutatásom jóváhagyásakor mindhárom vállalat szívesen vette a munkatársak megkérdezését, és kíváncsi volt azok eredményére. Az interjúk és a kérdőívek kapcsolata vállalatra lebontva nagyon jó visszajelzés számukra, hiszen egyértelműen látszik, hol vannak azok a rések, amikre a jövőben megoldást kell találniuk.

Dolgozatomban a fenti okok miatt vállalatra lebontva elemzem az interjúk és kérdőívek viszonyát. Feltárom vállalatonként azokat a pontokat, ahol a kívánt és a mért/bevallott értékek találkoznak vagy nagyon eltérnek egymástól.

3.3.1 Az első (A) nagyvállalat eredményei

Az első vállalattól a HR osztályon 6 fővel (munkatársi szint) az IT üzemeltetésről pedig 2 vezetővel készítettem személyes interjút. A vállalatnál van információbiztonsági alapképzés, melyet elektronikus formában tesznek kötelezővé minden munkavállaló számára. A tanfolyamot 3 évente kötelező megismételni, az elektronikus tananyag megtekintését követően vizsgával zárul, melynek legalább 75%-át jól kell teljesíteni. A vizsga megismételhető nem megfelelés esetén, de erre nagyon ritkán van a gyakorlatban példa. A tananyagot külső tanácsadó állította össze, de csak vállalati információkkal, színes, sok képet és videót tartalmazó alapozó tananyagról van szó. A tananyag a belső intraneten is elérhető, tehát bármikor megtekinthető. Az oktatások kezelését a HR osztály végzi.

További, külsős, a témába való oktatásra vagy előadásra a munkatársak jelentkezhetnek. Amennyiben ezek a képzések ingyenesek, a vállalat előszeretettel küldi el szakmai kollégáit továbbképzés gyanánt. A gyakorlatban sajnos ez csak a szakmabelieket érinti,

tehát az IT területen dolgozók ismerik ezeket a képzéseket és látnak lehetőséget abban, hogy ezeken részt is vegyenek. A témában nagyobb konferenciákon is megjelennek, szívesen adnak elő – bár szintén csak az IT osztályokról. Belső képzések során gyakran előfordul, hogy az IT egy-egy területéről megkérnek egy munkatársat, hogy más társosztályok számára tartson előadást – leginkább biztonságtudatossági (pl., hogy használjon egy új alkalmazást, mire figyeljen oda egy munkatársi készülék személyes használatakor, hogy adjon el egy már nem használt, de korábban vállalati tulajdonban lévő eszközt stb.) témában. Ezek az előadások eseti jellegűek és egyéni szervezésűek (pl. a HR nem tud róla, és a folyamatba ne is kell őket bevonni) de nagyon népszerűek.

Az IT ennél a vállalatnál említették a Shadow IT jelenlétét, bár a kérdőívek során ez a válaszokból nem derült ki. Voltak olyan helyzetek, amikor a munkatárs hibájából adódóan kár ért vállalati adatot, ezek nem is mindegyikéről tudnak. Amiről tudnak, azokat igyekeznek kezelni, a legnagyobb szankció eddig a munkaszerződés megszűntetésével járt, erre az elmúlt 3 évben egyszer volt példa.

A személyes kérdőívekből azonban az derül ki, hogy a munkatársak rendelkeznek mobileszközökkel, amin majdnem minden esetben használnak személyes használatra szánt alkalmazásokat is. Elérik a vállalati levelezést, amihez a mobileszköz lezárása és feloldására van szükség minden esetben (PIN-nel védeni szükséges), de az applikációk korlátozás nélkül letölthetők. Az információbiztonsági szabályzat meglétéről a megkérdezetteknek csak a 76%-a tud, a 17 főből 13, azt pedig, hogy hol található ez a dokumentum csak 11 fő tudja, bár ez az elektronikus tananyagban is szerepel. Megállapítható, hogy az oktatási anyag azon részei, amelyekre a gyakorlatban is ráerősítenek, ismertebbek a munkatársak körében (pl., jelszókezelés).

3.3.2 A második (B) nagyvállalat eredményei

A második vállalattól a HR osztályon 4 (munkatársi szint) az IT üzemeltetésről pedig 8 fővel (szintén munkatársi szint) készítettem személyes interjút. A vállalatnál van információbiztonsági alapképzés, melyet elektronikus formában tesznek kötelezővé minden munkavállaló számára. Az A vállalathoz képest szintén vizsgával zárul, ennek tartalmát azonban belsős munkatárs állítja össze. E-Learninges felületen jelenítik meg, a tananyag a későbbiekben nem elérhető a már levizsgázott hallgatók számára. A vizsgán való nem megfelelés bár szankciót nem von maga után, de nagy kellemetlenséget okoz a „bukott” hallgató számára, több vezetővel, három szinten engedélyeztetnie kell a vizsga

megismétlésének lehetőségét, és erről a kérvényezési folyamatról a HR-t is értesítik. Belső céges rendezvényeken egyre népszerűbb, hogy egy-egy előadás erejéig tartanak tudatosító oktatásokat. Az elmúlt két évben volt vállalati incidens – ezt követően vezették be ezen előadásokat. Azt tapasztalják, hogy az itt előadókat utána szívesebben megszólítják folyosón, vagy keresik fel őket a témában és kérnek tanácsot, akár személyes jelleggel is.

Az IT említette a Shadow IT meglétét cégen belül, amit leginkább úgy próbálnak kezelni, hogy ellenállóbb munkatársi gépeket adnak ki a felhasználók számára. Az MDM itt kísérleti jelleggel bevezetésre került, de használata nem volt kötelező, tiltást központilag nem tettek fel rá – a cég egyik termékeként tesztelte egy belső csoport.

A mobilkészülékek magánfelhasználásából eredően eddig nem azonosítottak kárt, a mobilkészülékeken ennél a vállalatnál csak az üzleti levelezés fut, amit belső szervereken működtetnek és minden esetben tűzfalon engednek át. Több probléma merül fel abból, hogy a mobilkészülékek szervízelése során a magánadatokkal mit kezdjenek – egy készülék gyári visszaállítását követően a vállalati levelezés, a címtár és a naptárfunkciók azonnal visszatölthetők, de sokszor kérés a felhasználó részéről, hogy a fényképeket valahogy szerezze vissza számukra a szerviz. Sajnos arra nincs mért adat, hogy a céges eszközökön a Facebook alkalmazás használatával céges címtár került-e illetéktelen kezekbe.

A mobilfelhasználásról kérdezve a munkatársakat - kérdőívek kitöltésekor – többen megjegyezték, hogy osztályon belül használják a Doodle-t, ügyfelekkel a Vibert, családtagokkal és barátokkal a Messengert, vagy a Facebook alkalmazásokat (Viber kivételével a többi alkalmazást laptopon is).

A munkatársi kérdőívek során az is kiderült, hogy az elektronikus oktatásokat általában kisebb csoportokban, együtt végzik el, az eredményeket megbeszélik. Az Információbiztonsági szabályzat meglétét majdnem annyian ismerték százalékosan, mint az A vállalat esetében (76%), arra, hogy hol találják, jobb eredményt hoztak. Informálisan ők mesélték a legtöbb olyan esetet, ami a kérdőívek során eszükbe jutott, és érdekesnek tartották megosztani. (Pl., az ügyfelekkel Viberen beszélnek, vagy a gyerekükkel Messengeren stb.)

3.3.3 A harmadik (C) nagyvállalat eredményei

A harmadik vállalattól 5 informatikai munkatárssal beszéltem az üzemeltetési területről, 3 középvezetővel a HR osztályról, és itt sikerült a HR vezetővel is személyes interjút készítenem. Ő beszélt arról, hogyan alakítottak ki egy viszonylag szigorúnak mondható biztonsági rendszert, ami az informatikai szabályokra is kiterjed. Ennek igénye leginkább az anyavállalattól érkezik, és az A és B vállalattól eltérően nemcsak a magyar piacra dolgoznak, hanem többnyire nemzetközi ügyfeleik vannak, üzleti nyelvként pedig az angolt használják. Mivel nagyobb nemzetközi piaccal dolgoznak, nagyobb a veszélye is annak, hogy szándékos támadás éri a cég informatikai rendszerét. Bár nagy mértékű támadás hazánkban nem érte a céget, ugyanakkor a nemzetközi tapasztalatok alapján inkább tartanak az ilyen jellegű támadásoktól, és inkább a túlzott felkészülést vállalják, minthogy egyszer kerüljenek nagyobb bajba.

Ezek az előzmények vezetnek oda, hogy az anyavállalattól érkező félelmeket a munkatársakba is viszonylag könnyen el tudják ültetni. Ehhez segítségükre vannak az írott szabályzataik – saját bevallásuk szerint ezek elég részletesek és szigorúak -, fontos, hogy a szabályzatoknak nemcsak a helyét, hanem a tartalmát is ismerjék a munkavállalók, és elismerik, hogy szándékos vagy akaratlan károkozást is szankcionálnak. A HR vezetők azt is megemlítették, hogy véleményük szerint nagyon sokat számít a biztonságtudatos magatartás során a példamutatás. Ennél a cégnél komoly mentorálási program működik, ahol a betanuló munkatárs a mentee-től nemcsak a mindennapi munkájához szükséges információkat sajátítja el, hanem olyan vállalati viselkedési mintát is kap, amiről tudja, ha nem tartja be, az nem elfogadható a vállalat vezetése részéről.

A témát felölelő oktatási tananyag itt is elektronikus, és kétévente tesznek vizsgát a vállalat dolgozói. A tananyagot ezért kétévente megújítják. A vizsgázók itt vizsgáznak a legszigorúbb körülmények között – az oktatási gépeken érik el a tananyagot, és a vizsgát, amit meghatározott időtartam alatt kel teljesíteniük.

A munkatársi kérdőívek – bár ennél a cégnél volt a legkisebb a mintavételem – során az derült ki, hogy mindenki tisztában van azzal, hogy a vállalat rendelkezik Információbiztonsági szabályzattal, és a 11 megkérdezett közül csak 2 nem tudja, hol találná meg elektronikusan. Tisztában vannak azzal, hogy a teljes tevékenységük monitorozva van (többen megjegyezték, hogy ezt a tényt a munkaszerződésük is tartalmazza), és szerintük ez a legnagyobb visszatartó erő, hogy ne okozzanak kárt a

vállalati adatvagyonban. A szankciókról bár tudnak, nagyon ritkán fordul elő – volt, aki nem is tudott róla -, többen tudatosan nem használják a vállalati ezközöket magáncélra.

3.4 Összefoglalás

A személyes interjúk és a kérdőívezés során arra a következtetésre jutottam, hogy a tudatosítás fontos, és nem elhanyagolható. Azonban abban az esetben, ha megfelelő biztonságtudatosságot szeretnénk kialakítani munkatársaink körében, nemcsak az oktatásra, hanem a szabályok megalkotását, bevezetését és betartatását is komolyan kell kezelnünk.

A kérdőívek feldolgozása során választ kaptam arra, a felhasználók azokat a szabályokat képesek visszaidézni és tartják be, melyeket a vállalat nemcsak az oktatás során mutat be, hanem a mindennapok során is kikényszerít. Ilyen például a jelszavak védelme, kezelése, hossza, elévülési ideje. Ezeket a szabályokat nemcsak a vállalaton belül, hanem a privát életükben is alkalmazzák.

A három vizsgált nagyvállalat közötti különbségek a kérdőívezés során is mérhetők voltak. A szabályokat és a szankciókat erősen használó nagyvállalat (C vállalat) esetében volt a legalacsonyabb felhasználók szabályoktól való eltérése. Ezek a felhasználók tudták a legtöbb szabályt, a legkülönfélébb szabályokat visszaidézni – és saját magukkal szemben is szigorúbbak voltak, amikor a vállalati információbiztonság fontosságáról kérdeztem őket. Tehát elmondható, hogy nemcsak az oktatás megléte, kialakítása és levezénylése számít a tudatosság kialakításában, hanem fontos, hogy a felhasználókra vonatkozó szabályok betarthatók legyenek, a rendszer vizsgálja, ellenőrizze, ne engedje az ettől való eltérést, valamint hibázás vagy szándékos károkozást követően olyan szankciót helyezzenek kilátásba, ami a felhasználók nagy részét óvatosságra, körültekintésre kényszeríti.

A biztonságtudatosság kialakítása csakis ezzel a hármas egységgel alakítható ki, ahol egyik tényező elhagyásával a kívánt siker már nem elérhető. A tudatosságot, mint rendszert kell vizsgálni, és nagy részben még mindig a felhasználón múlik biztonsági lánc kockázata, ugyanakkor a vállalat képes javítani annak minőségén, ahogyan azt a C vállalat esetében is láthattuk.

A személyes interjúkkal összevetve, mindhárom vállalatnál voltak eltérések az elvárt és a mért biztonságtudatosság között. A legnagyobb eltérést a B vállalat adta, a legkisebbet a C. Mindhárom vállalat esetében fontosnak tartom, hogy több visszamérési pontot

vezessenek be, ahol a munkatársak tudását ellenőrizhetik, a kétévenkénti elektronikus oktatást és a hozzá tartozó vizsgát pedig nagyon kevésnek találom. Mindhárom esetben mind az interjúk, mind pedig a kérdőívezés során azt a választ kaptam, hogy több életből vett példa, személyes történet, vagy gyakorlati példa mélyebben megmarad, mint az általános oktatási tananyag, amit nem tudnak mihez kötni.

Fontosnak találom, hogy az oktatást differenciálják, nemcsak életkor alapján, ahogyan azt az egyik IT vezető javasolta, hanem szakirány szerint is – itt rengeteg élő és jó példa esettanulmány létezik, amivel könnyebben tudnának azonosulni a munkatársak. A gyakoribb, de rövidebb, akár csak egy-egy szabályt bemutató előadás, videó, webinár, bejegyzés, vagy belső hálón megjelent cikk hasznosabb lenne, ezek segítségével a téma fontossága napirenden tartható, és beépül a munkatársak mindennapjaiba.

Ahogy a 3. hipotézisemben állítottam, a humán fejlesztés, valamint a vállalati szabályozás szoros kapcsolatban állnak, a HR és az IT vezetés hatással van a munkatársi biztonságtudatosság szintjére. Arra az eredményre jutottam, hogy amennyiben az oktatás rendszeres, az ott megszerzett tudás a gyakorlatban is elvárt a munkatárstól, a szabályok nem betartása pedig szankciókat von maga után, ott a munkatársak szabálytartása erősebb. Így a harmadik hipotézisemet elfogadom. Ennek a bizonyításához egy megelőző tanulmányt írtam, mellyel az ebben a fejezetben szerepelt eredményeimet előzetesen megalapoztam, „Serious Games Experience in Teaching Cloud Security” (II.), a International Association of Technology, Education and Development folyóiratban, valamint az Acta Technica Corviniensis-ben megjelent publikációm, melynek címe, „New Didactic Methods in Cloud Teaching” (IV).

4 AZ OKTATÁSOK SORÁN AZ ELKÖTELEZETTSÉG NÖVELÉSE A JÁTÉKOSÍTÁS ESZKÖZEIVEL

Bevezetés

A fejezetben a játékosítás módszerét vizsgálva jutok el egy használható eszköz ajánlásáig. A játékosítást oktatási feladataim során korábban is alkalmaztam, és azt tapasztaltam, hogy az ezzel a módszerrel átadott információ mélyebben épül be, valamint erősebb kötés épül fel az információ, az átélt élmény és a résztvevő között.

A fejezetben vizsgálom, hogy a felnőttkorban lévő tanulás befolyásolható-e a játékosítás eszközével, valamint az egyéni motiváció növelhető-e ezáltal. Ehhez ismertetem és elemzem a nemzetközi és hazai tapasztalatokat. A gyakorlati szemléltetéshez vizsgálom a projektben résztvevők elköteleződésének szerepét, az egyéni teljesítményük függvényében, továbbá azt, hogy hol jelennek vagy jelenhetnek meg saját motivációs eszközök a tanulási folyamat során.

A fejezetben bemutatok és elemzek egy általam tartott, játékosító elemekkel kiegészített oktatássorozatot. Az oktatás témája a felhőtechnológiákon belül is egy adott termékre koncentrálódik, ugyanakkor az összefüggések megértéséhez, illetve a termék összehasonlításához szükséges információk miatt a teljes felhőkínálat vizsgálatára sor került a képzés során.

Az oktatások célcsoportja IT tudásukat tekintve nagyon hasonlónak mondható, mind életkorukat, előképzettségüket, a témában való jártasságukat figyelembe véve. Az oktatások célja a célcsoport megfelelő felkészítése az önálló munkavégzésre, és jártasságuk megszerzése a felhőtechnológiák felhasználásában. A gyakorlati jártasságra több lépcsőben kialakított vizsgahelyzetekkel készítettem fel a résztvevőket, ahol a gyakorlati tudás mérése került fókuszba. A résztvevők ezen felül közvetve vizsgáznak, mivel ismereteiket ügyfeleik előtt kell tudniuk hasznosítani és érvényre juttatni.

A fejezetben bemutatom a teljes oktatássorozat folyamatát és módszertanát, a résztvevők által alkotta csoportokat, a mérföldköveket, valamint a vizsgáztatás és visszamérés pontjait és felépítését. Az oktatássorozat a vállalat egyik kiemelt projektjeként erős fókuszt kapott, így annak eredményei is fontosak voltak a vállalat számára.

Az oktatássorozat legkritikusabb pontjai egyrészt a résztvevők folyamatos motiválása, másrészt a téma fontosságának megértetése voltak. A felhőtechnológiák elterjedése az

üzleti életben és azon belül is nagyvállalati környezetben 2014-ben nem volt még olyan jelentős, mint napjainkban, ezért az üzleti ügyfelek meggyőzésének gátja nem az ügyfél és az értékesítő között, hanem a technológia és az értékesítő között lépett fel. Az értékesítő elfogadta az ügyfelek kifogásait, és a legtöbb esetben igazat adott partnereinek. A technológiának meg kellett hódítania mindkét tábort, és ennek egyik eszköze volt az általam végzett képzés. Így ezeknek a tréningeknek a célja nemcsak a biztonságos tudás, a széleslátókörű piaci ismeretek átadása volt, hanem a technológia kikerülhetetlenségének megvilágítása is. Ma már nem kérdés, hogy a felhőtechnológiák használata milyen előnyöket visz az üzleti életbe, 2014-ben azonban még sok cég gondolta úgy, hogy képes önerőből, hasonló erőforrású, biztonságú és szolgáltatás-gazdag infrastruktúrát kiépíteni.

4.1 A játék

A játék az ember számára az a tevékenység, amit önfeledten, egy magasabb érzelmi állapotban, a tevékenységbe feledkezve végez. Az ember a kezdetektől fogva játszik, mert a játék során élvezi a különböző szerepek kipróbálásának lehetőségét, a versenyt, mások legyőzését, a győzelmet – és veszítés esetén az újrakezdés lehetőségét. [114]. Játék során az ember egy befogadóbb tudatállapotba kerül, a játék szabályát gyorsan sajátítja el és azoknak igyekszik megfelelni, nehogy a játékból kizárják.

Lev Vygotsky pszichológus kutatásai alapján állíthatjuk, hogy „a gyermek, játszás közben előrébb tart a fejlődésben, mint a hétköznapi működése során”. Azok a gyerekek, akik az életből mintázott szerepjáték során szerepben vannak, a szerepen kívül is jobban teljesítenek a szerephez hasonló valós helyzetekben. Ezáltal túllépik saját életkorukat és sokkal erőteljesebben fejlődnek, mint bármilyen más tevékenység által. A játékban kreatívabbak, adott szabályrendszert követnek vagy alkotnak meg, és ezáltal fejlődnek értelmi, érzelmi szinten, valamint viselkedésükben. [115], [116], [117]

A játék korábban a szórakozás egy formája volt, jelentőségét vagy alkalmazási lehetőségét nem ismerték. Hiányzott a keretrendszer, a kutatáshoz szükséges módszertan. A játékosítás kutatása is csak a 20.században, 1950-ben kezdődött meg, Harlow megfigyeléseivel. Kísérletében figyelte a rhesusmajmokat feladatmegoldásaik közben. Ekkor figyelt fel a dopamin jelentőségére, ami biológiailag is alátámasztja, hogy a játék során működésbe lép a szervet belső jutalmazó rendszere, ami a dopamin szint emelkedésével jár együtt. [118]. Ha a személy/alany megold egy feladatot, ösztönösen

emelkedik a dopamin szintje, amitől boldogabbá válik. Ezen a ponton kapcsolódik össze a játék és a motivációs elméletek kutatása.

Korábban a tudomány két motivációs rendszert ismert, a jutalmazást és a büntetést. Azonban Harlow kísérlete bebizonyította, hogy ezen a két külső motivációs rendszeren kívül van egy harmadik is, ami a belső motiváció rendszere. Ennek megfelelően a motivációs rendszereket két nagy csoportra osztotta:

Intrinzik motiváció: belső hajtóerő, ami belülről motiválja az embert arra, hogy az előtte álló feladatokat megoldja, a kérdésekre választ találjon. Csíkszentmihályi Mihály ehhez kötötte a Flow élményét, [119], az Intrinziknek a játékosítás során lesz nagy szerepe. Ha a feladatot megoldjuk, a kérdésre választ találunk, a dopamin szint emelkedni fog, amivel az egyén saját magát jutalmazza.

Extrinzik motiváció: a külső forrásból kapott motivációs eszköz ideig óráig működik, különösen abban az esetben, ha az egyén korábban nem rendelkezett az adott motivációs eszközzel, és arra nagy szüksége van (pl. pénz, dicsőség, kinevezés, hatalomstb.). Az extrinzik motivációs rendszer hátulütője, hogy az egyén számára fontosabb lesz a teljesítmény, cél elérése, tehát a feladat elvégzése, nem pedig a belső célja (mit tanulok belőle, élvezem-e a feladatot stb.), tehát az egyén elveszíti a játék élményét a feladat elvégzése közben. A feladat elvégzését követően pedig nem vár rá a katarzis, nem lesz sikerélménye, fásulttá válik, unalmat érez [120], [121].

A fentiek alapján a játék elsősorban az intrinzik motivációra hat, ezáltal egy hosszútávú, valódi sikerélményt ígérő, belső jutalmazórendszerrel ellátott eszközről beszélünk. A játék esetében fontos, hogy a játékos képességeihez mérten (ne legyen sem könnyű, sem nehéz, sem gyorsan megoldható) legyen kialakítva, és belülről ösztönözze őt a játék megnyerésére.

4.2 A játékosítás

A történelem során talán először jutottunk el egy olyan korba, ahol fontossá válik a belső motivációs erő, amikor arra figyelünk, mennyire jó egy adott tevékenységben lenni. Azzal, ha az egyén számára nem a mindennapi létfenntartás a célja a feladatok elvégzésének, beléphet egy olyan tevékenység is, melyet az örömszerzés okán végez. Daniel Pink szerint a motiváció 3.0 korba való belépéssel az emberek a külső motivációs tényezőkön kívül törekednek arra, hogy saját maguknak okozzanak örömet, megtalálják az öröm forrását. Ezzel egy új korszak lép életbe, amikor az intézményrendszerek is a

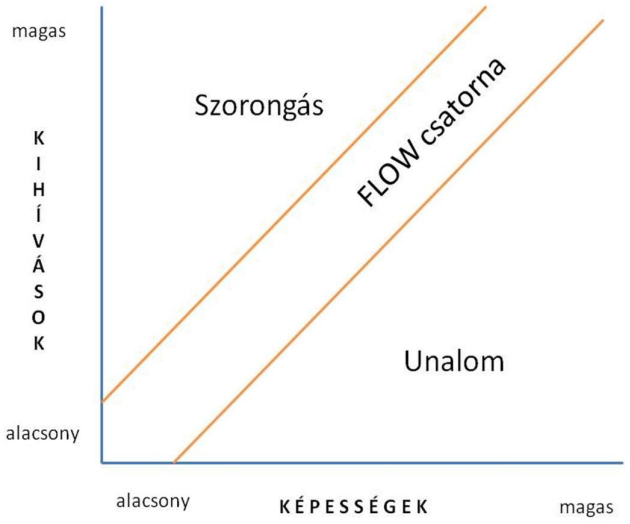
motiváció 3.0-ra építenek, alapozva az emberi igényekre, hogy saját belső motivációjuk alapján végezzék el a feladatiakat. [122] A tevékenységet nem jutalmazzák vagy büntetik, hanem olyan szinten játékosítják, amitől az adott egyén örömmel végzi azt.

Pink a motiváció 3.0-ban kétfajta embertípust különböztet meg, az:

X-típus: a jutalmazó/bűntető rendszerben gondolkodó embertípust, valamint az

I-típus: aki arra a belső igényre épít, hogy a saját életét maga irányítsa (1), új dolgokat hozzon létre (2), valamint környezetét jobbá tegye (3). [122]

A játékosítás alapja pedig a flow, akkor működik jól egy adott tevékenység, ha a belső motiváció erős, szeretjük azt, amit csinálunk, a nehézségek és a készségek megfelelő arányban vannak, tehát nem érezzük az adott feladatot sem túl könnyűnek (unalom), sem túl nehéznek (szorongás). [119], [123], [124]



25.ábra: A Flow csatornája [120] [121] alapján

A gamification (későbbiekben játékosítás) a századfordulót követően, a 2010 évektől használt fogalom. Azoknak a technikáknak, azoknak az elemeknek, amik a játékban is megtalálhatók, az átültetése egy olyan környezetbe, ami már nem játék. Célja, hogy a játék által formálja a játékost, tanítsa, vezesse, szórakoztassa vagy elkötelezetté tegye. A korábbi kutatások eredményeit felhasználva életünk több területén is találkozunk a játékosítással. Először a marketing, a foglalkoztatás-munkahely, az egészségügy, és az oktatás területén alkalmazták a játékosítást. [125] [126] Ahhoz, hogy a játék sikeres

legyen, fontos megtartani a flow élményét a játékosban, a játékos fejlődéséhez szükséges egy minimális stressz szint, amivel a fejlődése biztosítható. [127] [128]

A játékot abbahagyók között megfigyelhető, hogy egy idő után a játékot vagy unalmasnak, vagy pedig nehéznek tartották – tehát kimozdultak az egyensúlyt jelentő flow csatornából. A játék képes megmozgatni azt a résztvevőt is, aki korábban passzív volt. Játékosító módszerek használatával megfigyelhető, hogy ezek a résztvevők kinyílnak, motiváltak, csapatjátékosok, kreatívak, akár irányítók lesznek a játék során. [129] [130] A játékosítás segítségével képesek a saját határaikat átlépni, a tudásukat jobban kihasználni, a játék kedvéért magasabb szinten teljesíteni. [131]

A „mintha" élményen keresztül a játékosnak tudnia kell a játékban megtapasztalt helyzeteket a valóságba átültetni. Fel kell ismernie, hogy a játék nem valóság, ugyanakkor a játékban lévő karaktere által újabb és jobb készségekre tehet szert, mint ahogyan azt Vygotsky a gyermekek játékánál is megfigyelte. [115] [116], [117]

4.2.1 A játékosítás közege

A játékosítás úgy alakult ki, hogy abszolút az Internethez kötődik, és fő célcsoportja a netgeneráció. A netgenerációba tartozó y-ok, z-k és alfák már ösztönösen használják az infokommunikációs eszközöket, sem internet, sem pedig áram nélkül hosszútávon nem éreznék jól magukat.

Manapság a 2 és 40 év közöttiek nagy része tölti szabadidejét a virtuális térben – videojátékkal. Az amerikai Carnegie Hall Melon University kutatása alapján [132] egy mai gyerek 21 éves korára 10 000 órát tölt a virtuális térben játékkal. Ez egy annyira ijesztően magas szám, ami különös módon megegyezik azzal az idővel, amit ugyanez a gyerek az iskolában tölt el 10 és 18 éves kora között, ha minden órán részt vesz, és egyszer sem hiányzik. De a kutatás kiterjed arra is, hogy amennyiben 10 000 órát szánunk egy valamilyen tudás megszerzésére – pl. zongorázni tanulni -, abban kiemelkedő jártasságra teszünk szert. [133] [134]

A kutatás üzenete, hogy szeretünk videojátékkal játszani, és hajlandóak vagyunk az időnket online játékkal tölteni. Olyannyira szeretjük ezt a tevékenységet, hogy feláldozunk érte egy magas szintű tudás megszerzésére szánt időt is, csak azért, hogy szabadidőnkben videojátékkal játszhassunk. De valóban csak játszunk ezalatt az idő alatt?

Valóban nem ad semmilyen képességet, jártasságot a videojáték? És ha ezek a fiatalok mégiscsak megszereznek valamilyen tudást ezalatt a 10 000 óra alatt, akkor mi az a tudás és mire készíti fel őket? Fel tudjuk-e használni ezt a fajta elkötelezettséget arra, hogy a játék során valamilyen „hasznos", fontos ismeretet adjunk át a számukra, vagy egy jelenleg megoldatlan probléma megoldásába vonjuk be őket?

A válasz sokkal összetettebb, mint első ránézésre tűnik. Összegyűjtöttem olyan okokat, ami a videojátékokat sokkal szerethetőbbé teszi a játékosok számára, akár a valós életben való valós problémákban, helyzetekben való részvételnél is:

- Epikus küldetéssel rendelkezik
- Virtuális hős élményt ad
- Képességeknek megfelelő játékszinteken egyedi feladatokat ad – a kiválóság, egyediség érzetét keltve
- Konkrét és teljesíthető feladatokat nyújt a játék során
- Közösségi élményt ad
- Pozitív visszacsatolást ígér és nyújt

Nick Yee játékkutató állítása alapján a játékosok a játék során elemi motívumokat elégítenek ki. Ezek a motívumok a kíváncsiság (exploráció), a társas szociális dimenzió (interakcióba léphessen másokkal), kompetitív versengő motívum (össze tudjam hasonlítani magam másokkal). Yee fogalmazta meg, hogy a teljesítmény, a kapcsolat és az elmerülés a felfedezés motívumrendszere a legfontosabb a játék során. [135]

De a legnagyobb probléma manapság az, hogy a szórakoztató játékok, mint például a World of Warcraft vagy a Call of Duty a szórakoztatóipar termékei, és nem az oktatási piacon résztvevő fejlesztőcégek produktuma. Ez leginkább ott mutatkozik problémaként, hogy az oktatásra szánt játékok nem tudnak olyan grafikai minőséggel, sztorival, karakterkészlettel, összetettséggel megjelenni, ami a játékos számára szórakoztató, vagy legalábbis vonzó lenne. Daphne Bavelier agykutató szerint az oktató játék olyan, mint a brokkoli, míg a szórakoztató játék egy tábla csokoládéval szimbolizálható. A brokkoliról mindenki tudja, hogy egészséges, mégsem lehet annyira vonzó, mint egy tábla csokoládé. Tehát valahogyan e kettőt össze kell tudnunk tenni, de a csokoládés brokkoli még borzasztóbb valaminek hangzik, mint külön-külön a két dolog. [136] [137]

4.2.2 A játékos ember - A „Homo ludens”

A Homo Ludens kifejezést először Huizinga használta 1944-ben. Egyik meghatározó kijelentése, miszerint a „kultúra a játékban bontakozik ki”, mutatja, hogy már a múlt században megkezdődött a játék tevékenységének vizsgálata. [138]

A játékban résztvevők a belső motiváció miatt maradnak játékban. Általában, aki játszik, az a játékban kötelező tanulást nem érzi tanulásnak, hasonlóképpen a gamification-típusú munkavégzéshez, ahol az egyének a munkát játékként élik meg („a munkát nem érzem munkának”). Ezen egyének a hétköznapi élet kihívásait, problémáit is másként élik meg az átlaghoz képest, és azt mondják, hogy a probléma nem más, mint egy kihívás („a problémát nem érzem problémának”). [139] [140]

A játék használata során a játékos több és eltérő minőségű információt ad magáról, mint egy hagyományos, a büntető/jutalmazó oktatási rendszer esetében. Ezen információk összegyűjtésével és elemzésével az egyén pontosabban leírható, a későbbiekben pedig könnyebben ösztönözhető. Egy játékos megfigyelésével és a játékban lévő viselkedésének elemzésével egy következő játék testreszabása, kialakítása egyszerűbb feladat, hiszen ismertek a játékos igényei – flow csatornájának paraméterei.

A mai kor emberének a játék nem szükséges a megélhetéséhez, mégis az tapasztalható, hogy bármely területre behozott játékosító eszközök nagyobb hatással bírnak bármilyen más ösztönzést használó programoknál. Jane McGonigal szerint „a mai társadalomban a számítógépes és videojátékok olyan igazi emberi igényeket elégítenek ki, amelyeket a való világ jelenleg képtelen kielégíteni. A játékok olyan jutalmakkal szolgálnak, amelyekkel a valóság nem. Úgy tanítanak, inspirálnak és kötnek le, ahogy a valóság nem. Úgy összehoznak bennünket egymással, ahogy a valóság nem. A valóság elromlott, és ezért el kell kezdenünk olyan játékokat készíteni, amelyek helyrehozzák.” [134]. Talán McGonigal erősen fogalmaz. A tapasztalatok sajnos őt igazolják. Az új generáció – aki hozzájut az online és virtuális játékokhoz – arról számol be, hogy napjainak szerves része a játék. [134] [141] A napi tevékenységének része lett úgy, mint az étkezés, a munka vagy tanulás vagy éppen az alvás. Egy olyan tevékenységről beszélünk, amivel eltöltött idő számottevő, és amit közösségi szinten használhatunk a jövőben valami jobbra, egy közös cél elérése érdekében. [142]

Több példával találkozunk, amikor a videojátékban megszerzett tapasztalat a valós életben is használható tudást eredményez. [143] Az első ilyen példa a 12 éves norvég

kisfiú, aki az erdőben sétálva a húgával egy jávorszarvassal találkozott. A World of Warcraft játékban tanultakkal elcsalta az állatot, hogy a húga elszaladhasson, majd lefeküdt a földre és halottnak tettette magát. Így mentette meg mindkettejüket. [144], [145]

A másik, sokat hivatkozott példa a videojátékok gyakorlati haszna mellett a 29 éves Paxton Galvanek, aki erős játékszenvedélyével hatalmas gyakorlatra tett szert az "America's Army" játékban eltöltött idő alatt. Egy füstölő autóból mentett ki két embert és részesítette őket elsősegélybe, pontosan úgy, ahogyan azt a virtuális térben többször megtette korábban. [146]

4.2.3 A játékosító

„Lassan minden intézménynek szembe kell néznie azzal a ténnyel, hogy ezekben az években, évtizedekben olyan (Y és Z) generációk nőnek fel, amelyeknek a korábbi nemzedékektől gyökeresen eltérő szemléletük, attitűdjük és életmódjuk van. Minden eddigi intézményesített működési rendet (különösen az oktatás és a foglalkoztatás területén) a Motiváció 3.0 jegyében gyökeresen át kell alakítani, ha azt akarjuk, hogy azok életképesek maradjanak. Meg kell értenünk a netgeneráció új nyelvezetét, kommunikációs és motivációs struktúráját, és ennek megfelelő módon formálni újra a társadalmi intézmények működési mechanizmusait." [120] Fromann Richárd szociológus elmélete alapján a világ abba az irányba halad, amikor az intézményeknek kell az új generáció tulajdonságaihoz alkalmazkodni. Már nem igényekről vagy elvárásokról beszélünk, hanem arról, hogy mit ért meg, min keresztül kommunikál az új nemzedék – és hogyan kell megszólítanunk, amennyiben bevonni, partnerként kezelni akarjuk őket. [143]

Nemcsak a motivációs struktúra változott meg, hanem magának az információ befogadásának és közlésének, illetve a figyelemnek a kultúrája is. Napjainkban a multitasking típusú figyelemmegosztás nem ritka, ma már egyszerre több tevékenységet is végzünk egyazon idő alatt, hasonló intenzitással. Mindemellett az „információ-befogadási tartomány" is rövidebb lett, számos kutatás bizonyítja, hogy a netgenerációs személy legfeljebb 7 percig képes tartósan figyelni egy adott dologra. Ha ezalatt az idő alatt nem történik valami olyan, ami számára érdekes, egyszerűen tovább lép [147]. Az új generáció tagjait szinte csak a gyors, impulzív, élményalapú információ érdekli. Ezzel

párhuzamosan megváltoztak a kommunikációs szokások és megváltozott a kapcsolattartás módja is.

4.2.4 Mitől működik jól egy játékosított folyamat

A játékosítást befolyásoló első dimenzió a Flow jelenség [119]. Egy játék akkor lesz vonzó, vagy adott esetben addiktív, ha pontosan a játékos képességeihez igazodva, a flow csatorna ideális sávját biztosítja számára. Tehát a kihívás és a játékos képességei között helyezkedik el. Amikor a játékos számára nem az a fontos, hogy miben fejlődik, hanem az, hogy ott van. Részt vesz a folyamatban, játszik.

Második dimenziója a tanulási görbe, a „Learning Curve" alapján épül fel, tehát egy könnyű belépési szinttel kezdve fokozatosan, a játékos képességeihez mérten halad előre, új kihívások elé állítva a résztvevőt. [148] [149] [150]

Harmadik összetevője pedig a célok. A nagy célok és a kis célok elérése. Szükséges a játékosítás során a történet, mint nagy cél, a játék mögött kell lennie egy olyan történetnek, ami a játékost magával ragadja. Minden ember szereti magát beleképzelni helyzetekbe, egy történet szereplőjének a bőrébe bújni, ennél magasabb szinten egy történetnek aktív részese lenni. A történetnek van egy vége, van egy végcélja. A játékban egy közös cél van, minden játékos ismeri a szerepét, és annak megfelelően viselkedik a játékban, hogy együtt ezt a közös célt elérhessék. Szükség van azonban kis célokra is, ami az egyén saját célja vagy céljai a játék során. Ezeket a részcélokat eléri, és fontos, hogy ezáltal visszacsatolást kap, megerősítést nyer, hogy a részcélokat képes volt teljesíteni. Ez adja meg a játék jelenitását, ezt most azonnal kapja, és azt jelenti, hogy jó úton jár, közeledik a közös cél eléréséhez. A kis célok elérése adja a játékos számára a „meg tudom oldani ezt a problémát" érzést, amivel egy bizalmi együttműködés alakul ki a játék készítője és a játékos között. [151] Ez a bizalmi kötelék is segíti a játékost abban, hogy egyre inkább elköteleződjön a játék iránt. [152], [153], [154]

A célok eléréséhez szükséges a játékost jutalmazni, tehát a korábbi motivációs eszközt használja a játék is. A játékosítás során a jutalmazás azonnali, igazságos, minden esetben megtörténik, minden esetben pozitív. Elemei lehetnek pontok, szintek, ranglisták vagy virtuális javak. [120]

4.2.5 A játékosítás legfőbb eleme, az elköteleződés kialakítása

A játékosítás a legegyenesebb, legrövidebb út a felhasználó felé. A játékosítás során a játékos a játékkal folyamatos interakcióban van. A játékos határozza meg a játék

tempóját, irányát és végeredményét. A játék személyre szóló élményt ad, motivál és elkötelezetté tesz. A játékosítás további célja pedig egyéb, kívánt ismeretek fejlesztése.

A játékosítás egy lehetséges út a felhasználóhoz, ami képes érzelmeket, reakciókat kiváltani a résztvevőkből. Ez csak abban az esetben lehetséges, ha az adott játék képes elvarázsolni, képes az alábbi érzelmeket előcsalni a játékosból:

- Vágy
- Motiváció
- Feladattudatosság
- Kihívás
- Megfelelés
- Díj elérése
- Visszajelzés
- Kiválóság érzése

Amennyiben a játékos motivált abban, hogy a fentiek bármelyikére szert tegyen, és a játék elég vonzó ahhoz, hogy az érzelem/tulajdonság megszerzéséért és fenntartásáért konkrét áldozatot hozzon, a játékost elkötelezetté lehet tenni.

4.2.6 A játékosítás gyakorlati haszna az oktatás során

A játék önmagában nem megoldás a tudásátadásra. Azzal, ha játékot alkalmazunk, még nem biztosítjuk a megfelelő tudás birtoklását. A játéknak helye és szerepe kell, hogy legyen a tanulási/tanítási folyamatban, a megfelelő előkészítéssel, felvezetéssel, és a játékot követő visszajelzésekkel, megbeszéléssel. Amennyiben nem sikerül a játékot jól alkalmazni, a tudásátadás sem lehet sikeres.

A gyermek az első hat évében a játékon keresztül tanul. A játék az első módszer, amin keresztül új ismereteket sajátít el. Ezért nagyon fontos, hogy a későbbiekben is találkozzon ezzel a tanulási formával. Ma már nemcsak az általános iskolában, hanem a közép- és a felsőoktatásban is megjelenik a játék szerepe.

Ahhoz, hogy a játékosítás elérje a célját, előre meg kell határoznunk azokat a paramétereket, melyek a játékot és ezen keresztül az oktatást befolyásolják. A paraméterek függenek az átadni kívánt tartalomtól, a célcsoporttól, az oktató személyétől. A játék paraméterei az alábbi módon csoportosíthatók:

- lehet csoport– vagy egyéni játék
- a tananyaghoz szorosan kapcsolódó
- a játék tanulsága/élménye/a játék során tapasztaltak köthetők a tananyaghoz
- nemcsak a tananyagról, hanem a játékosról is szól
- általános információkat tartalmaz – a játékos érti és megérti a játékot magát
- képes szintetizálni a meglévő tudást – és képes azt feljebb emelni
- a meglévő tudásra épít
- a meglévő tudást egészíti ki és más megközelítést biztosít
- biztosítja a sikerélményt a játékban aktívan résztvevő számára

A digitálisan alkalmazott játékokkal szemben a korábban felsorolt elvárásokon kívül az alábbi szempontokat [155] kell figyelembe vennünk:

- a digitális játék legyen egyszerűen, könnyen használható, bevezethető
- elérhető legyen mind a tanár mind a diák számára is
- adjon visszajelzést a játékos számára
- legyen szép a dizájn
- használható legyen különböző eszközökön
- mérhetők legyenek az eredményei

A tanulási célokra használt játékok esetében nagyobb a hatékonyság, ha a tanulás közösségben történik. Tehát mindenképpen érdemes körüljárni azt a kérdést, hogyan lehet a felhőbiztonság témáját közösségre ültetve játékosítani, és a közösség erejét és szereplőit felhasználni a játékosítás élményének fokozására. Az alább felsorolt elemek képesek arra, hogy nagyobb élményt, elköteleződést adjanak a játékosított téma iránt:

- Sikerfal / pontszámfal
- Irányíthasson a játékos
- Azonnali visszajelzés küldése vagy fogadása
- Lehetősség a csoportos problémamagoldásra
- Lehetőség a master szint vagy magasabb tudásszintek elérésére

- Kapcsolat más játékosokkal
- Segítség a közösség többi tagjának

Egy kiválasztott csoport esetében az alábbi előnyöket kapjuk oktatóként a játékosítás bevezetésével

- A hallgatók sajátjukként kezelik az adott témát – hiszen a témának részesei
- Lehetőséget ad az egyéni munkára
- El lehet bukni és lehet elölről kezdeni a játékot mindenféle negatív megkülönböztetés nélkül
- Képes mélyebb és szélesebb kapcsolatokat létrehozni a csoporton belül
- Lehetőséget a differenciált oktatásra
- Láthatóvá és követhetővé válik az egyéni fejlődés
- kezelhető a kiadott feladatok és alfeladatok ellenőrzése és megbeszélése
- Hat a tanulók belső motivációjára

A játék mindig idővel jár. Több időt jelent a szabályokat megismerni, a szerepeket kialakítani és magunkra ölteni, a célokat megismerni és sajátunkká tenni. Idő továbbá maga a játék is. Ugyanakkor a játék során megszerzett ismeretek tovább velünk maradnak, és maga az élmény fokozza a megszerzett tudás intenzitását. A befektetett idő megtérül. A játék során azonban minden játékos számára másképpen telik az idő. Képességeihez mérten több vagy kevesebb időt tölthet a játékkal, és eléri ugyanazt a szintet, mint a többiek. A különbség véleményem szerint itt számottevő. Felállítjuk a szinteket, és a játékos számára vonzóvá tesszük azok elérését. A játékos időt fordít arra, hogy a szintet elérje, hiszen akkor van esélye a játékban tovább haladni. Nem kap esélyt arra, hogy alacsonyabb szinttel is beérje, viszont kap rá módot, hogy saját ritmusában, saját idő alatt érhesse el a kitűzött célt. Ebben lényegesen különbözik a játék, mint bármelyik oktatási forma, ahol időre kell teljesíteni, és ezt követően eldől, hogy az adott időkeret mire volt elég.

4.2.7 Sikeres és sikertelen játékosítási megoldások

A játékosítás vizsgálatakor fontos kitekintést tennünk a gyakorlati megvalósítások felé is. A játékosítás nemcsak digitális formában érhetők el és használhatók, ugyanakkor a tesztelésük digitális formában gyorsabb és több felhasználó érhető el így. A vizsgálatot Stempler Balázs a Játékosítás alkalmazása a munkavállalói elismerés és elkötelezettség növelésére c. munkájában összefoglalta, ahol 3 sikeres és 3 sikertelen applikációt

elemzett [156]. Stempler összegzése alapján elmondható, hogy a sikeresnek mondott alkalmazások sikere nem függ az életkortól, sem pedig egy adott társadalmi réteghez, azonban fontos, hogy minden esetben valamilyen hiányt fednek le, és megoldásukkal egyediek a piacon (Tinder, Duolingo, Zombies, Run!).

Érdemesebb azonban megvizsgálni, hogy a sikertelen játékosított alkalmazások esetében mi a sikertelenség oka. Stempler szerint „a játékosítás nem merül ki abban, hogy pontokat, jelvényeket és ranglistákat hozunk létre (ezeket együtt PBL-nek nevezi a szakirodalom az angol *points, badges and leaderboards* rövidítéseként), hanem meg kell érteni, hogy a felhasználó szemszögéből milyen tartalom lenne kívánatos, majd ennek eléréséhez lehet a játékosítás egy eszköz” [156].

A sikertelen megoldások mindegyikére jellemző, hogy azok nem rendszerben gondolkoznak, és nem illeszthetők valós felhasználói igényekhez. Stempler munkája 3 ilyen sikertelen megoldást említ, ezek mellett azonban sok olyan alkalmazás és próbálkozás került parkolópályára a nem megfelelő vagy elhamarkodott kialakítás miatt.

A játékosítás használata vállalati környezetben nem könnyű feladat. A bevezetni kívánt elemnek egyszerre kell vonzónak lennie a felhasználók számára, ugyanakkor a vállalat céljait is szolgálnia kell.

Amennyiben a két cél közül valamelyik nem tud megvalósulni a játékosítás eszközrendszerével, azaz nem lesz élvezetes a felhasználóknak vagy nem szolgálja a vállalati célt, aminek eléréséért a rendszert eleve létrehoztuk, a játékosítás bevezetése nem indokolt.

Fontos megvizsgálni, hogy pontosan ki lesz a célközönség, mert egy munkahelyen belül is lehetnek olyan osztályok vagy részlegek, melyek más eszközökkel motiválhatók. Például az értékesítéssel foglalkozók esetében a kompetitív megoldások nagy valószínűséggel működnek, míg máshol esetleg rontaná a morált, ezért a kollaborációt kell a középpontba helyezni. [157].

A vállalati játékosított rendszerek használatát azonban nem szabad minden résztvevő számára kötelezően előírni, mivel az alapvetően intrinzik érdeklődés helyét az extrinzik munkahelyi elvárás veszi át, ami kontraproduktív [158]. Lehetőséget kell azonban biztosítani arra, hogy a rendszerhez bármikor lehessen csatlakozni, ugyanakkor mindenki számára elérhetővé kell tenni azt.

4.2.8 Tanulás az online környezetben

Bár David Kolb modellje [159] [160] az online tanulás során használható, ugyanakkor itt a hangsúlyok eltolódnak, máshová kerülnek. Ennek legfőbb oka az információ feldolgozásának sorrendje, valamint a tanulásban résztvevő szereplők megváltozott szerepe és kapcsolata. Ugyanaz a téma másképpen dolgozható fel valós környezetben, mint online eszközök segítségével.

Mindazonáltal a tanulótípusok is változnak, míg a valós környezetben hamarabb ér el eredményt és látványosabb eredményt ér el, aki érzelmi vagy fizikai kapcsolatot keres az adott információval, online környezetben a figyelem és a gondolkodás – az előre modellezés képessége kerül előtérbe. Ez nem jelenti azt, hogy a modell bármely része elhanyagolható vagy kivehető lenne, csupán szükséges látni, hogy a tanulási környezet megváltoztatásával változik a tapasztalati tanulás módszertana.

A módszertan mellett, ha az új technológiák oktatását vizsgáljuk, azt tapasztaljuk, hogy a technológiai változásokat az idősebb generáció nem képes a változással azonos ritmusban követni. Ezáltal már nem az idősebb tanítja a fiatalabb generációt, hanem a legtöbb esetben elengedi a kezét, hogy szerezze meg egyedül a virtuális világhoz szükséges tudást. [152] Amennyiben a tudás megszerzése a ’nagy kép’ nélkül, összefüggések nélkül történik, a megszerzett tudásdarabkák egymáshoz nem, vagy csak nagyon nehezen tudnak kapcsolódni. Az online adatokra való rákereséssel töredezett válaszokat fog kapni. Nem lesz rendszer a fejében, nem fogja tudni elhelyezni a kapott választ. Hiányozni fog a módszertan, a logikai felépítettség, és az összefüggésekre való rávezetés is. Rab Árpád szerint a technológiai fejlődés lehagyta az embert, az ember nem képes olyan ütemben követni és megérteni a változásokat, mint amilyen gyorsan találkozunk ez újdonságokkal.

A megváltozott tanulási folyamatot befolyásolja annak a képessége, hogy bátrabban, automatikusan, „ösztönösen” nyúlunk a digitális tér adta tanulási lehetőségekhez. A másik oldalról ez jelentheti azt is, hogy nincs olyan ’guru’ mellettem, aki nagyobb tudással bírna, és tanulhatnék tőle. Tanulunk egymástól, előtérbe kerül az együttműködés, a tudás felszeletelése, ahol már nem fontos, és nem elvárt, hogy a tudással egy személyben rendelkezzünk, hanem sokkal fontosabb lesz, hogy az adott témában annyira legyünk jártasak, hogy megtaláljuk azt az információt, ami az adott helyzethez kellően mély, hiteles, tudományos, tájékoztató vagy éppenséggel szórakoztató.

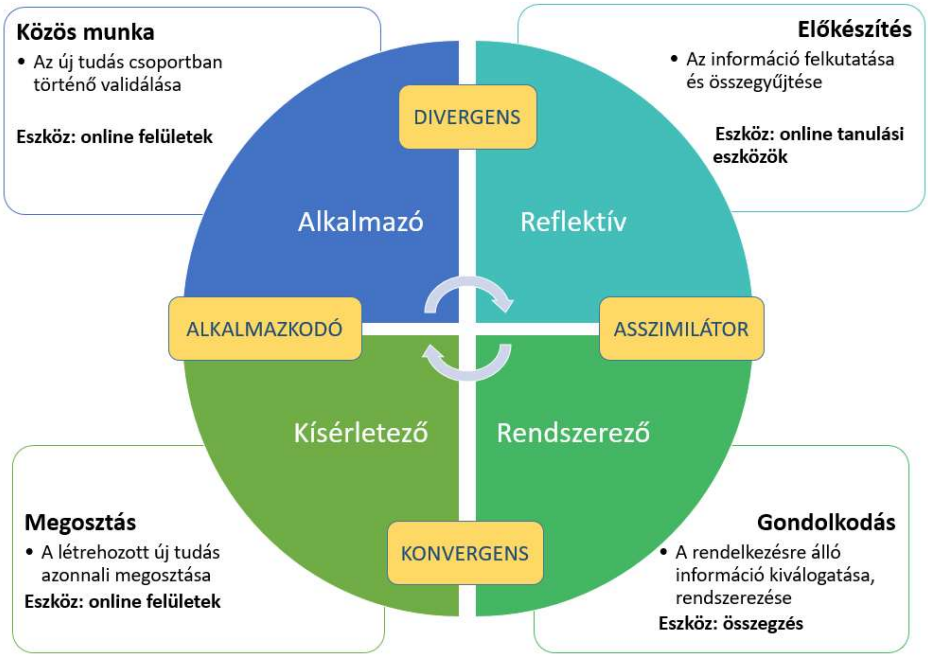
A tanulási folyamat résztvevői a mentor (oktató) és tanuló között hamarabb alakul ki bizalmon alapuló szakmai kapcsolat, mint a valós tanulási környezet esetében. Míg utóbbinál a tanulótársak nagy befolyással vannak az egyéni tanulóra, hatnak a motivációjára, a tananyaghoz fűződő kapcsolatára – mennyire elfogadott csoporton belül egy adott tantárgy kedveltsége – a tananyag számára lényeges információinak szelektálására, addig ez a hatás az online világban csökken – sőt, a tanulócsoportok vagy közösségek kialakulásánál nagy szerepe van annak, hogy hasonló véleménnyel fordulnak az egyes témák felé. Pont ez a hasonlóság az, amit az online világ könnyebben képes kezelni, hiszen eddig nem látott mértékben képes támogatni magát az együttműködési folyamatot. Míg a közös munka, a közös gondolkodás a valós térben sok szervezéssel, erőforrással és idővel jár, addig a virtuális tér azonnal kínálja ezeket a lehetőségeket. A fizikai tér akadályának leküzdésével, ugyanazzal az infrastruktúrával, ami az online tanulás lehetőségét is nyújtja, a virtuális tér kínálja a közös munka, a közös gondolkodás, a közös kutatótevékenység lehetőségét.

A tanító sem a klasszikus értelemben tanít, inkább mentorál, mert belátja, hogy vannak olyan területek a feldogozandó témában, amit a hallgató jobban tud, részletesebben ismer.

Az alábbi ábrán foglaltam össze az online tanulási folyamatot, aminek alapja David Kolb modellje, azonban a modell fázisai más tartalmat kapnak. Így a négy fázis az én elméletem alapján a következő:

1. **Felkészülés:** ami az egyéni felkészülést, az önálló ismeretszerzést takarja. Ennek a folyamati lépésnek része lehet a mentor vagy oktató is, ebben a pontban azonban a legfontosabb, hogy a tanuló képes legyen önállóan megszerezni az információt.
2. **Tudás feldolgozása, elhelyezése:** ez az a fázis, ahol a tanulónak illesztenie kell a megszerzett tudását a meglévőhöz, itt tud új gondolatot hozzáadni, és meg kell tudnia fogalmazni a megszerzett tudás rá gyakorolt hatását.
3. **Megosztás:** az online világban a fent említett okok miatt az általam „bélyegzett” megszerzett tudás hasonló gondolkodókkal való megosztása belső igénnyé válik, ezért fontos, hogy valamilyen módon azt a közösség kollektív tudásának részévé ajánlja fel a tanuló.

4. **A közös munka:** a közösség számára felajánlott egyéni tudások összegzésével, a csoport közös tudásra tehet szert. A tudásszeleteket együtt összeilleszthetik és felhasználhatják.



26.ábra: Tanulás az online térben, saját szerkesztésű ábra David Kolb modelljét újragondolva

4.2.9 Motiváció, jelenlét, interaktivitás az online tanulási folyamatban

Mind a motiváció, a jelenlét, az interaktivitás meglévő fogalmak, és ismert, vizsgált, megfigyelt jelenségek a klasszikus tanulás során. Az online világ azonban ezen fogalmaknak hozott más vagy többlet jelentést, és mind a három területen ezzel párhuzamosan az online világ nagyon sokat fejlődött a kezdetekhez képest. Ma már az online térben folyamatosan „jelen lenni” nem okoz problémát, és nem köt fizikailag egy zárt szobához, ahol a szükséges internetkapcsolat rendelkezésre áll. Nem jelent gondot az interaktivitás kialakítása sem – hiszen a birtokunkban lévő eszközökkel bármikor és bárhol könnyedén, minimális időráfordítással és minimális költségért részt vehetünk az általunk választott virtuális tér bármely területén. Tehát a fenti fogalmak mind meglévők, de az online térben eltérő jelentéstartalommal bírnak. Más a működési mechanizmusuk, mást váltanak ki a résztvevőből – és sok esetben más eszközökkel válthatók ki ezek a reakciók.

4.2.10 Motiváció a tanulás során

Oktatóként mindig érdekes kérdés, mi az az ok, ami a tanulót tanulásra ösztönzi. Az egyéni motiváció egy olyan csoda, aminek hatására az egyén fáradságot, időt és energiát fordít egy adott ismeret megszerzésére. A belső motiváció az, ami átsegíti őt a holtpontokon, ami az utolsó hajrához is erőt ad számára.

Minden egyén más motivációs szinttel érkezik, és eltérőek azok az okok, amiért ott van. Ma a játéktervezések során nagyobb hangsúlyt fektetnek a pszichológiai tervezésre, mint a grafikai kivitelezésre -– amivel éppen a motivációs szint megfelelő beállításán dolgoznak. Ahhoz, hogy a játék letehetetlen legyen, meg kell találni azt a flow csatornát, amiben az egyén a játék során van, és ami miatt veszteséget jelent számára a játékot megszakítani.

A motivációs szint ösztönzi az egyént a gyorsabb, a látványosabb, vagy magasabb szintek elérésére. A különböző megküzdési stratégiák pontos elemzése teszi lehetővé, hogy a játékosról a lehető legtöbb információ segítségével pontosabb és testreszabottabb játékkörnyezetet teremthessünk. Sokkal több energiát fordít a fejlesztő cég a felhasználó pontosabb és testreszabottabb szórakoztatására, mint bármely oktató a tanulóira. Ha csak annyi elemezhető adatunk lenne egy-egy tanuló tanulási szokásairól, mint játékos szokásairól, egy eredményesebb és testreszabottabb tanulási környezetet hozhatnánk létre, ami sikert hozna számára és oktatója számára is. Ezáltal a motivációja is magasabb szintre emelhetővé válna.

4.2.11 Jelenlét a játékosított oktatás során

A klasszikus oktatási formában a jelenlét szerepe nem kérdés. Az online tanulás során azonban ez az egyik legfontosabb tényező. A jelenlét segítségével alakítható ki szoros kapcsolat oktató és tanuló, vagy tanuló és tanulócsoport között. Az offline – tehát időben elcsúsztatott kérdés-válasz – kapcsolattartás befolyásolja a tanulónak az ismeretanyaghoz fűződő viszonyát és motivációs szintjét is. Amennyiben ezt a jelenlétet online módon vagyunk képesek kezelni, a feltett kérdésre a válasz is azonnal megérkezik, egy-egy adott probléma azonnal kezelhető.

Technikai oldalról a jelenlét megoldása ma sokkal egyszerűbb és változatosabb, mint akár 4-5 évvel korábban. Az internetelérés és a mobileszközök illetve felhőtechnológiák használatával képesek vagyunk olyan infrastruktúrát nyújtani, ahol a tanulási folyamat szereplői folyamatosan jelen tudnak lenni.

4.2.12 Interaktivitás

A folyamatos jelenlét biztosítása lehetőséget add az interaktivitásra is. A gyors kérdés és válasz önmagában hordozza az interaktivitás megszületését, és egy közvetlenebb kapcsolatot alakít ki.

A klasszikus tanulási formában is sokat változott az interaktivitás helye és szerepe, de az online kommunikáció alkalmazásával a klasszikus tanulási folyamatban résztvevők kapcsolatára is nagy hatással volt az online csatornák megnyitása. Gondoljunk csak egy bármilyen szinten lévő oktatási formára, ahol az oktató és diák a személyes környezeten kívül is képes egymással kommunikálni, E-mail, videochat vagy blog segítségével. Ez a kommunikáció információval egészíti ki az ismeretanyagon kívül a kapcsolatot is, ami ezáltal szorosabbá és mélyebbé válik.

4.3 A felhasználói oktatás a felhő alapjairól, technológiájáról, biztonságáról, szolgáltatási elemeiről

4.3.1 Hogyan tanítsuk a felhőbiztonságot

Mindenekelőtt nagyon fontosnak tartom a felhőbiztonság tudatosítását, népszerűsítését. Nem egyszer találkozom olyan felhasználóval, aki gondolkodás – olvasás - nélkül fogad el olyan adatkezelési nyilatkozatot, ami az adataira és azokon keresztül a személyére nézve veszélyes is lehet. Tehát foglalkoznunk kell ezzel a kérdéssel – és a fent említett célcsoportok körében népszerűsíteni kell az informatikai biztonsággal foglalkozó kérdések megvitatását. Sajnos a biztonsági kérdések ma már sürgősen kezelendő problémákat jelentenek, a kibertérben való lét fenyegetettségét sokszor nem vesszük komolyan.

Gyakorlatilag az informatika mára nem egy vállalati üzletág, hanem egy olyan bázis, egy olyan vállalati alapszolgáltatás, ami nélkül szinte majdnem minden más üzletág lebénul vagy megáll. Nehezen tudunk olyan munkakört, tevékenységet vagy ágazatot említeni, ami informatika nélkül is zökkenőmentesen, fennakadás nélkül képes működni. Az IT szolgáltatások ma már minden területen alapszolgáltatásként jelennek meg – kiszolgálva ezzel a vállalat akár fő tevékenységét is, aminek sikere az informatika folyamatos elérésén múlik.

Ugyanakkor az informatika új oktatási módszereket is hozott, az elektronikus oktatási formák, az online kurzusok vagy webinárok megjelenésével. A felhő használatával még előnyösebb megoldásokkal találkozhatunk – aminek segítségével egy hallgató akár egy

másik ország egyetemének hallgatójává is válhat – egy egyszerű informatikai kommunikációs eszköz használatával. [161], [162], [163] Ezáltal eltűnnek a fizikai határok, mobilabbá, függetlenebbé válik a felhasználó – aminek előnyeit rendkívül hamar felismeri.

A tudatos viselkedést a kibertérben megelőzi az ehhez szükséges információk megszerzése. Amennyiben a tudás megalapozott, lehet beszélnünk viselkedésmintákról.

A tudatos viselkedés alapja lehet:

1. Mit gondolunk a biztonságról
2. Mennyi ismeretünk van róla
3. Hogyan alkalmazzuk a kollektív ismereteket
4. Milyenek a környezeti tapasztalataink, milyen a csoportnyomás

Ezt követően lehet a fejlesztésre helyezni a hangsúlyt, ahol az alábbi módszereket vizsgáltam, és próbáltam ki:

1. Elektronikus tananyag: tények, tapasztalatok megosztásával
2. Személyes oktatás: egyedileg vagy csoportosan, testreszabottan, példákkal illusztrálva, de még mindig a tényekre alapozva
3. A hallgatók bevonásával elérni azt, hogy zsigerileg fókuszáljon a tudatosítás során, elkötelezetté tenni akármilyen eszközzel

Az esettanulmányom során ez utóbbi módszert próbáltam ki a gamification elemeinek segítségével.

4.3.2 Esettanulmány

A felhő biztonságának és használatának oktatását 2014 márciusában kezdtem meg 58 vállalati munkatárs képzésével egy hazai, multinacionális nagyvállalatnál. Az én feladatom volt a csapat minden tagját felkészíteni, a munkájuk elvégzéséhez szükséges IT alapok, felhő, IT biztonság és sales alapismereteket átadni. A feladatnak szintén része volt az oktatási stratégia és a tananyagok elkészítése, folyamatos karbantartása, valamint a tesztkörnyezet berendezése és testreszabása.

A projekt során döbbentem rá arra, hogy nemcsak a résztvevők motiváltsága alacsony, hanem a digitális adatvédelmi tudatosságuk is, a felhasználói szokáskultúrájuknak nem

része a privát adatok védelme, a digitális lábnyomuk minimalizálása. A résztvevőknek azonban fontos, hogy az ügyfeleikkel történő találkozások esetében hozzáértést, magabiztosságot és a témában való jártasságot sugározzanak, ezért már a projekt futása alatt egészítettem ki a képzéssorozatot az ezeket a készségeket erősítő tréningekkel. Magabiztosságukat a témában való ismereteik megszerzése adta, ahol nagyon fontos szempont volt számukra a közérthetőség, és az információk tovább adhatóságának lehetősége.

Mindazonáltal a projekt erős fókuszt kapott a vállalat életében is, a stratégiában való megjelenése mellett a vállalat vezetése komoly üzleti eredményeket várt el a projektben résztvevőktől. Ezért a projekt során nőtt az erőforrások száma, anyagi támogatást, motiváló eszközöket, időt és humán erőforrást is kaptunk. Bár a szervezeti folyamatok és a felelősségi körök változása időnként megakasztotta a résztvevők hozzáállását, sikerült a téma fontosságát figyelembe véve a kijelölt tanulási úton maradnunk.

4.3.3 A kezdeti feltételek

A projekt célja a termék oktatása és a termékhez kapcsolódó tágabb technológia ismertetése volt. A projektnek a kezdetekben nem volt része az értékesítési készségek fejlesztése és az információbiztonsági ismeretek átadása.

Mivel a képzés témája nagyobb részben technológiai, ezért indulásnál nem gondoltam arra, hogy élmény-elemekkel egészítsem ki a jóváhagyott tematikát. Úgy gondoltam, hogy a menedzsment támogatását élvezem, a képzés a vállalat stratégiájába illeszkedik, így a résztvevők elköteleződését nem nekem kell kialakítanom, hiszen mindenki látja, hogy a vállalat ebbe az irányba halad.

Az első képzési napokat követően döbbentem rá arra, hogy mind a termék, mind a technológiai háttér idegen a résztvevők számára, mint ahogyan a kijelölt stratégiai irány sem érthető számukra. A nemzetközi trendek, a felhőszolgáltatók gombamód terjedése, az eszközökön elérhető szolgáltatások száma sem volt meggyőző minden résztvevőnek, ezért olyan eszközt kellett találnom, ami az alaphozzáállásukat képes formálni. Bár a csoport tagjainak érdekében állt a felhőszolgáltatást megismerni, hiszen a termék értékesítésével bónuszhoz, magasabb fizetéshez juthatott, mégis többen választották az elkerülő utat a képzés kezdetekor. A külső motivációs eszközök biztosítása nem volt elég minden résztvevő megnyerésére.

A játékosítás elemeit azért kezdtem alkalmazni, hogy a minden héten egyszer látott résztvevő a következő héten is tiszteletét tegye a képzésen. Nem használhattam, és nem is akartam kényszerítő eszközöket alkalmazni, a muszáj részvételben nem hiszek és nem tartom eredményesnek. Fontos volt, hogy a hozzáállásán változtassak, a lehető legrövidebb idő alatt, sokszor csak egy alkalmat kaptam tőlük, hogy megnyerjem őket a projekt számára. Így, a kezdeti feltételek és a célcsoport megismerését követően azonnal be kellett vetnem olyan eszközöket, melyekkel az elköteleződése nagy mértékben nő, és a belső motivációját is erősítem abban, hogy az általa tanultak az élet más területén is hasznosak lesznek számára.

4.3.4 A tesztkörnyezet

A tesztkörnyezetet egy vezető informatikai vállalat bocsátotta a rendelkezésünkre. A tesztkörnyezeten belül saját játszótér (tanulói környezet) kialakítására kaptunk lehetőséget. A tesztkörnyezet használata fontos része volt a tanulási folyamatnak, a projektben résztvevők megismerték a rendszert, és megtanulták a termék használatát és ezen keresztül az értékesítését. A termék lehetőséget biztosít arra, hogy a résztvevők saját dokumentumokat, weblapokat, appokat használjanak vagy hozzanak létre a felületen. A tesztkörnyezet a valódi környezet frissítéseit is követi, tehát lehetőség van az újdonságok elérésére és kipróbálására. A környezet nemcsak a munka során, hanem a magánéletben is használható, amennyiben a résztvevő kíváncsiságát sikerül felkelteni. A környezet alapos megismeréséhez folyamatosan friss és bőséges irodalom áll rendelkezésre online módon, ezen felül több, használatot segítő videó és esettanulmány is elérhető az ingyenes oldalakon.

A csoportok tagjait különböző jogosultságokkal, feladatokkal láttam el, ahol az egyéni motivációt is figyelembe véve a csoport minden egyes tagja számot adott a megszerzett tudásáról, írásban és szóban is. A csoportok tagjai a tesztkörnyezetet úgy használhatták, mint valódi környezetet, magán célra szintén kipróbálhatták a termék akár minden elemét és funkcióját. A tesztkörnyezet nemcsak az oktatások alatt, hanem azon kívül is, nemcsak a vállalaton belül, hanem bárhonnan, bármilyen eszközről elérhető volt számukra.

A tesztkörnyezet alkalmas volt az ügyféldemók lebonyolítására is, segítette a résztvevő felkészülését a tárgyalásra, amivel a tárgyalás során előnyösebb helyzetbe kerülhetett. A felkészülés során az ügyfelére szabott környezetet alakíthatott ki, ami illeszkedik

ügyfelének jelenlegi helyzetéhez, és feltételezett informatikai nehézségére adhatott megoldást.

4.3.5 Az oktatás menete

Az oktatás során az 58 résztvevőt hat csoportra osztottam. A hat csoport egymást követve, időben eltolva vett részt a képzéseken. A képzés során személyes és online oktatási módszert használtam. A tréningekre heti két alkalommal, egyenként 1,5 órában került sor, 6 hónapon keresztül egy csoport számára.

Fontos szempont volt, hogy megismerjék a felhőtechnológia alapjait, azon felül pedig biztonságosan használják a tesztrendszer különböző funkcióit. A tesztrendszer funkciói a vállalati alkalmazásaiknak megfeleltethetők, ugyanakkor a tesztrendszert vállalaton belül, üzleti célra soha nem használták, annak funkciói nem kapcsolódtak sem a mindennapi munkájukhoz, sem pedig a vállalat bármelyik belső informatikai rendszeréhez.

A céges környezet és a tesztrendszer elemeinek egymással való megfeleltetése után az egyes funkciók értelmet és továbblépési lehetőséget nyújtottak. Egy-egy olyan probléma esetén, amire a céges környezet nem képes, az új rendszerben viszonylag könnyen – tehát meglévő tudásukat felhasználva megoldást találtak. Az egyetlen problémát az okozta, hogy a kétféle környezet közötti átjárás nem volt megoldott, tehát csak kezdetleges és nem automatizálható módszerekkel vihető át a kész munka (pl. E-mailben átküldve, vagy képernyőmentéssel, vagy lokális helyre rögzítve).

Mivel a képzés gyakorlat orientált és főként a fenti célok megvalósítását szolgálja (tudás megszerzése, magán IT biztonság kialakítása, jártasság az adott témában), azokat a résztvevőket sikerült elkötelezetté tenni, ahol a képzési célok és a saját célok között volt átfedés.

4.3.6 Információk a képzésen résztvevőkről

Kutatásomban 58 fő vett részt, akik a projekt ideje alatt különböző aktivitással használták a rendelkezésünkre álló tesztrendszert.

- felnőtt csoport 25-45 éves korig
- férfiak nők vegyesen
- telco és informatikai területről érkeznek
- korszerű, vezető informatikai rendszereket használnak

- a legújabb mobiltechnológia tesztelői
- csúcskategóriás informatikai eszközöket használnak
- mobileszközükön korlátlan adatforgalommal rendelkeznek
- az ország minden területéről érkeznek

A kezdeti információk alapján elvárhatnánk, hogy a csoport tagjainak hozzáállása minden esetben pozitív, és a terméket aktívan, egyedül is képes használni. Az oktatások során szerzett tapasztalat azonban nagyon eltérő motivációs szinteket mutatott, aminek okai az egységesített képzési csatorna a résztvevők számára, valamint az értékesítés bónuszrendszerének nem megfelelő kialakítása.

Az oktatások megkezdése előtt szintén elvártam, hogy a résztvevők rendelkeznek egy alapfokú informatikai biztonsági tudással, a saját eszközeiket fegyelmezetten, a vállalati policy—nak megfelelően használják, a magán és a vállalati felhasználást nem keverik. Megfelelő jelszavakat használnak és az üzleti alkalmazás tekintetében is ügyelnek arra, hogy az információ és adat sértetlen és megbízható maradjon. Azonban azt tapasztaltam, hogy a felhasználó csak azokat a szabályokat tartja be, amit a vállalat kikényszerít – tehát nincs módja másképpen cselekedni. Ahol lehetősége van másképpen dönteni, ott nem fordít több időt a biztonságosabb használatra, amennyiben az bonyolultabbnak tűnik. Pl. egy jelszóbeállításnál a rendszer nem követelte meg, hogy a 3 havonta megújítandó jelszavak között nem lehet karakteregyezés, tehát a felhasználók nagy része a jelszóban található számot eggyel növelve hozta létre az új jelszavát. Ez akkor derült ki, amikor többen panaszkodtak az új policy (nem lehet karakteregyezés a régi és az új jelszó között) bevezetését követően.

4.3.7 Felhasználói oktatások bemutatása

Az oktatások megszervezése és lebonyolítása, a tananyag, és a mérési rendszer kialakítása is az én feladatom volt. Mivel a felhasználók nem rendelkeztek stabil, nagyon hasonló IT tudással, a tesztkörnyezet funkcionalitását megelőzően a felhőtechnológia kapcsolódási területeinek és előzményeinek bemutatásával kezdtem a csoportokkal foglalkozni. Ezeken az alkalmakon derült ki, hogy a biztonságtudatosság nem kap fókuszt a mindennapi munkájuk során, a vállalat a kötelező IT biztonsági képzésen kívül (e-learninges tananyag, online vizsgával) nem fordít kellő figyelmet arra, hogy munkavállalóik tudatosan vigyázzanak a náluk lévő vállalati eszközökre (okostelefon, laptop, tablet), valamint az azokon tárolt vagy megjelenített adatokra. A felhőtechnológia

mellett a termék összetevőinek gyakorlati oktatása és használata, valamint a termékhez tartozó, a termék értékesítését támogató ismeretek is az oktatás célját képezték. Ennek megfelelően mind a 6 csoport az alábbi témaköröket sajátította el:

Alapképzés	**Termékképzés**	**Értékesítést támogató ismeretek**
IT alapok	O365 funkcionalitás	Benchmarking
Hálózati alapismeretek	Exchange Online	Ügyfélprofil készítése
VPN	OneDrive for Business	O365 FAQ
Mobil eszközök használata	Skype for Business	Haszonérvelés
Felhőtechnológia kialakulása	OneNote Tips&Tricks	Tárgyalástechnika
Információbiztonság	SharePoint Online	Kifogáskezelés
	Dokumentumtár	
	Munkafolyamatok	
	Yammer	
	Office ismeretek	

6. táblázat: A képzések tartalmi elemei (saját szerkesztésű táblázat)

Az oktatásokra személyre lebontva hetente egyszer, másfél órában került sor. A fenti tartalom ennek megfelelően a rendelkezésre álló 6 hónap alatt elsajátítható volt. A személyes, tantermi oktatások mellett online eszközökkel, akváriumgyakorlatokkal, helyzetgyakorlatokkal és éles (ügyfélnél történő) tárgyalási helyzetekkel színesítettük a tanulást. A tanulási folyamat szerves részei voltak a személyes vizsgák vagy a csoportos tesztek, valamint a vállalat számára volt alkalmunk olyan országos rendezvényeket szervezni, melyen a képzésen résztvevők egy része előadhatott a témában. Ezen rendezvények megszervezésében való részvétel, az előadások összeállítása, a marketinganyagok elkészítése, valamint a meghívottaknak szóló szakmai levél összeállítása is mind a csoportra hárultak, így minden résztvevő munkához juthatott.

4.3.8 Az oktatássorozat játékosító elemei

Az első csoporttal való közös munka során találtam ki, hogyan tehetem színesebbé a résztvevők számára a tanulást. Mivel a rendelkezésemre álló heti másfél óra/résztvevőt nem tartottam elégnek, szükségem volt olyan eszközre, amivel ráveszem a résztvevőket arra, hogy szabadidejükben is a közös projektünkkel foglalkozzon. Ezt úgy kellett tennem, hogy ne érezze kötelezőnek az extra időráfordítást, valamint, ha nem akar foglalkozni vele, hátránya ne származzon belőle. Viszont jutalmazhassam azokat, akik

időt és energiát fordítanak a termék elsajátítására. Különböző feladatokat találtam ki számukra, hogy aki szeretne, mindenképpen találjon olyat, amit meg tud oldani, és szívesen kipróbál vagy elvégez.

Az első csoport résztvevőinél azt tapasztaltam, hogy a csoport egy, maximum két tagja vevő az efféle feladatokra, azonban az ő szereplésüket és értékelésüket követően többen is kedvet kaptak az extra munkára. Mivel az indulásnál csak egyetlen egy csoporttal kezdtem foglalkozni, hamar híre ment a tréningek színességének, és jó hangulatának, többen kerestek meg a tréningeken kívül, hogy csatlakozhatnak-e a programhoz, vagy tervezek-e következő csoportot indítani. Az első csoport résztvevőitől azt a visszajelzést kaptam, hogy nem gondolták volna, hogy a termék ennyire izgalmas, vagy ennyi mindenre használható. A kezdetekben vezettem jelenléti ívet, amit a második hónaptól elhagytam, mert nem volt rá szükség. Minden héten két alkalommal tartottam ugyanazt a tréninget, tehát a résztvevő választhatott, hogy melyiken tud részt venni, lehetőséget adtam személyes pótlásra, a vidéki kollégák pedig online bejelentkezhettek a másfél órás tréningekre.

A képzéssorozat részei voltak a vizsgák, melyek eredményeire a vállalat vezetése, és egy nemzetközi külső partner is kíváncsi volt. A résztvevők számára fontossá vált, hogy az eredményeik jók legyenek, számomra pedig az volt fontos, hogy a termékismeretük és az ehhez kapcsolódó sales készségeik kialakuljanak és megerősödjenek. Ezért kezdtem el használni olyan trükköket, amikkel az önálló tanulásukat serkentem, ugyanakkor mérni is tudom, és beszámíthatom a vizsgaértékelésbe. Az első csoport segítségével és visszajelzéseivel alakítottam ki azt a rendszert, melyet utána a következő 5 csoporttal együtt használtunk.

A tantermi tanuláson kívül a következő feladatokat jutalmaztam:

1. Online részvétel szervezése (meghívó kiküldése a távol lévő kolléga részére, a tréningen behívása, a hang és a kép beállítása, kezelése), esetleges felvétele és megosztása a közös, tanulói térben
2. Következő heti tréning szervezése (időpontkijelölés, tárgyalófoglalás, résztvevők meghívása és kezelése, a tréning összefoglalójának megírása, megosztása a közös felületen) új eszközök használatával

3. Témához illő ügyfélélmény megosztása, ügyfél bemutatása, folyamatainak ismertetése, a termék illesztése elméletben az ügyfél infrastruktúrájába, az ügyfél számára legvonzóbb terméktulajdonság megtalálása, bemutatása
4. Megtörtént terméktárgyalás részletes bemutatása, elemzése
5. Rendezvényen való aktív részvétel (szervezés, ügyfelek tájékoztatása, előadás, saját példa bemutatása)
6. Osztályértekezleten való saját siker (aláírt szerződés) bemutatása
7. A tesztkörnyezetben saját weblap létrehozása és folyamatos tartalommal való ellátása
8. Segítségnyújtás a kollégák részére a vizsgára való felkészülés során
9. Médiafigyelés – közös hírportál szerkesztése, ahová gyűjtöttük azokat a híreket, amik a nagyvilágból érkeztek, és az adat- vagy információbiztonsággal, felhővel, informatikai helyzetekről szóltak.

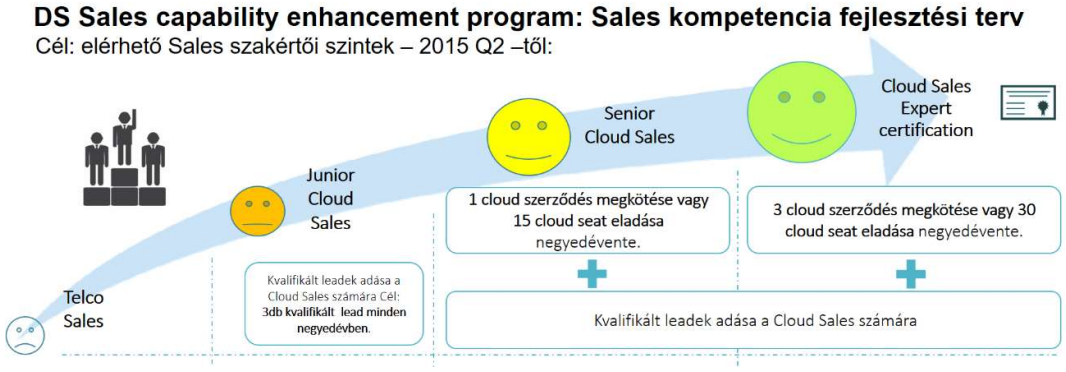
A fenti mérhető és értékelhető elemeken kívül sok olyan helyzetet hoztam be a tréningek alatt, amivel a szemléletmódjukat tudtam formálni. A leginkább azok a példák voltak hatással rájuk, amivel éreztek valamilyen kapcsolódási pontot. Ilyen példák voltak, hogyan vigyázzanak az adataik biztonságára, hogyan cseréljenek mobilkészüléket, hogyan védhetik meg a saját adataikat, hogyan használjanak ingyenes E-mail fiókot, hová szinkronizálják, mire használhatják a céges eszközeiket, és mire nem, mi értelme van a levelek bizalmassági szintjeinek besorolásának. Sokan hallottak már korábban is valamit a fenti témákról, de eddig nem értették a jelentőségét, vagy nem értették a módját annak, hogyan lehet megtenni ezt bárki eszközével.

A tréningeken ezért a személyes és a céges biztonság alapjaival is foglalkoztunk, leginkább ez a terület érdekelte őket, és könnyű volt a termékhez is kötni. Ehhez a témához szívesen hozzászóltak, és szívesen néztek utána az Interneten is. Figyelmesek lettek az IT vagy információbiztonsági hírekre és eseményekre, amit velem szívesen meg is osztottak. Ezeket az információkat – különösen azokat, amik a termékre valamilyen hatással voltak, egy közös felületen, a tesztkörnyezetben kezdtük el gyűjteni.

A személyes vizsgákra való felkészülés könnyebben ment a visszajelzéseik alapján, azokon eredményesen szerepeltek. Az ügyfeleknél elért sikereik pedig magabiztosságot

adtak számukra. A képzéssorozat két és fél éven keresztül történt, ami idő alatt a termék folyamatosan változott. Így a csoportok időről-időre visszatértek egy-egy képzési alkalomra, amikor ezeket a változásokat sorra vettük, valamint ők is lehetőséget kaptak a tapasztalataik megosztására.

A tanuláson kívül egy eredményösztönző rendszert alkottam meg, aminek segítségével a vállalat vezetése is mérhető eredményeket kapott. Az értékesítési eredmények alapján a résztvevők egyre magasabb szinteket érhettek el, elérve a legmagasabb, 'Cloud Sales Expert' fokozatot. A fokozat elérése plusz anyagi juttatással nem járt, de tulajdonosát előnyösebb helyzetbe hozhatta. Könnyebben válthatott magasabb pozícióra vállalaton belül, vagy részt vehetett pilot projektekben, volt, akit termékfejlesztési projektekbe is meghívtak. Ezen előnyök mentén a résztvevőnek magasabb lett a reputációja, az én szempontomból pedig nőtt az elköteleződése a terméken keresztül az oktatások iránt.



27.ábra: Az oktatások során létrehozott fejlődési szakaszok ábrázolása (saját szerkesztés)

4.3.9 Felhasználói oktatások értékelése és eredménye

A tréningeken résztvevők az oktatásokon személyesen és/vagy online módon vettek részt. A tréningek során meghatározott időnként vizsgát tettek, szóban vagy írásban, egyénileg, vagy csoportosan. Az írásbeli tesztre négyszer került sor, ebből kettőt személyesen, kettőt online módon, a vállalati E-Learninges keretrendszerben végeztek el. Ennek elfogadható eredménye alapfeltétele volt a következő tréningeken való részvételnek. A vizsgát a résztvevőnek meg kellett ismételnie, amennyiben az eredménye nem érte el a 60%-ot. Abban az esetben, amikor egy vizsga nem volt sikeres – egyetlen egy ilyen eset fordult elő – a vizsgát a résztvevő egy másik időpontban megismételhette.

A szóbeli vizsgákra egy fő esetében szintén 4 alkalommal került sor, melyek során nemcsak a termék biztos ismerete, de az értékesítői készség is értékelésre került. A szóbeli vizsgákról felvétel készült, a fejlődés vagy változás mérhető volt a felvételek

összehasonlításával. A szóbeli vizsgák értékelésének szubjektivitása miatt, a résztvevőket nem egymáshoz, hanem saját, korábbi teljesítményükhöz tudtam viszonyítani és értékelni. Az értékelésen kívül számítottam az extra eredményeket, melyeket a résztvevők egy része önként végzett el a képzés ideje alatt.

Az értékelési rendszer nem kívánt változtatást a projekt ideje alatt, így mind az 58 résztvevő ugyanazzal a szempontrendszerrel volt mérve. A vezetői riportok során a résztvevők eredményeit kumulálva és osztályra bontva használták fel, név nélkül.

Az 58 résztvevő közül 12 fő a képzés befejezése előtt távozott a vállalattól (ketten szülési szabadságra mentek, 10 fő pedig más vállalatnál folytatta karrierjét), így a 6 hónapos képzéssorozatot 46 fő végezte el eredményesen.

A megszerzett tudást a 6 hónapos (24 hetes) oktatássorozat alatt értékeltem az alábbiak szerint:

IT alapok	**Termékismeret**	**Termék sales ismeretek**	**Egyéni vizsgák 1.**	**Termékismeret 2.**	**Helyzet-gyakorlatok**	**Tárgyalási gyakorlatok**	**Egyéni vizsgák 2.**
2. hét	4. hét	6. hét	8. hét	12.hét	16. hét	20. hét	24. hét
50 pontos teszt	20 pontos teszt	Szóbeli	Szóbeli	20 pontos teszt	Szóbeli	Szóbeli	40 pontos vizsga
48 pont 96%	15 pont 75%	Kiváló	Kiváló	15 pont 75%	Kiváló	Kiváló	34 pont 85%
46 pont 92%	17 pont 85%	Megfelelt	Megfelelt	17 pont 85%	Megfelelt	Megfelelt	38 pont 95%
45 pont 90%	18 pont 90%	Nem megfelelt	Nem megfelelt	18 pont 90%	Nem megfelelt	Nem megfelelt	36 pont 90 %
42 pont 84%	19 pont 95%			19 pont 95%			
39 pont 78%							
38 pont 76%							
36 pont 72%							

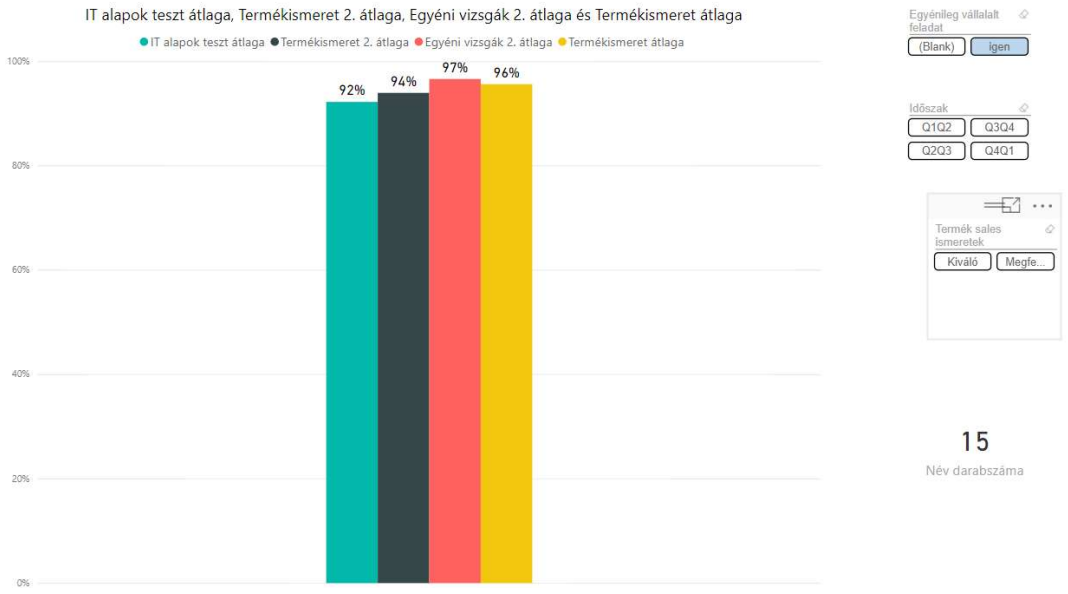
7. táblázat: Értékelési rendszer ütemezése és az értékelés szempontjai (saját szerkesztésű táblázat)

A tesztek megírása csoportosan, online vizsgák esetében egyéni ritmusban történtek. A szóbelikre személyesen, és egyéni alkalmakkal került sor. A vizsgák utólagos kiértékelésénél vizsgáltam, hogy a résztvevő eredményeit befolyásolja-e a témához való hozzáállása. A tapasztalataim azt mutatták, hogy kapcsolat van az elkötelezett résztvevők vizsgaeredményei és a játékosító elemek használata között.

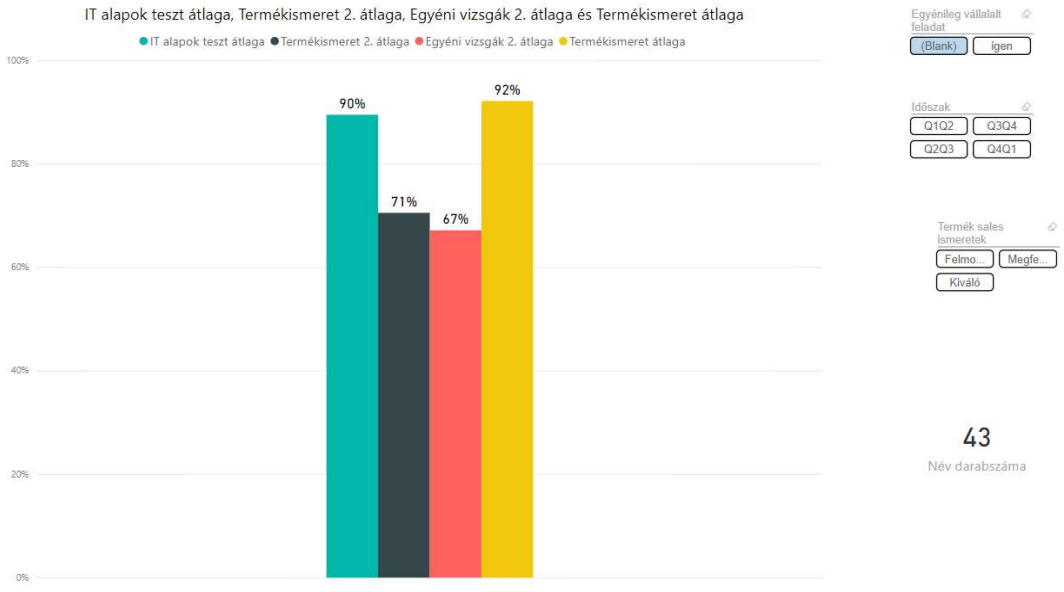
A tréningek során a résztvevőknek csak egy részét, 15 főt sikerült elkötelezett felhasználóvá tenni, ugyanakkor ezek a felhasználók a munkájuk során is használták a „csak” tréning célra bevezetett tesztkörnyezetet. Több esetben gondoltak megoldásként a tesztkörnyezetre, és valósították meg a csoportmunkát, a dokumentumtárat (sablonkezelést), vagy oldották meg a biztonságos, nagy méretű fájlok tárolásának és megosztásának problémáját. Az elkötelezett felhasználók több ügyfelet vonzottak és győztek meg a technológia mellett, aminek segítségével a vezetőik kulcsfelhasználóvá jelölték ki őket, ami több előnnyel, juttatással is járt számukra.

Az 58 résztevőből ez a 15 fő az előző fejezetben (4.3.8) felsorolt extra feladatok közül legalább egyet értékelhető módon elvégzett. Ezek a játékosító, motivációt, elköteleződést elősegítő feladatok erre a 15 főre a tapasztalataim szerint hatással voltak. A vizsgaeredményeik azt mutatják, hogy a többi résztvevőhöz képest (a többi résztvevő között szerepelnek annak a 12 főnek az eredményei is, akik a képzésen valameddig eljutottak, de a képzést nem fejezték be) jobban teljesítettek.

A számszerűsíthető tesztfeladatok során 94,75% eredményt értek el, míg a többi résztvevő átlageredménye 80% volt. A kiváló és megfelelt arány is magasabb volt az ő esetükben, a kiváló eredmények a játékosított hallgatóknál 66,5%, míg a többieknél 41,25% volt.



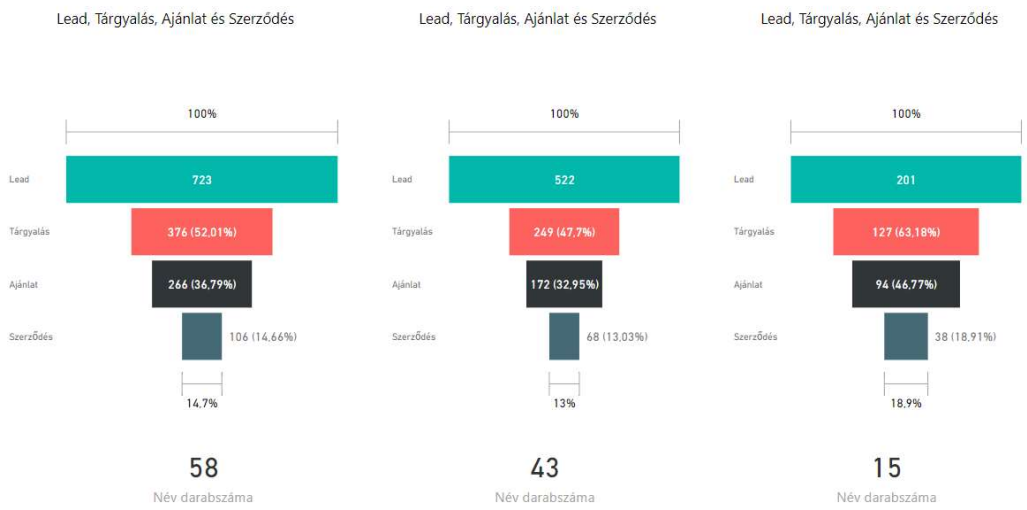
28.ábra: Az elkötelezett résztvevők teszteredményei



29.ábra: A többi résztvevő teszteredményei

A játékosító elemekkel motivált hallgatók nem véletlenszerűen lettek kiválasztva, ezek a résztvevők önként vállalták a plusz feladatokat. Tehát, azok a résztvevők éltek ezzel a lehetőséggel, akik eleve is elkötelezettek voltak a téma, a tanulás, a fejlődés, a technológia iránt. A többi résztvevő is eredményesen és sikeresen zárta a 6 hónapos képzéssorozatot, ám a játékosított hallgatók más előnyökre is szert tettek amellett, hogy jobb eredményeket értek el a részvizsgákon.

Mivel a képzés fő célja az volt, hogy a terméket hatékonyabban legyenek képesek értékesíteni, a képzés ideje (6 hónap egy csoport esetében) alatt mértem a résztvevők értékesítési mutatószámait is. Ez négy fázisból állt, a potenciális ügyfelek kiválasztásából (lead), a tárgyalás megszervezéséből és lebonyolításából (tárgyalás), az ajánlat elkészítéséből és elküldéséből (ajánlat) és szerződéskötésből. Az értékesítési folyamat ilyen módon mérhető számait vizsgálva azt tapasztaltam, hogy a játékosított résztvevők szerződéskötési aránya magasabb, 18,9%, a többiek 13%-ához képest.



30.ábra: Értékesítési eredmények a képzés ideje alatt

Az oktatások minden, ebben a témába tartozó szerződésre hatással voltak. A termék annyira vállalatidegen volt a résztvevők számára, hogy a potenciális ügyfelek kijelölésén kívül egyedül nem mentek végig az értékesítési folyamaton. A második, a tárgyalási fázisba már behívtak szakértőt, akik ettől a ponttól végigvezette az ügyfelet a folyamat lezárásáig. Megfigyelhető volt az egyes résztvevőknél, hogy a képzést elkezdve ugrásszerűen megnőtt a potenciális ügyfelek száma (leadgenerálás), majd elindult az „én egyedül!" folyamat, és egyre kevésbé igényelte szakértő bevonását. Ez a jelenség a játékosított résztvevők esetében hamarabb és erősebben jelentkezett, nemcsak szerződésszámban mutattak jobb értékeket, hanem magabiztosságuk és tárgyalási stílusuk is fejlődött ez alatt az idő alatt.

4.3.10 Az oktatások tapasztalata

Az oktatások során a legnagyobb döbbenetet számomra a résztvevők alaptudása okozta. A projekt elvállalásakor feltételeztem, hogy egy vezető multinacionális cég, technológiailag jól felszerelt munkatársai a vállalati IT infrastruktúrát ismerik, és azt biztonságosan, maximálisan képesek felhasználni, annak előnyeit kihasználni. Sajnos a biztonságtudatosság semmilyen szinten nem volt jelen a szervezetben, a résztvevők a valós fenyegetettséget nem ismerték fel, és tulajdonképpen kérdéseik sem voltak ebben a témában. A tréningek során ezért kezdtem alkalmazni a játékosítást, és bevonni olyan elemeket, amivel a résztvevőket meg lehetett ijeszteni, ki lehetett zökkenteni, vagy meghökkenteni, kiváltva ezzel belőlük egy alapvető érzetet, érzelmet vagy félelmet. A programot ezeken felül kiegészítettem olyan feladatokkal is, melyeket vállalva szélesebb

körű ismeretre tehet szert az adott résztvevő, vagy tudását vagy elköteleződését növelve ez által. Ennek hatására ezek a plusz feladatok, események, felkeltették a kíváncsiságukat, kérdéseik lettek, a játékos elemek bevezetését követően pedig elkötelezett tréning résztvevőkké váltak. Úgy gondolom, ahhoz, hogy a résztvevők kitartását és figyelmét 6 hónapon keresztül fenn tudtam tartani egy informatikai termék iránt, a játékosítás és a személyes fenyegetettség modellezése segítette.

Az előző fejezetben leírt számszerűsített adatokon kívül a program sikerére is hatással voltak a játékosított résztvevők. Az ő hozzáállásuk és eredményeik igazolták a módszer hatékonyságát – ugyanakkor bizonyították számomra azt is, hogy nem minden résztvevő játékosítható. Bár a program kötelező volt az összes résztvevő számára, az extra feladatokat mégis kevesen, csak 35%-uk próbálta ki, és a vizsgálatom során már az egy extra feladatot végző résztvevőt is a játékosított résztvevők közé soroltam.

Összefoglalás

A játékosítást vizsgálva, mind a nemzetközi, mind a hazai tapasztalatok azt mutatják, hogy erősebb elköteleződés alakítható ki a használatával, mint csak hagyományos oktatási módszereket használva. A nagyvállalati szférában is egyre gyakrabban nyúlnak ehhez az elemhez, és nemcsak, mint tudatosító, hanem mint motiváló (elköteleződést segítő) eszközként is tekintenek rá. A vállalati életbe könnyen integrálható, az oktatásokat színesíti, kiegészíti.

A saját esettanulmányom során azt tapasztaltam, hogy jobb mérhető és közvetett eredmények érhetők el használatával. Ugyanakkor a játékosítás nem egy csodaszer, alkalmazását csakis rendszerben, az oktatási lánc egyik láncszemeként érdemes alkalmazni. Mindemellett szükséges egy egységes oktatási politika kialakítása, ahol lehetőség van arra, hogy a játékosításnak megfelelő helye legyen, a módszertan ne egy külön egységként szerepeljen, hanem a meglévő folyamatokat támogathassa, az átadni kívánt tudást egy másik csatornán keresztül közvetítse.

Az oktatónak, aki a játékosítás eszközeit használni kívánja, nemcsak a tananyaghoz való illesztést kell megvizsgálnia és kialakítania, hanem a résztvevők egyéni céljait, külső és belső motivációs igényeit is figyelembe kell vennie. A játékosítás nem minden helyzetbe hozható be módszertanként – tehát azt is meg kell vizsgálni, az adott ponton működik-e a játékosítás valamennyi előfeltétele, valamint valóban hoz-e annyi eredményt, hogy érdemes legyen az oktatás során alkalmazni.

Esettanulmányomban fontos szerepet kapott, hogy a tejes oktatási anyagot végígkísérték a játékosítás bizonyos elemei, ugyanakkor a résztvevők számára egy választható irány volt, senki számára nem volt kötelező a játékosított elemek kipróbálása. Azok körében, akik azonban részt vettek ezen elemek kipróbálásában, a tudásukban magabiztosabbakká váltak. A tudás mellett azonban egy erősebb kapocs alakult ki a résztvevő és az oktatás témája között.

Mindenképpen úgy értékelem, hogy hasznos volt játékosító elemeket alkalmaznom az oktatás során, és azok megválasztását is eredményesnek ítélem. A résztvevők visszajelzései alapján egy összetettebb, komplexebb tudásra tettek szert, amit nemcsak a vizsgák során, hanem az élet egyéb területein is alkalmazni tudnak a későbbiekben. A játékosított résztvevők aktivitását az oktatások során végig fent lehetett tartani, és a későbbi kapcsolattartást is segítette ennek a módszernek a használata.

Negyedik hipotézisemben feltételezem, hogy a személyes élményeken keresztül fokozható a biztonságtudatos viselkedés és ennek tapasztalatai az oktatási programokba is beépíthetők. Az általam végzett oktatások során a játékosítás eszközeit használtam ahhoz, hogy személyes élményeken keresztül, tapasztalati úton is elsajátíthatók legyenek a vállalat által meghatározott felhőbiztonsági szabályok. Dolgozatom negyedik fejezetében bizonyatom, hogy az oktatássorozat alatt az elköteleződés és az ismeretek elsajátítása szoros kapcsolatban állnak. Bár mind az oktató, mind a hallgató részéről extra energiát igényel a játékosítás, mint eszköz használata – ugyanakkor nagyvállalati környezetben, felnőtt résztvevőkkel, meghatározott cél érdekében és hosszú távon jól alkalmazható. Kutatásom ezen eredményeit az „Intenzív játékélmény a cloud biztonság tudatosságának eszközeként” (III.) című cikkemben, valamint a „Gamification in Developing Cloud Security Awareness” (VI) publikációmban tettem közzé.

ÖSSZEGZETT KÖVETKEZTETÉSEK

Tanulmányaim, elméleti és gyakorlati kutatásaim, oktatási tapasztalatom mind azt támasztják alá, hogy az emberi tényező nem elhanyagolható szempont a szolgáltatási lánc során. Az emberi tényező megfelelő képzés és ellenőrzés nélkül nagy kockázatot jelent, és nagy mértékben befolyásolja a vállalat teljes biztonságát. Bár a vállalatok mindegyike komoly erőforrásokat éget annak érdekében, hogy munkatársai felkészültek legyenek az informatikai biztonságot tekintve, az eredmények azt mutatják, ezek az erőforrások még mindig kevesek.

Egyrészről a technológia folyamatos változása befolyásolja a munkatársak felkészültségét. Bár mindegyik vállalat használja valamilyen szinten (bevezetett vagy Shydow IT) az elérhető felhőszolgáltatások legalább egyik megoldását, az oktatási anyagokban az új technológia specialitásai nem találhatók meg. Bár az alapvető biztonságos informatikai eszközhasználat szabályai érvényesek a felhőszolgáltatások használata esetében is, tudatosan a két terület nincs összekötve a tananyagokban.

Másrészről a vállalati kultúra nem minden ponton követeli meg a szabályok betartását, valamint a példamutatást. Sajnos, amíg a rendszerekben „szabad” megtenni az egyébként tiltott informatikai műveleteket, addig mindig lesz felhasználó, aki véletlenül vagy szándékosan meg is teszi azokat.

Harmadrészről a felhasználók informatikai tevékenységének monitorozása sem megoldott minden esetben. Van lehetőség arra, hogy utólagosan, vagy alkalomszerűen vizsgáljanak egy-egy felhasználói tevékenységet vagy eszközt, tudatosan és proaktív módon nincs az egész vállalatra vonatkozóan kiépítve a monitorozó rendszer. Egyes vállalatok, egyes tevékenységi köre folyamatos ellenőrzés alatt áll, ahol a felhasználók mindegyike tisztában van tevékenységének megfigyelésével. Ezeken a területeken a biztonságtudatosság a legerősebb az összes vizsgált terület közül.

A vállalat azon területein, ahol a biztonság megtartására nagy hangsúlyt fektetnek, tehát mind az oktatás, a tanultak számonkérése, a felhasználók monitorozása valamint szükség esetén a kihágások szankcionálása megtörténik, ott a legerősebb a biztonságtudatossága a résztvevőknek.

A vállalati oktatásoknak van azonban pozitív hozadéka is. A munkatársak a megszerzett alapvető tudást a magánéletükre is kiterjesztik, és környezetükre (családtagjaikra) is

kiterjesztik azokat (pl. jelszókezelés, képernyővédelem, személyes adatok védelme). Az elmúlt években a biztonságtudatosság erősebb, és a napvilágra került, médiában is megjelent informatikai támadások óvatosságra intik a vállalati felhasználókat, mint magánembereket is.

A felhőtechnológia elterjedése ma már nem kérdés. Az elmúlt évek során vállalatok több, mint fele döntött a felhőszolgáltatások bevezetése mellett. Ennek oka a költségcsökkentések mellett a technológia biztonságossága is. Korábban a vállalati döntéshozók kételkedtek a technológia biztonságát illetően, ma már a felhőbe való költözés első három helyén nem szerepel a technológia biztonságosságának megkérdőjelezése. Ugyanakkor a vezető kockázatok mellett az emberi tényező megjelenik – ahol leginkább a felhasználó biztonságtudatosságának kérdései szerepelnek.

Vállalati szinten érzékelhető a munkavállalók túloktatása, aminek egyik tünete a tantermi és online oktatási anyagokra való immunitásuk. A játékosítás eszközével a résztvevők egy része motiválható, és az így megszerzett tudásuk hosszabb távon marad meg, kötődés alakul ki az oktatási anyag és a tanuló között. Bár a játékosítás eszköze nem használható minden helyzetben, és nem használható alkalomszerűen, ok nélkül. Tapasztalataim szerint a hatékony ismeretátadás egyik eszköze, ahol nem hanyagolhatók el a személyes és az e-learninges oktatási módszerek sem. Tehát minden, a rendelkezésünkre álló módszertant ötvözve érhetünk el számottevő eredményt, ahol a módszertanokat okosan, egymásra építve, folyamatban használjuk. A játékosítás eszközével a mélyebb integrációt, a másik nézőpontot tudjuk kínálni, valamint erős hatása van a résztvevők motivációjára és kötődésére. A játékosítás nem csodaszer, hanem egy eszköz, amivel egy újabb lehetőséget kapunk a munkavállalók megszólítására, elkötelezettségük erősítésére.

Új tudományos eredmények

1. A felhőtechnológiák hazai és nemzetközi irodalmát kutatva, a szabályozási környezetet megvizsgálva és a technológiára vonatkozó kockázati tényezők irodalomkutatásával majd a kockázati hatások összevetésével **bizonyítottam** első hipotézisemben felvetett feltételezésemet, **amelyben feltételeztem**, hogy a felhőszolgáltatás technológiája képes alacsony kockázati szinten kezelni az adattárolást és -hozzáférést minősített szolgáltató igénybevétele esetén, de ennek együtt kell járnia a humán faktor megfelelő, biztonságtudatos munkavégzésre történő felkészítésével. **Bizonyított eredményeim szerint** nem csökkenthetők

nullára a felmerülő kockázatok, de maga a rendszer – így a szolgáltatási lánc egyes elemeinek kockázata mérhető, a kockázati mátrixban elhelyezhető, tehát a technológia kockázataira a vállalat felkészíthető.

2. A második hipotézisemben felvetett tételt **bizonyítottam**, vagyis a számítási felhő, a kommunikációs hálózat, a vállalati informatikai rendszer és a felhasználó szolgáltatási láncnak az utolsó és leggyengébb láncszeme a felhasználó. Amennyiben a mobileszközök használatát – mivel ez a tevékenység szorosan köthető a felhasználóhoz – még a humánerőforrás szokásaihoz, biztonságtudatosságához kötjük, a hipotézisben megfogalmazottak bizonyíthatók.
3. Ahogy a 3. hipotézisemben állítottam, a humán fejlesztés, valamint a vállalati szabályozás szoros kapcsolatban állnak, **bizonyítottam**, hogy a HR és az IT vezetés hatással van a munkatársi biztonságtudatosság szintjére. **Igazoltam**, és arra az eredményre jutottam, hogy amennyiben az oktatás rendszeres, az ott megszerzett tudás a gyakorlatban is elvárt a munkatárstól, **a szabályok be nem tartása** pedig szankciókat von maga után, ott a munkatársak szabálytartása erősebb.
4. Negyedik hipotézisemben feltételezem, hogy a személyes élményeken keresztül fokozható a biztonságtudatos viselkedés és ennek tapasztalatai az oktatási programokba is beépíthetők. **Igazoltam**, hogy a játékosítás eszközeit használva, személyes élményeken keresztül, tapasztalati úton is elsajátíthatók a vállalat által meghatározott felhőbiztonsági szabályok. Továbbá dolgozatom negyedik fejezetében **bizonyítom**, hogy az oktatássorozat alatt az elköteleződés és az ismeretek elsajátítása szoros kapcsolatban állnak. Bár mind az oktató, mind a hallgató részéről extra energiát igényel a játékosítás, mint eszköz használata ugyanakkor nagyvállalati környezetben, felnőtt résztvevőkkel, meghatározott cél érdekében és hosszú távon sikeresen alkalmazható.

JEGYZÉKEK

Ábrajegyzék

Táblázatjegyzék

Rövidítésjegyzék

1.fejezet	
IT	Information Technology
Google Docs	A Google felhő alapon működő fájlok tárolására alkalmas nyilvános szolgáltatása
SLA	Service Level Agreement – minimálisan nyújtott szolgáltatási szint
NIST	National Institute of Standards and Technology - Amerikai Nemzeti Szabványügyi és Technológiai Intézet
Pay-as-you-grow	Pay-as-you-grow – olyan értékesítési modell, amely lehetővé teszi az ügyfelek számára, hogy szükség szerint fokozatosan vásároljanak nagyobb kapacitást
ROI	Return of Investment – a befektetés megtérülése
API	Application Programming Interface – Alkalmazásprogramozási felület
Image Library	egy szolgáltatásra vonatkozóan több megoldást a különböző konfigurációkhoz, platformokhoz
TIER	Az Uptime Institute által meghatározott adatközpont besorolási rendszer
IoT	Internet of Things
KKV	Kis- és Középvállalat
AWS	Amazon Web Services
GDPR	General Data Protection Regulation (Általános Adatvédelmi Rendelet)
IEEE	Institute of Electrical and Electronics Engineers - villamosmérnököket egyesítő nemzetközi szervezet
OCC	Open Cloud Consortium – Nyílt Cloud Konzorcium
CSCC	Cloud Standards Customer Council – Felhő szabványokkal foglalkozó Ügyféltanács
DMTF	Distributed Management Task Force, Inc. – Menedzselhető és elosztott rendszerek munkacsoport
ETSI	European Telecommunications Standards Institute - Európai Távközlési Szabványügyi Intézet

GICTF	Global Inter-Cloud Technology Forum – Nemzetközi Felhőtechnológiai Fórum
SNIA	Storage Networking Industry Association – Tároló Hálózatokkal foglalkozó Ipari Szövetség
CSA	Cloud Security Alliance – Felhőbiztonsági Szövetség
ENISA	Europian Union Agency for Network and Internet Society - Az Európai Unió Hálózati és Internetes Társasága
OWASP	The Open Web Application Security Project – Nyílt hálózati alkalmazások biztonsága
ISO	International Organization for Standardization – Nemzetközi Szabványügyi Szervezet
COBIT	Control Objectives for Information and Related Technologies - Vállalati információtechnológia irányításának és menedzsmentjének átfogó üzleti és vezetési keretrendszere
ITIL	Information Technology Infrastructure Library - informatikai rendszerek üzemeltetésére és fejlesztésére szolgáló módszertan
Togaf 9	The Open Group Architecture Framework - vállalati architektúra keretrendszer, amely megközelítést nyújt a vállalati informatikai architektúra tervezéséhez, testreszabásához, megvalósításához és irányításához
FitSM	Family of Standards for Lightweight IT service management - IT-szolgáltatás menedzsment szabványainak családja
NSA	National Security Agency - Nemzetbiztonsági Ügynökség
IEC	International Electrotechnical Commission – Nemzetközi Elektrotechnikai Bizottság
ACL	Access Control List
IPsec	Internetes protokollbiztonság
SDL	Security Development Lifecycle
TLS	Transport Layer Security
SSL	Secure Sockets Layer
AES-256	Advanced Encryption Standard
DES	Data Encryption Standard – Szimmetrikus kulcsú algoritmus
RSA 2048	Rivest–Shamir–Adleman publikus kulcsú titkosítás

TPM	Trusted Platform Module
MIL–STD–882C	United States military standard, standard practice for system safety, Biztonsági szabvány, itt: kockázatértékelés
2. fejezet	
GDP	Gross domestic product – Bruttó Hazai Termék
BCP	Business Continuity Plan - Üzletmenet Folytonossági Terv
DRP	Disaster Recovery Plan - Katasztrófa Visszaállítási Terv
HR	Human Resources – Emberi Erőforráskezelési osztály
SIM kártya	Subscriber identity module – előfizetői azonosítói modul
USD	United States Dollar – amerikai dollár
CRM	Customer Relationship Management – Ügyfélkezelő rendszer
PCI-DSS	Payment Card Industry Data Security Standard
GVP	General Vice President – Általános igazgatóhelyettes
CEO	Chief Executive Officer - Vezérigazgató
CPU	Central Processing Unit
VPN	Virtual Private Network – virtuális magánhálózat
Wi-Fi /wifi	Wireless Fidelity – vezetéknélküli hálózat
DLP	Data Loss Prevention – adatvesztés megelőzése
IAM	Identity and Access Management - Identitás és hozzáférés-kezelés
CASB	Cloud Access Security – Felhőszolgáltatásokhoz történő hozzáférés biztonságossága
3. fejezet	
IB	Információbiztonság
X generáció	1960-1980 között születettek
Y generációt	1980-2000 között születettek
IBSZ	Információbiztonsági Szabályzat
MDM	Mobile Device Management – mobileszköz menedzsment
4. fejezet	
O365	Office 365
FAQ	Frequently Asked Questions – Gyakran feltett kérdések

HIVATKOZOTT IRODALOM

[1] Ling QIAN, Zhiguo LUO, Yujian DU, and Leitao GUO, Cloud Computing: An Overview, pp 626-627 https://pdfs.semanticscholar.org/d3e9/1ade0afee6beb4a1737d601849af9e3f816f.pdf , elérhető: 2018.06.09

[2] MELL, Peter & GRANCE, Timothy (2011) - The NIST Definition of Cloud Computing, Special Publication 800-145, Computer Security Division Information Technology Laboratory National Institute of Standards and Technology Gaithersburg, MD 20899-8930 September 2011 http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-145.pdf, elérhető: 2018.06.09

[3] BŐGEL György (2009) Az informatikai felhők gazdaságtana, Közgazdasági szemle, (7-8), pp 673-688

[4] Gabriella, BÁBEL, Korszakhatárhoz érkeztek a magyar nagyvállalatok - Microsoft Magyarország Kft., https://news.microsoft.com/hu-hu/2017/03/17/korszakhatarhoz-erkeztek-a-magyar-nagyvallalatok/ 2017.03.17. elérhető: 2018.06.09

[5] Amazon Cloud Services, általános bemutatkozó weboldal a cég tevékenységéről, szolgáltatásairól, árairól - https://aws.amazon.com/pricing/ elérhető: 2018.06.09

[6] Sajee; Mathew, Overview of Amazon Web Services, 2014, https://www.sysfore.com/Assets/PDF/aws-overview.pdf, elérhető: 2019. 02. 08.

[7] HAFNER, Joachim; SCHWINGEL, Simon; Ayers, Tyler; Masuch, Rolf – Azure Strategic Implementation Guide for IT Organizations, Microsoft Corporation, https://azure.microsoft.com/mediahandler/files/resourcefiles/d817c644-5dac-442f-8839-7d704e828809/Azure_Strategic_Implementation_Guide_for_IT_Organizations.pdf, 2017, elérhető: 2018.06.09

[8] HARMS, Rolf; YAMARTINO, Michael – The Economics of the Cloud, Microsoft Corporation https://www.google.hu/url?sa=t&rct=j&q=&esrc=s&source=web&cd=2&cad=rja&uact=8&ved=0ahUKEwju2MW7gMbZAhXSPFAKHYz8ADYQFgguMAE&url=http%3A%2F%2Fdownload.microsoft.com%2Fdownload%2F6%2FE%2F4%2F6E4CB3D1-

5004-4024-8D90-6C66C83C17AA%2FThe_Economics_of_the_Cloud_W elérhető: 2018.06.09

[9] Google Products Plans, -általános weboldal a Google szolgáltatásairól, történetéről, felépítéséről, https://cloud.google.com/products/ elérhető: 2018.06.09

[10] Cheryl RITTS - Kickstarting Cloud ROI, ISACA JOURNAL VOL 6, 2016

[11] BENCSÁTH Boldizsár, BOGÁR Attila, ERDÉLYI Bálint Károly, JUHÁSZ Miklós, HORVÁTH Tamás, KINCSES Zoli, KÚN László, MARTOS Balázs, MÁTÓ Péter, ORVOS Péter, PAPP Pál, PÁSZTOR Miklós, PÁSZTOR Szilárd, RIGÓ Ernő, SZAPPANOS Gábor, TISZAI Tamás, TÓTH Beatrix - Az informatikai hálózati infrastruktúra biztonsági kockázatai és kontrolljai, IHM – MTA-SZTAKI, 2004.07.08 https://www.cert.hu/sites/default/files/MTA1_print.pdf elérhető: 2018.06.09

[12] HARDEN, Mark - John Deere to partner with Colorado company on cloud platform for farmers — the Denver Business Journal, 2015.10.13 https://www.bizjournals.com/denver/news/2015/10/13/john-deere-to-partner-with-colorado-company-on.html

[13] Microsoft ügyféltörténetek, Microsoft Magyarország Kft, 2015.04.21, https://customers.microsoft.com/en-us/story/graphisoft-felhoalapu-uzlet-es-it-minden-szinten elérhető: 2018.06.09

[14] KOVÁCS Zoltán - Felhő alapú informatikai rendszerek potenciális alkalmazhatósága a rendvédelmi szerveknél, Hadmérnök, VI. Évfolyam 4. szám - 2011. december, pp 176-188; http://hadmernok.hu/2011_4_kovacsz.pdf elérhető: 2019. 02. 08.

[15] Telekom üzleti szolgáltatások, Multiflex, SLA szint, https://www.telekom.hu/uzleti/szolgaltatasok/adatatviteli/multiflex , elérhető: 2018.06.09

[16] Microsoft Azure Blog - How do I choose a cloud service provider? https://azure.microsoft.com/en-us/overview/choosing-a-cloud-service-provider/ , elérhető: 2018.06.09

[17] McDonough, Jim - 7 Factors to Help You Choose the Right Cloud Service Provider, posted in Business Insights, Cloud Security Planning, 2017.08.31.

https://www.threatstack.com/blog/7-factors-to-help-you-choose-the-right-cloud-service-provider/ elérhető: 2018.06.09

[18] Jim FOLEY - 9 Requirements You Need to Offer Public Cloud, 2013.02.06 https://www.flexiant.com/2013/02/06/public-cloud-service-provider/ elérhető: 2018.06.09

[19] A Microsoft Azure szolgáltatás hivatalos honlapja, https://azure.microsoft.com/en-us/, elérhető: 2019. 02. 08.

[20] Google Cloud Security and Compliance Whitepaper How Google protects your data. - https://static.googleusercontent.com/media/gsuite.google.com/en//files/google-apps-security-and-compliance-whitepaper.pdf elérhető: 2019. 02. 08.

[21] Economic and social impacts of Google Cloud, Deloitte Financial Advisory, S.L.U., 2018. szeptember https://www2.deloitte.com/content/dam/Deloitte/es/Documents/tecnologia/Deloitte_ES_tecnologia_economic-and-social-impacts-of-google-cloud.pdf, elérhető: 2019. 02. 08.

[22] Az amazon Web Services hivatalos weboldala, https://aws.amazon.com/about-aws/#, elérhető: 2019. 02. 08.

[23] Overview of Amazon Web Services, AWS Whitepaper, Amazon Web Services, Inc. 2019 https://docs.aws.amazon.com/aws-technical-content/latest/aws-overview/aws-overview.pdf, elérhető: 2019. 02. 08.

[24] David Mitchell SMITH, Ed ANDERSON - Hype Cycle for Cloud Computing, 2017,

Published: 01 August 2017 ID: G00315206, https://www.gartner.com/newsroom/id/3797963 elérhető: 2018.06.09

[25] GDPR, The EU General Data Protection Regulation - https://www.eugdpr.org/ elérhető: 2018.06.09

[26] Getting to the GDPR: Four key use cases to jumpstart your efforts IBM Security Guardium helps simplify preparation for the General Data Protection Regulation, IBM, 2018 https://ecs-nordic.arrow.com/Arrow%20Common%20DAM/Arrow%20ECS%20-%20DK/Files/IBM/GDPR%20-%204%20Key%20Use%20Cases.PDF

[27] Az MSZ ISO/IEC 27000-es szabványcsalád, http://www.mszt.hu/web/guest/az-informaciobiztonsag-iranyitas-szabvanyai elérhető: 2018.06.09

[28] A Magyar Nemzeti Bank 2/2017. (I.12.) számú ajánlása a közösségi és publikus felhőszolgáltatások igénybevételéről, 2017, https://www.mnb.hu/letoltes/2-2017-felho-szolg.pdf elérhető: 2018.06.09

[29] 8 criteria to ensure you select the right cloud service provider, CIF - Cloud Industry Forum, https://www.cloudindustryforum.org/content/8-criteria-ensure-you-select-right-cloud-service-provider elérhető: 2019. 02. 08.

[30] ISO/IEC 27017:2015 Information technology - Security techniques - Code of practice for information security controls based on ISO/IEC 27002 for cloud services https://www.iso.org/standard/43757.html

[31] ISO/IEC 27002:2013 Information technology - Security techniques - Code of practice for information security controls https://www.iso.org/standard/54533.html

[32] Cloud Computing Risk Assessment Published: November 20, 2009 https://www.enisa.europa.eu/publications/cloud-computing-risk-assessment elérhető: 2018.06.09

[33] Marnix DEKKER, Dimitra LIVERI - Certification in the EU Cloud Strategy, 2014 November, https://www.enisa.europa.eu/topics/cloud-and-big-data/cloud-security és https://resilience.enisa.europa.eu/cloud-computing-certification/certification-in-the-eu-cloud-strategy elérhető: 2018.06.09

[34] Rich MOGULL, James ARLEN, Francoise GILBERT, Adrian LANE, David MORTMAN, Gunnar PETERSON, Mike ROTHMAN - Security Guidance For Critical Areas of Focus in Cloud Computing v4.0, 2017 https://downloads.cloudsecurityalliance.org/assets/research/security-guidance/security-guidance-v4-FINAL.pdf elérhető: 2018.06.09

[35] CLOUD SECURITY ALLI1ANCE: Big Data Working Group: Expanded Top Ten Big Data Security and Privacy Challenges (2013. április) https://downloads.cloudsecurityalliance.org/initiatives/bdwg/Expanded_Top_Ten_Big_Data_Security_and_Privacy_Challenges.pdf elérhető: 2018.06.09

[36] About The Open Web Application Security Project, https://www.owasp.org/index.php/About_The_Open_Web_Application_Security_Project elérhető: 2018.06.09

[37] Ezhil Arasan BABARAJ - Cloud Security – An Overview https://www.owasp.org/images/c/cc/Cloud_Security_–_An_Overview.pdf elérhető: 2018.06.09

[38] Eric SIMMON - Evaluation of Cloud Computing Services Based on NIST 800-145, National Institute of Standards and Technology (NIST), 2017.04.27 https://www.nist.gov/sites/default/files/documents/2017/05/31/evaluation_of_cloud_computing_services_based_on_nist_800-145_20170427clean.pdf elérhető: 2018.06.09

[39] Stephen MANN - ITIL Alternatives: Why is There so Little Uptake of ITSM Industry Frameworks? 2016.11.01 https://blog.freshservice.com/itil-is-not-all-there-is/ elérhető: 2018.06.09

[40] ITIL - az informatikaszolgáltatás módszertana - KFKI Számítástechnikai Rt Verzió: 3.1, 2002, http://www.itsmf.hu/documents/itil1attekintes_v3.1.pdf elérhető: 2018.06.09

[41] ISACA Official Home Page http://www.isaca.org/cobit/pages/default.aspx elérhető: 2018.06.09

[42] COBIT 5 Introduction 2012. február 28, https://www.isaca.org/COBIT/Documents/An-Introduction.pdf, elérhető: 2019. 02. 08.

[43] NAGY DEMETER Viktor – ABT Blog - A jó, a rossz és a csúf – felhő a gyakorlatban Megjelent: 2015. február 4., http://abt.hu/hu/a-felho-a-gyakorlatban/ elérhető: 2018.06.09

[44] Fergus O'SULLIVAN - Top Ten Major Risks Associated With Cloud Storage, 2018.05.07. https://www.cloudwards.net/top-ten-major-risks-associated-with-cloud-storage/ elérhető: 2018.06.09

[45] Vasant RAVAL, Don LUX - Blind Spots on the Cloud Platform, ISACA JOURNAL VOL 5, 2017

[46] OWASP Cloud Top 10 https://www.owasp.org/images/3/3f/OWASP_Cloud_Top_10.pdf elérhető: 2018.06.09

[47] David VOHRADSKY, CGEIT, CRISC, Cloud Risk—10 Principles and a Framework for Assessment (2012. vol.5) https://www.isaca.org/Journal/archives/2012/Volume-5/Pages/Cloud-Risk-10-Principles-and-a-Framework-for-Assessment.aspx elérhető: 2018.06.09

[48] SASVÁRI Péter - A felhőalapú számítástechnika elterjedésének empirikus vizsgálata a magyar vállalkozások körében, Karlovitz János Tibor (szerk.). Fejlődő jogrendszer és gazdasági környezet a változó társadalomban. ISBN 978-80-89691-21-0)

[49] The Security Development LifeCycle https://social.technet.microsoft.com/wiki/contents/articles/7100.the-security-development-lifecycle.aspx elérhető: 2018.06.09

[50] Az Office 365 háromlépcsős védelme – ezért nem kell féltened adataidat, 2016.02.16 http://www.var.hu/hu/blog/az-office-365-haromlepcsos-vedelme-ezert-nem-kell-feltened-adataidat/48?printable elérhető: 2018.06.09

[51] BOND, J - The Enterprise Cloud, online Book, O'Reilly https://www.safaribooksonline.com/library/view/the-enterprise-cloud/9781491907832/ch01.html elérhető: 2018.06.09

[52] Frank SIEPMANN – Managing Risk and Security in Outsourcing IT Services, Onshore, Offshore and the Cloud, 2013.12.09, ISBN 9781439879092, Auerbach Publications

[53] Encryption - Helping to protect data at rest and data in transit https://www.microsoft.com/en-us/trustcenter/security/encryption elérhető: 2018.06.09

[54] Ray SHAW - Lunch with Eugene Kaspersky - master of the dark side, 2015.06.10 https://www.itwire.com/business-it-news/security/68320-lunch-with-eugene-kaspersky-master-of-the-dark-side elérhető: 2018.06.09

[55] MUCK Tibor - Ennyit tettek hozzá a toplistás cégek a magyar GDP-hez, 2013.11.30, http://adozona.hu/altalanos/Ennyit_tettek_hozza_a_toplistas_cegek_a_mag_0FHEMO elérhető: 2018.06.09

[56] Samsung Developers Club, Remote Test Lab at Samsung: http://developer.samsung.com/remotetestlab/rtlAboutRTL.action elérhető: 2018.06.09

[57] Ericsson establishes collaborative cloud lab in Germany, Ericsson Cloud Whitepapers, 2015. július 14. https://www.ericsson.com/en/news/2015/7/ericsson-establishes-collaborative-cloud-lab-in-germany elérhető: 2018.06.09

[58] Ericsson opens a cloud lab in Italy for faster co-creation and innovation, https://www.ericsson.com/en/press-releases/2015/5/ericsson-opens-a-cloud-lab-in-italy-for-faster-co-creation-and-innovation 2015. május 26. elérhető: 2018.06.09

[59] TOSNER, Johan - ABB and Ericsson establish joint 5G industrial innovation lab, Ericsson Research Centre, 2017. október 12. https://www.ericsson.com/research-blog/abb-ericsson-establish-joint-5g-industrial-innovation-lab/ elérhető: 2018.06.09

[60] Varaprasad S. DOLLA - Science and Technology in Contremporary China, Interrogating Policies and Progress, p.219, Cambridge University Press 2015., ISBN 978 -1-107-08037-9
https://books.google.hu/books?id=kjPKBAAAQBAJ&pg=PA219&lpg=PA219&dq=R%26D+Labs+by+Telco+enterprises&source=bl&ots=ZxqG3M438j&sig=lfQvembpQ_yqf8VQGgfkokuNr44&hl=hu&sa=X&ved=0ahUKEwi3juSe9cXZAhUMvFMKHZYRBAkQ6AEILzAB#v=onepage&q=R%26D%20Labs%20by%20Telco%20enterprises&f=false elérhető: 2018.06.09

[61] GREEN, Joshua - IBM Developer Cloud, Choosing an Ideal IT Support Company , 2017 március 18. https://www.ibm.com/developerworks/community/blogs/e3ec7365-1b09-44f2-906f-19826275860f/entry/Choosing_an_Ideal_IT_Support_Company?lang=en elérhető: 2018.06.09

[62] IBM Budapest Lab néven új fejlesztőközpontot hozott létre az IBM, Műszaki Magazin, 2017. április 24. http://muszaki-magazin.hu/2017/04/24/ibm-budapest-lab-neven-uj-fejlesztokozpontot-hozott-letre-az-ibm/ elérhető: 2018.06.09

[63] Inspire The World, Samsung Electrronics Sustainability Report 2017, pp 25-27, p53, p56, pp 59-6 http://images.samsung.com/is/content/samsung/p5/global/ir/docs/Samsung_Electronics_Sustainability_Report_2017.pdf elérhető: 2018.06.09

[64] NICKELSBURG, Monica - Amazon sets meeting with Seattle officials in effort to improve relationship with its hometown, Geek Wire Magazine, 2018. január 23.,

https://www.geekwire.com/2018/amazon-sets-meeting-seattle-officials-effort-improve-relationship-hometown/ elérhető: 2018.06.09

[65] Amazon's new Austrian R&D centre working on drone systems, 2016. május 11, https://postandparcel.info/72944/news/amazons-new-austrian-rd-centre-working-on-drone-systems/ elérhető: 2018.06.09

[66] TOOPE, Steven - BT and Huawei announce five year collaboration with Cambridge, University of Cambridge, 2017. november 16. https://www.cam.ac.uk/news/bt-and-huawei-announce-five-year-collaboration-with-cambridge elérhető: 2018.06.09

[67] Nokia Corporation Report for Q4 2016 and Full Year 2016, 2017. február 2., https://www.nokia.com/en_int/news/releases/2017/02/02/nokia-corporation-report-for-q4-2016-and-full-year-2016 elérhető: 2018.06.09

[68] VASVÁRI György, CISM - Vállalati biztonságirányítás, Informatikai biztonságmenedzsment, 2007. http://www.tiphaz.hu/partner/vasware/Vallalati_Biztonsagiranyitas_Szakkonyv.pdf

[69] Zeljka ZORZ - Security awareness is good, but good security culture is better, 2017.05.08 https://www.helpnetsecurity.com/2017/05/08/build-security-culture/ elérhető: 2018.06.09

[70] Chris ROMEO - 6 ways to develop a security culture from top to bottom, 2018.01.18, https://techbeacon.com/6-ways-develop-security-culture-top-bottom elérhető: 2018.06.09

[71] Fran HOWARTH - Top Five Tips for Creating a Culture of Security Awareness at Work 2015.10.15 https://securityintelligence.com/top-five-tips-for-creating-a-culture-of-security-awareness-at-work/ elérhető: 2018.06.09

[72] Gwen GREENE, John D'ARCY - Assessing the Impact of Security Culture and the Employee-Organization Relationship on IS Security Compliance https://www.albany.edu/iasymposium/proceedings/2010/14-Greene&D%27Arcy.pdf elérhető: 2018.06.09

[73] Juhee KWON and M. Eric JOHNSON - Security Resources, Capabilities And Cultural Values: Links To Security Performance And Compliance

http://www.econinfosec.org/archive/weis2012/papers/Kwon_WEIS2012.pdf elérhető: 2018.06.09

[74] Gabriella ELVIN, Elin JOHANSSON - The impact of organizational culture on information security during development and management of IT systems, A comparative study between Japanese and Swedish banking industry, 2017.06, ISSN: 1650-8319, UPTEC STS 17019 http://www.diva-portal.org/smash/get/diva2:1112265/FULLTEXT01.pdf

[75] Human Behavior and Security Culture, Managing Information Risk through a Better Understanding of Human Culture, 2011, Ciso Workshop http://exec.tuck.dartmouth.edu/downloads/623/human_behavior_and_security_culture_ciso_workshop_overview.pdf elérhető: 2018.06.09

[76] Enrique CLAVER, Juan LLOPIS and M. Reyes GONZÁLEZ - The Performance Of Information Systems Through Organizational Culture https://pdfs.semanticscholar.org/3862/94e7b39874db15a779ea847cdba63e0537ba.pdf elérhető: 2018.06.09

[77] JOHANSSON, Björn; MEDINA, Ramino; Musabasic, MUAMER; Vukicevic, Stefan - The role of organizational culture on ERP implementation, Published in: Proceedings of The International Workshop of Information Technology and Internet Finance, 2014.01.01 Lund University http://portal.research.lu.se/portal/files/6254527/4778738.pdf elérhető: 2018.06.09

[78] Michael GALLIVAN, Mark SRITE - Information technology and culture: Identifying fragmentary and holistic perspectives of culture, 2005.02.08, doi:10.1016/j.infoandorg.2005.02.005 Elsevier, Information and Organization, pp 295-338
http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.571.6961&rep=rep1&type=pdf elérhető: 2018.06.09

[79] Dr. MICHELBERGER Pál, LÁBODI Csaba - Vállalati információbiztonság szervezése 2012, http://kgk.uni-obuda.hu/sites/default/files/10_Michelberger_Labodi.pdf elérhető: 2018.06.09

[80] Ji-Yeu PARK, Robles, Rosslin JOHN, Chang-Hwa HONG, Sang-Soo YEO, Ai-hoon KIM - IT Security Strategies for SME's, International Journal of Software Engineering and its Applications, Vol. 2. No. 3., 2008.07.10, pp. 91-98

[81] Daniel Yaw DUSHIE - Business Continuity Planning: An Empirical Study of Factors that Hinder Effective Disaster Preparedness of Businesses, Journal of Economics and Sustainable Development ISSN 2222-1700 (Paper) ISSN 2222-2855 (Online) Vol.5, No.27, 2014 pp.185-192 http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.663.9880&rep=rep1&type=pdf elérhető: 2018.06.09

[82] Ibukunoluwa AKINBOLA - A Step towards Resilience, Creating a Business Continuity Plan for WhiteRock Finland KY, 2018 Laurea University of Applied Sciences https://www.theseus.fi/bitstream/handle/10024/143538/Thesis%20Deborah%20Akinbola.pdf?sequence=1 elérhető: 2018.06.09

[83] Stephanie BALAOURAS - The State of Business Continuity Preparedness, Forrester Research, Disaster Recovery Journal, Winter 2015 http://drj.com/images/surveys_pdf/forrester/2014-Forrester-Survey.pdf elérhető: 2018.06.09

[84] ISO 27001 2013 A7 Human Resource Security Part 1- by Software development company in India, https://www.slideshare.net/Hitz_I4/iso-27001-2013-a6-human-resource-security-part-1 elérhető: 2018.06.09

[85] Vishal SALVI - Information Security Management at HDFC Bank: Contribution of Seven EnablersVolume 1, January 2014

[86] Dirk Steuperaert - COBIT 5 as IT Governance Framework and Implementation Method – A Literature Mapping, CEUR Workshop Proceedings, Vol.2027, PoEM 2017 Doctoral Consortium and Industry Track Papers, Conference on the Practice of Enterprise Modelling (PoEM 2017), Leuven, Belgium, November 22-24, 2017. Edited by: Jolita Ralyté, Ben Roelens, Serge Demeyer pp 58 - 69, http://ceur-ws.org/Vol-2027/paper23.pdf, elérhető: 2019. 02. 08.

[87] https://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=1&cad=rja&uact=8&ved=2ahUKEwjBhZL8q6zgAhURZlAKHQxxDYwQFjAAegQIBxAC&url=https

%3A%2F%2Fwww.digitaliser.dk%2Fresource%2F425296%2Fartefact%2FCobitControlPractices.pdf%3Fartefact%3Dtrue%26PID%3D425298&usg=AOvVaw1fuVuKTcUYYCu7BEyaRb99

[88] PO7 Manage IT Human Resources, Process Description, ISACA, https://www.isaca.org/popup/Pages/PO7-Manage-IT-Human-Resources.aspx elérhető: 2018.06.09

[89] DS7 Educate and Train Users, Process Description, ISACA https://www.isaca.org/popup/Pages/DS7-Educate-and-Train-Users.aspx elérhető: 2018.06.09

[90] RUBÓCZKI Edit - How to develop cloud security awareness Applied Computational Intelligence and Informatics (SACI), 2015 IEEE 10th Jubilee International Symposium on pp. 323-326, 2015

[91] Laura SHIN - Work From Home 2018: The Top 100 Companies For Remote Jobs, 2018.01.17, Forbes Research https://www.forbes.com/sites/laurashin/2018/01/17/work-from-home-2018-the-top-100-companies-for-remote-jobs/#3070047376f0 elérhető: 2018.06.09

[92] Pavló Péter - Nem csak álom, hogy otthonról dolgozhat – ha bírja, 2014.04.28 http://hvg.hu/tudomany/20140428_nem_csak_alom_egyre_tobben_egyre_tobbszor elérhető: 2018.06.09

[93] Industry's Largest Cloud Survey Reveals Cloud Momentum Driving Enterprise To 'Re-Orchestrate' Strategy, North Bridge Research, 2016 http://www.northbridge.com/industry's-largest-cloud-survey-reveals-cloud-momentum-driving-enterprise-'re-orchestrate'-strategy elérhető: 2018.06.09

[94] Cisco Global Cloud Index: Forecast and Methodology, 2016–2021 White Paper, 2018.02.01, Document ID:1513879861264127 https://www.cisco.com/c/en/us/solutions/collateral/service-provider/global-cloud-index-gci/white-paper-c11-738085.html, elérhető: 2018.06.09

[95] Joachim MAYER - Reducing total cost of ownership with cloud ERP solutions, Outperform Your Competition, 2017.05.11 https://blogs.dxc.technology/2017/05/11/reducing-total-cost-of-ownership-with-cloud-erp-solutions/ elérhető: 2018.06.09

[96] 12 Benefits of Cloud Computing, https://www.salesforce.com/hub/technology/benefits-of-cloud/ elérhető: 2018.06.09

[97] Aleks PETERSON - The Real Dangers of Shadow IT, 2014.11.19 http://technologyadvice.com/blog/information-technology/real-dangers-of-shadow-it/ elérhető: 2018.06.09

[98] Travis Wilkins - The Hidden Dangers of Shadow IT to Cloud Security, 2017.12.05, https://www.threatstack.com/blog/the-hidden-dangers-of-shadow-it-to-cloud-security elérhető: 2018.06.09

[99] HORVÁTH Zsolt – Az információbiztonság alapjai, IBIR kézikönyv, Óbudai Egyetemi jegyzet, (V.01. / 2016-09-03),

[100] Cisco Global Cloud Index: Forecast and Methodology, 2016–2021 White Paper, Document ID:1513879861264127, 2018, 02.01 https://www.cisco.com/c/en/us/solutions/collateral/service-provider/global-cloud-index-gci/white-paper-c11-738085.html elérhető: 2018.06.09

[101] Karel Vandenbroucke, Denzil Ferreira, Jorge Goncalves, Vassilis Kostakos, Katrien De Moor - Mobile Cloud Storage: A Contextual Experience, MobileHCI 2014, Sept. 23–26, 2014, Toronto, ON, CA, pp 101-110, http://ubicomp.oulu.fi/files/mobilehci14b.pdf elérhető: 2018.06.09

[102] Rania EL-GAZZAR. A Literature Review on Cloud Computing Adoption Issues in Enterprises. Birgitta Bergvall-Kåreborn; Peter Axel Nielsen. Transfer and Diffusion of IT (TDIT), Jun 2014, Aalborg, Denmark.Springer, IFIP Advances in Information and Communication Technology, AICT-429, pp.214- 242, 2014, Creating Value for All Through IT. <10.1007/978-3-662-43459-8_14>. <hal-01381189>, https://hal.inria.fr/hal-01381189/document elérhető: 2018.06.09

[103] Factors Influencing Users' Willingness to Use Cloud Computing Services: An Empirical Study, https://www.researchgate.net/publication/281103865_Factors_Influencing_Users%27_Willingness_to_Use_Cloud_Computing_Services_An_Empirical_Study elérhető: 2018.06.09

[104] GÁLFFY Csaba - Bankok a felhőben, 2013. szeptember 25. https://www.hwsw.hu/hirek/51010/eurocloud-day-felho-iaas-paas-saas-biztonsag-bank-informatika.html elérhető: 2018.06.09

[105] Arthur RAHUMED, Henry C. H. CHEN, Yang TANG, Patrick P. C. LEE, and John C. S. LUI - A Secure Cloud Backup System with Assured Deletion and Version Control, DOI: 10.1109/ICPPW.2011.17 · Source: DBLP, 2011.09.16 https://www.researchgate.net/publication/221617563_A_Secure_Cloud_Backup_System_with_Assured_Deletion_and_Version_Control elérhető: 2018.06.09

[106] Global Cloud Backup Market Research Report- Forecast 2023, ID: MRFR/SEM/2274-HCRR, 2018.06.01 https://www.marketresearchfuture.com/reports/cloud-backup-market-3152 elérhető: 2018.06.09

[107] Schulze, Holger - Insider Threat, CA Technologies, Cybersecurity Insiders, 2018 Insider Threat Report, https://www.ca.com/content/dam/ca/us/files/ebook/insider-threat-report.pdf, elérhető: 2019. 02. 08.

[108] The Human Factor, 2017, Proofprint Report,

[109] " A felhasználó a bűnözők legjobb szövetségese? " című online cikk-Biztonsagportal.hu - 2016.03.01. https://biztonsagportal.hu/a-felhasznalo-a-bunozok-legjobb-szovetsegese.html elérhető: 2018.06.09

[110] BOURNE, James - Why human error is still the biggest risk to your cloud system going down, 2015.06.05, https://www.cloudcomputing-news.net/news/2015/jun/05/why-human-error-still-biggest-risk-your-cloud-system-going-down/ elérhető: 2018.06.09

[111] Cloud at Risk From Security, Management and Compliance Failings, WinMagic Research Centre, 2018. január 9. https://www.winmagic.com/corporate/press-releases/winmagic-research-finds-cloud-workloads-at-risk-from-security-management-and-compliance-failings, elérhető: 2019.02.08

[112] Cloud Threat Report, Keeping Pace at Scale: The Impact of the Cloud-enabled Workplace on Cybrsecurity Strategies, Oracle and KPMG, 2018. https://assets.kpmg/content/dam/kpmg/kz/pdf/Oracle-and-KPMG-Cloud-Threat-Report_2018_Limited.pdf elérhető: 2019. 02. 08.

[113] FALCON, Allen - The Human Risk with Cloud Storage 2015.10.09, http://www.cumulusglobal.com/the-human-risk-with-cloud-storage/] elérhető: 2018.06.09

[114] ZICHERMANN, Gabe – Gamification, Az üzleti játékok forradalmasítása, Játékosítás a piaci verseny leküzdésére, Z-Press Kiadó, 2013, ISBN 978 963 9493 69 8

[115] VYGOTSKY, L. (1978). The Role of Play in Development (pp. 92-104). In Mind in Society. (Trans. M. Cole). Cambridge, MA: Harvard University Press.https://www.colorado.edu/physics/EducationIssues/T&LPhys/PDFs/vygot_chap7.pdf elérhető: 2018.06.10

[116] VASSEL, Tahlia - Socio-Cultural Rules and Roles of games in Play- Vygotsky Perspectives, 2014.04.29. https://prezi.com/mx-qxze4w3xc/socio-cultural-rules-and-roles-of-games-in-play-vygotsky-perspectives/ elérhető: 2018.06.10

[117] LANGFORD, Peter E. - Vygotsky's Developmental and Educational Psychology, Psychology Press, New York, 2005, ISBN 0-203-49957-3 Master e-book, ISBN 0-203-59516-5 (Adobe eReader Format) https://zodml.org/sites/default/files/%5BPeter_E._Langford%5D_Vygotsky%27s_Developmental_and_E_0.pdf elérhető: 2018.06.10

[118] HARLOW, H.F. (1953): Motivation as a Factor in the Acquisition of New Responses, In Current Theory and Research on Motivation. Lincoln: University of Nebraska Press 46

[119] CSÍKSZENTMIHÁLYI Mihály – Flow, az áramlat, a tökéletes élmény pszichológiája, Akadémiai Kiadó, 1997, ISBN 978 963 05 8833 1

[120] FROMANN Richárd – Játékoslét, a Gamifikáció világa, Typotex Kiadó, 2017, ISBN 978 963 279 954 4

[121] RAB Árpád – A gamifikáció lehetőségei a nem üzleti célú felhasználások területén, különös tekintettel a közép- és felsőoktatásra. Oktatás-Informatika, 4. 1-2 sz., 2013, http://www.oktats-informatika.hu/2013/03/rab-arpad-a-gamifikacio-lehetosegei-a-nem-uzleti-celu-felhasznalasok-teruleten-kulonos-tekintettel-a-kozep-es-felsooktatasra elérhető: 2018.06.10

[122] – PINK, Daniel – Motiváció 3.0, Ösztönzés másképp, 2010, HVG Kiadó, ISBN 978 963 30 4 020 1

[123] Pszichológia és Személyiségfejlesztés Tananyag, 2013 https://www.tankonyvtar.hu/hu/tartalom/tamop412b2/2013-0002_pszichologia_es_szemelyisegfejlesztes_i/tananyag/JEGYZET-07-1.3._A_pszichologia_iranyzata.scorml elérhető: 2018.06.10

[124] Jacob HANCHAR - VYGOTSKY, Cognitive Flow and Gameplay, 2014.05.03 https://www.digitaldreamlabs.com/blog/vygotsky-cognitive-flow-gameplay/ elérhető: 2018.06.10

[125] Viola LLOYD, A brief history of Gamification, Extract from Dan's whitepaper:

Gamification in e-learning, 201403.25 https://www.thehrdirector.com/features/gamification/a-brief-history-of-gamification/ elérhető: 2018.06.10

[126] CASTRO-SÁNCHEZ, Enrique; KYRATSIS, Yiannis; IWAMI, Michiyo; RAWSON, Timothy M.; HOLMES, Alison H. (2016-01-01). "Serious electronic games as behavioural change interventions in healthcare-associated infections and infection prevention and control: a scoping review of the literature and future directions". Antimicrobial Resistance and Infection Control. 5: 34. doi:10.1186/s13756-016-0137-0. PMC 5062920 . PMID 27777755 https://www.ncbi.nlm.nih.gov/pmc/articles/PMC5062920 elérhető: 2018.06.10

[127] Sebastian DETERDING; Dan DIXON; Rilla KHALED; Lennart NACKE (2011). From game design elements to gamefulness: Defining "gamification". Proceedings of the 15th International Academic MindTrek Conference. pp. 9–15. doi:10.1145/2181037.2181040

[128] LISTER, Cameron; WEST, Joshua H; CANNON, Ben; SAX, Tyler; BRODEGARD, David (2014-08-04). "Just a Fad? Gamification in Health and Fitness Apps". JMIR Serious Games. 2 (2): e9. doi:10.2196/games.3413. http://games.jmir.org/2014/2/e9 elérhető: 2018.06.10

[129] RUBÓCZKI Edit - Intenzív játékélmény a cloud biztonság tudatosságának eszközeként, In: Rajnai Zoltán, Fregán Beatrix, Marosné Kuna Zsuzsanna (szerk.), Tanulmánykötet a 7. BBK előadásaiból. 492 p.

Konferencia helye, ideje: Budapest, Magyarország, 2016.05.19-2016.05.20. Budapest: Óbudai Egyetem, Bánki Donát Gépész és Biztonságtechnikai Mérnöki Kar, 2016. pp. 199-203.,

[130] Thomas, OWEN (October 5, 2010). "Should you run your business like a game?". Venture Beat. https://venturebeat.com/2010/10/05/gamification-business/ elérhető: 2018.06.10

[131] GRACE, Lindsay. "Gamifying Archives, A Study of Docugames as a Preservation Medium". Computer Games (CGAMES), 2011 16th International Conference on. IEEE Press. Retrieved 13 September 2016. http://ieeexplore.ieee.org/xpl/articleDetails.jsp?arnumber=6000335 elérhető: 2018.06.10

[132] Luis von AHN, Laura DABBISH – Designing Games with Purpose, DOI: 10.1145/1378704.1378719 , Communication of the ACM, 2008.08, Vol.51., No.8. pp 58-67 https://www.cs.cmu.edu/~biglou/GWAP_CACM.pdf elérhető: 2018.06.10

[133] MCGONIGAL, Jane - Be a Gamer, Save the World , 2011.01.22 http://myweb.uiowa.edu/dlgould/lifeclas/docs/Be%20a%20Gamer,%20Save%20the%20World%20(1.22.11)docx.pdf

[134] MCGONIGAL, Jane – Reality is Broken: Why Games Make Us Better and How They Can Change The World, New York, The Penuin Press, 2011, ISBN 978 014 312 061 2

[135] YEE, Nick – The Psychology of Massively Multi-User Online Role-Playing Games, http://vhil.stanford.edu/pubs/2006/yee-psychology-mmorpg.pdf elérhető: 2018.06.10

[136] C. Shawn GREEN & Daphne BAVELIER - Action video game modifies visual selective attention, 2003 Nature Publishing Group, NATURE, VOL 423, 2003.05.29, pp 534-537 https://www.cin.ucsf.edu/~houde/coleman/green.pdf elérhető: 2018.06.10

[137] Daphne BAVELIER, C. Shawn GREEN, Doug Hyun HAN, Perry F. RENSHAW, Michael M. MERZENICH and Douglas A. GENTILE - Brains on video games - NATURE REVIEWS | NEUROSCIENCE, VOLUME 12, 2011.12., Macmillan Publishers, pp 763-768 http://drdouglas.org/drdpdfs/Nature2011.pdf elérhető: 2018.06.10

[138] HUIZINGA – Homo ludens: Kísérlet a kultúra játékelemeinek meghatározására, Budapest, Atheneum, 1944 ISBN 963-385-033-2

[139] FROMANN Richárd – Gamification – Épülőben a Homo Ludens társadalma? pp11-24, 2012, http://jatekoslet.hu/letoltes/publikaciok-fiatalkutatok.pdf elérhető: 2018.06.10

[140] FROMANN Richárd - http://jatekoslet.hu/letoltes/publikaciok-gamification.pdf, Huizinga és McGonigal kapcsolata Fromann könyv 169.o) World Without Oil Game - McGonigal

[141] Jane MCGONIGAL - 'This Is Not a Game': Immersive Aesthetics and Collective Play, MelbourneDAC 2003, https://janemcgonigal.files.wordpress.com/2010/12/mcgonigal-jane-this-is-not-a-game.pdf elérhető: 2018.06.10

[142] FUCHS, Mathias; FIZEK, Sonia; RUFFINO, Paolo; SCHRAPE, Niklas, eds. (2014). Rethinking Gamification. meson-press. ISBN 978-3-95796-000-9.

[143] Brendan READ, "Microsoft Uses Gamification to Boost Performance, Skills and Communication across Thousands of Agents" (PDF). Frost & Sullivan 2016. http://www.gameffective.com/wp-content/uploads/FS_CS_GamEffective-AgentProductivity_BBR_112916_CAM-v2.pdf elérhető: 2018.06.10

[144] CAVALLI, Ernest - Boy Survives Moose Attack Thanks To World Of Warcraft, Wired Magazine, 2007. december 6., https://www.wired.com/2007/12/boy-survives-mo/ elérhető: 2018.06.10

[145] MENSVOORT, Van - Norwegian boy saves sister from moose attack using world of warcraft skills, https://www.nextnature.net/2010/05/norwegian-boy-saves-sister-from-moose-attack-with-world-of-warcraft-skills/ Next Nature, 2010. május 31. elérhető: 2018.06.10

[146] MEZOFF, Lori - Army Game's Medic Training Helps Save Two Lives 2008. január 22., US Army Online Magazin, https://www.army.mil/article/7065/army_games_medic_training_helps_save_two_lives, elérhető: 2018.06.10

[147] Adults' media use and attitudes Report 2017.06., Ofcom Research Document, https://www.ofcom.org.uk/__data/assets/pdf_file/0020/102755/adults-media-use-attitudes-2017.pdf elérhető: 2018.06.10

[148] WRIGHT, T.P., "Factors Affecting the Cost of Airplanes", Journal of Aeronautical Sciences, 3(4) (1936): 122–128.

[149] RITTER, F. E., & SCHOOLER, L. J. The learning curve. In International Encyclopedia of the Social and Behavioral Sciences, 2002.11.22, 8602-8605. Amsterdam: Pergamon, http://ritter.ist.psu.edu/papers/ritterS01.pdf elérhető: 2018.06.10

[150] NEWELL, A., & ROSENBLOOM, P. S. (1981). Mechanisms of skill acquisition and the law of practice. In J. R. Anderson (Ed.), Cognitive skills and their acquisition. 1-51. Hillsdale, NJ: Lawrence Erlbaum Associates, Inc.

[151] RAB Árpád - Digitális kultúra – A digitalizált és a digitális platformon létrejött kultúra. 2007, In R. Pintér (Ed.), Az információs társadalom. Az elmélettől a politikai gyakorlatig. Budapest: Gondolat - INFONIA.

[152] RAB Árpád – A digitális kultúra hatása az emberi viselkedésre a gamifikáció példáján keresztül, 2015, Doktori Értekezés, Corvinus Egyetem, Szociológia Intézet, http://phd.lib.uni-corvinus.hu/916/1/Rab_Arpad.pdf

[153] RAB Árpád - Digitális kultúra, A digitalizált és a digitális platformon létrejött kultúra In: Az információs társadalom, Tankönyv: Gondolat, Új Mandátum 2007 pp. 182---201

[154] RAB Árpád - A gamifikáció lehetőségei a nem üzleti célú felhasználások területén, különös tekintettel a közép---és felsőoktatásra In: Oktatás--- Informatika 2012/1---2.

[155] RUBÓCZKI Edit - Serious Games Experience in Teaching Cloud Security; ICERI 2016., ISBN: 978-84-617-5895-1

[156] Stemper Balázs - Játékosítás alkalmazása a munkavállalói elismerés és elkötelezettség növelésére, Országos Tudományos Diákköri Konferencia, Budapesti Műszaki és Gazdaságtudományi Egyetem, Nemzetközi gazdálkodás alapszak BA, 2017, https://tdk.bme.hu/GTK/Menelmelet/Gamification-alkalmazasa-a-munkavallaloi

[157] BURKE, B. (2014): Gamify: How Gamification Motivates People to Do Extraordinary Things. Bibliomotion Inc., New York City, New York

[158] MOLLICK, E. – ROTHBARD, N. (2013): Mandatory Fun: Consent, Gamification and the Impact of Games at Work. The Wharton School, University of Pennsylvania, Pennsylvania. elérhető: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2277103

[159] KOLB, David A., (1984) Experiential Learning: Experience as the Source of Learning and Development (2nd Edition), ISBN-13: 978-0133892406

[160] KOLB, David A., (1976) Management and the Learning Process, California Management Review, Vol. XVIII./No.3., pp 21-31

[161] Harvard Online Learning https://online-learning.harvard.edu/ elérhető: 2018.06.10

[162] University of Birmingham online https://landing.birmingham.ac.uk/uob/overview?utm_source=I-%20StudyPortals&utm_medium=ppi&utm_campaign=distancelearning elérhető: 2018.06.10

[163] Online Learning at Boston University https://www.bu.edu/online/ elérhető: 2018.06.10

FÜGGELÉK

Az ENISA, a CSA és az OWASP szervezetek által rangsorolt felhő kockázatok

Kockázat	ENISA rangsor	CSA rangsor	OWASP rangsor
Visszaélés és véletlenszerű használat anonim felhasználók által	-	1	-
Bizonytalan interfészek és alkalmazási programozási felületek (API-k) *- az interfészek és az API-k gyakran anonim hozzáférést, egyértelmű szöveges hitelesítést vagy tartalom továbbítást is lehetővé tesznek*	-	2	-
Rosszindulatú felhasználók *- A felhőszolgáltatók minimális betekintést adnak saját ellátási láncukba, biztonsági menedzsmentjükhöz vagy eseménykezelési folyamataikhoz.*	8	3	-
A megosztott technológiából eredő kockázatok *– egy tenant visszaélhet (véletlenül vagy szándékosan) egy másik tenant biztonságával, teljesítményével.*	3	4	7
Az adatok tulajdonjoga és az elszámoltathatóság kockázata *- a felhőben jelentkező kihívások: adat tulajdonjog, titkosítás, átvitel, működési meghiúsulás, adatvesztés és rendelkezésre állás*	1 (tulajdonjog) 7 (adat törlés)	5	1 (tulajdonjog) 5 (adatvesztés)
Fiók vagy szolgáltatás eltérítés *(beleértve a menedzsment interfészt is) - adathalászat, csalás vagy sérülékenység kihasználása esetén a támadók veszélyeztethetik a titkosságot, az integritást és megbízhatóságot*	5	6	9
Ismeretlen profil kockázata *- A felhőszolgáltatók minimális információt adnak a szolgáltatásuk megfeleléséről, a biztonságról, konfigurációkezelésről, naplózásról és felügyeletről, így az ügyfelek számára ez ismeretlen kockázatot jelent*	-	7	8
Felhasználóazonosító federáció *- Több felhőalapú szolgáltatás szigetként kezelése*	-	-	2
Szabályozói megfelelés *- A szabályozási környezetek országonként és régiókban különböznek, különösen a magánélet tiszteletben tartása tekintetében.*	4	-	3
Üzleti folytonosság és rugalmasság *- melyek a felhő-szolgáltatóra vannak delegálva, és ezért nem feltétlenül megfelelő az ügyfél számára.*	-	-	4

Szolgáltatás és adatintegráció/védelem *– az adatkezelés vagy az adatvédelem sérülésének kockázata az adatátvitel során (a végfelhasználó és az adatközpont, vagy az adatközpontok között)*	6	5 (a korábban említett kockázattal azonos szinten áll)	6
A felhőszolgáltatásokat gyakran használják a tervezés, a fejlesztés és a tesztelés fázisaiban, melyek jellemzően kevésbé ellenőrzöttek.	-	-	10
Beragadni egy szolgáltatási környezetben *– minimális azon eszközök, eljárások, szabványok vagy interfészek megléte, melyek biztosítják az adatok, alkalmazások, szolgáltatások vagy üzleti folyamatok hordozhatóságát egy másik szolgáltatóhoz.*	2	-	-

Kérdőív – Publikus felhőben történő Adatkezelés és a vállalati információbiztonság vizsgálata

Tisztelt Válaszadó!

Kérem, töltse ki a felhőben történő adatkezelést és a vállalati információbiztonságot vizsgáló kérdőívemet, amely kutatási célokat szolgál. A kérdőívre adott válaszait névtelenül és titkosan kezelem, vállalatának nincs módja betekinteni az ön válaszaiba. A kutatás eredményét statisztikai összesítésekben őrzöm meg, utána a kérdőíveket megsemmisítem. Dolgozatomban sem az Ön neve, sem vállalatának neve nem szerepel.

Együttműködését előre is köszönöm.

Rubóczki Edit

1.Demográfiai adatok

1.1 Kérem, adja meg a nemét!

a. Nő b. Férfi

1.2 Kérem, adja meg az életkorát!

b. 22 – 28 év b. 29 - 35 év c. 36 – 44 év d. 45 – 53 év e. 54 év feletti

1.3 Mi a legmagasabb iskolai végzettsége?

c. Középiskola b. Főiskola c. Egyetem

1.4 Kérem, adja meg, hány adatbiztonsággal kapcsolatos képzésen vett részt!

1.5 Kérem, adja meg, a jelenlegi pozíciójában eltöltött idejét!

2.Technológiára vonatkozó kérdések

2.1 Rendelkezik-e a cége által biztosított laptoppal?

a. igen b. nem

2.2 Rendelkezik-e a cége által biztosított okostelefonnal?

b. igen b. nem

2.3 Milyen arányban használja a vállalati laptopot magáncélra? (A magáncélú használatot a vállalata nem tiltja.) Kérem, válaszát százalékban adja meg!

magáncélú használat: …%

2.4 Milyen arányban használja a vállalati okostelefont magáncélra? (A magáncélú használatot a vállalata nem tiltja.) Kérem, válaszát százalékban adja meg!

magáncélú használat: …%

3.Biztonságra vonatkozó kérdések

3.1 A vállalat, ahol ön jelenleg dolgozik, rendelkezik-e adatbiztonságra és információbiztonságra vonatkozó szabályokkal?

igen nem nem tudom

3.2 Amennyiben igen, ez a szabálygyűjtemény az ön számára is elérhető helyen van?

igen nem nem tudom

3.3 Tudja, hol találhatja meg ezt a szabálygyűjteményt?

igen nem

3.4 Kérem, idézzen fel 5 szabályt a vállalati adatbiztonságra és információbiztonságra vonatkozó szabálygyűjteményből!

3.5 Az alábbi pontok közül melyik szerepel a vállalati adatbiztonságra és információbiztonságra vonatkozó szabálygyűjteményben?

	3.5	3.6 Rangsor	3.7 Szabály felidézése
Szóbeli vállalati információk kezelésének szabályai			
Papíralapú dokumentumok kezelésének, tárolásának és megsemmisítésének módja			
A vállalat informatikai rendszereinek használatához kapcsolódó biztonsági szabályok			
Publikus felhőalapú rendszerek használatának vállalati szabályai			
A biztonságos telefonálás vállalati szabályai			
Vállalati szabályok a biztonságos E-mail használatra vonatkozóan			
Jelszókezelés szabályai (jelszó védelme, változtatása, megőrzése, felelőssége)			
Adathordozók, hordozható informatikai eszközök biztonságos használatának vállalati szabályai			
Külső helyszínen történő adattárolás (pl. Google drive) vállalati szabályai			
Szigorúan bizalmas besorolású dokumentumok e-mailben történő kezelésének szabályai			

3.6 Kérem, a fentieket rangsorolja fontosság szerint, a szabályzatban nem szereplő tételnek ne adjon sorszámot!

3.7 Kérem, ismertesse, mit jelentenek a fenti, a 3.4-es kérdésben megfogalmazott szabálykörök!

3.8 Kérem, a fenti felsorolás segítségével fogalmazzon meg három információbiztonsági szabályt, melyeket ön nélkülözhetetlennek tart!

1) .
2) .
3) .

3.9 A mindennapok során mennyire tartja be ezt a három, ön által legfontosnak ítélt szabályt? Kérem, válaszát százalékban adja meg!

1. ….%
2. ….%
3. ….%

3.10 Véleménye szerint a kollégái mennyire tartják be az ön által legfontosabbnak ítélt háromvállalati adatbiztonsági és információbiztonsági szabályokat? Kérem, válaszát százalékban adja meg!

1. ….%
2. ….%
3. ….%

3.11 Véleménye szerint melyiket a legkönnyebb betartani (csak a 3.5-ös válaszában jelölt szabály számát adja meg)?

3.12 Véleménye szerint melyiket a legnehezebb betartani (csak a 3.5-ös válaszában jelölt szabály számát adja meg)?

3.13 Mit tehetne a vállalat annak érdekében, hogy az alkalmazottak betartsák ezeket a szabályokat?

3.14 Ön mennyire veszi komolyan a vállalat vezetése az adat és információbiztonsági szabályok betartását?

1) Lazán állok hozzá
2) Betartom, amit fontosnak tartok
3) Általában betartom a vállalati szabályokat
4) Komolyan veszem a vállalat adat és információbiztonsági szabályait
5) Komolyan veszem és be is tartom azokat

3.15 Mit gondol, ellenőrzik-e, mit csinál a vállalati eszközön, mobilkészüléken, vagy hálózaton?

1) Nem gondolom, hogy erre bárkinek is feladata lenne
2) Már megfordult a fejemben
3) Talán ellenőrzik
4) A legtöbb eszközt figyelik
5) A cégem minden vállalati eszköz forgalmát ellenőrzi

3.16 A vállalati szabályok közül melyeket alkalmazza a magán adatainak és információbiztonságának kialakítására? Soroljon fel néhányat.

3.17 Hány olyan esetről tud az utóbbi két évben, amikor sérült a felhő adatbiztonsága? Mi volt ezeknek az oka? (amennyiben az előző pontban megtalálható, azt írja be)

1) ……. …. esetben
2) …… … esetben

3.18 Ön szerint mennyire növelné a szabálytartást a munkatársak körében, ha tudnák, hogy a rendszergazda rendszeresen ellenőrizi az adatkezelési és a biztonsági szabályok betartását?

1) Mindenképpen javítana a jelenlegi helyzeten
2) Segítheti a biztonságtudatosság növelését
3) Nem tudom
4) Talán
5) Semmilyen összefüggés nincsen a kettő között

3.19 Ön szerint ellenőrzi a rendszergazda a felhőben tárolt adathasználat biztonságát a rendszerbe belépőknél?

a. Igen, gyakran
b. Igen, szúrópróba szerűen
c. Lehet, hogy igen, lehet, hogy nem

d. Nem tartom valószínűnek

e. Semmiképpen sem Úgy tudom, hogy nem

4.Biztonságtudatosság oktatása

4.1 Mit változtatna a meglévő információbiztonsági képzésen, hogy hatékonyabb legyen? (Milyen eszközöket, módszertant, stílust stb., használna?)

4.2 Mennyire tartja hatékonynak a vállalatnál lévő információbiztonsági oktatási programot? (10-es skálán)

4.3 A képzések mely elemeit tartotta hatékonynak?

a. ……..

b. …….

4.4 És melyeket nem?

a. ……

b. …….

4.5 Véleménye szerint milyen gyakran lenne indokolt vállalatánál az információbiztonsági oktatás?

a.negyedévente b.félévente c.évente d.esetenként e.csak a felvételnél (munkába állásnál)

4.6 Szívesen képezné magát információbiztonsági témában?

a. Igen

b. Ha nem túl hosszú a képzés

c. Ha nincs jobb dolgom

d. Általában nem érdekel a téma

e. Nem

4.7 Milyen tényezők veszélyeztetik ön szerint a felhőben kezelt adatok, információk biztonságát?

	Súlyos kockázat	Erős kockázat	Kockázat	Kezelhető kockázat	Nincs jelentősége
a felhasználók, mert nem tartják be a biztonsági szabályokat					
hekkerek, külső támadók					
belső támadók					
vírusok					
az informatikai rendszer hardverének hibái					
az informatikai rendszer szoftverének hibái					
a vállalati folyamatok nem megfelelően működnek					
Egyéb:					

PUBLIKÁCIÓS LISTA

I. Peter Schmidt, Edit Rubóczki

Elektronické testovanie študentov a jeho prepojenie na akademický informačný system

2016. pp. 223-226.

(ISBN:978-80-552-1503-7)

II. Rubóczki Edit

Serious Games Experience in Teaching Cloud Security

International Association of Technology, Education and Development (IATED), 2016. pp. 1388-1393.

(ISBN:978-84-617-5895-1)

III. Rubóczki Edit

Intenzív játékélmény a cloud biztonság tudatosságának eszközeként

2016. pp. 199-203. 2.

(ISBN:978-615-5460-97-5)

IV. Edit Szilvia Rubóczki

New Didactic Methods in Cloud Teaching

ACTA TECHNICA CORVINIENSIS – BULLETIN OF ENGINEERING 8:(3) pp. 81-84. (2015)

V. Z Rajnai, E. Ruboczki

MOVING TOWARDS CLOUD SECURITY

INTERDISCIPLINARY DESCRIPTION OF COMPLEX SYSTEMS 13:(1) pp. 9-14. (2015)

VI. Rubóczki E

Gamification in Developing Cloud Security Awareness

2015. pp. 145-148.

(ISBN:978-86-918815-0-4)

VII. Rubóczki E Sz

How to Develop Cloud Security
10th Jubilee IEEE International Symposium on Applied Computational Intelligence and Informatics (SACI 2015). 572 p.
Place & Time of Conference: Timisoara, Romania, 2015.05.21-2015.05.23. Budapest: Óbudai Egyetem, 2015. pp. 323-326.
(ISBN:978-1-4799-9910-1)

VIII. Rubóczki Edit
Comprehensive Implementation of Cloud Services in Enterprise Environment
In: Gabriela Kristová, Peter Schmidt, Miroslav Hudec, Janette Brixová, Mária Szivosová, Pavol Jurík (szerk.)
Reviewed Proceedings: Fifth International Scientific Videoconference of Scientists and PhD. students or candidates: Trends and Innovations in E- business, Education and Security. 129 p.
Place & Time of Conference: Bratislava, Slovakia, 2015.11.18 Bratislava: University of Economics in Bratislava, 2015. pp. 81-86.
(ISBN:978-80-225-4191-6)

IX. Rubóczki E
Biztonság a felhőben. A publikus felhők biztonsági kérdései
In: Rajnai Zoltán, Fregan Beatrix, Ozsváth Judit (szerk.)
Az 5. Báthory-Brassai Konferencia tanulmánykötetei. 709 p.
Place & Time of Conference: Budapest, Hungary, 2014.05.21-2014.05.22. Budapest: Óbudai Egyetem Biztonságtudományi Doktori Iskola, 2014. pp. 459-466.
1-2. köt.
(ISBN:978-615-5460-38-8)

KÖSZÖNETNYILVÁNÍTÁS

Először is szeretném megköszönni segítségét, kitartását, szakmai hozzáértését és minden bátorítását Prof. Dr. Rajnai Zoltánnak, témavezetőmnek. Köszönöm a közös cikkeket, a felejthetetlen szakmai konferenciákat, és a szakmai iránymutatását. Voltak pillanatok, amikor jobbnak láttam volna feladni, voltak kétségeimmel magammal szemben, de ő mindig megtalálta azokat a szavakat, amikkel új erőre kaptam, és végül sikerült idáig eljutnom. Mert messziről indultam.

Köszönöm a családomnak, hogy mellettem álltak, hogy hagytak időt arra, hogy az értekezésem elkészülhessen. Ez az öt év számukra is lemondásokkal járt, sok olyan gyerekrajz készült ebben az időszakban, ami Anyát ábrázolja németórán, vagy cikkírás közben. Külön köszönök mindent férjemnek, aki teljes mellszélességgel hagyta, hogy azt tehessek, amit valóban szeretnék. Köszönöm férjem szüleinek a támogatásukat, a gyerekkel eltöltött idejüket, és a gyerekek étkeztetését, ami nálunk nem kis feladat.

Köszönöm Dr. Suplicz Sándornak a kutatásomban való segítségét. Bármikor és bármilyen kérdés esetén számíthattam rá, az ő segítségével sikerült pontosabb, strukturáltabb, a doktori iskolákhoz méltó értekezést készítenem.

Köszönöm Dr. Velencei Jolánnak mindenfajta támogatását! Köszönöm a közösen felrajzolt MindMap-eket, a kutatói szemléletem kialakítását, amin azért van még mit csiszolni, és a bátorító szavait.

Köszönöm Hronyecz Erikának, Magócsi Grétának és Lévay Katalinnak az iskolai adminisztrációm kezelését, mert ebben különösen nagy segítségre szorultam.

Köszönöm Dr. Szenes Katalinnak, és Dr. Danyi Pálnak, hogy elolvasták az értekezésemet és értékes megjegyzésekkel segítettek annak javításában, néhol újragondolásában.

Köszönöm azoknak a nagyvállalatoknak, akik a kutatásom során segítségemre voltak, és kíváncsian várták, mi sül ki belőle. Itt szeretném megköszönni minden olyan kutató korábbi munkáját, amiket forrásként használtam, és hatással voltak a dolgozatom elkészítésére.

És végül köszönöm minden barátomnak, akik mellettem álltak ezalatt a hosszú munka alatt, és a maguk módján rengeteget segítettek abban, hogy elkészüljek ezzel az értekezéssel.