ÓBUDAI EGYETEM
ÓBUDA UNIVERSITY

DOKTORI (PHD) ÉRTEKEZÉSTERVEZET

FEHÉR-POLGÁR PÁL

Biztonsági stratégia kialakítása saját tulajdonú mobileszközök használatára döntéstámogató keretrendszer kialakításával

Témavezető:

Prof. Dr. Michelberger Pál

BIZTONSÁGTUDOMÁNYI DOKTORI ISKOLA

Budapest, 2023. április 5.

TARTALOMJEGYZÉK

BEVEZETÉS

Ma már el sem tudjuk képzelni mindennapjainkat okoseszközeink nélkül. Úton-útfélen gyakran belebotlunk olyan emberekbe, – akár szó szerint is – akik a nap 24 óráján keresztül végzik munkájukat hordozható eszközeiken. Ezen belül is széles körben elterjedtek az olyan vállalati megoldások, melyeknél a munkavállaló saját tulajdonú eszközét – leggyakrabban okostelefonját – nemcsak saját, személyes céljaira, de munkahelyi feladataira is használja, szinte hely- és időkorlát nélkül.

Az elmúlt két évtized alatt informatikai eszközök sora hódította meg munkahelyeinket, irodáinkat, otthonainkat. Kiterjesztve szórakozási, kapcsolattartási és munkavégzési lehetőségeinket.

A kétezres évek elején megjelenő okostelefonok nem csak az állandó kapcsolattartást, az internet – szinte – bárhonnani elérését hozták magukkal., hanem a bárhonnan bármikor történő munkavégzést is.

A mobileszközök méretüket és árukat tekintve teljesítményarányosan egyre kisebbek, kapacitásuk és képességeik pedig egyre jobbak lettek. A mobil távközlési hálózat teljesítménye, sávszélessége és lefedettsége folyamatosan javul. A mobileszközök vállalati célra történő alkalmazása megkerülhetetlen. [1] [2] Az információvédelmi lehetőségek azonban korlátozottak. [3] [4] Az erős titkosítás és a hitelesítés nem mindig jelent magasabb szintű védelmet. A mobileszközök számos (meta)adatot küldenek el a kommunikáció során (például fizikai hely koordinátái, környezeti paraméterek, sebesség és gyorsulási adatok, hálózati partnerek elérhetősége). A mobil kommunikáció, ill. annak lehallgatása szinte ellenőrizhetetlen (rádióforgalmazás, például Bluetooth lehallgatása). A telefonbeszélgetés esetén pedig maga a hang is adatnak számít. [5] [6] [7]

A mobilinformatikai eszközök (okostelefonok és tabletek) mára olyan széleskörűen elterjedtek, ami alapján kijelenthetjük: a mindennapjaink nélkülözhetetlen(nek hitt) részeivé váltak.

Ezeken az eszközökön olvasunk, tanulunk, szórakozunk és dolgozunk, tartjuk a kapcsolatot az ismerősökkel és intézzük a hivatalos ügyeket. Ily módon mind a magán, mind a munkahelyi életünknek szerves részei, s ma már teljesen természetesnek vesszük használatukat.

Felmerülnek azonban kétségek: Ennek a természetességnek, kényelemnek része-e a biztonságtudatos használat? Törődünk-e ezen eszközök, és az azokon elérhető, tárolható – akár magán, akár munkával összefüggő, munkahelyi – adatok, információk biztonságával?

A BYOD (Bring your own device - „hozd a saját eszközöd") ebben a kontextusban a saját tulajdonú mobileszközök munkacélú használatát jelenti. Vagyis ezeken a nem vállalati tulajdonú eszközökön keresztül a munkahelyi erőforrások, mint például vállalati adatok, vállalat irányítási rendszerek, vállalati felhő stb. elérését.

S mint minden, a vállalati adatokkal kapcsolatos folyamatot, így az ilyen célú hozzáférést is szabályozni, felügyelni szükséges.

Az emberek nagy része manapság már nem élheti az életét okoseszközök nélkül. Egy részük munkához is táblagépeket, okoseszközöket használ. Egy részük pedig a saját tulajdonú eszközét használja munkavégzés céljára is a magán használat mellett. Jó példa az ilyen munkavégzésre, hogy az ember úton, ingázás közben is letölti munkahelyi e-mailjeit, vagy akár hozzáférve a vállalati információs rendszerhez, kritikus üzleti adatokkal dolgozik. Vagy éppen akár személyes adatokhoz, vagy más védendő adatokhoz férhet hozzá, miután persze ugyanarról az eszközről hozzáfért valamely, vagy az összes, közösségi alkalmazásához.

Rengeteg ember így lényegében idő- és térbeli határok nélkül képes munkát végezni. Annak ellenére, hogy ez kockázatos lehet mind a vállalat, mind pedig a munkavállaló részére, gyakran a vállalkozások ezt nem, vagy nem kellő részletességgel szabályozzák. Ráadásul a legtöbb vállalat még nem is hozott stratégiai döntést a BYOD-ról.

A globalizáció és a növekvő gazdasági aktivitás különösen a fejlődő országokban egyre nagyobb és nagyobb energia- és fogyasztási igényt vált ki, ami általában a környezet károsodásához vezet. Van azonban néhány elmélet, amely úgy véli, a szennyezés problémája megoldódik, amint a fejlődő országok elérik a megfelelő gazdasági szintet, és ez lehetővé tenné számukra, hogy megengedhessék maguknak a környezetbarát technológiákat, valamint a környezetvédelmileg előnyös szabályozást és politikát. [8]

Az elmúlt néhány évben az elektronikus eszközök területén az okoseszközök dinamikus terjedését tapasztaltuk. Először széleskörben elterjedtek az okostelefonok és táblagépek,

majd az elmúlt években az intelligens viselhető eszközök (okosórák, karkötők, szemüvegek, stb.). A biztonság kérdésével foglalkozók körében van egy mondás; a leggyengébb láncszem az ember. [9] [10] [11] [12] Ez az okoseszközök biztonságának területén is feltételezhető. A szervezeti biztonság kérdéskörébe így hangsúlyozottan figyelembe kell venni annak emberi oldal biztonsági jellemzőit, azok mérését, a biztonságtudatosságot és annak szintjét, amelynek javulása csak az oktatással, az emberek tudásának növekedésével érhető el.

Ezek alapján,

1. kutatási célom a BYOD eszközök fogalmának megalkotása, mely segít eligazodni a különböző saját tulajdonú okoseszközök és azok IT infrastruktúrán belüli használatát lehatárolni, valamint megkülönböztetni ezen eszközöket a többi, a szervezetben használt szervezeti vagy saját tulajdonú eszköztől. Tekintettel ezek sajátságos tulajdonságaira, melyeket a definíció megalkotásának folyamata során tárok fel és ismertetek. E kutatásomhoz elsősorban irodalomkutatást kívánok alkalmazni, számos forrás felhasználásával. Ezek közül kiemelném James Gareth cikkét (Smartphone risk: Malicious threats to Smartphones) [13], mely 2004-ben a Network Security című szakfolyóiratban jelent meg, amelyben az okostelefonok használatának biztonsági kérdéseit vetette fel. Ezen felül a további kutatási céljaim eléréséhez végzett primerkutatásom során nem strukturált csoportos interjút is tervezek, mely segít a definíció megalkotásában.

2. kutatási célom a BYOD használat során jelenlévő IT kockázatok rendszerbefoglalása, ezzel segítve a kockázatok azonosítását, másrészt a kockázat becslést, harmadrészt a kockázat minimalizálást átláthatóbbá és kezelhetőbbé tenni. E célom megvalósítására szekunderkutatást tervezek. Kiválasztom a megfelelő, e témában alkalmazható kockázat fogalmat. Több forrást feldolgozva Renn Concepts of risk: a classification [14] című cikkében ismertetett kockázat fogalmat használom munkám során. Korábbi kutatások és ajánlások alapján összegzem és meghatározom azokat a kockázat csoportokat, melyek kifejezetten a BYOD eszközök használatára vonatkoznak és abból következnek. A kockázatkezelés támogatására irodalomkutatás segítségével megvizsgálom és kiválasztom az általam javasolt módszertant. Ezek közül kiemelném Baillette, Barlette és Leclercq-Vandelannoitte "Bring your own device in organizations: Extending the reversed IT adoption logic to security paradoxes for CEOs and end users" [15] és Kadena és Kovács The need for BYOD security strategy [16] című műveit.

3. kutatási célom, hogy a feltárt ismeretek alapján alapstratégiákat fogalmazzak meg a BYOD eszközök használatára. Ehhez döntéstámogatási módszertant tervezek készíteni, mely segíti a döntéshozót választani a lehetséges alapstratégiák közül a korábban ismertetett kockázatcsoportosításra építve. Az alapstratégiák valamint a döntéstámogatási módszertan kialakítása témavezetőmmel Prof. Dr. Michelberger Pállal végzett munkánkra alapul [P10].

4. kutatási célom az IT kockázatvállalási hajlandóság vizsgálata, mert a BYOD okoseszköz használat kiemelkedő kockázatforrása az emberi tényező, így ezt külön is vizsgálni szeretném. S ez alapján kívánok létrehozni egy olyan javaslatot, mely a kockázatvállalási hajlandóság mérhetővé tételét segíti. Ezzel a leendő munkavállalók várható IT kockázatbecslésének mérhetőségét is javítani kívánom. Ehhez egyrészt az emberi tényező feltárására irodalomkutatást tervezek, másrészt tervezem a gyakorlatban is vizsgálni, primer kutatás segítségével (kérdőíves felmérés), az általam az irodalomkutatás eredményeképpen kiválasztott eszköz gyakorlati alkalmazását és eredményeinek kiértékelését.

5. kutatási célom annak vizsgálata, hogy az általam szekunder kutatás alapján választott általános kockázatvállalási hajlandóságot mérő eszköz képes-e az IT biztonsággal kapcsolatos kockázatvállalási hajlandóságot is mérni, s ez alapján javaslatot tenni annak alkalmazására.

Az 4. és az 5. kutatási célomhoz a szakirodalmi kutatásom forrásai közül kiemelném Weber, Blais és Betz A Domain-Specific Risk-Attitude Scale: Measuring Risk Perceptions and Risk Behaviors [17] valamint Blais és Weber A Domain-Specific Risk-Taking (DOSPERT) Scale for Adult Populations [18] műveit, melyekben a szerzők ismertetik a DOSPERT módszertant és annak használatát, amire építve dolgoztam ki a 4. és 5. kutatási célomat.

1 AZ ÚJ GENERÁCIÓ

Dolgozatom során a primerkutatásomat egyetemi hallgatók körében tervezem végezni, mert ők a jelen és a közeljövő munkavállalói, kiknek IT biztonsággal kapcsolatos attitűdje már a jelenben is, de a jövőben kiemelkedően meghatározó lesz a szervezetek IT biztonságában.

1.1 Az új generáció általános jellemzői

Millenniumiak, „ezredfordulósak", digitális bennszülöttek, vagy másnéven az Y és Z generáció, a „we want it now – most akarom" generációja új minőséget hozott magával a technikai és csoportmunka képességeikben, gyorsaságukban és nyitottságukban. A hétköznapokban használt technológiai fejlődés és e generációs változás új igényeket fogalmazott meg, az oktatás s később a munka területén is. Annak érdekében, hogy a biztonság tudatosság irányából elérjük őket, meg kell ismernünk milyen módszerekkel tudjuk elkötelezni ezt a generációt a biztonság felé?

Az új generációk értékrendjét széleskörűen kutatták már, s próbálták meghatározni legfontosabb tulajdonságaikat. [19] A kutatók feltérképezték az ehhez a generációhoz kapcsolódó pszichológiai jelenségeket, amelyek közül a következőkben a legfontosabbakat részletesebben is elemzem:

Sebesség: Az Y és Z generáció tagjait gyakran nevezik "digitális bennszülötteknek". [20] [21] Ezek a fiatalok belenőttek a technológiai fejlődésbe, és könnyedén használják az információs technológia vívmányait. Ha kérdésük van, információra van szükségük, a könyvtár helyett csak "gugliznak", és másodpercek alatt annyi választ találnak, amennyit elődjeik egy egész emberöltő alatt nem tudtak volna felkutatni. Társadalmi és magánéletükről, társaik napi eseményeiről a különböző közösségi médiaplatformokon keresztül valós időben tájékozódnak, és azonnal akarnak, és tudnak is reagálni rájuk.

A személyes kapcsolatok hanyatlása: Az online közösségek átalakították a személyes kapcsolatokat. Ez a leginkább érintett generáció, és általában a modern világban már nem kell valódi levelet írni, ha a másik távol van - elég, ha a valamelyik online felületen küldünk néhány szót. Nem szükséges előre megbeszélni, hogy mikor és hova megyünk - elég bejelentkezni egy weboldalra vagy alkalmazásba, és megnézni, hogy ki van már ott. A folyamatos online jelenlét a személyes életünk megosztását jelenti, ami elvárássá is válik. Aki offline van és hiányzik, könnyen úgy érezheti, hogy mások számára nem

létezik. A "szelfi" korszakban egyre kevésbé fontos a valódi, élő kapcsolat, a közös élmények.

Szabadság és kaland: Ez a generáció erős idegennyelv-tudással rendelkezik, ezért az internet adta lehetőségek lehetővé teszik számukra, hogy akár virtuálisan akár a valóságban is bebarangolják a világot. [22] [23] A fejlett technológiának köszönhetően az internetkapcsolat ma már szinte mindenhol biztosított. Lehetőség nyílik arra, hogy a világ szinte minden országában szabadon utazhassanak, sőt, a legegzotikusabb helyekről dolgozhassanak, miközben "digitális nomádként" határozzák meg magukat. [24]

Egyediség és individualizmus: Megpróbálják meghatározni magukat a megjelenésükön keresztül, és kitűnni a tömegből. Virtuális világukat saját imázsukhoz alakítják, sokan egyre tudatosabban építik online közösségi megjlenésüket. A digitális technológia átalakítja az identitásukat. [25] Mindezt persze a tökéletességre törekedve teszik, csak a legjobb pillanatokat töltik fel és mutatják meg, ami jelentős önértékelési problémákat okoz. [26] Ez még nagyobb versenyt generál az egyének és a közösségi médiaprofiljaik között. Az a "győztes", aki több "like"-ot gyűjtött, szélesebb közönséget ért el és vonzott, ily módon mások irigylik.

Egyszerűség, egyszerűsítés: Jó példa erre a kép- és rövidvideómegosztó weboldalak és alkalmazások, platformok (Instagram, Tumblr, Snapchat, TikTok, stb.) elterjedése, ahol a szöveges tartalom minimális. E generációk tagjai egyre kevesebb offline médiát vagy könyvet olvasnak. Egyre nő az olvasásértéssel küszködők száma. Ha egy szöveg nem fér el a mobil kijelzőjén, túl hosszúnak tűnik az olvasáshoz.

Biztonság: A biztonság nem a kaland ellentéte, hanem a megbízható márkák és csoportok iránti igényt fejezi ki, amely hozzájárul a személyiségük fejlődéséhez. Gyakran online közösségek jelentik számukra a biztonságos, biztos környezetet. Az ezredfordulósok általában igénylik a társas interakciókat, a megerősítést és a támogatást, különösen a társaiktól.

Divat: Az internetnek köszönhetően nagyon gyorsan értesülnek a legújabb trendekről. Minden csoportban vannak az úgynevezett "divatújítók", influencerek, akik modernebbnek, izgalmasabbnak, élvezetesebbnek, színesebbnek és érettebbnek tartják magukat, mint mások, a divatot követők. [19] [27]

FoMo: E generációk tagjainak egy teljesen új jelenséggel kell szembenézniük, ez pedig a FoMo (fear of missing out). Arról a szorongásról van szó, amit akkor érez valaki, amikor mások egy élvezetes, vidám tevékenységet végeznek, míg ő távol van. [28] Negatív hatással van a fiatalok pszichológiai elégedettségére és életminőségére, mivel rengeteg negatív érzést generál, és az egyéneket a közösségi médián keresztül folyamatos versengésre készteti. Az erős hatás miatt nem meglepő, hogy több marketingkampány is erre a félelemre épül, és a következő szavakat, kifejezéseket használja: "ne hagyd ki", "csatlakozz hozzánk" stb.

Az Y generációs egyetemi hallgatók a gyakorlatias tanulást, a csoportmunkát és a technológia használatát részesítik előnyben. [29] [30] Vizuálisan tanulóknak is nevezik őket, akik innovatív megoldásokat követelnek, amelyek gyorsan és könnyen, egy gombnyomással elérhetőek. [31] Közösségi hálózatokhoz tartoznak, és hajlamosak hasonló online platformokat és csatornákat használni az információszerzéshez. Az ECAR The Future of Education felmérésére a válaszadók több mint fele nyilatkozta, hogy bízik online társaiban és iskolatársaiban. 39%-uk arra számít, hogy az oktatás a jövőben még inkább virtuális lesz. [32] [33] Melyet az tesz leginkább lehetővé, hogy e generáció tagjai a technológia ilyen vagy bármilyen más célú használata "könnyed" és "természetes". [21]

Az Y generációs egyetemi hallgatókat „technológiai multitasker”-ekként is jellemzik; vagyis több eszközt és alkalmazást használnak párhuzamosan, amelyek lehetővé teszik számukra, hogy akár munkával kapcsolatos, akár személyes tevékenységeket folytassanak szinte folyamatosan, szinte egyszerre. [20] [21] A felmérés eredménye szerint 24 országból 14-ben a 18-29 évesek legalább fele azt állítja, hogy folyamatosan online van. Azok, akik „neteznek”, általában elkötelezett felhasználókká válnak. A legtöbb vizsgált országban az internetezők fele vagy több mint fele azt állítja, hogy naponta használja az internetet. [34]

Nem meglepő ezek alapján, hogy az egyetemi hallgatók körében is népszerű a "hozd a saját eszközöd" (BYOD) gondolata. A diákok a saját eszközeiket használják, melyeket már jól ismernek. Egy felmérés alapján már 2014-ben az egyetemi hallgatók többsége (86%) rendelkezett okostelefonnal vagy táblagéppel az Egyesült Államokban, [35] erre válaszul a főiskolák és egyetemek meghatározó hányada indította el BYOD-stratégiáját.

Ez a trend hivatalos, támogatási stratégiák nélkül is terjed. [36] [37] A hallgatók hozzászoktak a modern és hatékony IKT-rendszerekkel való munkához, így e tapasztalataik is befolyásolják az oktatási intézményükkel való általános elégedettségüket is. [38]

A fiatalok, az Y generáció tagjai globális világpolgárként gondolnak magukra. Lehet, hogy egy országhoz tartoznak, de személyiségük és tapasztalataik több kultúrán alapul, és sokféle ember, nemzetközi média stb. befolyásolja őket. [39]

Az ezredfordulósok, a "most akarjuk" generáció kritikusabb a technikai kérdésekkel kapcsolatban, és kevésbé türelmes az idő kérdésében. Gyors és kielégítő "azonnali" megoldásokat akarnak. Ezt a vonalat követve könnyen szembesülhetünk egy másik (az előzőhöz hasonlóan fontos) jelenséggel, a digitális kultúrsokkkal.

Bár az IKT-eszközök, és -rendszerek bizonyos tekintetben univerzálisak vagy globálisak, e generáció tagjait fogadó intézményben (felsőoktatásban vagy munkahelyen) bizonyos nehézségeket tapasztalhatnak, amikor szembesülnek a helyi beállításokkal, a számítógépek számával vagy sebességével, a hozzáférhetőséggel. Korlátozott hozzáférések, mind időben, mind tartalomban, különböző szoftverek, és platformok elérhetőségével, valamint olyan jelszavakkal és szabályokkal, melyek az informatikai szolgáltatások használatához szükségesek. [38]

E problémák és nehézségek negatív tapasztalatok lehetnek e generációnak, ami pedig akár a ShadowIT (árnyék informatikai rendszer) kialakulásához vezethet. A ShadowIT a szervezet által kialakított, szabályozott és üzemeltetett vállalati informatikai rendszer(ek) mellett és/vagy helyett a munkavállaló(k) által kialakított informatikai megoldásokat jelentenek, melyek többek között biztonsági kockázatokat rejthetnek magukban, de akár a folyamatoptimalizáció forrása is lehet. [40] [41]

1.2 Az új generáció okostelefon-használati szokásai

Az elmúlt években több kutatásomban is foglalkoztam a felsőoktatásban résztvevő hallgatók, okostelefonhasználati szokásaival. E fejezetben ezeket fogalom összsze.[P1][P2][P3][P4][P5][P6][P8][P12][P13][P14][P15]

Az okostelefon definíciója alatt általánosságban is, és a kutatásaim alapján a válaszadók is, olyan mobiltelefont értenek, amely számítógépszerűen is használható, és amely csatlakozik az internethez. Operációs rendszerrel rendelkezik, amire további, harmadik féltől származó szoftvereket lehet telepíteni. Olyan megjelenítővel rendelkezik, mely lehetővé teszi az általános munkavégzést.

Ahogy az elmúlt 20 évben nőtt az internetképes eszközök elterjedtsége, úgy nőtt a felhasználók igénye az idő- és helyfüggetlen szélessávú adatkapcsolatra. A felhasználók nagy része számára az internetkapcsolat fenntartása személyes és szakmai okokból egyaránt elengedhetetlenné vált. [42]

Már 2015-ben az eNET a felnőttek körében 62%-os internethasználatot mért, és azon belül is 51% használt okostelefont internet elérésre. Az okostelefont használó válaszadók között 94%-ra mérte azok arányát, akik interneteléréssel is használták a telefonjukat. E 94% tovább osztható volt; a válaszadók 36%-a csak WiFi-n keresztül csatlakozott az internethez az eszközéről, és csak 3% mondta azt, hogy kizárólag mobilinternetet használ, WiFi-t nem. Míg a válaszadók többsége, 55% használta mind a kétféle csatlakozási módot. [43]

2022-re az okostelefon-felhasználók száma Magyarországon meghaladta a 6.2 milliót a felnőtt lakosság körében, közülük 6 millióan interneteztek is ezekkel. [44]

A válaszadók első telefonjukhoz átlagosan 12.4 évesen jutottak. A válaszokból megfigyelhető volt, hogy minél idősebb a válaszadó, annál idősebb volt, amikor az első telefonját birtokolta. (Pearson Correl.: 0,767, Sig.: 0,000). A mintából az is megfigyelhető volt, hogy a lányok hamarabb (átlagosan 11.5 évesen) jutottak első okostelefonjukhoz, mint a fiúk (13.1 évesen).

A minta alapján – megállapításaim szerint – csak töredékük használ biztonsági eszközöket mobil eszközein, és csak egy részük gondolkodik az eszközeik informatikai vagy adatbiztonságáról. Általánosságban elmondható, hogy a mobilbiztonsághoz való hozzá-

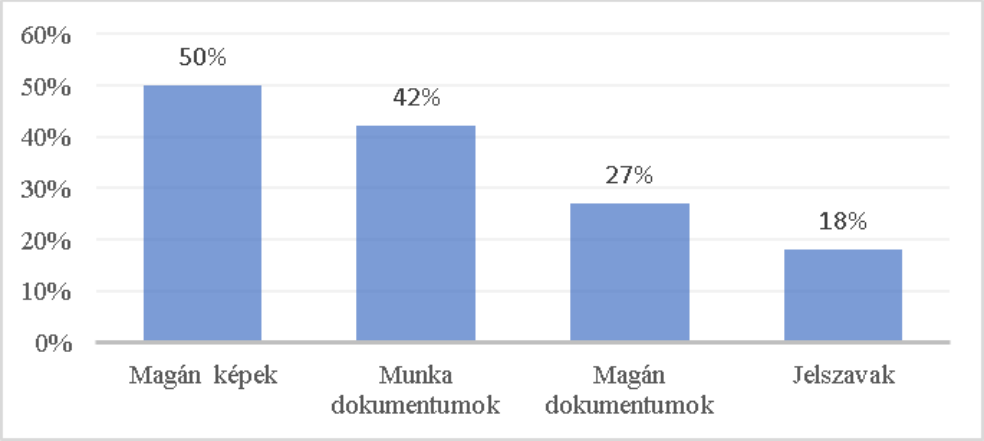
állásuk rossz. Még azok sem, akik már megtapasztalták a mobileszközük elvesztését annak teljes tartalmával együtt, vagy azok sem, akik internetbankot használnak, nem megfelelően felkészültek és/vagy tudatosan nem foglalkoznak a mobiljukat fenyegető veszélyekkel és kockázatokkal.

2013-ban az ENISA, az Európai Unió Információs és Hálózatbiztonsági Ügynöksége felmérte, hogy mik a legnagyobb kockázatok, amelyek az okostelefonokat fenyegetik. A három legfontosabb ezek közül:

1. Adatok kiszivárgása az eszköz elvesztése vagy ellopása miatt.
2. Az adatok akaratlanul történő közzététele.
3. A használt, de nem megfelelően kezelt eszközök támadása, melyekről adatokat szerezhetnek meg támadók. [45]

Az ENISA által azonosított három fő biztonsági kockázati tényezőre tekintettel megkérdeztem a hallgatókat, hogy tárolnak-e adatokat a telefonjaikon, és ha igen, akkor milyen jellegű adatokat tárolnak. [46]

A válaszadók 64%-a tárol számára fontos adatokat a telefonján.



1. ábra A válaszadó okostelefonján tárolt legjellemzőbb típusú adatok a kérdőív válaszai alapján
Forrás: Saját szerkesztés a kérdőíves felmérés alapján

A válaszadók csaknem 60%-a fontos adatokat tárol a telefonján, és 62%-uk készít biztonsági mentést a telefonjáról.

A leggyakrabban tárolt tartalmak a következők voltak:

1. táblázat A válaszadók megoszlása a saját okostelefonjain tárolt tartalmak alapján

	Informatikus hallgatók	Közgazdász hallgatók	IT cég munkavállalói
Partner lista,	69%	62%	67%
Jegyzetek, feladatlista,	57%	53%	57%
Privát képek,	57%	60%	45%
Határidők,	49%	48%	44%
Tanulmányaikhoz és/vagy munkájukhoz kapcsolódó adatok	44%	38%	40%

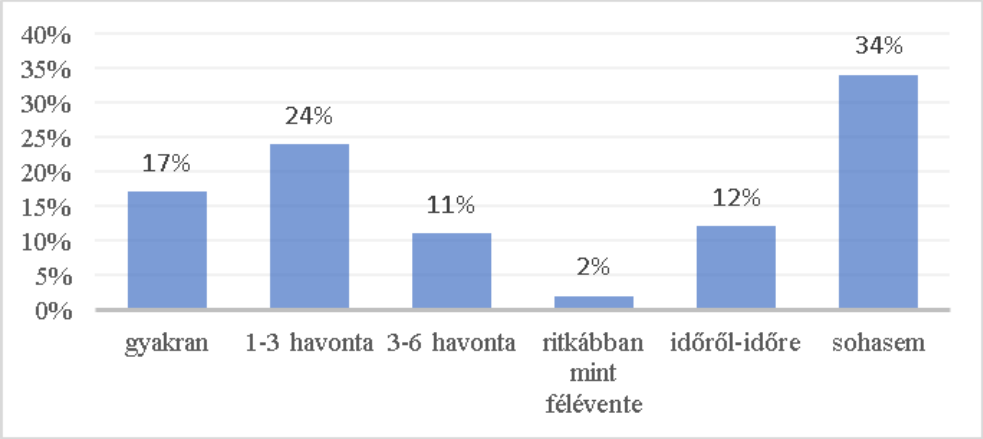
Forrás: Saját szerkesztés a kérdőíves felmérés alapján

A válaszadói csoportok között nem volt szignifikáns különbség. Csak abban a kérdésben figyelhetünk meg eltérést, hogy magánjellegű képeket tárolnak-e a készülékükön.

Mint ebből a felsorolásból is látható, a válaszadók okostelefonjaikon tárolt adatokat biztonsági kockázatok veszélyeztetik, melyek bekövetkezése nem kívánatos eredményekhez vezethetnek, amire az ENISA jelentése is rámutatott.

A kérdőívet kitöltők többsége időről-időre biztonsági mentést készít. A válaszadók 41%-a 3 hónapnál gyakrabban készít biztonsági mentést. Közel egyharmaduk azonban nem készít biztonsági mentést a mobilján tárolt adatokról, ami rossz szokás, hiszen tudjuk, hogy adataink biztonsági mentése az első lépés az adatvesztés megelőzésére.

A válaszadók megoszlását a mobilon végzett biztonsági mentések gyakorisága szerint a következő grafikon mutatja.



2. ábra A válaszadók megoszlása az okostelefonjukról történő biztonsági mentés gyakorisága szerint
Forrás: Saját szerkesztés a kérdőíves felmérés alapján

Bár 86,4%-uk már telepített külső forrásból származó szoftvereket, mindössze 14,5% telepített valamilyen biztonsági eszközt a mobiltelefonjára. A válaszadók csoportjait külön vizsgálva elmondható, hogy azok, akik a dolgoznak, és azok, akik az informatikai karon tanulnak, inkább használnak biztonsági szoftvereket a telefonjukon, de a különbség nem volt szignifikáns.

Feltételeztem, hogy azok, akik fontos adatokat tárolnak a telefonjukon, biztonsági mentést is készítenek. A mintán végzett vizsgálatom eredményeképpen várakozásommal ellentétes módon, nem volt semmiféle összefüggés a fontos adatok tárolása és a biztonsági mentés készítése, illetve annak gyakorisága között. Ez azt jelenti, hogy a mobiltulajdonosok/felhasználók többsége nincs tisztában azzal, hogy milyen veszélyekkel kell szembenéznie, amikor adatokat tárol a mobileszközökön.

Vélelmeztem, hogy azok, akik telefonjukat elvesztették már, vagy ellopták, nem tárolnak fontos adatokat a telefonjukon, vagy legalábbis gyakrabban készítenek biztonsági mentéseket. Az elvégzett vizsgálatok alapján nem mutatkozott összefüggés aközött, hogy akik már megtapasztalták a mobileszközük elvesztését - annak teljes tartalmával együtt - azok gyakrabban készítenének biztonsági mentéseket. Emellett csak gyenge korrelációt találtam a között, hogy ha valaki elveszítette már az eszközét, az kisebb valószínűséggel fog fontos adatot tárolni az eszközén. (Pearson-féle korreláció: -0,205, Szignifikancia szint: 0,002).

Az internetbank használata pénzügyi adatok és biztonsági információk megosztását és továbbítását jelenti a mobileszközön keresztül. Valószínűsítettem, hogy azok, akik ilyen alkalmazásokat használnak, jobban tisztában vannak a biztonsági kockázatokkal, és ennek megfelelően használják eszközeiket, akár a szoftverének gyakori frissítésével, akár speciális biztonsági beállításokkal, harmadikféltől származó biztonsági szoftverek telepítésével. Rendkívül gyenge, de szignifikáns összefüggést tapasztaltam a mintában a válaszadók frissítési szokásai és a mobiltelefonon történő internetbankolás használata között (Pearson-féle korreláció: 0,192, Szignifikancia szint: 0,000). Nem volt azonban összefüggés az internetes bankolás használata és a telefonjukon lévő biztonsági beállítások között.

Feltételeztem, hogy azok, akik mobilinternetet vagy WiFi kapcsolatot használnak telefonjukon, frissítik mobiltelefonjuk operációs szoftverét. Hisz az internet mobilon történő

használata a mobiltelefon szoftverén keresztül történő kapcsolatot jelent távoli kiszolgálókkal, mely kockázatokat rejt magában. A Mobile Pwn2Own 2012 verseny például olyan szoftverhibák felfedésével zárult, amelyek az okostelefonok webböngészőin keresztül távoli kódfuttatáshoz vezethetnek. Ezért a szoftverek folyamatos frissítése elengedhetetlen. Vélelmeztem azt is, hogy akik aktívan használják az internetet a telefonjukon, azok a szoftverüket is frissítik, hogy minimalizálják a szoftversebezhetőségek biztonsági kockázatait. Gyenge összefüggést találtam a mobilhálózaton keresztüli internethasználat és a mobilszoftver frissítése között (Pearson-féle korreláció: 0,234, Szignifikancia szint: 0,000). Másrészt szintén gyenge korrelációt találtam a WiFi-n keresztüli internethasználat és a mobilszoftver frissítése között (Pearson-féle korreláció: 0,317, Szignifikancia szint: 0,000).

Azok a hallgatók, akik fontos adatokat tárolnak a telefonjaikon, különböznek-e a biztonsági kérdésekben társaiktól?
A tárolás kérdését tekintve nem volt kimutatható korreláció semelyik biztonsági kérdéssel, így megállapítható, hogy a mintában nincs kimutatható összefüggés a között, hogy valaki tárol-e a telefonján számára fontos adatot, azzal, hogy hogyan viszonyul a telefonja biztonságához.

Azt viszont statisztikailag igazoltam, hogy a mintában, aki többet használja a telefonját, az nagyobb valószínűséggel tárol is a telefonján biztonsági szempontból is fontos tartalmakat; dokumentumokat (Pearson-féle korreláció: 0,226, Szignifikanciaszint: 0,011), határidőket (Pearson-féle korreláció: 0,298, Szignifikancia szint: 0,001), jelszavakat (Pearsonféle korreláció: 0,241, Szignifikancia szint: 0,006).

Feltártam, hogy azok, akik okostelefont használnak, a telefonjukon valószínűbben tárolnak dokumentumokat, jelszavakat, személyes információkat; (Pearson-féle korreláció: 0,213, Szignifikancia szint: 0,016), (Pearson-féle korreláció: 0,283, Szignifikanciaszint: 0,001), (Pearson-féle korreláció: 0,213, Szignifikancia szint: 0,016).

Igazoltam, hogy azok, akiknek nincs okostelefonjuk, azok inkább tárolnak fontos információkat a telefonjaikon (Pearson-féle korreláció: 0,258, Szignifikancia szint: 0,003). Ez

utóbbi biztonsági szempontból ugyan pozitívnak tekinthető, mert egy „buta telefon” távoli elérésének kockázata kisebb, mint egy okostelefoné, azonban könnyen belátható, hogy mint általános válasz a biztonsági kérdésekre, nem jellemző.

A válaszadók 90%-a rendelkezett okostelefonnal, ez duplája annak az aránynak, amit az adatfelvétel idején a teljes felnőtt lakosságon elvégzett reprezentatív kutatások mutattak. A hallgatók háromnegyede használ mobilinternetet, míg 90%-uk használ WiFi-t mobiltelefonnal. 16,4%-uk több mint 1 készülékkel rendelkezik. A használt telefonok átlag kora 16,68 hónap volt.

Online bankolást a megkérdezettek 47%-a használt a kérdőív kitöltés idején. Gyakori, hogy az ilyen online rendszerek olyan kétlépcsős beléptetést alkalmaznak, melynél az azonosítás egy felhasználóinév-jellegű állandó azonosítóval és jelszóval, valamint egy a munkamenetet azonosító átmeneti időre érvényes jelszóval történik, melyet az ügyfél mobiltelefonjára SMS-ben küldenek meg.

Ez alapján érdekesnek tűnt megkérdezni, hogy végeznek-e a telefonjukon online banki műveleteket. Az eredmények szerint a válaszadók 31%-a végez ilyen jellegű tevékenységet különböző gyakorisággal. Mint korábban láthattuk, a válaszadók több, mint 83%-a egy darab telefonnal rendelkezik, így feltételezhető, hogy a válaszadó ugyanarról a telefonról végzi az online műveleteket, mint amelyre a munkamenetet azonosító átmeneti jelszót kapja. S ezzel máris a kétlépcsős beléptetési rendszer fő előnyét szünteti meg, miszerint két külön csatornán azonosítja magát a felhasználó. Ezt a szokást pedig különböző módszerekkel támadó szándékkal ki lehet használni.

Feltételeztem, hogy azok, akik a telefonon tárolt adatokról biztonsági mentéseket készítenek, nagyobb arányban frissítik a telefonjukat azoknál, akik nem készítenek biztonsági mentéseket. Azon hallgatók válaszaiból, akik az informatikai karra jártak, kimutatható gyenge összefüggés (Pearson-féle korreláció: 0,348, Szignifikancia szint: 0,006). A gazdasági kar hallgatói esetében nem volt kimutatható összefüggés. Így az informatikai karra járók esetében elfogadható a hipotézis, míg a gazdasági kar diákjaira nem fogadható el.

Feltételeztem, hogy azok a hallgatók, akik az operációs rendszert frissítik, nagyobb arányban telepítenek a telefonjukra valamilyen biztonsági programot is. A hipotézis vizsgálatában statisztikai kapcsolatot nem sikerült feltárnom egyik kar hallgatói esetében sem.

A mobilinternetet használó hallgatók nagyobb arányban készítenek biztonsági mentést a mobilinternetet nem használókhoz képest. A gazdasági kar hallgatói esetében sikerült az összefüggést igazolnom (Pearson-féle korreláció: 0,287, Szignifikancia szint: 0,001) Az informatikai karon nem volt ilyen kimutatható összefüggés.

Vélelmeztem, hogy van legalább egy olyan a biztonsági kérdések közül, melyben a két kar hallgatói hasonlóképpen válaszoltak. Vizsgáltam azt is, kétmintás független F-próbával, hogy vajon bármelyik biztonsággal kapcsolatos válaszban tekinthetőek-e egy csoportba tartozónak a két különböző karra járó válaszadók. Erre a megengedhető szignifikancia szint mellett nem találtam bizonyítható összefüggést.

Az elvégzett vizsgálatok meglepő módon azt sugallják, hogy a két különböző karra járó hallgatók mobiltelefon használatában szignifikáns különbségek nem találhatók, melyet az elvégzett kétmintás független F-próba is igazolt. A várt eredménnyel ellentétben a megkérdezettek között az informatikai karról érkezett válaszok nem mutattak biztonságtudatosabb magatartást és megfelelőbb attitűdöt a biztonság felé.

Következtetésül elmondható, hogy az okoseszközök használata a 2010-es években az Y és Z generációs hallgatók körében, alig néhány kivételtől eltekintve, szinte teljes mértékben vált jellemzővé, ezen eszközök biztonságtudatos használata, a rajtuk tárolt adatok megfelelő szintű védelme viszont nem jellemző.

2022 tavaszán megismételtem a 2016-os felmérésemet. Sajnos ebben az esetben a minta nagysága és az azt alkotó hallgatók képzései közötti sokszínűség elmaradt a korábbitól, így direkt összehasonlítást nem tett lehetővé. [P15]

A 2022-es hallgatói minta kizárólag gazdaságinformatikus hallgatókat tartalmazott. A válaszaikból levont következtetések a következők: A nem okostelefon használat teljesen eltűnt a mintából. A válaszadók érzékeny, számukra fontos adataiknak tárolása az okostelefonjaikon nagymértékben jellemző. Az eszközökhöz való hozzáférés szoftveres korlátozása pin kóddal, jelszóval, feloldási mintával, vagy biometrikus azonosítással (ujjlenyomat, FaceID, írisz mintázat, egyéb) teljes körű a mintában. Az eszközökön tárolt adatok biztonsági mentése, és ezáltal az adatvesztés kockázatának csökkentése viszont nem általános. A válaszadók közel egy harmada nem végez semmilyen biztonsági mentést, és aki végez is, döntően inkább eseti jelleggel, vagy nagyon ritkán menti le a számára fontos adatait eszközeiről. [P15]

2 AZ OKOSESZKÖZÖK VÁLLALATI HASZNÁLATA ÉS A BYOD

Az elmúlt években a mobilinformatikai eszközök robbanásszerű terjedését figyelhettük meg.

Kutatásaim során mobil informatikai eszközök alatt olyan hordozható infokommunikációs készülékeket értek, amelyeket a felhasználók nem tekintenek számítógépnek, de funkcionálisan megközelítik azt. [47] [48] [49] Így tehát a különböző rendszerű okostelefonokat és tableteket, ezekből is hangsúlyosabban a kényelmesen, szinte bárhol, szinte bármikor használható okostelefonokat.

Ezeknek az okoseszközöknek a mérete egyre kisebb és kisebb lett az évek során, majd egy optimumot elérve a méreteket tekintve a hordozhatóság, a használhatóság szempontjából fejlődtek és fejlődnek évről évre jobban és jobban. Képességeik is egyre széleskörűbbek. Funkcióik a kezdeti mobiltelefonáláson és SMS küldésen fogadáson túl olyan funkciókkal gazdagodtak, melyekhez korábban számítógépre volt szükség. Így mára a tabletek és okostelefonok a laptopok és számítógépek alternatívájává váltak.

Emellett a mobilhálózataink képességei is egyre erősebbek. Ezeknek a hálózatoknak a sávszélessége és lefedettsége az európai országokban jó hátteret biztosíthat ahhoz, hogy szinte bárhonnan, bármikor dolgozhassunk.

Ennek megfelelően ezeket az eszközöket ma már nemcsak a magánéletünkben, hanem a szakmai életünkben is széles körben használjuk. Így felhasználásukban is változások következtek be. A barátokkal, rokonokkal, üzleti partnerekkel történő kapcsolattartáson, a szórakoztatás és informálódás fő platformja mellett, így már vállalati szempontból is érdemes vizsgálni ezeket az eszközöket. Hisz a munkavállalók nem mindig tekintik és használják úgy ezeket az eszközöket, ahogyan a számítógépeket. Ugyanakkor ezek az eszközök hozzáférhetnek a vállalati adatokhoz, és feldolgozhatják (megnyithatják, szerkeszthetik, beszúrhatnak, törölhetnek stb...) vállalati adatokat. Ezért sok szempontból, kiemelten kezelve az információ biztonságot, az IT-infrastruktúra egy eszközeként kell kezelni őket.

Sok olyan eset van, amikor a munkavállaló okoseszközt szeretne használni munka céljára is. A legfontosabb felhasználási területe ezen eszközöknek a kommunikáció. A munka-

helyi e-mailek lekérdezés okostelefonon ma már mindennapos helyzet, de egyéb üzenetküldő rendszerek is szóba jöhetnek, ahol vállalati adatokat kell továbbítani a felek között. Ezekkel az eszközökkel használhatjuk a cég informatikai infrastruktúráját is, elérhetjük a hálózati meghajtókat, a megosztott dokumentumokat, a megosztott adatbázisokat, sőt a cég vezetői információs rendszerét is, és még sok minden mást. Csakúgy, mint egy számítógép esetében. A kérdés az, hogy milyen kockázatokkal járnak, és hogyan lehet szabályozni?

De a mai munkavállaló messzire mehetne ezen az úton. Számos olyan felhasználási eset van, amikor a saját eszközeinket szeretnénk használni a munkában. Ezt a jelenséget nevezzük a saját eszközzel való használatnak (Bring Your Own Device, BYOD).

2.1 Az okoseszközök elterjedése

Az eNET még 2012-ben végzett egy 1000 fős reprezentatív mintán felmérést, ami azt mutatta ki, hogy a válaszadók 29%-a rendelkezik okostelefonnal. [50]

A Thinking insights with Google oldal felmérése alapján, ugyanez a részarány 2012-ben 22%-os, míg 2013-ban 34,4%-os volt. [51]

Az NRC 2013-as nem reprezentatív piackutatásán a válaszadók 45%-a nyilatkozott úgy, hogy okostelefonnal rendelkezik, míg 51% mondta azt, hogy okostelefonnal és/vagy tablettel rendelkezik. [52]

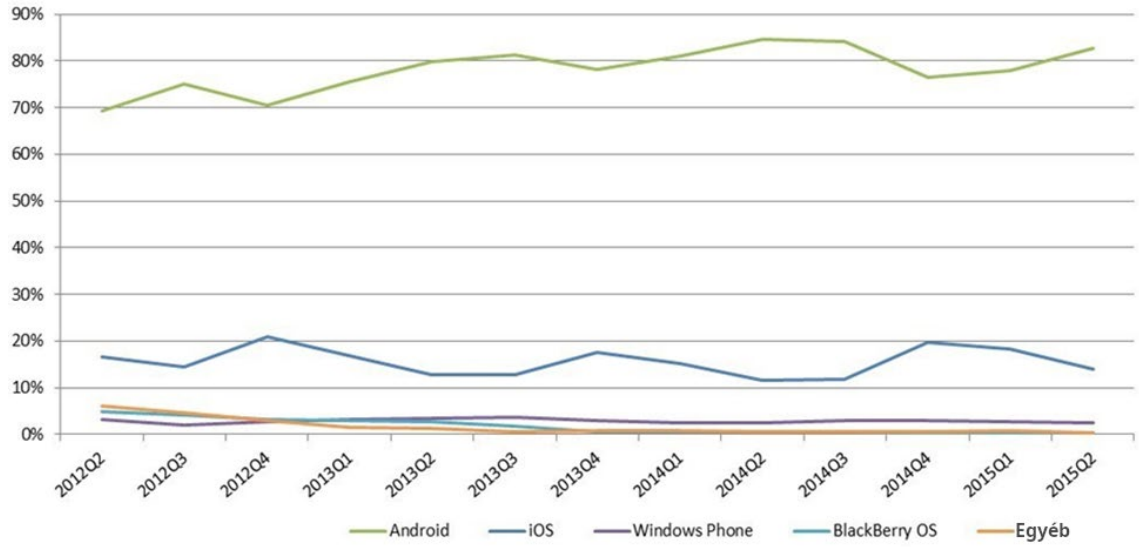
A felmérések vizsgálták a válaszadókat demográfiai és iskolázottsági szempontból is. Az eredmények szerint az okostelefonok részaránya a magasan iskolázott, fiatal felnőttek körében a legnagyobb. Ez az a demográfiai csoport, melynek tagjai első éveiket töltik aktív keresőként vagy még felsőfokú tanulmányaikat végzik. [50] [52]

Ezek alapján megállapítható, hogy bár még az okostelefonok piaci penetrációja ezekben az években nem érte el a 40%-ot, és elmaradt az 5 legnagyobb európai mobiltelefon piaccal rendelkező országtól utolsó helyezettjétől is, de akár csak azokban az országokban, Magyarországon is egy erőteljes növekedést figyelhettünk meg. Az eNET 2015 októberében készített felmérése alapján már 3,3 millió fő használt okostelefont. [53]

2015 végére világ szinten a szakértők szerint az okostelefont használók száma megközelíthette a 2 milliárdot, s bár a növekedés üteme lassult, de még mindig erőteljesen nőtt ebben az időben is a felhasználók száma. S bár az első okostelefonok megjelenése óta az

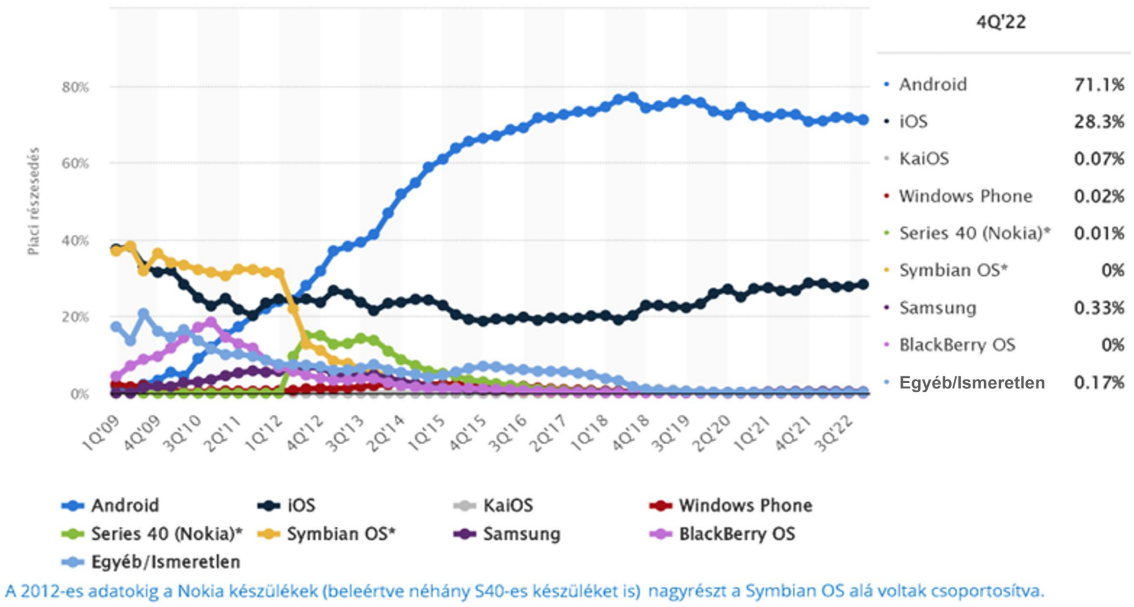
eszközök darabszáma folyamatosan nőtt, az ezeken futó operációsrendszer és szoftverkörnyezet változatossága viszont folyamatosan csökkent. Ez jól megfigyelhető a következő két ábrán is.

A 2012 és 2015 második negyedéve között az IDC Research Inc. által készített felmérésben még 4 nagyobb rendszer jelenlétét figyelhetjük meg, bár már ekkor is az okostelefonok domináns operációs rendszere az Android 82,8%-os piaci részesedéssel, a következő az Apple iOS rendszere 22,3%-kal, a harmadik pedig a Windows Phone 4,2%-kal.



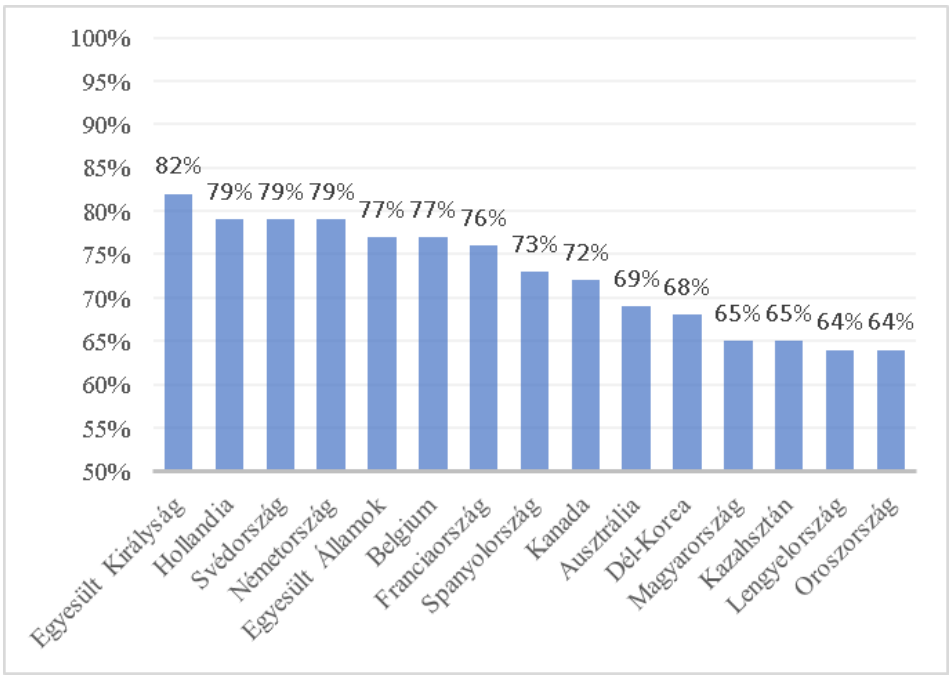
3. ábra Az okostelefon operációs rendszerek piaci részesedései 2012 2. és 2015 2. negyedéve között. Forrás: Smartphone OS Market Share IDC research Inc. [54]

A következő ábrán viszont már azt láthatjuk, hogy 2022-re a piac domináns operációs rendszere még mindig az Android, míg a második helyen az iOS áll, ketten együtt a piac 99,4%-át fedik le.



4. ábra Az okostelefonok operációs rendszerének piaci részesedése
2009 első és 2022 negyedik negyedéve között.
Forrás: Statista - Market share of mobile operating systems worldwide 2009-2022 [55]

A NewZoo felmérésében 50 nagyobb országban mérte fel az okostelefonok elterjedését 2017-ben. A következő ábrán a 14 leginkább érintett országot, valamint Magyarország adatait tűntettem fel. Ez utóbbi a Consumer Barometer with Google, The Connected Consumer Survey felmérésből származó adat, mely azonos mérési módszerrel mérte fel a magyar piacot. [56] [57] [58]



5. ábra Okostelefon tulajdonosok részaránya a felnőtt lakosság körében a választott országokban (2017)
Forrás: Saját szerkesztés a NewZoo [56] és a The Connected által végzett felmérés alapján

A Nemzeti Média és Hírközlési Hatóság 2020 novemberi mobilpiaci jelentése alapján az elmúlt 5 évben az okostelefonok elterjedtsége 4,36 millióról 6,65 millióra nőtt. [59]

6. ábra Az okostelefonokban használt SIM kártyák darabszámának növekedése
2015 4. és 2020 2. negyedéve között Magyarországon.
Forrás: Saját szerkesztés a A Nemzeti Média és Hírközlési Hatóság mobilpiaci jelentése [59] alapján

Ez a növekedés a mai napig tart. Az E-NET 2022 májusában végzett reprezentatív kutatása alapján ma Magyarországon a felnőtt lakosság (18-74 év) körében az okostelefont használók száma meghaladta a 6,2 millió főt. [44]

Nem csak a felhasználók száma, de a felhasználók háttere is nagyban változott, kiszélesedett. A 2000-es évek elején még csak üzletembereknek vagy politikusoknak lehetett okostelefonjuk. Mára szinte bárki megengedhet magának egy ilyen eszközt.

Noha az információ biztonsági kockázatok már az első okostelefonok megjelenésével is már veszélyeztették a felhasználókat és azok adatait, ez csak viszonylag kisszámú, ugyanakkor nagy hatáskörű embert érintett, s az azokat kihasználó támadások, ártó szándékú szoftverek száma is ekkor még igen alacsony volt. Mára már ez is változott. [13]

Ezek alapján joggal mondhatjuk, hogy az okoseszközök ma már mindennapos kísérőink.

2.2 A mobileszközök biztonsága

Az okostelefonokkal kapcsolatos biztonsági aggályok kérdése nem új. Gareth James már 2004-ben a Network Security című szakfolyóiratban megjelent cikkében foglalkozott e témával. Az ő akkori felmérése azt mutatta, hogy ebben az időben nem léteztek még ártó szándékú szoftverek, melyek az okostelefonokat támadták volna. Azonban talált olyan sebezhetőségeket, amelyek lehetővé tették volna, hogy ilyen szoftverek kárt okozzanak. E cikk úgy jellemezte az akkori állapotokat, hogy bár az okostelefonok elterjedése alacsony, jellemzően olyan magas beosztású emberek rendelkeznek ilyen telefonokkal a politikai és üzleti élet területeiről, akik tevékenységi körükből fakadóan célpontjai lehetnének támadásoknak. [13]

Ezzel szemben, ahogy láthattuk, ma már az okostelefonok elterjedési köre igen széles. Ma már nem csak magas beosztású emberek privilégiuma egy okostelefon, hanem szinte bárki megengedheti magának, hogy okostelefonja legyen. A biztonsági helyzet, a kockázatok sora viszont nőtt az elmúlt közel húsz évben.

Szinte nem múlik el úgy hét, hogy ne olvashatnánk egy-egy felfedezett támadásról, vagy befoltozott, eddig kihasználhatónak tekinthető biztonsági résről. A rosszindulatú szoftverek száma gyorsan növekszik. Már 2012-ben, egy az F-Secure által végzett kutatásban, a felmérésük indításáig 238 ártó szándékú szoftvert tartottak számon, míg csak 2012-ben további 804 új rosszindulatú programot találtak az Android operációs rendszerhez. [60] A Kaspersky lab 2014 első negyedévében több mint 2500 ártó szándékú egyedi programot tartott nyilván, melyek a mobilbankolási folyamatot támadták Android platformon, s ezek közül több mint ezret 2014 első negyedévében találták meg. [61] [62]

Természetesen az Apple iOS operációsrendszeréhez is kötődnek biztonsági incidensek már ebből az időszakból. 2014 nyarán nagy visszhangot keltett Jonathan Zdziarski publikációja, melyben az iOS-ben lévő backdoor-okat és támadási pontokat vizsgálta, s talán ennek hatására is szeptember 17-én az Apple 7 frissítésben 55 CVE-t (Common Vulnerabilities and Exposures) zárt le. [63] [64]

Ez csak két példa, de jól mutatják, hogy mai mobiltelefonjaink platformjainak biztonsági kockázata igen magas.

Azonban a szoftveres oldal mellett kiemelten kell kezelni a mobiltelefonokkal kapcsolatban a rajtuk tárolt adatok adatbiztonságát is.

Még 2014-ben az ESET biztonsági cég készített Londonban egy felmérést, melyben 300 taxisofőrt kérdeztek meg arról, hogy utasaik miket hagytak már a taxikban. A felmérés azt mutatta ki, hogy egy londoni taxisofőr évente átlagosan 8 db mobiltelefont talál. S ha ezt az eredményt kivetítjük arra a 24 000 taxisra, akik a város területén dolgoznak, akkor az átlagosan körül-belül évi 190 000 db elhagyott mobiltelefont jelenthetett ebben az évben. [65] Az elhagyott telefonok okozta információbiztonsági kockázat az ENISA (2013) által meghatározott [46] három legfőbb kockázati csoportból [lásd 1.2-es fejezet] az elsőre értékeltbe kockázati csoportba tartozik.

Mark James, az ESET egy biztonsági szakértője azt is kiemelte e felmérés kapcsán, hogy „mindannak ellenére, hogy mekkora publicitást kap a kiberbűnözés manapság, a felhasználók még mindig nem tekintik magukat valós célpontnak. E gyakorlat naiv és rossz. A bűnözők nagyon jól tudják, hogy a mobiltelefonjaink kapcsolódási pontok lehetnek a vállalati hálózatokhoz és akár érzékeny tartalmakat is tárolhatnak.” S ennek ellenére az okostelefon tulajdonosok nem védik kellően a telefonjaikat és az azokon tárolt adatokat. [65]

Kijelenthető, hogy manapság a mobiltelefonjainkat több irányból is fenyegetik biztonsági kockázatok, amik az eszközök használatát figyelembe véve nem csak privát adatainkra, de vállalati adatainkra is veszéllyel lehetnek, melyre nem mindenki van felkészülve. Sokaknak nincs meg a kellő biztonságtudata, aminek hatására a mobiltelefonjaikat és a rajtuk tárolt adatokat kevesebb biztonsági kockázat fenyegetné.

K. Parsonsa és munkatársai vizsgálatuk alapján megállapították, hogy egy szervezet biztonsági szintjére nagy kihatással van tagjainak biztonsághoz való hozzáállása, attitűdje. [66] Megállapították, hogy a biztonsági irányelvek és folyamatok ismerete és megértése nem elegendő, a szervezet tagjainak ki kell alakítaniuk a biztonsághoz való jó hozzáállást, attitűdöt, amellyel jó alapot teremthetnek a szervezet biztonságához.

A mobileszközök egyre olcsóbbak, ugyanakkor egyre nagyobb kapacitással, jobb képességekkel és jobb használhatósággal rendelkeznek. Emellett folyamatos növekedés tapasztalható a mobilkommunikáció internetes teljesítményében, a sávszélesség és a lefedettség terén.

Következésképpen a mobileszközök üzleti célú használata megkerülhetetlen. Az információbiztonsági eszközök kínálata azonban korlátozott. A magas szintű titkosítás vagy hitelesítés nem feltétlenül jár együtt magasabb szintű védelemmel. A mobileszközök kommunikáció közben számos adatot továbbítanak (pl. földrajzi koordináták, környezeti

paraméterek, sebességre és gyorsulásra vonatkozó információk, hálózati partnerek hozzáférési adatai stb.) A mobilkommunikáció és annak lehallgatása szinte ellenőrizhetetlen (gondoljunk csak a Bluetooth-ra, WiFi-re, NFC-re stb.). S maguk a telefonbeszélgetések (hangkommunikáció) is adatnak számítanak.

2.3 Bring Your Own Device - BYOD

A céges hálózatokban növekszik a mobil informatikai eszközök használata. [67]

Ha a munkavállaló olyan munkakörben dolgozik, ahol éjjel-nappal, akár az irodán kívül is rendelkezésre kell állnia, fontos kérdés a kommunikáció módja és költsége. Ha a munkavállalónak mobileszközre van szüksége a céggel való kapcsolattartáshoz, akkor felmerül a kérdés, hogy alkalmazható-e itt a BYOD? Ha alkalmazható, akkor az a kérdés, hogy az alkalmazottak eszköze használható-e erre? Például az eszközük operációs rendszere integrálható-e vagy sem a cég infokommunikációs technológiájába. [6] [7]

Ha egy eszközt tulajdonjoga a vállalaté, akkor teljes mértékben szabályozhatja az eszköz használatát. [68] Eldöntheti, hogy az alkalmazott használhatja-e az eszközt személyes célokra vagy sem. Ez a szabályozás könnyen alkalmazható, ha az eszközt csak fizikailag és hálózatilag is csak a vállalkozás telephelyén, telephelyein használják. Ha azonban az eszközt a vállalati környezeten kívül is használják, akkor problémák merülhetnek fel az eszközhasználat ellenőrzésével. Mindenképpen szükséges ilyen esetben óvintézkedéseket kell tenni a vállalat infokommunikációs technológiájának védelmére, például MDM-szoftverek használatával.

Másrészt, ha a munkavállaló tulajdonában van az eszköz, az ellenőrzés nem kezelhető olyan könnyen. Ha a cég megtiltja a saját tulajdonú eszközök munkahelyi használatát, ez új kérdéseket vethet fel. A munkavállaló dönthet úgy, hogy nem használja a cég által biztosított eszközt, és szélsőséges esetben felmondhat.

Másrészt a munkavállaló a tiltás ellenére is használja a saját eszközeit a munkához. Ezt a jelenséget nevezzük ShadowIT-nek, amikor a munkavállalók a saját eszközeiket használják munkájukhoz. Az előírásoktól való leggyakoribb eltérés a munkával kapcsolatos e-mailek és mellékleteik továbbítása magánpostafiókokba, magáneszközre. [69] [70] [71] [72] [73] [74]

A BYOD a Bring Your Own Device – hozd magaddal a saját eszközöd (a munkába). [75] [76] [77] [78] [79]

Bár az “eszköz“ fogalma általánosságban a munkavállalók tulajdonában lévő vállalati célból használt dolgok széles skáláját jelenthetné, kezdve a saját autótól a munkavállaló tulajdonában lévő szerszámok használatáig, a BYOD rövidítés széleskörben elterjedt és elfogadott jelentése a saját informatikai eszközök, például laptopok, táblagépek, okostelefonok vállalati célú felhasználását jelenti.

A Macmillan English Dictionary szerint a BYOD a „bring your own device: the practice of allowing employees or students to bring their own computing devices to work, college etc and use them on the organization’s network” – vagyis a diákok és munkavállalók egy szokása, mely szerint saját számítástechnikai eszközeiket hozzák magukkal munkába vagy egyetemre, iskolába, stb., ahol az adott szervezet hálózatát használják. [80]

Baillette, Barlette, Leclercq-Vandelannoitte szerint „BYOD involves the use in a professional context of privately owned consumer devices, such as laptops, tablets and smartphones.” A BYOD a magántulajdonban lévő eszközök, például laptopok, táblagépek és okostelefonok munkahelyi környezetben történő használatát jelenti. [15]

Budai Balázs Benjamin szerint „A ByOD a Bring Your Own Device mozaikszava, amelyet leginkább úgy fordíthatnánk: „Hozd a saját kütyüdet”, és dolgozz azzal!” [81]

S bár ez utóbbiakat széleskörben nem tekintjük számítógépeknek, mégis a munkacélú felhasználásuk magában foglalhatja a vállalati levelezőrendszerekhez vagy más informatikai rendszerekhez történő hozzáférést, ami pedig jelenti a bizalmas vállalati adatokhoz történő hozzáférést is. [49]

A vállalat munkatársai kényelmük és a különböző korlátoktól való szabadulási igényük miatt ma már elvárják, elvárhatják, hogy személyes mobil eszközeik munkájukhoz ugyan olyan hozzáférést és szolgáltatásokat nyújtsanak (többek között a vállalati felhőhöz, intranethez, ERP rendszerhez, levelezőprogramokhoz, stb.), mint a munkahelyi számítógépük, ahogyan teszik ezen eszközök lehetővé a személyes használat esetén a kapcsolattartást , a böngészést, tartalomkészítést. Az alkalmazások elérhetősége iránti növekvő igény a biztonsági szint csökkenéséhez vezethet. [49] [15] [82]

Az eddigiek alapján meghatározható a BYOD eszköz fogalma: Olyan hordozható informatikai eszköz, mely képességeit tekintve közel azonos egy általános számítógép képességeivel; hálózati átviteli kapacitás, képernyő felbontás, memória kapacitás és számítási kapacitás tekintetében, azonban a felhasználó megítélése szerint nem laptop vagy számítógép, és a munkavállaló tulajdonában áll.

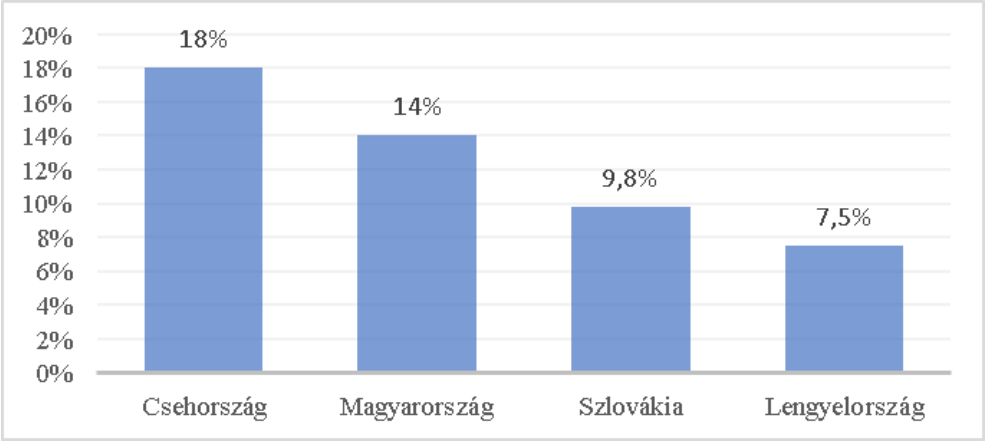
2.4 A saját tulajdonú mobilinformatikai eszközök munkahelyi felhasználásának terjedése

A BYOD fogalma először Ballagas és szerzőtársai 2004-es BYOD: Bring Your Own Device című munkájukban kerül elő. [83] Ebben többek között azt mutatják be, hogy hogyan lehetne a saját tulajdonú mobileszközöket felhasználni nagy kivetítők vezérlésére. Bár ez a használat távol esik a mai BYOD fogalmától (lásd később) ez jól mutatja, hogy a saját tulajdonú mobileszközök munkára való használatának ötlete nem újkeletű. [83]

Ugyanebben az évben (2004) publikálta James Gareth, a korábban is idézett cikkében, hogy még nem ismert olyan ártó szándékú program az ekkor használatban lévő okoseszközökre; PDA-kra (personal digital assistant) és okostelefonokra, mely kárt okozhatna. Azonban azt is kiemelte, hogy ismertek ezeknél az eszközöknél olyan sérülékenységek és biztonsági rések, melyeket kihasználva nagy károkat lehetne okozni. Mert bár e készülékek elterjedése mind a lakosság körében, mind az eladott mobiltelefonok közötti részaránya alacsony, azonban pont azok az emberek rendelkeznek ilyen készülékekkel (politikusok, cégvezetők, igazgatók stb.), akik számára ezen eszközök megtámadása nagy károkat okozhatna, így ezek biztonságával mindenképpen foglalkozni kell. [13]

A BYOD terjedése együtt mozgott az okoseszközök terjedésével. 2009-ben az Intel a saját dolgozói körében ismerte fel azt a trendet, hogy egyre több dolgozójuk szeretné a saját eszközét használni munkája elvégzéséhez. Azt is felismerték, hogy a tiltás, mint egyszerű szabály, nem lenne megfelelő, mert a dolgozók mindenképpen használnák a saját eszközeiket a tiltás ellenére is. Így inkább több kísérlet után 2010 januárjában bevezettek egy olyan szabályozást, mely megítélésük szerint megfelelőképpen képes kezelni a BYOD-ban rejlő kockázatokat, de mégis növeli a dolgozók munka kedvét azáltal, hogy a saját eszközeiken végezhetik munkájukat. [84]

A Kelet-Közép-Európai régióban a BYOD elterjedését 2013-ban az Intel felmérése alapján a következő ábra mutatja. A felmérésben a régió országainak eredményeit összehasonlítják más régiókkal is, ez alapján a 2013-as helyzet szerint régiónkban a saját tulajdonú okoseszközök munkahelyi célú használatának aránya alacsonyabb, mint akár Nyugat-Európában, vagy az Egyesült Államokban. Részletesebben megvizsgálva a Visegrádi Négyek országait, Magyarországon elterjedtebb volt a BYOD, mint Szlovákiában, vagy Lengyelországban és csak Csehország előzi meg. [85]



7. ábra A BYOD elterjedése a V4-es országokban.
Forrás: Saját szerkesztés az Intel 2013-as felmérése [66] alapján.

A BYOD, mint piac, a Global Market Insights kutatócsoport szerint 2014-es 30 milliárd dolláros becsült összpiaci értékéről 2022-ig 367 milliárd dollárosra bővülhetett. [86]

2016-ban az Ipsos európai szintű kutatást végzett a digitális trendekről 20 országban a kis-, közép- és mikrovállalkozások szektorában. Magyarországon a kisvállalkozások 57%-a válaszolta, hogy támogatja a BYOD-ot, ami növekvő tendenciát mutat, hiszen 2014-ben 38%-os elfogadottságot mértek. Míg a mikrovállalkozások 67%-a válaszolt pozitívan erre a kérdésre, a közepes méretű válaszadók elfogadottsága pedig 51%-os volt. [87]

Egy 2018-as tanulmány szerint a vállalatok mindössze 17 százaléka biztosít mobiltelefont minden alkalmazottnak, míg 31 százalékuk egyiknek sem, és ehelyett teljes mértékben a BYOD-ra támaszkodik. A fennmaradó 52 százalék valamilyen hibrid megközelítést alkalmaz, ahol egyes alkalmazottak vállalati mobiltelefont kapnak, másoknak pedig elvárják, hogy hozzák magukkal a sajátjukat. [88]

Az Oxford Economics és a Samsung 2022-ben felmérést végzett 500 vezető és 1000 munkavállaló megkérdezésével, 2500-nál kevesebb alkalmazottat foglalkoztató vállalatoknál világszinten. Ennek legfőbb megállapítása, hogy az okoseszközök használata a vállalatok számára kritikus fontosságú. A munkavállalók 57%-a úgy nyilatkozott, hogy az okostelefon a munkájukhoz feltétlenül szükséges. Annak ellenére, hogy az okostelefonok egyre nagyobb jelentőséget kapnak a mindennapi munkában, csak a válaszadó vállalkozások 15%-a biztosít okostelefonokat minden alkalmazott számára. A fennmaradó részük vagy BYOD-politikát vezetett be (39%) - ami arra épül, hogy minden alkalmazott használja a saját eszközeiket, vagy pedig vegyes megközelítést alkalmaznak. (46%), ahol egyes alkalmazottak kapnak telefont, mások nem. [89]

A következő pontban a saját tulajdonú mobilinformatikai eszközök használatához kapcsolódó néhány gyakran előforduló eset jogi szabályozottságát fogom bemutatni.

A bizalmas üzleti információk védelme megköveteli, hogy a szervezetek újfajta biztonsági politikát vezessenek be. Miközben alapvető fontosságú, hogy a mobileszközök üzleti célú használata elkülönüljön a magánhasználattól. Azonban ez kiemelkedő önfegyelmet és odafigyelést igényel, s nem várható el, ha ezen eszközök tulajdonosa és/vagy a vonatkozó mobilszolgáltatásokat részben vagy egészben saját maguk fizetik. [2]

Ezen okok miatt a biztonsági erőfeszítéseket két irányban kell végrehajtani. Egyrészt, meg kell határozni egy írásos és követhető eljárási keretrendszert a szervezeti műveletek és a bizalmas üzleti információk kommunikációjának ellenőrzésére. Másrészt, a szervezetnek ki kell alakítania, vagy ki kell választania és el kell fogadnia az infokommunikációs technológiák és IT-biztonsági megoldások (például MDM vagy Mobile Device Management) egyikét. [16] S ha még ezt nem tették meg, akkor mielőbb meg kell tenniük, mert az egyre inkább heterogén információs technológiákkal rendelkező szervezeteknél az egységesítés és szabályozottság bevezetése egyre nehezebbé válik. [71] [90]

A személyes tulajdonú eszközök munkahelyi használatának gyakorlata a múltban sem példa nélküli. A saját munkaruha viselése a munkahelyen vagy a saját autó használata üzleti úton tipikus példa erre. Az ilyen használathoz kapcsolódó biztosítási, költségtérítési vagy adózási kérdéseket már régóta a bevett eljárások keretében kezelik. S ezekhez hasonlóan a BYOD-eszközök használatának szabályozása során is a munkáltatók különböző gyakorlatokat követhetnek:

a. egyes munkáltatók kifejezetten tiltják a személyes mobileszközök üzleti célú használatát;

b. a munkáltatók többsége egyszerűen "eltűri" a személyes mobileszközöket, miközben nem fogad el semmilyen vonatkozó szabályzatot vagy eljárási rendet; [91]

c. A BYOD esetenkénti szóbeli vezetői engedélyhez is köthető, külön-külön esetenként bizonyos technikai korlátozásokkal kiegészítve;

d. kialakíthatnak hivatalos, írásos szabályzatot, amely kiterjed az információbiztonsági kérdésekre is (a vállalati rendszerekhez való hozzáférés rendelkezésre álló protokolljainak meghatározása, a jóváhagyott eszközök és alkalmazások listájának meghatározása, az elfogadható operációs rendszer és a kötelező biztonsági szoftvereszközök meghatározása, a mobileszközön keresztül végzett megengedett adatfeldolgozási műveletek felsorolása [pl. adatlekérdezés és új adatbevitel megengedett, törlés nem], a naplózásra és a személyes adatoknak a szervezeti/vállalati adatoktól való elkülönítésére vonatkozó kötelező eljárások leírása); [49] [82] [3]

e. a munkáltatók kifejezetten ösztönözhetik is akár a személyes mobileszközök üzleti célú használatát. [92]

Ezzel a felosztással láthatjuk a munkáltatók által választható BYOD-val kapcsolatos döntési lehetőségeket.

8. ábra A saját tulajdonú okoseszközök szabályozási lehetőségeinek szintjei
Forrás: saját szerkesztés az irodalomkutatásom alapján [49] [82] [84] [91] [92]

2.5 A munkaadók és a munkavállalók attitűdje a BYOD-hoz

A mobileszközök (okostelefonok és táblagépek) nagyfokú elterjedése új információbiztonsági kockázatokat és fenyegetéseket hordoz magában. Ezeket komolyan kell vennünk, mert nemcsak a személyes biztonságunkat gyengítik, hanem a szervezetek biztonságát is. Ahogyan azt korábban Parsonsa és munkatársainak kutatása alapján állítottam, a szervezetek biztonsága elsősorban a szervezeti tagok biztonsághoz való hozzáállásán alapul. Az ő hozzáállásuk befolyásolja, illetve fogja befolyásolni annak a szervezetnek a biztonságát, ahol dolgoznak vagy dolgozni fognak. [93] [9] [94]

A felhasználók messze nem készültek fel a kockázatokra és veszélyekre, amelyek sokkal közelebbiek és sokkal nagyobbak, mint gondolnák. A felhasználóknak mégsem olyan erős a biztonságtudata, miközben használják az okoseszközeiket. Inkább egy gyorsabb, mint egy biztonságosabb eszközt választanának, ami különösen veszélyes is lehet nemcsak a felhasználó privát adataira, de a vállalati adatokra nézve is. [95] [96] [97]

Nem lehet azonban mindenre szabályunk, és nem tudunk mindent kontroll alatt tartani a szabályokkal. Szükségünk van a munkatársak tudatosságára, ami sokkal fontosabb és hatékonyabb, mint bármilyen szabály, vagy alapvető információbiztonsági alapelv. Jól tudjuk azt is, hogy önmagában csak a technológia nem tud megvédeni minket. [98]

Hétköznapinak és elcsépeltnek hangzik, de mégis nagyon igaz, hogy a rendszer leggyengébb része maga az ember. [94]

Ugyanez a helyzet akkor is, ha az okostelefon-felhasználókról beszélünk. Az okostelefonok száma napról napra nő, ezzel együtt a biztonsági kockázatok is, és a potenciális célpontok száma is növekszik. Bár az okostelefonok biztonsági fenyegetései és kockázatai nem jelentenek új gondot a biztonsági személyzet számára.

Vannak olyan munkáltatók, amelyek megkövetelik alkalmazottjaiktól, hogy 24/7 készenlétben álljanak, néha még a cég telephelyétől távol vagy otthonukban is. A munkáltató számára alapvető fontosságú, hogy a kommunikáció a lehető legalacsonyabb költségek mellett hatékony legyen. A munkavállalók részéről pedig felmerülhet az igény olyan többcélú mobil eszköz iránt, amely ismerős felhasználói felületet kínál, és megfelel a preferenciáiknak (pl. szabadon választható operációs rendszer). Szélsőséges esetben minden munkavállaló ragaszkodhat egy adott mobileszköz-modellhez is. [72] [73]

A vállalati tulajdonban lévő mobileszközök felett, szükség esetén, a munkáltató teljes ellenőrzést gyakorolhat, és a szervezet infokommunikációs technológiáért felelős részlege, munkatársa gondoskodhat azok kezeléséről. A szervezet meghatározhatja alkalmazottai számára, hogy milyen célra és mikor használhatják ezeket a mobileszközöket, de kifejezett szándék és alkalmazott technológia nélkül nem tudja igazán ellenőrizni és kontroll alatt tartani az ilyen felhasználásokat, mivel a felhasználói tudatosság és fegyelem másképp működik a munkahelyen és a munkahelyen kívül. A magánhasználat teljes tiltása és az eszköz korlátozása a munkavállalók tiltakozásához (vagy akár felmondásához) vezethet, vagy alternatív informatikai megoldásokra (ShadowIT) való áttérésre ösztönözhet. [99]

A munkavállaló nem szereti a biztonságot, ha az kellemetlenséget okoz neki. Például nem szeretnek hosszú jelszavakat használni, vagy azokat bizonyos gyakorisággal (pl. havonta) változtatni. Itt fontos közbevetni, hogy a jelszavak gyakori cseréje, egyéb kiegészítő okok nélkül, nem emeli a cég biztonsági szintjét, sőt Keszthelyi szerint csökkenti azt. [100] Az eszközök tulajdonjogához kapcsolódó azonosítási formák szintén nagyon kényelmetlenek lehetnek a munkavállalók számára és az esetleges kerülőutak kiépítésével a biztonsági szintek csökkenéséhez vezethetnek. A biometrikus hitelesítési formák (ujjlenyomat, retinaminta stb.) használata pedig további technikai és jogi kérdéseket vethet fel. [47] [69] [70] [49] [101]

Míg a munkáltató általában költségmegtakarítás szempontjából profitál abból, hogy alkalmazottai üzleti célokra használják személyes mobileszközeiket, a magánjellegű egyidejű használat ilyen körülmények között biztosan elkerülhetetlen.

Az eszközök vegyes tulajdonlása (például céges SIM kártya a magán tulajdonú eszközben) még bonyolultabbá teheti a helyzetet. [71] [74] Márpedig a munkavállalók szeretik és kívánják a kényelmet munka közben is. [102]

A BYOD használat során az eszköz priváthasználata veszélyeztetheti a munkáltató által megkövetelt munkahatékonyságot. Ebben az esetben a magánügyek arányos korlátozása, de nem teljes kizárása egy lehetőség. Magyarországon a munkáltató nem gyakorolhat ellenőrzést munkavállalói magánélete és magánadatai felett, de megkövetelheti tőlük, hogy munkaköri kötelezettségeikhez méltóan viselkedjenek a munkahelyen és azon kívül is.

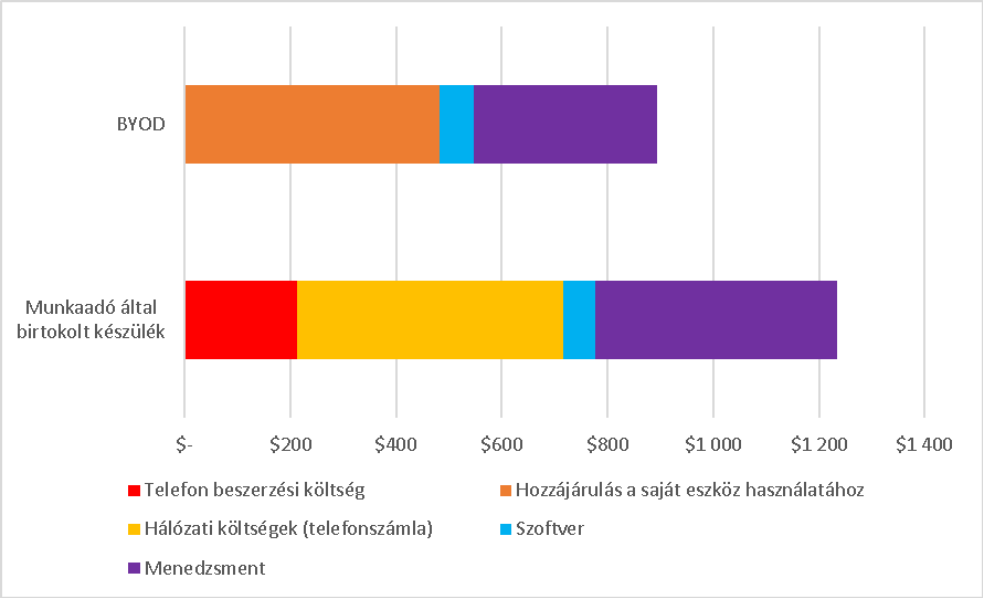
Tanulmányok azt mutatják, hogy a különböző kulturális háttérrel rendelkezők eltérő környezeti attitűdökkel és viselkedéssel rendelkezhetnek az egyén értékorientációja (pl. a személy kulturális értékei, etikai és politikai értékei) erős kapcsolatot mutat az emberi viselkedéssel. Horner és Kahle (1988) rámutatott a személyes értékek, attitűdök és a biztonságtudatos viselkedés közötti összefüggésekre, így a BYOD használatára vonatkozóan is. [103]

2.6 BYOD előnyei

Nyilvánvaló, hogy a személyes mobileszközök üzleti célú használata mind a munkáltató, mind az alkalmazottak számára előnyös. [77] Hétköznapi szóhasználattal élve, bármikor, bárhol, tudnak munkát végezni az okostelefonjukat használva. [47] Teoretikusan mondhatjuk, hogy a BYOD használatával az alkalmazottak a hét minden napján éjjel-nappal, földrajzi kötöttségek nélkül végezhetik a munkájukat.

A felhasználó/alkalmazott által megvásárolt és részben vagy egészben fizetett előfizetéssel a munkáltató költségeket takaríthat meg.

A SAMSUNG és az Oxford Economics által végzett kutatásban azt mutatták ki a kérdőívükre válaszadók adataiból, hogy egy 250 fős vállalkozás esetében a BYOD 324 dolláros megtakarítással járhat. Természetesen ez az összeg és a valós megtakarítás vállalkozásról vállalkozásra erőteljesen különbözhet!



9. ábra Munkaadó által birtokolt készülékek és a BYOD költségeinek összehasonlítása a SAMSUNG és az Oxford Economics által készített felmérés eredményei alapján
Forrás: saját szerkesztés az Oxford Economics és a SAMSUNG által végzett felmérés alapján [89]

2. táblázat Munkaadó által birtokolt készülékek és a BYOD költségeinek összehasonlítása

	Munkaadó által birtokolt készülék	BYOD
Telefon beszerzési költség	$ 212	-
Hozzájárulás a saját eszköz használatához	-	$ 482
Hálózati költségek (telefonszámla)	$ 504	-
Szoftver	$ 60	$ 66
Menedzsment	$ 458	$ 345

Forrás: saját szerkesztés az Oxford Economics és a SAMSUNG által végzett felmérés alapján [89]

A munkavállalók elégedettsége növekedhet, mert az emberek szívesebben használják a saját választásuk szerinti eszközöket. A munkavégzés valószínűleg hatékonyabbá válik, és a munkavállalók valószínűleg kényelmesebbnek fogják találni ezen eszközök használatát, hisz saját mobileszközeik lesznek az egyetlen olyan eszközök, amelyeket magukkal kell vinniük a munkahelyükre, vagy bárhová ahol a munkájukat kell végezniük. [104]

Az informatikai infrastruktúra konfigurálása és működtetése sok tekintetben egyszerűbbé válhat a munkavállaló és akár a munkáltató számára is. Az üzleti folyamatok irányítása gyorsabbá és hatékonyabbá válhatnak. [2]

3 A BYOD-BAN REJLŐ KOCKÁZATOK

3.1 A kockázat fogalma

A kockázat fogalmának sokféle meghatározása létezik. Dolgozatom alapdefiníciójaként Renn definícióját választottam, amely szerint két meghatározás uralkodik:

A kockázat olyan helyzet vagy esemény, ahol valami emberi érték (beleértve magukat az embereket is) forog kockán, és ahol a kimenetel bizonytalan.

A kockázat egy esemény vagy tevékenység bizonytalan következménye valamilyen emberi értékkel kapcsolatban. [14]

Köztudott, hogy nincs olyan, hogy 100%-os biztonság. A magasabb biztonsági szint elérésére fordított összeg exponenciálisan növekszik, ezért meg kell határoznunk az optimális biztonsági szintet, amely a legjobb a költségek és a biztonság szempontjából. [105]

3.2 A BYOD-val kapcsolatos kockázatok

Ahhoz, hogy elérjük a kívánt biztonsági szintet, a személyes és üzleti biztonságunkban is szabályokkal kell rendelkeznünk.

A vállalati adatok védelme ma új megközelítést igényel a cégektől. A személyes és a vállalati adatok szétválasztása a mobileszközökön elengedhetetlen. Nem lehetünk biztosak abban, hogy ha egy alkalmazott a vállalattól kap mobileszközt munkavégzésre, akkor azt csakis munkára fogja használni, és személyes adatok nem lehetnek rajta. Valamint a munkavállaló saját eszközére is másolhat vállalati adatot. [47] [15] [106]

A mobileszközök vállalati alkalmazásának legfőbb kockázati tényezői:

1. Abban az esetben, ha munkavállalótól elvárt a 24 órás, heti hétnapos készenlét fontos szempont a kapcsolattartás költségének minimalizálása. A munkavállalók általában nem szeretnek több eszközt is maguknál tartani ehhez. Szeretnék az általuk preferált, ismert felhasználói környezetet, telefontípust, operációs rendszert, szoftverkörnyezetet használni. Szélsőséges esetben ragaszkodhatnak egy konkrét mobil eszköz típushoz is. [72] [73]
2. A vállalati tulajdonban lévő eszközök felett a vállalat szükség esetén teljes kontrollt gyakorolhat. Az ICT részleg tartja karban az eszközt. Megszabhatja és kikényszerítheti a munkavállalótól a szabályszerű használatot. A magánjellegű használat teljes tiltása azonban ellenállást válthat ki, szélsőséges esetben a munkavállaló kilépéséhez

is vezethet. Ezzel szemben a saját tulajdonú eszköz vállalati célú használata magasabb kockázati szintet eredményezhet magasabb fokú produktivitás mellett. Viszont, ha erre nincs megfelelően betartott szabályzat, vagy azt nem tartják, nem tartatják be, akkor a munkavállaló a kifejezett tiltás ellenére is a vállalati adatokat saját eszközére továbbíthatja. (A leggyakoribb fegyelmezetlenség a vállalati levelek automatikus továbbítása a privát postafiókba.) [70] [71] [74]

3. A munkavállaló általában a „kényelmes" munkavégzést szereti. A hosszú jelszavak használata, azok rendszeres időközönkénti cseréje kontraproduktív. Ezen öncélú, más okból nem következő jelszócsere nem is növeli a biztonság szintjét. [100] A különböző hardver alapú biztonsági kulcsok használata sem könnyíti meg az eszközök kezelését. A biológiai alapú felhasználóazonosítás (ujjlenyomat, írisz, arc azonosítás) technikai és jogi kérdéseket vethet fel. A kiemelt pozíciókba kerülő – általában IT területen dolgozó - vezető beosztású munkavállalók (ún. power userek) sokszor szükségtelenül széleskörű jogosultságot is szerezhetnek. [49] [101] [107]

4. A magánhasználatú eszközök vállalati célú használata nem új gyakorlat. Példaként említhető saját gépkocsi használat. Ennek biztosítása, költségtérítése, adózása mára már megfelelőképpen szabályozott. BYOD eszközök esetében a cégek különböző gyakorlatokat folytatnak;

    a. legtöbb vállalatnál ezek az eszközök „megtűrtek" és szabályozás nincs, [91] [108]

    b. használatuk szóbeli vezetői engedélyen alapul, itt már a technikai korlátozások is előfordulhatnak, [108]

    c. írott szabályzat van, amely esetenként kitér az információbiztonsági kérdésekre is. (A szabályzatban megadják a vállalati hálózathoz történő csatlakozás lehetséges protokolljait. A használható eszközök és alkalmazások felsorolását, az elfogadott operációs rendszert, típust, verziót, a kötelezően alkalmazandó biztonsági szoftvereket, a mobileszközről kezdeményezhető tranzakciókat (pl. lekérdezés és új adat felvétele igen; törlés nem), az alkalmazott naplózási rendet, a magán- és céges adatok szétválasztásának szabályait) [49] [82]

    d. a munkáltató kifejezetten ösztönzi a saját tulajdonú mobileszközök vállalati célú alkalmazását. [82] [108]

e. A BYOD mobileszközöknél a magánélet és a munkáltató által elvárt eredményesség konfliktusba kerülhet. Ebben az esetben a magánélet nem zárható ki, de arányosan korlátozható. Magyarországon a magánéletet a munkáltató nem ellenőrizheti, de a munkakörhöz méltó magatartás - munkaidőn kívül is – elvárható (2012. I. törvény, 8. §). [108]

5. Problémát jelenthetnek még az alábbi biztonsági kérdések;

   a. Milyen minőségű, megbízhatóságú és biztonságú vállalati és vállalaton kívüli hálózathoz történhet kapcsolódás?

   b. Hová és milyen módon történnek a munkavállaló eszközén végzett adatmentések?

   c. 24 órás üzemidőt várunk el, vagy korlátozzuk azt, és szolgáltatási „időablakot" jelölünk ki, akár az eszközön, akár az eszköz által elért távoli erőforrásokon?

   d. Hány hibás bejelentkezés esetén blokkol a rendszer? Kizárható-e az adott eszköz és/vagy felhasználó a rendszerből?

   e. Milyen az autentikációs sorrend (1. felhasználó, 2-3. eszköz, 2-3. SIM kártya)?

   f. Elérhet-e a felhasználó több „postaládát" (pl. főnök-titkár viszony esetén)? [108] [109]

   g. Csatlakoztathatóak-e adathordozók az adott eszközhöz, s ha igen akkor az azokon található adatokat bejuttathatja-e a felhasználó a vállalati erőforrásokra? [110]

Elméleti szempontból a saját tulajdonú mobileszközök használatának legfontosabb kockázati forrásai a következők:

1. A vállalati adatok feletti ellenőrzés elvesztése, a munkavállaló engedély és gondosság nélkül átviheti azokat az eszközökre.
2. Az eszköz típusa, mivel ezeket az eszközöket véletlenül sem tudja a cég ellenőrizni.
3. Amikor a biztonság érzése „túl kényelmetlen”, mivel láthattuk, hogy a kényelem motiváló tényező a munkavállaló számára, és ez a hardver és/vagy szoftver kockázatos megoldásainak használatához vezethet.
4. A saját tulajdonú eszközök szabályozatlan használata. Mivel értékes információk veszhetnek el a nem védett, nem ellenőrzött eszközökön keresztül.

Egyéb fontos kérdések a saját tulajdonú okoseszközök használatának kockázati forrásairól:

1. A hálózati kapcsolat minősége és biztonsága, amin keresztül az eszköz csatlakozik a cég rendszereihez.
2. Biztonsági mentések – hogyan készít az eszköz biztonsági mentéseket például hálózati hiba esetén? Rendelkezik-e az eszköz biztonságos tárolóval, amelyet a mi biztonságos alkalmazásunkon kívül más nem érhet el?
3. A céges adatok a nap 24 órájában az év 365 napján elérhetőek-e hálózaton keresztül bárhonnan, vagy van-e, illetve tudunk-e idő- és térbeli szabályozást alkalmazni?
4. Ki tudjuk-e zárni a felhasználót? Például három sikertelen bejelentkezési kísérlet után lezárjuk-e a felhasználó hozzáférését?
5. Hogyan hitelesítsük a felhasználót? Felhasználói szintről (tudás alapon, például jelszóval, vagy biometrikai megoldással például ujjlenyomattal) vagy eszközszintről (eszközazonosító, biztonságos chip, SIM-kártya, stb.), vagy ezek valamilyen kombinációjával?
6. Egy felhasználó milyen hozzáféréssel rendelkezzen a megosztott postafiókokon és megosztott mappákon? Például egy titkárnő elérheti az igazgatója postafiókját és leveleit? Akár fizikailag megosztva is, például a munkahelyén tartózkodva hozzáférhet az adatokhoz, de távolról már nem, vagy csak erős azonosítás után?

7. A munkavállaló csatlakoztathat-e adattároló eszközt (memóriakártyát, pendrive-ot, külső meghajtót stb.), és elérheti-e az azon lévő adatokat a biztonságos alkalmazásból, és átviheti-e az adatokat a biztonságos partícióra?

Ezeket a BYOD kockázatokat párosíthatjuk a ShadowIT (vagyis árnyék informatikai technológia felhasználással): A ShadowIT, más néven StealthIT vagy ClientIT, a szervezeten belül, kifejezett szervezeti jóváhagyás nélkül kiépített és használt informatikai (IT) rendszerek. Például az informatikai részlegen kívüli részlegek által választott és telepített rendszerek. [111] [112] [113] [114]

2013-ban az ENISA, az Európai Unió Információs és Hálózatbiztonsági Ügynöksége felmérte, hogy mik a legnagyobb kockázatok, amelyek az okostelefonokat fenyegetik. [46]

A három legfontosabb ezek közül:

1. Adatok kiszivárgása az eszközök elvesztése, vagy ellopása miatt.
2. Az adatok akaratlanul történő közzététele.
3. A használt, de nem megfelelően kezelt eszközök támadása, melyekről adatokat szerezhetnek meg támadók.

Ezek a kockázatok aggodalomra adnak okot az eszközön tárolt adatok biztonsága szempontjából. Mivel a BYOD használat esetén az okostelefonok tulajdonosai nemcsak privát, hanem üzleti célokra is használják a készülékeket. Így a biztonsági fenyegetések és kockázatok nem csak a magánéletünkre, hanem a szervezetekre nézve is aggodalomra adnak okot. [46]

Az ENISA szerint az eszközzel kapcsolatos személyes és szervezeti kockázatok által érintett dolgok széles köre érintett lehet:

- személyes adatok
- vállalati szellemi tulajdon
- minősített információk
- pénzügyi eszközök
- eszközök és szolgáltatások rendelkezésre állása és működőképessége
- személyes és politikai hírnév

Ugyanakkor több IT szakértő is pozitív véleménnyel van a ShadowIT-ról, úgy tekintenek rá, mint az innováció és a problémamegoldás alapvető forrására, hisz ez esetben a felhasználók maguk oldják meg az igényeik kielégítését, s adhatnak így példát a folyamatok jobb és hatékonyabb megoldására. [115]

Azonban, természetesen, a ShadowIT megoldások gyakran nem teljesítik a vállalat által támasztott elvárásokat a kontroll, a dokumentáció, a biztonság, a megbízhatóság és további más, az infokommunikációs technológiákat érintő biztonsági kérdésekben.

3.3 Esettanulmányok a kockázatokat kihasználó támadásokra

Közel másfél évtizeddel az iPhone és az első Android alapú okostelefonok megjelenése után, [116] ma már el se tudjuk képzelni modern világunkat okostelefonok és tabletek nélkül. Használati szokásainkban a hangsúly egyre inkább áttolódik a klasszikus hanghívásokról és rövid szöveges üzenetekről a különböző applikációkon keresztül történő információ fogyasztásra és megosztásra. [117] [118] Ehhez általában vagy a gyártó beépített applikációit, vagy harmadik fél által készített alkalmazásokat használunk. Rájuk bízva olykor igencsak érzékeny személyes és vállalati adatainkat is. [119]

A következő példák jól mutatják, hogy adataink védelmében kiemeleten fontos szerepet játszik a mobileszközeink tudatos használata.

3.3.1 Előre telepített rosszindulatú programok

Amikor átvesszük új okoseszközünket az értékesítőtől vagy a munkahelyünkön, már rendelkezik előre telepített operációs rendszerrel, valamint általában az eszköz gyártójának néhány alkalmazásával, a szolgáltató által telepített programokkal és néhány harmadik féltől származó alkalmazással. Adataink védelme érdekében ezen a ponton óvatosnak kell lennünk. Meg kell fontolnunk, hogy milyen típusú eszközöket fogunk használni és milyen céllal, milyen folyamatokban, milyen kockázati besorolású vállalati és privát adatokkal fogunk dolgozni ezen az eszközön, mert lehet, hogy a támadó már az eszközben van.

2017-ben a Check Point kutatóközpont kutatói 36 olyan telefontípust találtak, melyeken ártó szándékú program (malware) volt az előre telepített szoftvercsomagban. 2018 elején a Dr. Web biztonsági cég 40 féle telefontípust azonosított, melyekre az Android.Triada.231 malware az előretelepítéskor a szoftvercsomaggal együtt installálásra került. E program a különböző banki adatok lehallgatására volt képes. Ezen keresztül a támadók

hozzáférhettek a felhasználó banki adataihoz, akár átutalásokat indíthattak, vásárlásokat bonyolíthattak le. [117] [120] [121] [122] [123]

3.3.2 A felhasználó által az eszközre telepített alkalmazások problémája

Azonban nem csak az előre telepített alkalmazások kémkedhetnek a felhasználók után. 2017 októberében jelent meg a hír, hogy a széleskörben használt Uber applikáció az iOS készülékeken titokban megfigyelheti a készülék kijelzőjét. A problémát feltáró Will Strafach szerint az applikáció egy interfészen keresztül fért hozzá az iOS akkor bevezetett képernyőrögzítő funkciójához. Ez letőséget adott arra, hogy akár biztonságkritikus személyes és/vagy pénzügyi adatok is kijuttatásáról a készülékről, mint például jelszavakat, használati szokásokat, banki adatokat, igazából bármit, amit az eszköz a kijelzőjén megjelenített. A korlátozatlan megfigyelés lehetősége igen magas biztonsági kockázatot jelent. Amikor ez a sérülékenység kiderült, az Uber változtatott azapplikációján, s a sérülékenységet lehetővé tevő körülményekről is részletesen beszámolt. Az applikáció fejlesztése során egy új szolgáltatást vezettek be az új Apple Watch funkcióinak kihasználására s, hogy ez a szolgáltatás működhessen, szükség volt az eszköz képernyőjéhez való teljes, korlátozatlan hozzáférésre. Azt is hozzátették, hogy applikációjuk hibásan működő, sérülékenységet lehetővé tevő verziója csak egy teszt verzió volt, nem tervezték publikálni a nagyközönség felé, de itt (is) hibáztak. Elgondolkodtató, hogy egyáltalán az eszköz és az operációs rendszer gyártója hogyan biztosíthat ilyen jogosultságot külső szoftvergyártók számára. S bár konkrét visszaélés nem ismert, ami kihasználta volna ezt a lehetőséget, az Uber az applikáció következő verziójában megszűntette ezt a sérülékenységet. De hasonló esetek tucatja történt már meg a mobileszközök világában, ami az adatok ellopását, vagy a felhasználó számára a hozzájuk férést megakadályozta például ransomware applikációk. Az ismert kártevők száma már ma is igen magas, számuk pedig igen gyorsan növekedik. [124] [125] [126] [127] [128] [129] [130] [131]

3.3.3 Adatszivárgás a felhasználó beleegyezésével

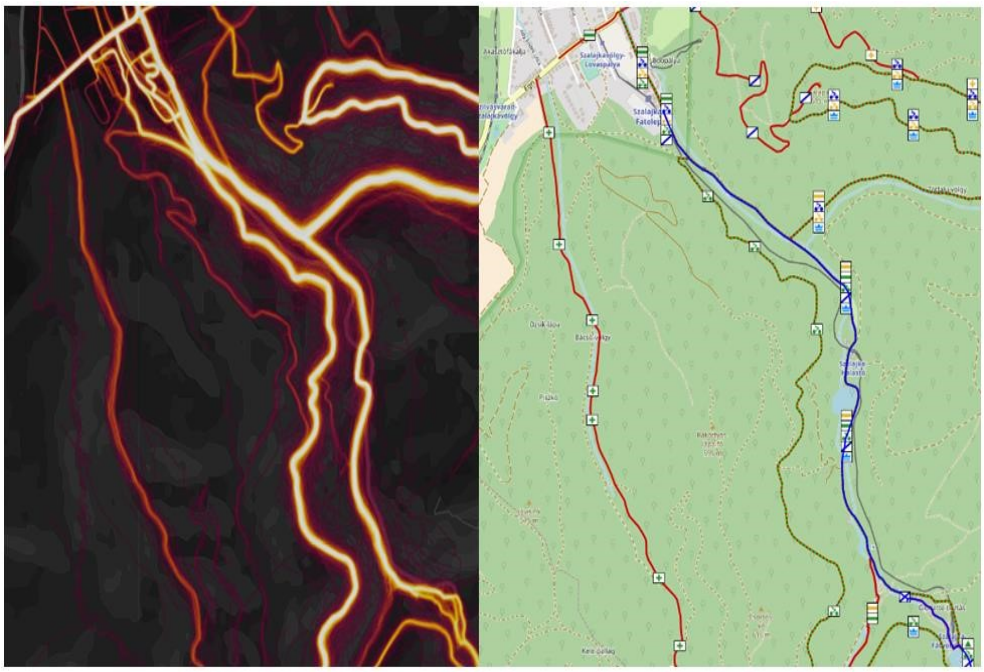
Alkalmazásaink az eszközeink különböző szolgáltatásait használhatják. Teljesen egyértelmű például, hogy egy fényképeket készítő applikációnak működéséhez elkerülhetetlen, hogy az eszköz kameráját használhassa. Egy térkép program, ha használhatja az eszközbe épített navigációs lehetőségeket, sokkal szélesebb körű funkcionalitásra lehet képes, mint anélkül. Felmerülhet a kérdés azonban, hogy egy-egy applikáció az eszköz mely szolgáltatásához férhet hozzá.

De tényleg szüksége van-e például egy üzenetküldő alkalmazásnak az eszközbe épített mikrofon használatára, vagy sem?

Megvizsgálandó lenne, hogy a különböző alkalmazásaink, milyen szolgáltatásokat és milyen céllal vesznek igénybe.

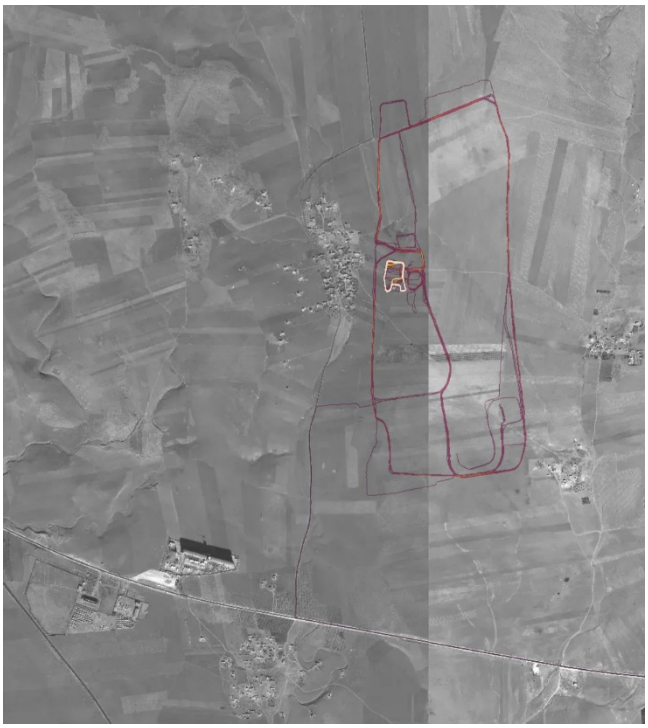
Teljesen érthető például, ha egy testmozgást naplózó applikáció engedélyt kér a helyadatok használatára. Sokan használnak olyan applikációkat, melyek segítségével mérhetővé válik a megtett út, a bejárt útvonal, az elégetett kalóriák száma. Azonban könnyen belátható, hogy e hozzáféréseken keresztül akár szenzitív adatok is rossz kezekbe kerülhetnek.

Ilyen adatszivárgásról adott hírt 2018. január 27-én Nathan Ruser az Institute for United Conflict Analysts alapítója. [132] [133] A széleskörben elterjedt Strava fitnesz applikáció készítői a felhasználók eszközeiből gyűjtött adatokból egy igen részletes térképet készítettek és tettek közzé. Több mint 3 milliárd GPS koordinátát használtak fel. Jól mutatja a térkép részletességét és a felhasználók szokásait a következő ábra, melynek bal oldalán láthatjuk a Strava térképének Szilvásvárad és a Fátyol-vízesés közti részletét, míg a jobb oldalán a turistautak.openstreetmap.hu közel azonos kivágását. Jól látszik, hogy a felhasználók milyen útvonalakat jártak be, hol követték a kijelölt turista útvonalat, hol vágtak át az erdőn.



10. ábra Strava applikáció felhasználói adatok vizualizációja (bal oldalt)
és ugyanazon hely turista térképen (jobb oldalt).
Forrás: Saját szerkesztés a Strava térképének és a turistautak.openstreetmap.hu felhasználásával

S bár az egyes felhasználók nem, vagy csak nagyon korlátozottan azonosíthatóak be az útvonalak alapján, azonban a felhasznált GPS pontok olyan helyekről is származtak, melyek Nathan Ruser szerint többek között az Egyesült Államok bázisait, és azon belül és körül a felhasználók mozgását is nyilvánosságra hozta.



11. ábra Strava által rögzített felhasználói mozgás GPS adatpontok alapján készített vizualizációja egy ismert amerikai előretolt bázis környékéről a Közel-Keleten.
Forrás: Nathan Ruser Twitter bejegyzése a Strava térképének részletével [134]

Bár a Strava szerint az adatok lezárása 2017 novemberben történt, mégis érzékeny, akár a jelenre is kihatással levő információkat tartalmazhattak a térkép publikálásakor. Az adatgyűjtés a felhasználók beleegyezésével történt az applikáció használatakor. A szoftver csak akkor küldi el a hely adatokat a Strava szervereire, ha a felhasználó ezt nem kapcsolja ki. Itt tehát az érzékeny adatok a felhasználók tudtával, vagy tudatlansága miatt kerültek nyilvánosságra.

Hasonló eset történt 2014-ben, amikor egy orosz katona az Instagramra feltöltött fényképével megosztotta a kép készítésének helyét is. Ezzel feltárva, hogy ukrán területen végeznek tevékenységeket. [135]

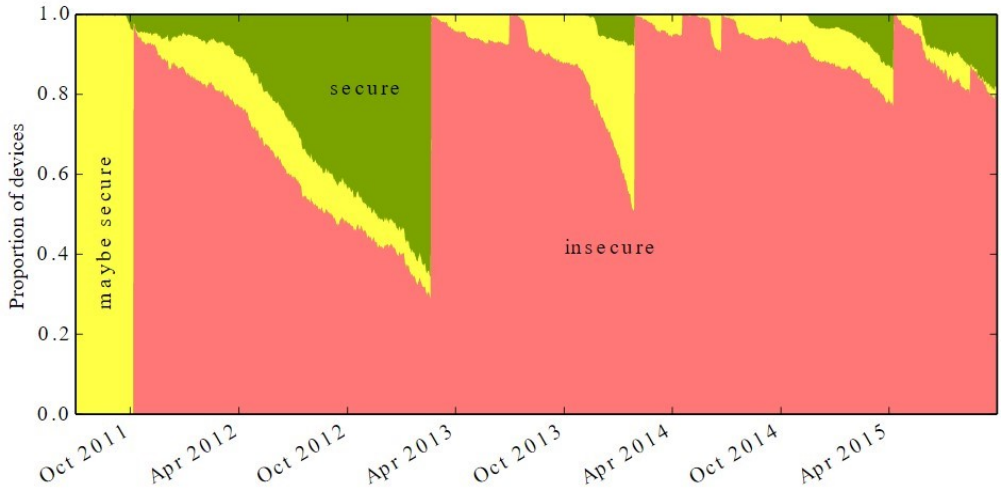
3.3.4 Ismert korábbi sérülékenységek és azokat kihasználó támadó szoftverek

Az okostelefonok megjelenésével és elterjedésével az ezeken használt operációs rendszerek és szoftverkörnyezetek is egyre jobban terjednek. Ugyanakkor, mint minden szoftverben, így ezekben is lehetnek, sőt vannak hibák, amik esetleg kihasználható sérülékenységekhez vezethetnek. Ilyen sérülékenységeket pedig a rosszindulatú támadók és támadó szoftverek kihasználhatják.

Például az Android operációs rendszerben rengeteg sebezhetőség ismert, főként a régebbi, ma már javított, frissített verziókról. [136] Az aktív eszközök számát és azok operációsrendszer és biztonsági frissítés verziószámok alapján pedig többé-kevésbé az érintett eszközök száma is megállapítható. Néhány konkrét, a széles körben ismert eset, a legfontosabbak éves bontásban:

- 2011 - “RageAgainstTheCage adb”, “TacoRoot”
- 2012 - “exploid udev”,
- 2013 - “Motochopper”,
- 2014 - “keystore buffer”, “WeakSauce”,
- 2015 “Stagefright”, “Stagefright 2”, “PingPongRoot”, “pipe inatomic” [137] [138]

Az androidvulnerabilities.org készített még 2015-ben egy vizualizációt az álaluk ismert sérülékenységekről.



12. ábra Az android operációs rendszerű eszközök operációsrendszerének biztonsági megítélése 2011 októbere és 2015 áprilisa között az androidvulnerabilities.org szerint.
Forrás: androidvulnerabilities.org [137]

Bár az androidvulnerabilities.org készítőit sokan kritizálták a módszerük miatt, publikációjuk rávilágít az Android ökoszisztéma régebbi eszközökhöz való hozzáállásának biztonsági problémáira.

3.4 Kockázatvállalás

A valós élethelyzetekben ritkán rendelkezhetünk teljes információval döntési helyzetekben. Így csak a fejünkben lévő valóságmodellek alapján tudunk döntéseket hozni. Nem tudjuk összegyűjteni és kezelni a helyzetünket befolyásoló összes tényezőt. Valamint az is előfordulhat, hogy az optimális időzítéshez képest túl későn vagy túl korán kell döntenünk valamiről.

A döntéseinkkel kapcsolatos fő kérdés az, hogy milyen információkat használunk fel a döntési folyamat során, milyen információk alapján döntünk.

Még ha képesek is lennénk összegyűjteni az összes olyan információt, amely hatással lehet a döntésünkre, ami az esetek nagyon korlátozott számában fordulhat csak elő, az emberi elme egyszerre csak korlátozott számú információt képes feldolgozni és párhuzamosan kezelni. Még ezek összehasonlításával, osztályozásával, rendszerezésével és pontozásával is gondjaink vannak, amikor mérlegelnünk majd döntenünk kell.

Ilyen körülmények között a döntéseink meghozatalakor meg kell birkóznunk a bizonytalansággal, és vállalnunk kell a döntéseink negatív és pozitív következményeit is.

A kockázatvállalás a személyiségünk egy tulajdonsága, s ez személyenként nagy mértékben eltérő is lehet. Számos tanulmány készült a kockázatvállalás különböző kultúrákba tartozó és különböző hátterű emberekről. [139] [140] [141] [142] [143]

Hofstede kutatásai alapján a magyar embereket a kockázat- és bizonytalanságkerülés jellemzi. [144]

3.5 Az egyén szerepe a vállalati biztonságban

Egy szervezet nem egyenlő a benne dolgozó emberekkel és az általuk végrehajtott vállalati folyamatokkal. Ezért a vállalati folyamatok biztonságát nem lehet csak procedurális módon meghatározni, mindenképpen szükséges az emberek biztonsággal kapcsolatos viszonyát is vizsgálni. [66]

Az 1990-es évek végére tehető az az időszak, amikortól a vállalati informatikai biztonságban a vállalati kultúra szerepét kezdték vizsgálni. E kultúra Da Veiga és Eloff [145]

szerint a következőkből áll: attitűdök, meggyőződések, hitek, értékek és tudás. Parsons és munkatársai [66] azt állapították meg, hogy a szervezeti biztonságot erőteljesen befolyásolja a szervezet tagjainak biztonsághoz való attitűdje. Megállapították, hogy a tudás és a megértés mellett szükséges egy megfelelő attitűd kialakítása a vállalati biztonsághoz. [146]

A biztonsági szint eléréséhez szükség van szabályokra, mind a személyes biztonság, mind a vállalati biztonság esetén is. Azonban nem lehet mindent szabályozni. Szükség van egyfajta tudatosságra, mely Szabó Attila a T-Systems Magyarország szenior információvédelmi menedzsere szerint, [147] sokkal fontosabb, mint bármilyen szabályozás, bármilyen információvédelmi alapelv. Mint tudjuk, a technológiák önmagukban nem védenek meg bennünket. Közhelyszerű, de igaz, hogy minden biztonsági rendszer leggyengébb láncszeme az ember. [10] Az embert pedig, mint biztonsági kockázatot pedig csak oktatással, a biztonságtudatosság növelésével lehet javítani, s elérni a biztonságtudatosság egy magasabb, érettebb szintjét. [148] [149]

Schoop és Vasvári a következőképpen határozta meg a biztonságtudatosság érettségi modelljét:

13. ábra A biztonságtudatosság érettségi modellje Schoop és Vasvári munkája alapján
Forrás*:* Saját szerkesztés Schoop Attila, Vasvári György (2012) Tudatos biztonság, alapján [150]

0 (Nem létező): Teljesen hiányzik a jó gyakorlat.

1 (Kezdő): Ad hoc formában van néhány bizonyíték, hogy a szervezet felismerte a biztonságtudatosság fontosságát.

2 (Ismételhető, de intuitív): A felismerés növekvő, van törekvés e kérdés kezelésére, bár ezek az erőfeszítések nem megalapozottak, és nem dokumentáltak.

3 (Meghatározott folyamat): Egy mérsékelt szintű jó gyakorlat és folyamatok vannak jelen, és a munkatársak tudatában vannak a felelősségüknek.

4 (Menedzselt és mérhető): A jó gyakorlat egy szintje és a folyamatok jelen vannak és dokumentáltak, valamint a munkatársak tudatában vannak felelősségüknek.

5 (Optimalizált): A folyamatok fejlettek, megfelelnek a követelményeknek, folyamatosan karban vannak tartva egy önértékeléssel.

Összegzésként elmondható, hogy a biztonságtudat kialakítása mind a személyes biztonság, mind vállalati biztonság szférájában elengedhetetlenül szükséges. Ahhoz azonban, hogy ez a biztonságtudat megfelelő legyen, folyamatos képzésre és/vagy önképzésre van szükség.

3.6 BYOD kockázatok csoportosítása

Az információbiztonságnak, mint állapotnak három alapvető attribútuma van (az ISO/IEC 27001 szabvány szerint):

- bizalmasság (az információhoz csak az arra jogosult személyek férhetnek hozzá),
- sértetlenség (az információ teljességét, pontosságát és eredeti formátumát meg kell őrizni), és
- rendelkezésre állás (a jogosult felhasználók bárhol és bármikor hozzáférhetnek az információkhoz). [151]

Az információbiztonsággal összefüggésben a kockázatok sebezhetőséget jelentenek.

Egy kockázat addig elfogadható, amíg alacsony szintű és/vagy alacsony valószínűségű. Különben (ha jelentős vagy kritikus következményekkel bíró biztonsági incidens, vagy nagy valószínűségű) a kockázatot kezelnünk kell (ISO 31000, kockázatkezelés alapján) a következőkkel:

- a kockázat bekövetkezési valószínűségének csökkentése és a potenciális kár proaktív mérséklése,
- a kockázat átruházása (pl. egy IKT-szolgáltatón keresztül),
- a kockázat megosztása (pl. biztosítási megoldások alkalmazásával). [152]

A BYOD-ból eredő kockázatok többféleképpen osztályozhatók. Az alább javasolt osztályozás a vonatkozó szakirodalom kutatásán alapul. [15] [153] [16] :

K1. A készülék szoftverének vagy hardverének jogosulatlan módosítása

K2. A hangkommunikáció lehallgatása vagy kiszivárogtatása

K3. Rosszindulatú szoftverek, beleértve a vírusokat, zsarolóprogramokat, trójai vírusokat, kémprogramokat stb.

K4. Túlterheléses támadások és szolgáltatásmegtagadás, különösen, ha a készüléket túlterhelik, ezzel az eszköz lefagy, lesüketül, vagy a kommunikációt lehetetlenné teszik.

K5. Az eszközökhöz kapcsolódó szoftveres kockázatok (amelyek a firmware-ből, az operációs rendszerekből és a telepített programokból erednek). A biztonsági frissítések rendszeres telepítésének ellehetetlenítése, a szoftverek megbízhatatlan helyekről történő telepítése és egyéb szoftveres kockázatok.

K6. Adatátviteli kockázatok, mint például az eszköz lehallgatása az adatátviteli csatornákon keresztül vagy man-in-the-middle támadások.

K7. A felhasználók gondatlansága és a biztonságtudatosság hiánya, például gondatlan adatfeldolgozás, az eszköz felügyelet nélkül hagyása, az eszköz elvesztése vagy ellopásának lehetővé tétele, az emberi viselkedést kihasználó támadások (social engineering technikák), az üzleti és a magánélet szétválasztásának hiánya.

K8. Az eszköz elidegenítésével kapcsolatban felmerülő kockázatok, ideértve többek között az adatok nem teljes törlését vagy a hozzáférési jogosultságok nem megfelelő törlését.

K9. Heterogén/ellenőrizhetetlen végponti IKT-infrastruktúra (eszközök és operációs rendszerek sokfélesége) és emiatt nem megfelelő informatikai támogatása.

4 A SAJÁT TULAJDONÚ MOBILESZKÖZÖK VÁLLALATI HASZNÁLATÁNAK ALAP STRATÉGIÁI

4.1 A BYOD jogi szabályozása

A BYOD jogi szabályozásának kérdésében az első, amit megállapíthatunk, hogy nincs önálló szabályozása. Nincs tehát olyan törvény vagy rendelet, amely kifejezetten a saját tulajdonú okoseszközök munkavégzési célú használatát szabályozná. Szabályozza azonban a saját tulajdonú eszközök használatát többek között a Munka Törvénykönyve, az Adatvédelmi törvény és a Büntető Törvénykönyv is.

A Munka Törvénykönyve kimondja (VIII. fejezet 51.§), hogy a munkáltató kötelessége a munkavállaló számára a munkához szükséges eszközök biztosítása. De ettől külön megállapodás alapján el lehet térni, ez teszi lehetővé a saját tulajdonú eszközök használatát.

A legfontosabb elv, ami a BYOD esetében a használatot befolyásolja, az adott helyzetben általánosan elvárható magatartás betartása. Például, hogy csak akkor használja a munkavállaló a mobilinformatikai eszközét munkacélra, ha arra megállapodást kötött a munkáltatóval. Az Ovum, mely egy informatikai és kommunikációs piacra szakosodott elemzőcég, egy 2012-es 17 országot és 3796 fogyasztót érintő felmérésében [154] azt találta, hogy a válaszadók 46%-a úgy használta saját eszközét munkavégzésre, hogy arról munkáltatója vagy nem is tud, vagy tud róla ugyan a munkáltató, de nincs a használatra vonatkozó szabályzat, vagy ha van is szabályzat, azt a munkavállaló nem írta alá. A hanyagságok a munkáltatói oldalról kimerítik az aktív jogsértés fogalmát, vagyis felelősségre vonhatóak az esetleges következményekért.

Amennyiben a munkaadó nem köt a munkavállalóval külön megállapodást a saját eszközének használatáról, akkor a munkaviszony megszűntekor, vagy az adott eszköz cseréjekor, nehezen fogja tudni megvédeni a céges adatait. Hiszen vagy a privát adatokat is ellenőrzi az adott eszközön, ezzel megsértve a munkavállaló adatvédelmi jogait, vagy egyáltalán nem ellenőrzi az eszközt, s ezzel az üzleti titok megtartására vonatkozó szabályokat szegi meg. E kockázat mértékét jelzi, hogy az Európai Unió Hálózatbiztonsági Ügynökségének (ENISA) 2013-ban megjelent tanulmánya szerint, [46] a három legfőbb kockázat az okostelefonok munkahelyi használatával kapcsolatban az ezeken az eszközökön tárolt adatok kiszivárgása.

A saját tulajdonú eszköz használata azért is érdekes egy kérdés, mert egy ilyen eszközben egy helyen tárolódnak a használó személyes adatai és vállalati adatok. A jog védi mind az eszköz használójának személyes adatait, mind a vállalati adatokat is. A személyes adatok esetében a munkáltatónak nincs joga hozzáférnie a munkavállaló eszközén tárolt személyes adatokhoz, még akkor sem, ha erős a gyanúja, hogy a munkavállaló esetleg adatokat juttat ki a vállalattól. Ebben az esetben, ha ténylegesen üzleti titoksértés történt, akkor a munkavállaló (Büntető Törvénykönyv 418.§) és a munkaadó is felelősségre vonható a Polgári Törvénykönyv 81.§-a alapján.

4.2 A BYOD stratégiák

Az elméleti bevezetés és az esettanulmányok alapján is látható, hogy az embereknek és a vállalatoknak mobil eszközeik adatbiztonságával foglalkozniuk kell. [9] Tudatosan kell tervezniük, hogy milyen adatok, milyen körülmények között kerülhetnek ezen eszközökre.

Az eszközök kiválasztását, védelmét és felhasználását körültekintően meg kell tervezni. A kiválasztásnál törekednünk kell olyan gyártó eszközét választani, amelyik az eszköz tervezett élettartama alatt biztosítja rendszereinek biztonsági frissítését. A kiválasztott eszközre az elérhető biztonsági megoldásokat alkalmazni kell. Amennyiben lehetséges, megbízható víruskeresőt, vagy komplex biztonsági megoldást kell telepíteni. A készülék beállításainál is az adatbiztonságot kell előtérbe helyezni. Ha más körülmény nem indokolja, csak megbízható forrásból telepítsünk, leellenőrzött alkalmazásokat! Ezen alkalmazásoknak a hozzáférését szűkítsük le, csak a használatukhoz feltétlenül szükséges jogosultságokat engedélyezzük! A használat során pedig legyünk tisztában azzal, hogy milyen adatokat, kapunk, dolgozunk fel, továbbítunk, az adott applikáción keresztül!

A bizalmas vállalati adatok védelme új biztonságpolitikát kíván a szervezetektől. A magáncélú és vállalati használat szétválasztása alapvető fontosságú, de a vállalati alkalmazottaktól nehezen várható el, hogy a nap 24 órájában náluk levő okos telefont vagy bármilyen más mobil eszközt ne használják magán célra, különösen akkor, ha a készülék az ő tulajdonukban van (Bring Your Own Device - BYOD), vagy mobilszolgáltatás díját részben, vagy egészben ők fizetik. [49] [15]

A védelmi tevékenység itt kettéválik. Egyrészt szükség van egy szervezeti működést, bizalmas vállalati adatok kommunikációját szabályozó – leírt és betartható – rend kialakítására, a másrészt az infokommunikációs eszközök védelmére. [2] [7] [15] [155]

A dolgozók által használt mobilkészülékeken keresztüli adatlopás nem elhanyagolható kérdés. Ezt támasztja alá a Balabit által végzett széleskörű kutatás is, melyben 500 magasan képzett szakembert kérdeztek meg a vállalatokat leginkább veszélyeztető IT fenyegetettségekről. [69] Kiemelendő kérdés a megfelelő védelmi megoldásokat kínáló cégek (MDM - Mobile Device Management) ajánlatai közül történő választás. Ez utóbbi heterogén információtechnológia esetén igen nehéz feladat. [70] [71] [156]

Javasolt az IT- és információbiztonsági szabályozással foglalkozó szakemberek számára, hogy a vállalatnál ne csak a felhasználói profilokat határozzák meg, hanem a vállalati hálózatba bejelentkező különböző eszközökét is. Más legyen a hozzáférési jogosultsága ugyanannak a felhasználónak a belső hálózatra kötött munkaállomásra történő bejelentkezésénél, mint a nyilvános helyen használt, nyilvános hálózaton keresztül a vállalati rendszerekhez csatlakozó saját tulajdonú mobil eszköz esetében.

A cégeknek a kifejezetten informatikai problémák mellett erőteljesen figyelembe kell venniük dolgozóik biztonságtudatosságát is. [157] Ahogyan a két utolsó példában is látható volt, a vállalat alkalmazottai akár szándékosan, akár figyelmetlenségből, juttathatják ki az érzékeny vállalati adatokat mobileszközeik segítségével.

S bár ezen intézkedések következtében sem érhetjük el a 100%-os biztonság állapotát, de akár költségmentesen, vagy legalábbis a védekezési költség/kár arány alacsonyan tartásával is elérhetünk komoly biztonsági szintnövelést.

Ahhoz, hogy megbirkózzunk a szervezetünket érintő biztonsági kockázatokkal, a szervezetünk biztonságának alapjaként kockázatelemzésre van szükségünk. A megfelelő kockázatelemzéssel olyan optimális szabályrendszert alakíthatunk ki, amely segíthet a kívánt biztonsági szint elérésében. [158]

Ha a munkavállaló a saját eszközét használja a munkájához, akkor szinte biztos, hogy személyes adatokat tárol rajta és személyes szükségleteit kielégítő alkalmazásokat és szolgáltatásokat fog használni rajta. Ez új kérdéseket vet fel. Először is a cég szempontjából a vállalati adatvédelem szükséges. A munkavállaló szempontjából a személyes adatokat bizalmasan kell kezelni, úgy, hogy ahhoz a vállalat ne férhessen hozzá. Ehhez egy jól kidolgozott szabályozásra van szükség, amely meg tudja védeni a cégek érdekeit, miközben biztosítja a munkavállalók számára személyes adataik védelmét. Számos jó gyakorlat létezik a szabályozásra, és számos szoftver létezik a cég által az ilyen eszközök kezelésére. (MDM – Mobile Device Management) [2] [5] [6] [67] [82]

Ahogyan azt láthattuk, a saját tulajdonú eszközök munkahelyi használata nem újdonság, hosszú múltra tekint vissza. Ha például a munkavállaló saját autóját használja üzleti útra, akkor bizonyos költségtérítést kaphat. Az okoseszközök kérdésében azonban a BYOD szabályozási kérdéseket vethet fel:

a. számos cégnél nincs szabályozás a BYOD-ra vonatkozóan, [101] [107]

b. egyesesetekben az IT megoldásokat szabályozó vezetők csak szóbeli engedélyt adnak, részletes szabályozás nélkül, esetleg néhány tanácsot adnak a technológiával kapcsolatban és esetileg szabályozzák a saját eszközök vállalati használatát, [20]

c. részletes írásos szabályozás készül, amely az IT biztonságra vonatkozó előírásokat és eljárás rendeket is tartalmaz. [16] [82] Előírásokat alkothatunk arra vonatkozóan, hogy a BYOD-eszközök hogyan csatlakoztathatóak a cég számítógépes hálózatához, milyen protokollok használhatók. Részletes szabályozás vonatkozhat arra, hogy milyen típusú eszközök, operációs rendszer verziók és alkalmazások használhatók. Előírások lehetnek a kötelezően telepítendő biztonsági szoftverekről. Szabályozható a használat (azaz milyen tranzakciókat lehet a BYOD-eszközökön végezni, és milyeneket nem). Milyen naplózást kell alkalmazni stb..

d. A munkáltató támogatja a BYOD-ot, és ösztönzi a munkavállalókat a saját eszközeik használatára. [89]

Egyes vélemények szerint a BYOD eszközök használata negatív hatással lehet a termelékenységre, hisz ilyen eszközök használatakor a magánhasználat vagy legalábbis annak lehetősége állandóan ott van a munkacélú használat mellett. Mindenképpen szükséges a termelékenység szintjét folyamatosan felügyelni. [101]

Bár a munkáltatók többségénél vannak írásos biztonsági irányelvek, ezek nem mindig tesznek különbséget a magántulajdonban lévő és a vállalati tulajdonban lévő mobileszközök között.

4.3 BYOD stratégia kialakítása

A BYOD-stratégia és -irányelv felé tett első lépéshez a munkáltatónak stratégiai döntést kell hoznia. Az uralkodó vállalati hozzáállástól függően a szervezet vezetésének stratégiai döntést kell hoznia.

14. ábra A saját tulajdonú okoseszközök szabályozási lehetőségeinek szintjei
Forrás: saját szerkesztés az irodalomkutatásom alapján [49] [82] [84] [91] [92]

Egy ilyen döntést a legjobban a BYOD-dal kapcsolatos, fentebb tárgyalt kockázatok előzetes felmérése támogathat. A stratégiai döntés támogatására témavezetőmmel Prof. Michelberger Pállal alakítottunk ki és teszünk javaslatot a stratégia kialakítására. [P8]

A stratégiai döntés meghozásához a korábban a 3.6 fejezetben bemutatott 9 kockázati-csoport felhasználásával egy komplex kockázatelemzés készítését javasoljuk, mely segít egyrészt e komplex döntési helyzetet átlátni, másrészt a kockázat-csoportok segítségével kialakítható egy megalapozott stratégiai döntés.

Amennyiben egy stratégiai döntési lehetőség (tiltás, tűrés vagy ösztönzés) bármelyik kockázati csoport eleme elviselhetetlenül vagy kezelhetetlenül magas szintjével jár, azt el kell utasítani (a 3. cselekvési változatban szereplő példában a BYOD ösztönzése elviselhetetlen és kezelhetetlen kockázatot jelent). Ez a folyamat a stratégiai döntéshozatalt megelőző előszűrésként szolgál.

Minden kockázatot a három osztály egyikébe való besorolás után lehet értékelni (aszerint határozható meg, hogy melyik információbiztonsági attribútumot fenyegeti).

A munkáltató akkor hozhat megfelelő döntést, ha az összes kockázatot súlyozták és értékelték (osztályozták). Erre a feladatra a Combinex-et, egy elismert több kritériumon alapuló összehasonlítási módszert javasoljuk. [159]

A kockázati súlyszámok összege 100% vagy 1,00. Az osztályozás történhet 0-tól 100-ig terjedő skálán, de ettől való eltérés is lehetséges; például egy 1-5 vagy 1-7-ig terjedő érték skála a jobb kezelhetőség érdekében.

Azért, hogy a döntéshozatali modell átlátható és érvényes legyen, minden kockázatot ugyanazon a skálán kell értékelni, minden egyes döntési alternatíva esetében. Tehát a különböző szempontok esetén ugyan annak az osztályzatnak egy körülbelül azonos kihatású kockázatnak kell megfelelnie.

Amennyiben a meghozott döntés a tolerált vagy támogatott BYOD irányába mutat, megkezdődhet a BYOD-irányelv tényleges kidolgozása és annak integrálása a mobileszközkezelési megoldásba.

3. táblázat Az információbiztonsági kockázatok összefoglaló értékelése egy "BYOD tiltott" forgatókönyv esetén (példa)

BYOD nélküli állapot

Kockázat	Elfogadhatóság	Kezelhetőség	Kockázati szint (1-5) (becsült)	Súlyérték (0-100%)	Súlyozott pontszám (risk level × weight)
K1	Nem	Igen	3	20%	0.60
K2	Igen	Nem szükséges	2	10%	0.20
K3	Nem	Igen	3	20%	0.60
K4	Nem	Igen	2	12%	0.24
K5	Igen	Nem szükséges	1	5%	0.05
K6	Nem	Igen	2	10%	0.20
K7	Igen	Nem szükséges	1	12%	0.12
K8	Igen	Nem szükséges	1	6%	0.06
K9	Igen	Nem szükséges	1	5%	0.05
Összesítve				100%	2.12

Forrás: Saját szerkesztés kockázat becslés alapján [P9]

4. táblázat Az információbiztonsági kockázatok összefoglaló értékelése egy "BYOD tűrt" forgatókönyv esetén (példa)

Részleges BYOD alkalmazás

Kockázat	Elfogadhatóság	Kezelhetőség	Kockázati szint (1-5) (becsült)	Súlyérték (0-100%)	Súlyozott pontszám (risk level × weight)
K1	Nem	Igen	4	18%	0.72
K2	Nem	Igen	4	11%	0.44
K3	Nem	Igen	3	20%	0.60
K4	Nem	Igen	3	10%	0.30
K5	Nem	Igen	3	6%	0.18
K6	Nem	Igen	3	9%	0.27
K7	Nem	Igen	2	12%	0.24
K8	Nem	Igen	3	8%	0.24
K9	Nem	Igen	3	6%	0.18
Összesítve				100%	3.17

Forrás: Saját szerkesztés kockázat becslés alapján [P9]

5. táblázat Az információbiztonsági kockázatok összefoglaló értékelése a "BYOD ösztönzése" forgatókönyvben (példa)

Teljes BYOD alkalmazás kockázatbecslése (egy kimagasló kockázati értékkel)

Kockázat	Elfogadhatóság	Kezelhetőség	Kockázati szint (1-5) (becsült)	Súlyérték (0-100%)	Súlyozott pontszám (risk level × weight)
K1	Nem	Igen	4	18%	0.72
K2	Nem	Igen	4	11%	0.55
K3	Nem	Igen	3	16%	0.48
K4	Nem	Igen	3	11%	0.44
K5	Nem	Igen	3	7%	0.21
K6	Nem	Igen	3	9%	0.36
K7	Nem	Igen	2	12%	0.24
K8	Nem	**Nem**	3	9%	0.45
K9	Nem	Igen	3	7%	0.28
Összesítve				100%	3.73

Forrás: Saját szerkesztés kockázat becslés alapján [P9]

E példában a K8 kockázati csoport kezelhetetlennek bizonyul, így a szervezet vezetésének el kell vetnie a BYOD ösztönzésének stratégiai lehetőségét.

A három stratégiai BYOD-alternatíva értékelése és a közülük való döntés eltér a klasszikus, több szempontú összehasonlításon alapuló döntéshozataltól. Gyakorlatilag egy ve-

zetői döntéshozatali folyamat támogatására végzett kockázati szintű értékelésről van ebben az esetben szó (3. táblázat, 4. táblázat, 5. táblázat). Ezért itt kizárólag ordinális skálát használunk. Véleményem szerint a három stratégiai alternatíva az informatikai infrastruktúra és a felhasználói tudatosság különbségei miatt eltérő súlyszám-mintázatokkal társulhat. Az értékeléssel a végső cél egy összesített kockázati szint meghatározása, minél alacsonyabb, annál jobb. Az alábbi három szemléltető értékelés szubjektív.

Minden munkáltató/szervezet egyedi, és így a folyamatok kezelésének módja is. Általában a kockázatértékelés eredménye néhány további tényezőtől is függ, mint például a helyi sajátosságok vagy az értékelő csoport szakmai képességei. A teljes BYOD példában (5. táblázat) ezt a stratégiai döntési alternatívát elfogadhatatlan kockázat miatt ki kell zárni a döntési lehetőségek közül.

A BYOD-ról történő döntés nem egy pontszerű döntés a vállalat életében. Az egyszer meghozott stratégiai döntés után folyamatosan követni, frissíteni kell a kockázat csoportok értékeit, az azokat alkotó egyes tényezők külső és belső változása alapján. [P8]

Ezenkívül a kockázati szintek értékelését is frissíteni, aktualizálni szükséges időről-időre, valamint meg kell vizsgálni a kockázatcsökkentés lehetőségeit is. Erre alkalmazható a klasszikusnak mondható PDCA-ciklus (Plan-Do-Check-Act, Tervezés-Cselekvés-Ellenőrzés-Beavatkozás) módszertan is, ami segíthet minden egyes iterációban javítani a kockázat kezelést, és ezzel a BYOD biztonsági szintet, valamint ezen keresztül a teljes vállalat biztonsági szintjét növelni.

Kerülendő gyakorlat, hogy az üzleti adatok ellenőrizetlen módon kerüljenek az alkalmazottak mobilkészülékére. Ez valószínűleg mind a munkáltató, mind a munkavállaló adatvédelmi kötelezettségeinek megszegését jelenti, és az üzleti titkok is sérülhetnek. A munkáltató nem kötelezheti munkavállalóit arra, hogy személyes mobileszközeiket vállalati célokra használják.

Az ellenőrizetlen BYOD-gyakorlat a munkavállaló személyes adatainak keveredéséhez vezethet a munkával összefüggésben feldolgozott vállalati adatokkal. A mindkét fél által elfogadott és aláírt vonatkozó szabályzat hiányában a vállalati adatok teljes visszaszerzése fáradságos (ha nem reménytelen) erőfeszítésnek bizonyulhat, míg a munkáltató a munkaszerződés megszűnésekor hozzájuthat a személyes adatokhoz. Az üzleti titkok védelme felülírja-e a munkavállaló védelmét szolgáló adatvédelmi követelményeknek való megfelelést? [15]

A nem szabályozott, de tolerált BYOD-gyakorlat érvényesülése esetén a munkáltatónak nehéz lesz ellenőrizni, hogy a munkavállalók hogyan használják személyes mobileszközeiket a munkahelyen.

A lehetséges jogi problémák és a BYOD teljes betiltásának megvalósíthatatlansága miatt elengedhetetlen a BYOD-stratégia kidolgozása, valamint a mindkét fél által elfogadott, írásos irányelvek bevezetése és rendszeres felülvizsgálata. Ezekhez a munkákhoz azonban szükség lesz egy informatikai szakemberre, valamint az adatvédelmi szabályozásokban és a munkajogban egyaránt jártas jogtanácsosra.

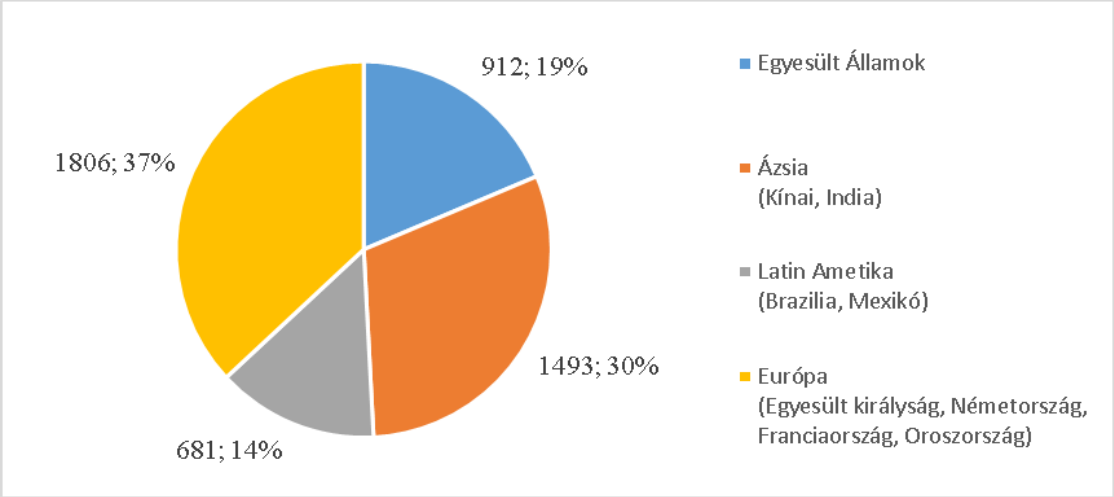
A mobileszközök általános használata és üzleti célú elérhetősége miatt szükségessé vált a mobileszközök központi kezelése. A szakirodalomban az ennek az igénynek a kielégítésére kifejlesztett szoftvermegoldásokat mobileszköz-kezelő (MDM) rendszereknek nevezik. [160]

Elsősorban a mobileszközök vállalati használatának ellenőrzésére szolgálnak, lehetővé téve a mobileszközök használatát a munkahelyi feladatok ellátására, miközben a vállalati információbiztonság megfelelő szintjének fenntartását szolgálják. Az MDM-rendszer által lefedett funkciók a következők:

- A felhasználók és eszközök azonosítása/hitelesítése;
- A vállalati biztonsági irányelveknek és a hatályos ellenőrzött eljárásoknak való megfelelés;
- A vállalati szoftverkörnyezet - beleértve a felhasználói alkalmazásokat és a biztonsági szoftvereszközöket is - naprakészen tartása és használatra való felkészültségük biztosítása;
- A felhasználói feladatok zökkenőmentes ellátását biztosító szoftverprogramok és folyamatok támogatása;
- Az eszközhasználat nyomon követése, beleértve a felhasználói szokásokat, valamint az eszközök állapotát és földrajzi elhelyezkedését;
- Az eszközökön lévő vállalati és személyes adatok védelme és külön kezelése;
- Távoli beavatkozás a mobileszközökön biztonsági eseményekre reagálva, például vállalati adatok eltávolítása és hozzáférési jogosultságok eltávolítása egy felmondani készülő munkavállaló mobileszközéről, vagy az alábbiak észlelése vagy megelőzése célzott támadások felderítése vagy megelőzése.

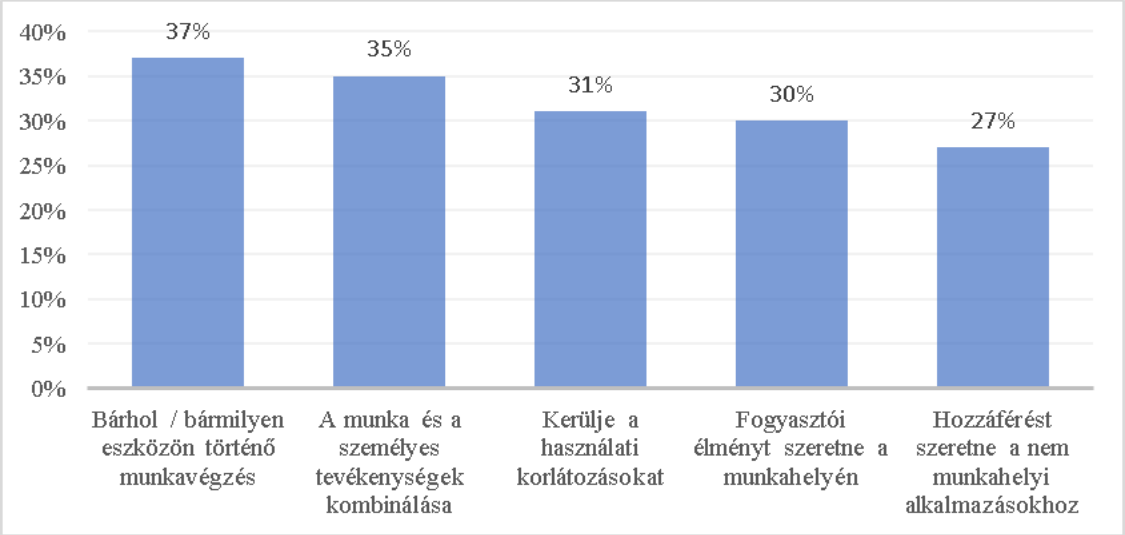
Amint a fenti felsorolásból kitűnik, az MDM-rendszereknek számos feladatot kell ellátniuk, miközben figyelembe kell venniük az eszközparkok sokféleségét és a felhasználói igények különbözőségét. Könnyen belátható tehát, hogy a munkáltató megkönnyítheti az MDM-rendszer bevezetését azáltal, hogy vagy meghatározza a jóváhagyott készülékmodelleket, vagy maga biztosítja az eszközöket a munkavállalói számára. Ezzel azonban megakadályozná, hogy alkalmazottai személyes mobileszközeiket használják.

A Cisco 2012-ben nyolc országban és három régióban kérdezte meg a nagyvállalatok (több mint 1000 alkalmazott) és középvállalatok (500-999) informatikai döntéshozóit. [161]



15. ábra A válaszadók megoszlása CISCO BYOD felmérésben készült minta régiói és országai szerint
Forrás: saját szerkesztés a CISCO BYOD: A Global Perspective Harnessing Employee-Led Innovation [161]

A minta 600 vállalatot, 312 közepes méretű vállalatot tartalmazott az Egyesült Államokból és 2805 vállalatot, 1175 közepes méretű vállalatot a másik három régióból. Az első érdekes kérdés az volt, hogy miért szeretné egy munkavállaló a saját eszközeit használni a munkájához. Amint a második ábrán láthatjuk, a legfontosabb okok a kényelemmel és a használat szabadságával kapcsolatosak az idő, a hely és a használt hardver és szoftver kérdésében.



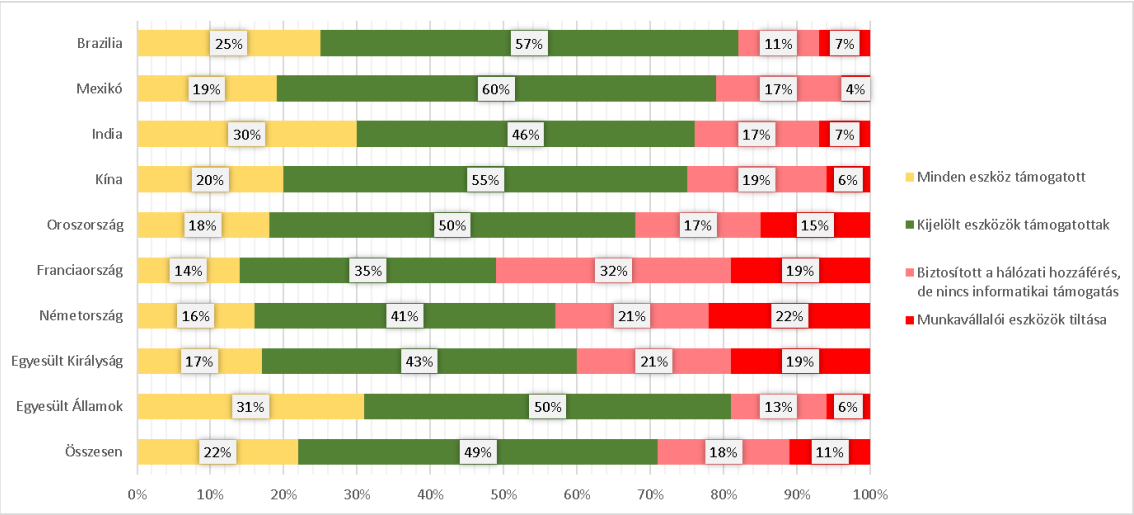
16. ábra A legfontosabb okok, amiért a munkavállalók saját eszközeiket használják munkájukhoz a CISCO felmérése alapján
Forrás: saját szerkesztés a CISCO BYOD: A Global Perspective Harnessing Employee-Led Innovation [161]

Az alkalmazottak ilyen jellegű kéréseire a cég informatikai részlegének kell választ adnia. A kutatásban a Cisco négy választ adott.

A kutatásban szerepelt egy olyan kérdés, hogy a BYOD-ot milyen szinten fogadják el a cégek.

- Minden eszköz támogatott
- Kijelölt eszköz támogatott
- Biztosított a hálózati hozzáférés, de nincs informatikai támogatás
- Munkavállalói eszközök tiltása

Mint látható, a két legelfogadóbb régió az Egyesült Államok és India (31%, 30%) volt, ahol minden eszköz támogatott. Az is érdekes, hogy átlagosan a válaszadók több mint hetven százaléka mondta, hogy támogatja a dolgozói eszközöket (kiválasztott, vagy mindenféle). Ez azt jelenti, hogy sok vállalatnak kell foglalkoznia a BYOD-dal. Másrészt az európai régióban magasabb azoknak a vállalatoknak a száma, ahol tilos a BYOD, mint a többi régióban. Szintén ebben a régióban a legmagasabb azoknak a vállalatoknak az aránya, amelyek csak a hálózati hozzáférést engedélyezték, de nem nyújtottak IT-támogatást. [161]



17. ábra A vállalati IT-támogatás szintjei és megoszlásuk a munkavállalók tulajdonában lévő eszközök esetében a CISCO által végzett felmérés mintájában
Forrás: saját szerkesztés a CISCO BYOD: A Global Perspective Harnessing Employee-Led Innovation [161]

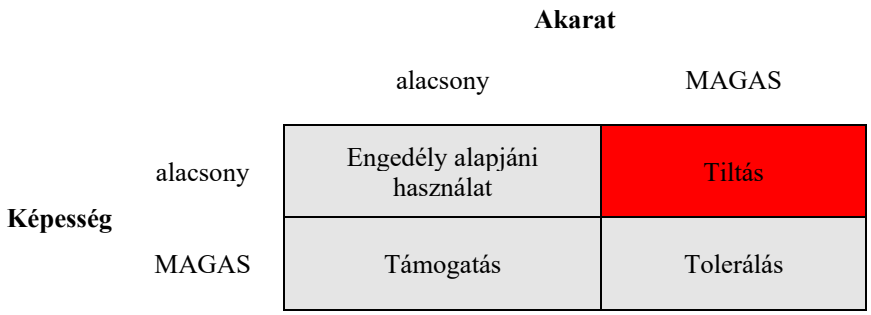
A Cisco kérdőívében láthattuk a munkavállalók tulajdonában lévő eszközök informatikai támogatásának szintjét. A cég vezetői szintjén ez a vezetői döntés négy szintjére alakítható át a következők szerint:

- Tiltott
- Tűrt
- Esetileg szóban szabályozott
- Írásban szabályozott
- Támogatott

Ennek a vezetői döntésnek az előkészítéseként Lazányi szerint a bizonytalanság a következő eljárások kombinációjával csökkenthető: [95]

- Gyűjtsön össze annyi információt az életképes lehetőségekről, amennyit csak lehet, figyelembe véve, hogy a teljes körű tájékoztatás állapotát nem lehet elérni, valamint a fogyasztható időt és költségeket.
- Keressen információt hasonló döntésekről a cég múltjából vagy külső információforrásokból, és alakítsa át ezt a tudást a jelenlegi helyzetre.
- Olyan referencia döntéshozó kiválasztása, aki képes merőben csökkenteni a bizonytalanságot.

A megfelelő döntési lehetőség kiválasztásához a képesség-akarat mátrix is használható. E kétdimenziós mátrixnak az egyik dimenziója a munkavállaló hajlandósága a BYOD alkalmazására, míg a másik dimenzió a munkavállaló IT biztonsági attitűdje és képessége a megfelelő használathoz.



18. ábra BYOD-ra alkalmazott képesség-akarat mátrix a Paul Hersey és Ken Blanchard által alkotott szituáción alapuló vezetési modell alapján
Forrás: saját szerkesztés [162] alapján

4.4 Stratégiai kérdések összegzése

Összességében elmondható, hogy vezetői stratégiai döntésre van szükség a következő kérdésekben. Milyen típusú adatok, milyen körülmények között és milyen formában (azaz csak az eszköz biztonságos tárolójában) lehetnek jelen a mobileszközökön? Dönteni kell a használható eszközök kiválasztásáról, és meg kell határozni azokat a felhasználási eseteket és felhasználási paramétereket is, amikor az alkalmazottak saját eszközeiket használhatják. Ehhez megfelelő informatikai és információbiztonsági szabályozásra és használatra van szükség!

Meg kell határozni szervezeti szerep szerint, munkakör szerint, hogy az adott munkakörhöz tartozó feladatokból mi az amit BYOD eszközön lehet végezni és mi az amit nem. Törekedve a túlszabályozás elkerülésére, ugyan akkor az adott munkakörben dolgozók számára értelmezhető, betartható módon.

Azonban a munkakörök szerinti definíció önmagában nem elégséges, érdemes megvizsgálni egyén szintjén is, hogy mekkora IT biztonsági kockázatot jelent az adott munkavállaló a cég számára és annak megfelelő jogosultsági szintet meghatározni számára a BYOD eszközeire.

5 MÓDOSÍTOTT DOSPERT KÉRDŐÍVES KUTATÁS A KOCKÁZATVÁLLALÁSI HAJLANDÓSÁGRÓL

Az Új Nemzeti Kiválósági Program keretében vizsgáltam az emberi tényező szerepét az informatikai biztonságban. Kutatásom célja volt feltárni az emberi tényező szerepét és jelentőségét az informatikai biztonságban és rámutatni arra, hogy nincs olyan hardver vagy akár szoftver megoldás, amely ne igényelné az emberi tényező tudatos interakcióját, illetve olyan rendszer, melynek a megfelelő biztonságtudatos viselkedés hiánya ne növelné a rendszer sérülékenységét.

5.1 DOSPERT kérdőív

Az irodalomkutatásom során megvizsgáltam különböző kockázat definíciókat és biztonsági modelleket. Ezekből kiemeltem az emberi tényezővel foglalkozó és felméréséhez használható eszközöket. Kiemeltem Weber, Blais és Betz 2002-ben publikált DOSPERT (Domain-Specific Risk-Taking) tanulmányukat, melyben a kockázatvállalás témájában egy új pszichometriai felmérési eszközt hoztak létre, amely az élet különböző területeiben méri a kockázatvállalási hajlamot. [17]

Az eszköz által mért domainek:

- Pénzügyi,
- Egészségügyi / Biztonsági,
- Sport és rekreáció,
- Etikai,
- Szociális

A válaszadók a kérdőív kérdéseit egy hétfokozatú likert skála értékének kiválasztásával tudják megválaszolni. Ezek a kérdések az érzékelt kockázatra, a várható nyereségre és az adott cselekvési lehetőség választásának valószínűségére kérdeznek rá.

A kockázatviselési hajlandóság mérése a kérdőív példáján:

„A kockázati attitűdöt a pénzügyekben használt kockázatos választás kockázati-nyereség keretrendszerében lehet megfogalmazni. Ebben a keretben az emberek kockázatos opciók iránti preferenciája feltételezhetően az opció várható hozama - amelyet általában a várható értékkel (EV) tesznek egyenlővé - és kockázatossága közötti kompromisszumot tükrözi. A pénzügyekben egy opció kockázatosságát annak varianciájával azonosítják, de a

pszichológiai kockázat-nyereség modellek az észlelt kockázatosságot olyan változónak tekintik, amely egyénenként eltérő lehet, valamint a tartalom és a kontextus függvénye:”

Ez alapján meghatározható a következő a válaszadó preferenciája az adott kérdésben:

Preferencia (X) = a(Várható haszon(X)) + b(észlelt kockázat(X)) + c [163]

Munkájuk nagy fokú érdeklődést váltott ki tudományos körökben és sok visszajelzést, szakmai krtikát kaptak, mely alapján átdolgozták, javították kérdőívüket, melyet 2006-ban publikáltak. [18]

5.2 DOSPERT kérdőív módosítása

Kutatásomhoz a kérdőív 2006-os változatának Radnóti István által magyar nyelvre lefordított változatát módosítottam; A kérdőívet kiegészítettem egy új területtel (domainnel), mely az információs és kommunikációs technológia biztonságával kapcsolatos attitűdöt méri és amely öt új kérdést tartalmaz. Ezek egyszerű, szituatív kérdések, amelyek illeszkednek a kérdőív eredeti kérdéseihez, mind tartalmukban, mind formájukban. [P12]

Ezek a kérdések a következők:

- Továbbítana-e vállalati adatokat a privát e-mail címére?

- Csatlakozna-e nyilvános, nyílt WiFi-hez?

- Engedné-e, hogy valaki az Ön előzetes beleegyezése nélkül használja az okoseszközét?

- Használná-e a pinkódját - jelszavát - feloldási mintáját mások előtt?

- Másolna-e vállalati adatokat a saját tulajdonú okostelefonjára?

Annak érdekében, hogy a kérdőív, mely a módosítás előtt 40 kérdést tartalmazott, ne váljon hosszabbá, minden domainből eltávolítottam egy-egy kérdést. Az elhagyandó kérdések kiválasztásához és az új területhez kapcsolódó kérdéseket egy kisebb mintán teszteltem. Majd a kapott eredményeket kiértékelve kisé módosítottam, és kutatásomban az előző bekezdésben bemutatott kérdéseket alkalmaztam.

A kérdések megalkotásakor törekedtem olyan viselkedési formák rövid, könnyen érthető megfogalmazására, melyek olyan cselekvésekre kérdeznek rá, melyek IT biztonsági kockázattal rendelkeznek és szinte bárki megvalósíthat.

Kutatásom célja az volt, hogy vizsgáljam magát a DOSPERT kérdőívet. Alkalmas-e a kérdőív önmagában a IT biztonsággal kapcsolatos kockázatviselést is mérni-e egyetemi hallgatók körében. Illetve, hogy a módosított kérdőív válaszadói között az adott mintában van-e szignifikáns különbség a tekintetben, hogy milyen szakon tanulnak.

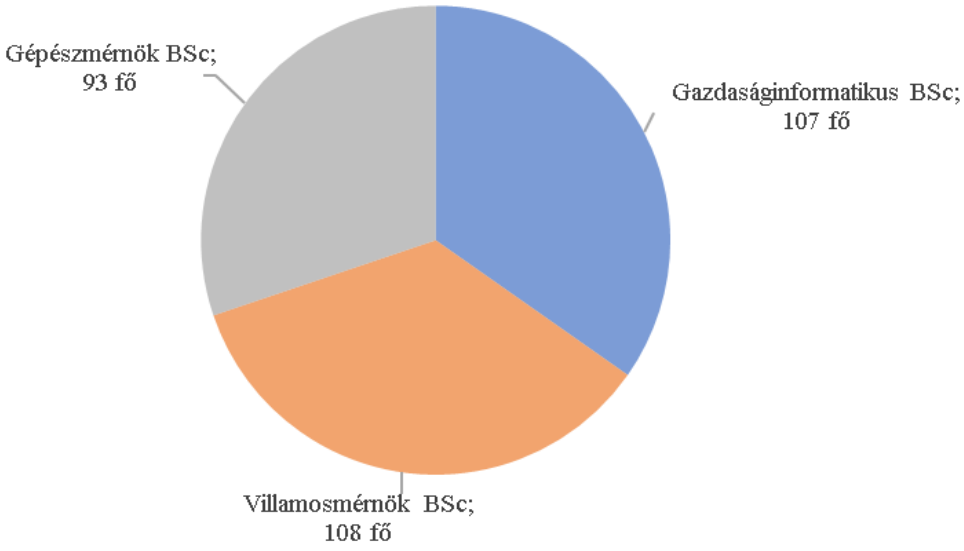
Feltételeztem tehát, hogy az IT biztonsággal kapcsolatos kérdésekben szignifikáns különbség lesz tapasztalható a hallgatók által tanult szakok alapján.

Valamint, feltételeztem, hogy a kockázatvállalási hajlandóság egy általános személyiségi tényező, mely az élet különböző domainjeiben kimutatható szinten korrelálnak egymással, s így az IT biztonsági kockázatvállalási hajlandóságot nem szükséges külön mérni.

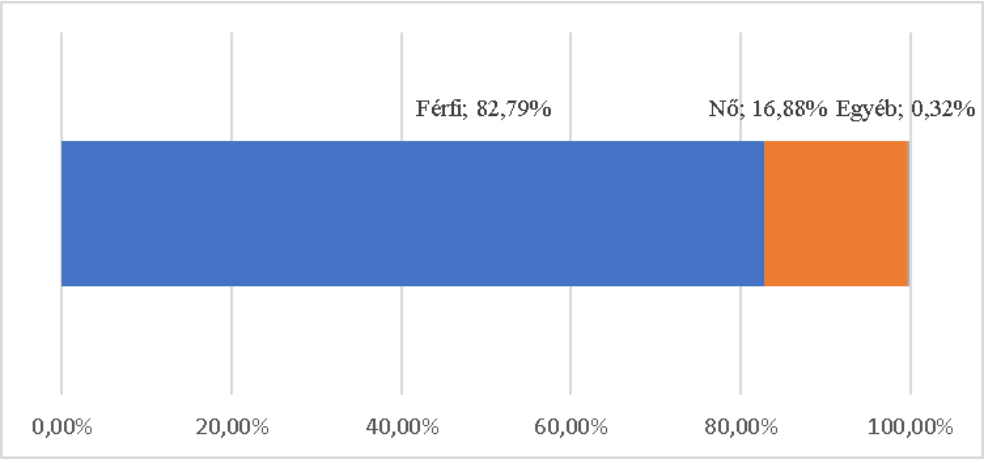
5.3 Módosított DOSPERT kérdőív – különböző szakos hallgatók vizsgálata

5.3.1 A minta jellemzése

A módosított DOSPERT kérdőívet először arra használtam, hogy megvizsgáljam van-e különbség a válaszadók között az alapján, hogy milyen szakon tanulnak.



19. ábra A mintát alkotó hallgatók általuk hallgatott szak szerint
Forrás: saját szerkesztés a minta alapján



20. ábra A mintát alkotó hallgatók nem szerinti megoszlása
Forrás: saját szerkesztés a minta alapján

5.3.2 Következtetések és javaslatok

Amint az ábrán látható, a mintában férfiak magasan felülreprezentáltak, emiatt nem tudtam vizsgálni a nemek hatását a válaszokra. Az információs és kommunikációs technológia biztonságával foglalkozó kérdések eredménye azt mutatta, hogy az érzékelt kockázat (ahol a minimum 1, a maximum 7) 3,56 és 5,51 között volt. A legmagasabb érzékelt kockázat a mások előtti pinkód/jelszó használat esetében volt, míg a legalacsonyabb értékelt kockázattal a nyilvános, nyílt WiFi hálózatokhoz történő csatlakozás rendelkezett.

6. táblázat Az IT biztonsággal kapcsolatos érzékeltkockázat értékének átlaga szakonként

	Gazdaságinformatikus Bsc	Gépészmérnök BSc	Villamosmérnöki szak BSc
Továbbítana-e vállalati adatokat a privát e-mail címére?	4,77	4,86	4,93
Csatlakozna-e nyilvános, nyílt WiFi-hez?	3,8	3,56	3,97
Engedné-e, hogy valaki az Ön előzetes beleegyezése nélkül használják a okoseszközét?	4,51	4,72	5,26
Használná-e a pinkódját - jelszavát - feloldási mintáját mások előtt?	4,98	5,06	5,51
Másolna-e vállalati adatokat a sajáttulajdonú okostelefonjára?	4,8	4,62	5,04

Forrás: saját szerkesztés a minta alapján

A kutatás első hipotézise az volt, hogy az IKT biztonsági terület észlelt kockázata lesz a legmagasabb. (H1)

A második hipotézisem az volt, hogy az IKT-biztonság szignifikánsan fontosabb az informatikai területen tanulók számára, mint a többi diák számára (H2).

7. táblázat Az érzékelt kockázatok domainenként és szakonkénti megoszlása

Field of study		Social	Financial	Health and Safety	Ethical	Recreational	Security of ICT
Business Informatics Engineer	Mean	3,8626	4,6112	4,8355	5,2336	4,6579	4,5738
	N	107	107	107	107	107	107
	Std. Deviation	,78878	1,00970	1,05502	1,03868	1,20502	1,10883
Electronical Engineering	Mean	4,0630	4,7815	5,1389	5,4500	4,5704	4,9407
	N	108	108	108	108	108	108
	Std. Deviation	,75400	,82418	,84608	,92610	,90184	1,03554
Mechanical Engineering	Mean	3,9892	4,5183	4,9806	5,2387	4,5183	4,5656
	N	93	93	93	93	93	93
	Std. Deviation	,60675	,90132	,91131	,84404	,83366	,96532
Total	Mean	3,9711	4,6429	4,9857	5,3110	4,5851	4,7000
	N	308	308	308	308	308	308
	Std. Deviation	,72833	,91871	,94806	,94625	,99819	1,05306

Forrás: saját szerkesztés a minta alapján

Amint a táblázatban látható, az IT biztonsággal kapcsolatos domain a lista közepén helyezkedik el. A gazdaságinformatikus hallgatók számára ez a terület az utolsó előtti helyen áll. Így az első hipotézisem megdőlt.

Vizsgáltam a különböző szakok hallgatói közötti különbségeket is. Csak két területen láthattunk érzékelhető különbségeket. Ezek a következők voltak:

A villamosmérnök és a gépészmérnök hallgatók között az egészség és biztonság területén, illetve - meglepő módon – a villamosmérnök és a gazdaságinformatikus hallgatók között az IT biztonság területén. Ugyanakkor a várakozásaimmal ellentétben a villamosmérnök hallgatók válaszai mutattak magasabb érzékelt kockázatot ezen a területen, így a második hipotézisem is el kellett vetnem ebben a kutatásban.

8. táblázat A T-próba eredménye a gazdaságinformatikus és a villamosmérnök hallgatók vizsgálatára

Independent Samples Test

		Levene's Test for Equality of Variances		t-test for Equality of Means						
		F	Sig.	t	df	Sig. (2-tailed)	Mean Difference	Std. Error Difference	95% Confidence Interval of the Difference	
									Lower	Upper
Health and Safety	Equal variances assumed	2,139	,145	-2,327	213	,021	-,30337	,13037	-,56035	-,04639
	Equal variances not assumed			-2,325	202,623	,021	-,30337	,13050	-,56069	-,04606
Security of ICT	Equal variances assumed	,114	,736	-2,508	213	,013	-,36691	,14631	-,65531	-,07851
	Equal variances not assumed			-2,507	211,725	,013	-,36691	,14635	-,65541	-,07841

Forrás: saját szerkesztés a minta alapján

Az érzékelt kockázat kérdésében nem volt szignifikáns különbség a gazdaságinformatikus és a gépészmérnök hallgatók csoportja között.

Következtetések: A kérdőívre adott válaszok alapján az IT-biztonság érzékelt kockázata a többi öt területet összehasonlítva a mintában a középmezőnyben vagy a középmezőny alatt van. Ez azt jelenti, hogy a minta diákjai nem érzékelnek magas kockázatot a vizsgált helyzetekben. Különösen nem gondolják, hogy a nyílt WiFi hálózatokhoz való csatlakozás magas biztonsági kockázattal járhat.

Ha részletesebben is folytatjuk az összehasonlítást a területek között, akkor láthatjuk, hogy az etikai és az egészségügyi/biztonsági területek észlelt kockázata magas, míg a szociális és az információs és kommunikációs technológiákhoz kapcsolódó biztonság területeken alacsonyabb.

Az eredményeim alapján kimondható, hogy az eredeti hipotézisem, mi szerint a gazdaságinformatikus hallgatók kockázatosabbnak érzik az IT biztonsági kérdéseket, mint a

többi diák, valamint, hogy a hallgatók körében az IT biztonsági kockázatok szerepelnek majd a legmagasabb érzékelt kockázattal, megdőlt.

Ez arra enged következtetni, hogy diákjainknak magasabb szintű IKT-biztonsági oktatásban kellene részesülniük, nem csak a nem IT szakokon.

5.4 Kutatás a módosított kérdőív IT biztonsági kérdéseiről és a válaszadók IT biztonsággal kapcsolatos szokásairól

2021-ben Buzánszky Péter hallgatómmal szakdolgozatában vizsgáltuk az IT biztonsági szokásokat egy kérdőívvel, melyet együtt állítottunk össze egy korábbi IT biztonsági szokásokat tartalmazó kérdőív és a DOSPERT kérdőívhez általam hozzáadott 5 IT biztonsági kockázattal kapcsolatos kérdésből. Buzánszky Péter szakdolgozatában az IT biztonsági szokások kutatására koncentrált, míg én az IT biztonsági magatartással kapcsolatos kérdések és azérzékelt kockázattal kapcsolatos kérdések összefüggéseit vizsgáltam, melyből 2021-ben tudományos cikk is készült. [P13]

5.4.1 A minta jellemzése

A kérdőívre válaszolók mintáját hólabda-módszerrel választottuk ki. A válaszadók életkora 18 és 60 év közötti skálán mozgott, az átlagéletkor 33,58 év, a szórás 10,33 év volt. A férfiak felülreprezentáltak a mintában, mivel a válaszadók 61%-át ők tették ki. A válaszadók 66%-a azt válaszolta, hogy még soha nem tanult szervezett formában informatikai biztonságot. Sajnos a minta mérete, valamint annak nem reprezentatívitása nem teszi lehetővé a nagymértékű általánosítást.

5.4.2 Módszertan és eredmények

Az összehasonlításhoz, figyelembe véve a minta nagyságát és a kérdések típusait, Spearman-féle korrelációt alkalmaztam. A kérdések közötti összefüggéseket vizsgálva több területen gyenge és közepes korrelációt találtam, amelyek közül a legérdekesebbek és legjelentősebbek a következők voltak:

Összefüggés a nyílt WiFi hálózatokhoz való csatlakozás kockázatának érzése és a a kétfaktoros hitelesítés használata között (n=129)

			Feeling risky for connecting open WiFi networks
Spearman's rho	Usage of two-factor authentication	Correlation Coefficient	,233**
		Sig. (2-tailed)	,008

**. Correlation is significant at the 0.01 level (2-tailed).

21. ábra Összefüggés vizsgálata a nyílt WiFi hálózatokhoz való csatlakozás kockázatának érzése és a a kétfaktoros hitelesítés használata között (n=129)
Forrás: saját szerkesztés a minta alapján

A nyílt WiFi hálózatokhoz való csatlakozás magas kockázatának érzése és a kétfaktoros hitelesítés használata közötti kapcsolat szignifikánsnak bizonyult. Ez úgy értelmezhető, hogy azok, akik kockázatosnak érzik a nyílt WiFi hálózatokhoz való csatlakozást. megnövekedett biztonságtudattal rendelkeznek, és nagyobb valószínűséggel alkalmaznak kétfaktoros hitelesítést, ahol ez lehetséges.

A nyílt WiFi hálózatokhoz való csatlakozás és az operációs rendszerek frissítése és biztonsági frissítések telepítése közötti összefüggés (n=129)

			Connecting to open WiFi networks
Spearman's rho	Installing security updates for the operating system.	Correlation Coefficient	-,205*
		Sig. (2-tailed)	,035

*. Correlation is significant at the 0.05 level (2-tailed).

22. ábra Összefüggés vizsgálata a nyílt WiFi hálózatokhoz való csatlakozás és az operációs rendszerek frissítése és biztonsági frissítések telepítése közötti összefüggés (n=129)
Forrás: saját szerkesztés a minta alapján

A nyílt WiFi hálózathoz való csatlakozás valószínűsége és a biztonsági frissítések és operációs rendszer frissítések telepítés között negatív irányú kapcsolat volt mérhető. Ez azt jelenti, hogy azok, akik nagyobb valószínűséggel telepítik a biztonsági frissítéseket a szoftvereikhez, kisebb valószínűséggel csatlakoznak nyitott, és ezért valószínűsíthetőleg nem biztonságos, WiFi hálózatokhoz.

Összefüggés a vállalati adatok privát okostelefonra történő másolása és a biztonsági frissítések és operációs rendszer frissítése között (n=129)

			Copying corporate data to private smartphone
Spearman's rho	Installing security updates for the operating system.	Correlation Coefficient	,197*
		Sig. (2-tailed)	,021

*. Correlation is significant at the 0.05 level (2-tailed).

23. ábra Összefüggés vizsgálata a vállalati adatok privát okostelefonra történő másolása és a bizton-sági frissítések és operációs rendszer frissítése között (n=129)
Forrás: saját szerkesztés a minta alapján

A mintában összefüggést tapasztaltam a biztonsági frissítések telepítése, valamint a vállalati adatok saját okostelefonra másolása között. S míg az előző kérdésben az összefüggés a biztonságtudatos magatartást támasztotta alá, itt az ellenkezőjét figyelhetjük meg, hisz míg a frissítések nyomon követése, és azok telepítése segíti a biztonsági szint növelését, addig a vállalati adatok saját okostelefonra történő másolása biztonságtudatossági kérdéseket vethet fel. A kapcsolat itt úgy értelmezhető, hogy aki törődik az eszközeinek biztonságával, az informatikai megoldásokra nyitottabb és inkább használja okostelefonját munkára is. Azonban ez magas kockázatú viselkedésnek számítanak, mivel a vállalati adatokat a cég számítógépes rendszeréből küldik ki, és így kikerülnek a vállalat ellenőrzése alól.

A vállalati adatok saját okostelefonra történő másolása és a jelszókezelő szoftver használata közötti összefüggés (n=129)

			Copying corporate data to private smartphone
Spearman's rho	Usage of password management software.	Correlation Coefficient	-,200*
		Sig. (2-tailed)	,020

*. Correlation is significant at the 0.05 level (2-tailed).

24. ábra Összefüggés vizsgálata a vállalati adatok saját okostelefonra történő másolása és a jelszókezelő szoftver használata közötti összefüggés (n=129)
Forrás: saját szerkesztés a minta alapján

A felhasználó saját okostelefonjára történő vállalati adatok másolása és a jelszókezelő szoftverek használat között egy gyenge fordított kapcsolat volt megfigyelhető. Ez a kapcsolat úgy értelmezhető, hogy akik nagyobb valószínűséggel használnak jelszókezelő

szoftvereket, azok kevésbé valószínű, hogy vállalati adatokat másolnának saját okostelefonjaikra. Mindkét viselkedési forma, mind a jelszókezelő eszközök használata, mind pedig a vállalati adatok biztonságos kezelése a biztonságtudatosság szempontjából pozitívra érékelhetőek.

Összefüggés a vállalati adatok privát e-mailben történő elküldése és az emailek csatolmányának biztonságtudatos kezelése között (n=129)

			Sending corporate data to private email
Spearman's rho	How safety conscious of dealing with an incoming email with an attachment	Correlation Coefficient	-,231**
		Sig. (2-tailed)	,009

**. Correlation is significant at the 0.01 level (2-tailed).

25. ábra Összefüggés vizsgálata a vállalati adatok privát e-mailben történő elküldése és az emailek csatolmányának biztonságtudatos kezelése között (n=129)
Forrás: saját szerkesztés a minta alapján

A minta egy másik érdekes összefüggése volt, hogy azok, akik biztonságtudatosan kezelik bejövő emailjeik csatolmányait, azok kisebb valószínűséggel küldenének ki vállalati adatokat személyes emailjükre. Ez egy, a biztonságtudatosságra utaló kapcsolat, mert a szakértők szerint az emailben kapott csatolmányok és linkek jelentette veszély ellen az elsődleges védvonal a felhasználó biztonságtudatossága. Ha a felhasználó minden linkre rákattint, vagy minden csatolmányt megnyit, amit emailben kap, mindenféle előzetes szűrés nélkül, az nagyobb valószínűséggel fog veszélyes csatolmányt megnyitni, vagy veszélyes weboldalra látogatni.

5.4.3 Következtetések és javaslatok

A Buzánszky Péter segítségével végzett kutatás mintanagysága alacsony volt és a minta nem volt reprezentatívnak tekinthető, így széleskörben nem tudjuk általánosítani az általunk végzett kutatás és elemzés eredményeit, mégis a mintából származó adatokat más kutatások eredményével összehasonlítva érdekes és hasznos eredményeket határozhatunk meg.

Valamint a kutatás alapján az is kijelenthető, hogy érdemes a DOSPERT kérdőívet kiegészítő IT biztonsággal kapcsolatos kérdéseket a biztonságtudatos magatartás vizsgálatára is használni.

5.5 Kutatás a módosított kérdőív szükségességéről

5.5.1 A módosított kérdőív szükségességének vizsgálata

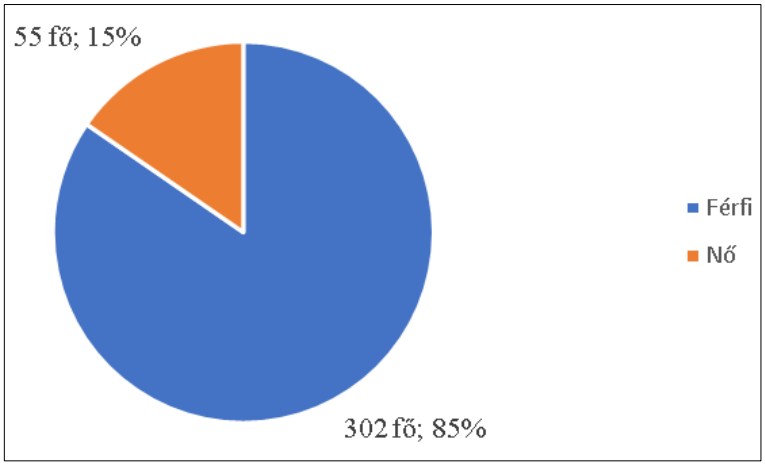
A korábban módosított DOSPERT kérdőív használata során felmerült a kérdés, mely szerint szükséges-e kifejezetten az IT biztonsággal kapcsolatos kockázatvállalási hajlandóság mérése, vagy a DOSPERT kérdőív eredeti kérdései közül a meghagyott 35 kérdés képes-e előre jelezni az általam megalkotott kérdésekre adott válaszokat.0

Ennek vizsgálatához regressziószámítást alkalmaztam, melynek eredményeit a következő alfejezetekben ismeretetem.

5.5.2 A minta jellemzése

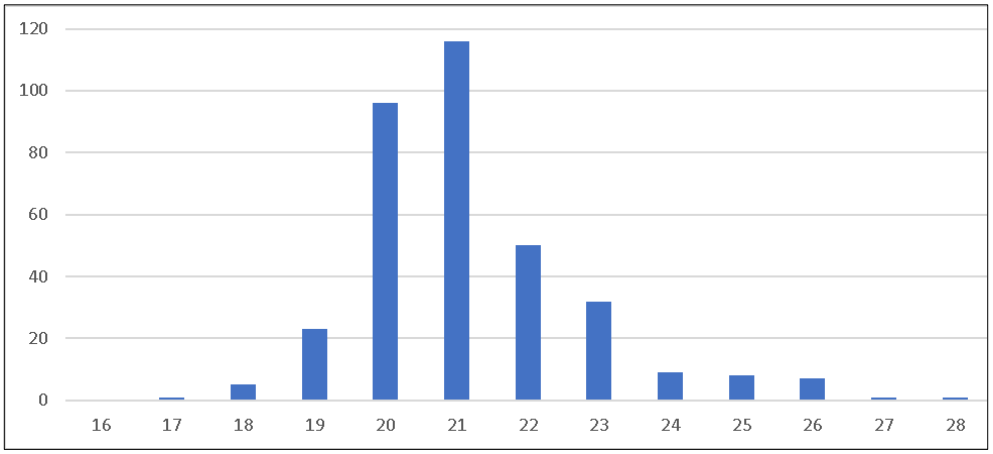
A minta felvételére 2019. őszén került sor online kérdőív segítségével. A hallgatóktól a kockázatvállalási hajlandóságon kívül minimális demográfiai adatfelvétel történt (kor, nem, hallgatott szak).

A minta nagysága 357 fő volt. Ebből 302 férfi, 55 nő volt.



26. ábra A nemek aránya a mintában
Forrás: saját szerkesztés a minta alapján

A válaszadók átlagos kora 21,479 év volt, az átlagtól való átlagos eltérés pedig 2,684 év volt, így mondhatjuk, hogy a mintában döntően 19-24 év közötti válaszadók voltak.



27. ábra A válaszadók kor szerinti megoszlása
Forrás: saját szerkesztés a minta alapján

A képzések és megoszlásuk a következő volt:

9. táblázat A válaszadó hallgatók által tanult szakok megoszlása a mintában

Szak	fő
Gépészmérnök BSc	96
Mechatronikai mérnök BSc	1
Villamosmérnöki szak BSc	135
Gazdasági Informatikus BSc	72
Műszaki Menedzser BSc	2
Gazdálkodási és menedzsment BSc	28
Kereskedelem és marketing BSc	17
Kereskedelem és marketing felsőoktatási szakképzés	3
Gazdálkodási és menedzsment felsőoktatási szakképzés	3

Forrás: saját szerkesztés a minta alapján

5.5.3 Eredmények

Továbbítana-e vállalati adatokat a privát e-mail címére?

Model Summary - ICT KOCKÁZAT Vállalati adatokat a privát emailcímemre továbbítani. 3

Model	R	R^2	Adjusted R^2	RMSE
H_0	0.000	0.000	0.000	1.614
H_1	0.576	0.332	0.277	1.372

ANOVA

Model		Sum of Squares	df	Mean Square	F	p
H_1	Regression	307.977	27	11.407	6.061	< .001
	Residual	619.155	329	1.882		
	Total	927.132	356			

Note. The intercept model is omitted, as no meaningful information can be shown.

Coefficients

Model		Unstandardized	Standard Error	Standardized	t	p
H_0	(Intercept)	3.852	0.085		45.094	< .001
H_1	(Intercept)	-0.125	0.472		-0.265	0.791
	E KOCKÁZAT Megkérdőjelezhető költségeket leírni az adóbevallásban.3	0.217	0.069	0.186	3.141	0.002
	E KOCKÁZAT Más munkáját a sajátomként felhasználni. 3	0.103	0.062	0.090	1.666	0.097
	E KOCKÁZAT Egy barát titkát kifecsegni. 3	0.030	0.059	0.027	0.510	0.611
	E KOCKÁZAT Egy kisgyereket magára hagyni otthon egyedül, amíg elmegy a boltba. 3	0.180	0.056	0.175	3.238	0.001
	E KOCKÁZAT Egy 50.000 Ft-ot tartalmazó pénztárcát megtartani. 2	0.028	0.050	0.030	0.570	0.569
	F KOCKÁZAT A napi jövedelmem feltenni lóversenyre. 3	0.053	0.070	0.047	0.748	0.455
	F KOCKÁZAT Az éves jövedelmem 10% -át befektetni egy mérsékelt növekedésű, diverzifikált alapba. 3	0.001	0.064	8.192×10^{-4}	0.016	0.987
	F KOCKÁZAT Egy napi jövedelmet feltenni egy kockázatos pókerjátszmában. 3	-0.100	0.071	-0.090	-1.422	0.156
	F KOCKÁZAT Az éves jövedelmem 5%-át egy magaskockázatú befektetésbe fektetni. 3	-0.014	0.063	-0.013	-0.232	0.817
	F KOCKÁZAT Egy napi jövedelmet feltenni egy sportmérközésre. 3	0.065	0.070	0.061	0.929	0.354
	F KOCKÁZAT Az éves jövedelmem 10%-át egy új üzleti lehetőségbe fektetni. 3	0.059	0.067	0.049	0.884	0.378
	H KOCKÁZAT Túl sok alkoholt fogyasztani egy társadalmi eseményen, például egy esküvőn. 3	0.047	0.052	0.049	0.917	0.360
	H KOCKÁZAT Biztonságiöv viselése nélkül vezetni. 3	0.064	0.069	0.061	0.934	0.351
	H KOCKÁZAT Bukósisak nélkül motorozni.3	-0.039	0.079	-0.031	-0.494	0.622
	H KOCKÁZAT Naptej nélkül napozni. 3	-0.042	0.056	-0.039	-0.761	0.447
	H KOCKÁZAT Hazasétálni egyedül egy nem biztonságos városrészben. 3	0.241	0.064	0.201	3.760	< .001
	R KOCKÁZAT Olyan sípályán lesiklani, ami meghaladja a képességeim. 3	-0.042	0.065	-0.036	-0.649	0.517
	R KOCKÁZAT Vadvizi evezésre menni tavasszal, nagy vízállás esetén.3	-0.004	0.063	-0.004	-0.063	0.950
	R KOCKÁZAT Ejtőernyőzni.3	-0.011	0.064	-0.011	-0.172	0.864
	R KOCKÁZAT Bungeejumpingozni egy magas hídról. 3	0.034	0.066	0.034	0.519	0.604
	R KOCKÁZAT Kis repülőgépet vezetni. 3	-0.101	0.058	-0.095	-1.721	0.086
	S KOCKÁZAT Beismerni egy barátomnak, hogy az ízlésem különbözik az övétől.3	-0.063	0.059	-0.053	-1.069	0.286
	S KOCKÁZAT Egy hatósági személlyel összekülönbözni.3	0.063	0.069	0.052	0.912	0.362
	S KOCKÁZAT Izgalmasabb karrierbe kezdeni egy biztosabb karrirer helyett. 2	-0.077	0.081	-0.052	-0.954	0.341
	S KOCKÁZAT Egy kellemetlen témáról beszélni egy munkahelyi megbeszélésen. 2	0.040	0.069	0.031	0.569	0.569
	S KOCKÁZAT A családtól és a rokonoktól távolra költözni. 3	0.148	0.063	0.124	2.361	0.019
	S KOCKÁZAT Harmincötévesen új karrierbe kezdeni. 2	0.157	0.075	0.118	2.076	0.039

28. ábra Regresszió számítás eredménye
a privát e-mail címre továbbított vállalati adatok kérdése és a további kérdések között
Forrás: saját szerkesztés a minta alapján

Az eredményekből az látszik, hogy nagymértékű összefüggés e kérdés és a többi kérdés között nem mutatható ki. Érdekes módon egyedül a „Hazasétálni egyedül egy nem biztonságos városrészben” kérdéssel kapcsolatban mutatható ki gyenge pozitív kapcsolat.

Csatlakozna-e nyilvános, nyílt WiFi-hez?

Model Summary - ICT KOCKÁZAT Egy nyilvános wifihez csatlakozni. 3

Model	R	R^2	Adjusted R^2	RMSE
H_0	0.000	0.000	0.000	1.568
H_1	0.425	0.181	0.114	1.476

ANOVA

Model		Sum of Squares	df	Mean Square	F	p
H_1	Regression	158.293	27	5.863	2.692	< .001
	Residual	716.564	329	2.178		
	Total	874.857	356			

Note. The intercept model is omitted, as no meaningful information can be shown.

Coefficients

Model		Unstandardized	Standard Error	Standardized	t	p
H_0	(Intercept)	2.714	0.083		32.715	< .001
H_1	(Intercept)	0.443	0.508		0.872	0.384
	E KOCKÁZAT Megkérdőjelezhető költségeket leírni az adóbevallásban.3	-0.033	0.074	-0.029	-0.439	0.661
	E KOCKÁZAT Más munkáját a sajátomként felhasználni. 3	0.048	0.066	0.043	0.722	0.471
	E KOCKÁZAT Egy barát titkát kifecsegni. 3	0.088	0.064	0.081	1.382	0.168
	E KOCKÁZAT Egy kisgyereket magára hagyni otthon egyedül, amíg elmegy a boltba. 3	-0.093	0.060	-0.093	-1.551	0.122
	E KOCKÁZAT Egy 50.000 Ft-ot tartalmazó pénztárcát megtartani. 2	0.012	0.054	0.013	0.226	0.821
	F KOCKÁZAT A napi jövedelmem feltenni lóversenyre. 3	-0.014	0.076	-0.013	-0.182	0.855
	F KOCKÁZAT Az éves jövedelmem 10% -át befektetni egy mérsékelt növekedésű, diverzifikált alapba. 3	0.065	0.069	0.055	0.951	0.342
	F KOCKÁZAT Egy napi jövedelmet feltenni egy kockázatos pókerjátszmában. 3	-0.134	0.076	-0.123	-1.765	0.078
	F KOCKÁZAT Az éves jövedelmem 5%-át egy magaskockázatú befektetésbe fektetni. 3	0.065	0.067	0.058	0.960	0.338
	F KOCKÁZAT Egy napi jövedelmet feltenni egy sportmérközésre. 3	-0.045	0.075	-0.043	-0.599	0.549
	F KOCKÁZAT Az éves jövedelmem 10%-át egy új üzleti lehetőségbe fektetni. 3	0.017	0.072	0.014	0.233	0.816
	H KOCKÁZAT Túl sok alkoholt fogyasztani egy társadalmi eseményen, például egy esküvőn. 3	0.023	0.056	0.024	0.408	0.684
	H KOCKÁZAT Biztonságiöv viselése nélkül vezetni. 3	0.122	0.074	0.118	1.643	0.101
	H KOCKÁZAT Bukósisak nélkül motorozni.3	-0.043	0.085	-0.035	-0.504	0.614
	H KOCKÁZAT Naptej nélkül napozni. 3	0.090	0.060	0.086	1.511	0.132
	H KOCKÁZAT Hazasétálni egyedül egy nem biztonságos városrészben. 3	0.205	0.069	0.176	2.966	0.003
	R KOCKÁZAT Olyan sípályán lesiklani, ami meghaladja a képességeim. 3	-0.024	0.070	-0.021	-0.345	0.730
	R KOCKÁZAT Vadvízi evezésre menni tavasszal, nagy vízállás esetén.3	-0.026	0.068	-0.024	-0.384	0.701
	R KOCKÁZAT Ejtőernyőzni.3	-0.034	0.069	-0.034	-0.493	0.622
	R KOCKÁZAT Bungeejumpingozni egy magas hídról. 3	0.017	0.071	0.018	0.241	0.809
	R KOCKÁZAT Kis repülőgépet vezetni. 3	0.130	0.063	0.126	2.060	0.040
	S KOCKÁZAT Beismerni egy barátomnak, hogy az ízlésem különbözik az övétől.3	0.110	0.063	0.096	1.743	0.082
	S KOCKÁZAT Egy hatósági személlyel összekülönbözni.3	-0.021	0.074	-0.018	-0.281	0.779
	S KOCKÁZAT Izgalmasabb karrierbe kezdeni egy biztosabb karrirer helyett. 2	0.019	0.087	0.013	0.214	0.831
	S KOCKÁZAT Egy kellemetlen témáról beszélni egy munkahelyi megbeszélésen. 2	0.181	0.075	0.149	2.427	0.016
	S KOCKÁZAT A családtól és a rokonoktól távolra költözni. 3	-0.006	0.067	-0.005	-0.091	0.927
	S KOCKÁZAT Harmincötévesen új karrierbe kezdeni. 2	0.075	0.081	0.059	0.929	0.354

29. ábra Regresszió számítás eredménye
a nyilvánosan elérhető nyílt WiFi hálózatokhoz való csatlakozás kérdése és a további kérdések között
Forrás: saját szerkesztés a minta alapján

A következő kérdés a csatlakozna-e nyilvános, nyílt WiFi hálózathoz volt, ez és másik kérdések között nem volt szignifikáns kapcsolat kimutatható a mintában.

Használná-e a pinkódját - jelszavát - feloldási mintáját mások előtt?

Model Summary - ICT KOCKÁZAT Mások előtt a pinkódomat / biztonsági mintámat használni. 2

Model	R	R^2	Adjusted R^2	RMSE
H_0	0.000	0.000	0.000	1.536
H_1	0.567	0.322	0.266	1.316

ANOVA

Model		Sum of Squares	df	Mean Square	F	p
H_1	Regression	270.084	27	10.003	5.776	< .001
	Residual	569.798	329	1.732		
	Total	839.882	356			

Note. The intercept model is omitted, as no meaningful information can be shown.

Coefficients

Model		Unstandardized	Standard Error	Standardized	t	p
H_0	(Intercept)	4.176	0.081		51.376	< .001
H_1	(Intercept)	0.645	0.453		1.423	0.156
	E KOCKÁZAT Megkérdőjelezhető költségeket leírni az adóbevallásban.3	-0.071	0.066	-0.064	-1.072	0.285
	E KOCKÁZAT Más munkáját a sajátomként felhasználni. 3	0.156	0.059	0.144	2.638	0.009
	E KOCKÁZAT Egy barát titkát kifecsegni. 3	0.113	0.057	0.107	1.993	0.047
	E KOCKÁZAT Egy kisgyereket magára hagyni otthon egyedül, amíg elmegy a boltba. 3	0.056	0.053	0.057	1.047	0.296
	E KOCKÁZAT Egy 50.000 Ft-ot tartalmazó pénztárcát megtartani. 2	0.026	0.048	0.028	0.536	0.592
	F KOCKÁZAT A napi jövedelmem feltenni lóversenyre. 3	0.009	0.067	0.009	0.139	0.890
	F KOCKÁZAT Az éves jövedelmem 10% -át befektetni egy mérsékelt növekedésű, diverzifikált alapba. 3	-0.034	0.061	-0.030	-0.561	0.575
	F KOCKÁZAT Egy napi jövedelmet feltenni egy kockázatos pókerjátszmában. 3	0.003	0.068	0.003	0.048	0.962
	F KOCKÁZAT Az éves jövedelmem 5%-át egy magaskockázatú befektetésbe fektetni. 3	0.086	0.060	0.079	1.435	0.152
	F KOCKÁZAT Egy napi jövedelmet feltenni egy sportmérkőzésre. 3	-0.046	0.067	-0.046	-0.692	0.489
	F KOCKÁZAT Az éves jövedelmem 10%-át egy új üzleti lehetőségbe fektetni. 3	-0.015	0.064	-0.013	-0.240	0.811
	H KOCKÁZAT Túl sok alkoholt fogyasztani egy társadalmi eseményen, például egy esküvőn. 3	0.058	0.050	0.063	1.180	0.239
	H KOCKÁZAT Biztonságiöv viselése nélkül vezetni. 3	0.054	0.066	0.053	0.812	0.418
	H KOCKÁZAT Bukósisak nélkül motorozni.3	0.111	0.076	0.094	1.469	0.143
	H KOCKÁZAT Naptej nélkül napozni. 3	0.104	0.053	0.100	1.944	0.053
	H KOCKÁZAT Hazasétálni egyedül egy nem biztonságos városrészben. 3	0.212	0.062	0.186	3.453	< .001
	R KOCKÁZAT Olyan sípályán lesiklani, ami meghaladja a képességeim. 3	-0.056	0.062	-0.050	-0.900	0.369
	R KOCKÁZAT Vadvízi evezésre menni tavasszal, nagy vízállás esetén.3	-0.062	0.061	-0.059	-1.020	0.308
	R KOCKÁZAT Ejtőernyőzni.3	-0.101	0.061	-0.105	-1.651	0.100
	R KOCKÁZAT Bungeejumpingozni egy magas hídról. 3	0.241	0.063	0.256	3.839	< .001
	R KOCKÁZAT Kis repülőgépet vezetni. 3	-0.075	0.056	-0.075	-1.340	0.181
	S KOCKÁZAT Beismerni egy barátomnak, hogy az izlésem különbözik az övétől.3	0.055	0.056	0.049	0.977	0.330
	S KOCKÁZAT Egy hatósági személlyel összekülönbözni.3	0.011	0.066	0.009	0.162	0.871
	S KOCKÁZAT Izgalmasabb karrierbe kezdeni egy biztosabb karrirer helyett. 2	-0.086	0.078	-0.060	-1.103	0.271
	S KOCKÁZAT Egy kellemetlen témáról beszélni egy munkahelyi megbeszélésen. 2	0.095	0.067	0.080	1.430	0.154
	S KOCKÁZAT A családtól és a rokonoktól távolra költözni. 3	-0.054	0.060	-0.048	-0.908	0.364
	S KOCKÁZAT Harmincötévesen új karrierbe kezdeni. 2	0.143	0.072	0.114	1.982	0.048

30. ábra Regresszió számítás eredménye
a válaszadó pinkódjának vagy jelszavának használata mások előtt kérdés és a további kérdések között
Forrás: saját szerkesztés a minta alapján

Annál a kérdésnél, engedné-e a válaszadó, hogy más lássa az ő jelszavát, vagy pinkódját két gyenge kapcsolat volt kimutatható. Az egyik ismételten a „hazasétálni egyedül egy nem biztonságos városrészben” kérdés volt, míg a másik, a „Bungeejumpingozni egy magas hídról”.

Engedné-e, hogy valaki az Ön előzetes beleegyezése nélkül használják a okoseszközét?

Model Summary - ICT KOCKÁZAT Hagyni, hogy más használja a telefonját a tudta nélkül. 3

Model	R	R^2	Adjusted R^2	RMSE
H_0	0.000	0.000	0.000	1.566
H_1	0.552	0.305	0.248	1.358

ANOVA

Model		Sum of Squares	df	Mean Square	F	p
H_1	Regression	266.259	27	9.861	5.345	< .001
	Residual	606.956	329	1.845		
	Total	873.216	356			

Note. The intercept model is omitted, as no meaningful information can be shown.

Coefficients

Model		Unstandardized	Standard Error	Standardized	t	p
H_0	(Intercept)	3.843	0.083		46.364	< .001
H_1	(Intercept)	0.501	0.468		1.071	0.285
	E KOCKÁZAT Megkérdőjelezhető költségeket leírni az adóbevallásban.3	0.049	0.069	0.043	0.716	0.475
	E KOCKÁZAT Más munkáját a sajátomként felhasználni. 3	0.017	0.061	0.015	0.281	0.779
	E KOCKÁZAT Egy barát titkát kifecsegni. 3	0.232	0.059	0.214	3.954	< .001
	E KOCKÁZAT Egy kisgyereket magára hagyni otthon egyedül, amíg elmegy a boltba. 3	0.069	0.055	0.069	1.257	0.210
	E KOCKÁZAT Egy 50.000 Ft-ot tartalmazó pénztárcát megtartani. 2	0.042	0.050	0.045	0.841	0.401
	F KOCKÁZAT A napi jövedelmem feltenni lóversenyre. 3	0.009	0.069	0.008	0.127	0.899
	F KOCKÁZAT Az éves jövedelmem 10% -át befektetni egy mérsékelt növekedésű, diverzifikált alapba. 3	-0.032	0.063	-0.027	-0.498	0.619
	F KOCKÁZAT Egy napi jövedelmet feltenni egy kockázatos pókerjátszmában. 3	-0.008	0.070	-0.007	-0.112	0.911
	F KOCKÁZAT Az éves jövedelmem 5%-át egy magaskockázatú befektetésbe fektetni. 3	-0.132	0.062	-0.119	-2.134	0.034
	F KOCKÁZAT Egy napi jövedelmet feltenni egy sportmérkőzésre. 3	0.143	0.069	0.138	2.065	0.040
	F KOCKÁZAT Az éves jövedelmem 10%-át egy új üzleti lehetőségbe fektetni. 3	-0.059	0.066	-0.051	-0.898	0.370
	H KOCKÁZAT Túl sok alkoholt fogyasztani egy társadalmi eseményen, például egy esküvőn. 3	-0.002	0.051	-0.002	-0.035	0.972
	H KOCKÁZAT Biztonságiöv viselése nélkül vezetni. 3	0.021	0.068	0.020	0.308	0.758
	H KOCKÁZAT Bukósisak nélkül motorozni.3	-6.432×10^{-4}	0.078	-5.340×10^{-4}	-0.008	0.993
	H KOCKÁZAT Naptej nélkül napozni. 3	0.092	0.055	0.087	1.671	0.096
	H KOCKÁZAT Hazasétálni egyedül egy nem biztonságos városrészben. 3	0.155	0.063	0.133	2.438	0.015
	R KOCKÁZAT Olyan sípályán lesiklani, ami meghaladja a képességeim. 3	0.112	0.064	0.099	1.750	0.081
	R KOCKÁZAT Vadvízi evezésre menni tavasszal, nagy vízállás esetén.3	0.002	0.063	0.002	0.040	0.968
	R KOCKÁZAT Ejtőernyőzni.3	-0.053	0.063	-0.053	-0.829	0.408
	R KOCKÁZAT Bungeejumpingozni egy magas hídról. 3	0.081	0.065	0.084	1.242	0.215
	R KOCKÁZAT Kis repülőgépet vezetni. 3	-0.136	0.058	-0.133	-2.355	0.019
	S KOCKÁZAT Beismerni egy barátomnak, hogy az ízlésem különbözik az övétől.3	0.037	0.058	0.032	0.630	0.529
	S KOCKÁZAT Egy hatósági személlyel összekülönbözni.3	-0.034	0.068	-0.029	-0.506	0.613
	S KOCKÁZAT Izgalmasabb karrierbe kezdeni egy biztosabb karrirer helyett. 2	0.079	0.080	0.054	0.977	0.329
	S KOCKÁZAT Egy kellemetlen témáról beszélni egy munkahelyi megbeszélésen. 2	0.137	0.069	0.113	1.999	0.046
	S KOCKÁZAT A családtól és a rokonoktól távolra költözni. 3	0.079	0.062	0.068	1.270	0.205
	S KOCKÁZAT Harmincötévesen új karrierbe kezdeni. 2	0.014	0.075	0.011	0.193	0.847

31. ábra Regresszió számítás eredménye
a beleegyezés nélküli használat kérdése és a további kérdések között
Forrás: saját szerkesztés a minta alapján

A kérdésnél, hogy a válaszadó engedné-e más számára, hogy a beleegyezése nélkül használja az okostelefonját vagy tabletjét egy gyenge kapcsolat volt kimutatható azzal, hogy a válaszadó szerint mennyire kockázatos egy barát titkát kifecsegni, de e két kérdés között is a kapcsolat erőssége gyenge pozitív volt.

Másolna-e vállalati adatokat a sajáttulajdonú okostelefonjára?

Model Summary - ICT KOCKÁZAT Munkahelyi adatok, dokumentumok mobiltelefonra másolása. 3

Model	R	R^2	Adjusted R^2	RMSE
H_0	0.000	0.000	0.000	1.702
H_1	0.529	0.280	0.221	1.502

ANOVA

Model		Sum of Squares	df	Mean Square	F	p
H_1	Regression	288.405	27	10.682	4.734	< .001
	Residual	742.407	329	2.257		
	Total	1030.812	356			

Note. The intercept model is omitted, as no meaningful information can be shown.

Coefficients

Model		Unstandardized	Standard Error	Standardized	t	p
H_0	(Intercept)	3.868	0.090		42.953	< .001
H_1	(Intercept)	-0.328	0.517		-0.634	0.527
	E KOCKÁZAT Megkérdőjelezhető költségeket leírni az adóbevallásban.3	0.269	0.076	0.218	3.548	< .001
	E KOCKÁZAT Más munkáját a sajátomként felhasználni. 3	0.127	0.067	0.105	1.880	0.061
	E KOCKÁZAT Egy barát titkát kifecsegni. 3	0.067	0.065	0.057	1.028	0.305
	E KOCKÁZAT Egy kisgyereket magára hagyni otthon egyedül, amíg elmegy a boltba. 3	0.126	0.061	0.117	2.076	0.039
	E KOCKÁZAT Egy 50.000 Ft-ot tartalmazó pénztárcát megtartani. 2	0.010	0.055	0.010	0.184	0.854
	F KOCKÁZAT A napi jövedelmem feltenni lóversenyre. 3	0.110	0.077	0.093	1.433	0.153
	F KOCKÁZAT Az éves jövedelmem 10% -át befektetni egy mérsékelt növekedésű, diverzifikált alapba. 3	0.037	0.070	0.029	0.533	0.595
	F KOCKÁZAT Egy napi jövedelmet feltenni egy kockázatos pókerjátszmában. 3	-0.121	0.077	-0.103	-1.570	0.117
	F KOCKÁZAT Az éves jövedelmem 5%-át egy magaskockázatú befektetésbe fektetni. 3	0.156	0.069	0.129	2.282	0.023
	F KOCKÁZAT Egy napi jövedelmet feltenni egy sportmérkőzésre. 3	-0.033	0.077	-0.029	-0.429	0.668
	F KOCKÁZAT Az éves jövedelmem 10%-át egy új üzleti lehetőségbe fektetni. 3	0.104	0.073	0.083	1.430	0.154
	H KOCKÁZAT Túl sok alkoholt fogyasztani egy társadalmi eseményen, például egy esküvőn. 3	-0.015	0.057	-0.014	-0.263	0.793
	H KOCKÁZAT Biztonságiöv viselése nélkül vezetni. 3	0.010	0.076	0.009	0.138	0.891
	H KOCKÁZAT Bukósisak nélkül motorozni.3	-0.050	0.086	-0.038	-0.581	0.561
	H KOCKÁZAT Naptej nélkül napozni. 3	-0.013	0.061	-0.011	-0.215	0.830
	H KOCKÁZAT Hazasétálni egyedül egy nem biztonságos városrészben. 3	0.130	0.070	0.103	1.853	0.065
	R KOCKÁZAT Olyan sípályán lesiklani, ami meghaladja a képességeim. 3	-0.122	0.071	-0.099	-1.714	0.087
	R KOCKÁZAT Vadvízi evezésre menni tavasszal, nagy vízállás esetén.3	0.021	0.069	0.018	0.299	0.765
	R KOCKÁZAT Ejtőernyőzni.3	0.123	0.070	0.114	1.751	0.081
	R KOCKÁZAT Bungeejumpingozni egy magas hídról. 3	-0.009	0.072	-0.009	-0.128	0.898
	R KOCKÁZAT Kis repülőgépet vezetni. 3	0.003	0.064	0.002	0.042	0.967
	S KOCKÁZAT Beismerni egy barátomnak, hogy az ízlésem különbözik az övétől.3	-0.044	0.064	-0.036	-0.687	0.493
	S KOCKÁZAT Egy hatósági személlyel összeküllönbözni.3	0.032	0.075	0.025	0.422	0.673
	S KOCKÁZAT Izgalmasabb karrierbe kezdeni egy biztosabb karrirer helyett. 2	-0.044	0.089	-0.028	-0.492	0.623
	S KOCKÁZAT Egy kellemetlen témáról beszélni egy munkahelyi megbeszélésen. 2	0.208	0.076	0.157	2.730	0.007
	S KOCKÁZAT A családtól és a rokonoktól távolra költözni. 3	-0.031	0.068	-0.025	-0.454	0.650
	S KOCKÁZAT Harmincötévesen új karrierbe kezdeni. 2	0.012	0.083	0.008	0.141	0.888

32. ábra Regresszió számítás eredménye
a vállalati adatok saját tulajdonú okostelefonra történő másolásának kérdése és a további kérdések között
Forrás: saját szerkesztés a minta alapján

A munkahelyi adatok, dokumentumok telefonra történő másolása kérdés és a „megkérdőjelezhető költségeket leírni az adóbevallásban” kérdés között volt kimutatható gyenge pozitív kapcsolat.

Összességében elmondható, hogy a hipotézisemmel ellentétben szignifikáns összefüggés általánosságban nem mutatható ki a mintában az IT biztonsági kérdések és más kérdések kockázatvállalási hajlandósága között.

5.5.4 Következtetések, javaslatok a kutatás alapján

Az eredményeim alapján kijelenthető, hogy a minta esetében a DOSPERT eredeti kérdései önmagukban nem voltak képesek előre jelezni az IT biztonsággal kapcsolatos kérdésekre adott válaszokat; közöttük egyértelmű, erős vagy akár csak közepes regressziós kapcsolat nem volt bizonyítható.

Ez alapján, azon feltételezésem, mely szerint a DOSPERT kérdőív önmagában képes lehet a IT kockázatvállalási hajlandóság előrejelzésére elvetendő. Így önmagában e kérdőív alkalmazása fiatal felnőttek IT biztonsági kockázatvállalási hajlandóságára nem alkalmazható, szükséges egy új biztonságtudatossági felmérési eszköz készítése, mely segítheti a leendő és jelenlegi munkavállalók IT kockázatvállalási szokásainak felmérését, így a vállalati IT biztonsági szint növelését.

6 ÚJ TUDOMÁNYOS EREDMÉNYEK

I. Megalkottam a saját tulajdonú mobileszközök definícióját és rendszerbe foglaltam a saját tulajdonú eszközök vállalati használatának kockázatait. [P1][P2][P3][P4][P5][P6][P7][P9]

Definiáltam, hogy mit tekinthetünk olyan mobil informatikai eszköznek, mely használata különösen nagy kockázattal rendelkezik; olyan hordozható informatikai eszköz, mely képességeit tekintve közel azonos egy általános számítógép képességeivel; hálózati átviteli kapacitás, képernyő felbontás, memória kapacitás és számítási kapacitás tekintetében, azonban a felhasználó megítélése szerint nem laptop vagy számítógép és a munkavállaló tulajdonában áll.

II. Bizonyítottam az ember-eszköz-infrastruktúra információbiztonsági kölcsönös függését [P1][P2][P3][P4][P5][P6][P7]

Mely alapján kimondható, hogy információbiztonság-tudatos felhasználó, kockázat minimalizált saját tulajdonú mobil eszköz és hálózati infrastruktúra nélkül kezelhetetlen. A kockázatok javasolt csoportosítása a következő:

K1. A készülék szoftverének vagy hardverének jogosulatlan módosítása

K2. A hangkommunikáció lehallgatása vagy kiszivárogtatása

K3. Rosszindulatú szoftverek, beleértve a vírusokat, zsarolóprogramokat, trójai vírusokat, kémprogramokat stb.

K4. Túlterheléses támadások és szolgáltatásmegtagadás, különösen, ha a készüléket túlterhelik, ezzel az eszköz lefagy, lesüketül, vagy a kommunikációt lehetetlenné teszik.

K5. Az eszközökhöz kapcsolódó szoftveres kockázatok (amelyek a firmware-ből, az operációs rendszerekből és a telepített programokból erednek). A biztonsági frissítések rendszeres telepítésének ellehetetlenítése, a szoftverek megbízhatatlan helyekről történő telepítése és egyéb szoftveres kockázatok.

K6. Adatátviteli kockázatok, mint például az eszköz lehallgatása az adatátviteli csatornákon keresztül vagy man-in-the-middle támadások.

K7. A felhasználók gondatlansága és a biztonságtudatosság hiánya, például gondatlan adatfeldolgozás, az eszköz felügyelet nélkül hagyása, az eszköz elvesztése vagy ellopásának lehetővé tétele, az emberi viselkedést kihasználó támadások (social engineering technikák), az üzleti és a magánélet szétválasztásának hiánya.

K8. Az eszköz elidegenítésével kapcsolatban felmerülő kockázatok, ideértve többek között az adatok nem teljes törlését vagy a hozzáférési jogosultságok nem megfelelő törlését.

K9. Heterogén/ellenőrizhetetlen végponti IKT-infrastruktúra (eszközök és operációs rendszerek sokfélesége) és emiatt nem megfelelő informatikai támogatása.

III. Kialakítottam a BYOD alapstratégiákat (tiltott, tűrt, támogatott) és kialakítottam egy olyan döntéselméleti módszertant, mely segít a szervezetek, vállalatok számára a BYOD alapstratégia kiválasztására és a BYOD kockázatok minimalizálására. Ehhez kapcsolódóan megalkottam egy olyan szabályozásra vonatkozó ajánlást, mely alkalmas a PDCA alapú BYOD biztonsági keretrendszer megalkotására és üzemeltetésére. [P8]

A szervezetekben a BYOD-val kapcsolatban szükséges kialakítani egy alapstratégiát, mely javaslatom szerint három alapstratégia lehet: tiltott, tűrt és támogatott.

A támogatott alapstratégiát választva három alkalmazási szintet különböztettem meg:
- esetileg szóban szabályozott,
- írásban szabályozott,
- írásban szabályozott és aktívan támogatott.

Témavezetőmmel kialakítottunk egy olyan kockázatbecslésen alapuló döntéstámogatási módszertant, mely a II-es számú eredményben ismeretetett kockázatcsoportok kockázatbecslésével segít dönteni az adott szervezetben alkalmazott BYOD stratégiák közül. Az így kiválasztott alapstratégia alapján kialakított szabályozást javaslatom szerint PDCA alapú folyamos javítás elve szerint szükséges karbantartani.

A PDCA (Plan-Do-Check-Act) elv egy a mérnöki tervezési folyamatokban régóta használt, és gyakorlatban is bizonyított folyamatos, iteratív javítás elve, az egyre magasabb szintű megvalósítás felé. A folyamat minden egyes iterációban a tervezett javítás végrehajtása után visszacsatol és egy magasabb szintű megvalósítás cél megtervezésével folytatódik.

Ez az elv alkalmazható a BYOD szabályzatok folyamatos karbantartására, hogy lekövesse a szervezetben és a környezetben a legutolsó iteráció óta bekövetkezett változásokat. A karbantartás során érdemes megvizsgálni, hogy történt-e olyan változás, mely a BYOD alapstratégia megváltoztatását igényelné, illetve a részszabályzatok módosítását, például egyes munkavállalók, vagy csoportok, vagy munkakörök és hatáskörök változása szükségessé teszi-e e részszabályzatok módosítását.

IV. Úgy módosítottam Weber, Blais és Betz által alkotott DOSPERT kérdőívet, hogy az képes legyen az IT biztonságtudatos magatartás és az IT kockázatvállalási hajlandóság mérésére. S e kérdőívet felhasználva bizonyítottam, hogy az információbiztonsági tudatosság nem függ a hallgatók által tanult szaktól az adott mintában, így szükséges egy átfogó IT biztonságtudatossági fejlesztés minden szakon és minden hallgatónak. [P10][P12][P13]

A Weber, Blais és Betz 2002-ben publikált DOSPERT (Domain-Specific Risk-Taking) kérdőívét használtam kiindulási alapként, mely egy széleskörűen elfogadott eszköz a válaszadók különböző körülmények közötti kockázatvállalási hajlandóságának mérésére, de az IT biztonsággal kapcsolatos kockázatvállalást, mint domaint nem méri.

A kérdőív módosításához olyan, a személyes és a szervezeti IT biztonságra nagy kihatással lévő használati eseteket választottam, melyeket bárki elkövethet. A kérdések meghatározását több lépcsőben, a kérdőív tesztelésével végeztem, illetve más biztonságtudatossági kérdések segítségével teszteltem.

- Továbbítana-e vállalati adatokat a privát e-mail címére?
- Csatlakozna-e nyilvános, nyílt WiFi-hez?
- Engedné-e, hogy valaki az Ön előzetes beleegyezése nélkül használja az okoseszközét?
- Használná-e a pinkódját - jelszavát - feloldási mintáját mások előtt?
- Másolna-e vállalati adatokat a sajáttulajdonú okostelefonjára?

Az információbiztonsági tudatosság méréséhez a választott mintám egyetemista fiatal felnőttekből állt, mert ők a jelen és a közeljövő munkavállalói és döntéshozói, akiknek a biztonsági attitűdje meghatározó a szervezetek IT biztonságában. A témában végzett kérdőíves kutatásaim során az alapszakos gépész- és mechatronikai-, és villamosmérnök, gazdaságinformatikus, és közgazdász hallgatókat vontam be a mintáimba.

A kutatás első hipotézise az volt, hogy az IKT biztonsági terület észlelt kockázata lesz a legmagasabb. Míg a második hipotézisem az volt, hogy az IKT-biztonság szignifikánsan fontosabb az informatikai területen tanulók számára, mint a többi diák számára. E hipotéziseket a minta eredményei alapján azonban el kellett vetnem. Ebből pedig azt a következtetést vontam le, hogy az információbiztonsági tudatosság nem függ a hallgatók által tanult szaktól az adott mintában, így szükséges egy átfogó IT biztonságtudatossági fejlesztés minden szakon és minden hallgatónak.

V. Bizonyítottam, hogy önmagában az IT biztonsággal kapcsolatos kockázatvállalási hajlandóság mérésére a DOSPERT kérdőív eredeti formájában nem alkalmazható. [P14][P15]

Kutatásaim során módosítottam a DOSPERT kérdőívet, majd a módosított kérdőív eredményei alapján statisztikailag kimutattam, hogy az általam alkotott kérdésekre adott válaszok a többi domain kérdéseire adott válaszokkal csak legfeljebb gyenge kapcsolatban állnak, így nem mutatnak összefüggést az IT domainre adott válaszokkal. Ez alapján pedig kijelenthető, hogy a DOSPERT kérdőív önmagában nem alkalmas az IT biztonsággal kapcsolatos kockázatvállalási hajlandóság mérésére.

Ezért szükséges egy IT specifikus kockázatviselési hajlandósági domain létrehozása a kérdőívhez, vagy egy önálló IT kockázatviselési hajlandóság felmérési módszertan kialakítása az IT specifikus kockázatviselési hajlandóság mérésére.

IRODALOMJEGYZÉK

1 LEE James, WARKENTIN Merrill, CROSSLER Robert E., OTONDO Robert F., Implications of Monitoring Mechanisms on Bring Your Own Device Adoption, Journal of Computer Information Systems , vol. 57, no. 4, pp. 309-318, 2017. ISSN:0887-4417
DOI:10.1080/08874417.2016.1184032
[Utolsó megtekintés: 2023. február 7.]

2 WEEGER Andy, WANG Xuequn, GEWALD Heiko, It Consumerization: Byod-Program Acceptance and its Impact on Employer Attractiveness, Journal of Computer Information Systems , vol. 56, no. 1, pp. 1-10, 2016. ISSN:0887-4417
DOI:10.1080/08874417.2015.11645795
[Utolsó megtekintés: 2023. február 7.]

3 MICHELBERGER P., HORVÁTH J., BEINSCHRÓTH G.K., The Employe - An Information Security Risk, ACTA OECONOMICA UNIVERSITATIS SELYE , vol. 2, no. 1, pp. 187-200, 2013. ISSN 2644-5212
http://acta.fei.ujs.sk/uploads/papers/finalpdf/AOUS_2(1)_from22to22.pdf
[Utolsó megtekintés: 2022. december 27.]

4 MICHELBERGER Pál, LÁBODI Csaba: "Vállalati információbiztonság szervezése" in *Vállalkozásfejlesztés a XXI. században II.*, NAGY Imre Zoltán, Ed. Budapest, Magyarország: Óbudai Egyetem, 2013 , pp. 241-302 ISBN 978-615-5018-33-6.
http://kgk.uni-obuda.hu/sites/default/files/10_Michelberger_Labodi.pdf
[Utolsó megtekintés: 2022. december 29.]

5 KE Chih-Kun, LIN Zheng-Hua, An Approach for Secure Data Exchange: Experiments on Android-based Mobile Device, Scientia Iranica , vol. 22, no. 4, pp. 1586-1593, 2015. ISSN:1026-3098
http://scientiairanica.sharif.edu/article_3736_5df2245ab8ec92e9cfc086d4cbd6df18.pdf
[Utolsó megtekintés: 2023. február 7.]

6 WANG Yu, LI Hanshang, LI Ting, Participant selection for data collection through device-to-device communications in mobile sensing, Personal and Ubiquitous Computing , vol. 21, no. 1, pp. 31-41, 2017. ISSN:1617-4909 DOI:10.1007/S00779-016-0974-0
[Utolsó megtekintés: 2023. február 7.]

7 GLISSON William Bradley, STORER Tim, MAYALL Gavin, MOUG Iain, GRISPOS George, Electronic retention: what does your mobile phone reveal about you?, International Journal of Information Security , vol. 10, no. 6, pp. 337-349, 2011. ISSN:1615-5270
DOI:10.1007/S10207-011-0144-3
[Utolsó megtekintés: 2023. február 7.]

8 HUBER Richard, RULTENBEEK Jack, DA MOTTA Seroa Ronaldo: Instrumentos de mercado para la politica ambiental en América Latina y Caribe: lecciones de once países, No. 381 S;. Washington, D.C.

9 MICHELBEGER Pál: Információ-, folyamat- és vállalatbiztonság;. Budapest, Magyarország Óbudai Egyetem, Keleti Károly Gazdasági Kar, 2022. ISBN 978-963-449-289-4

10 KESZTHELYI András, Paradigmaváltás - biztonság - emberi tényező, Taylor : gazdálkodás- és szervezéstudományi folyóirat , vol. 7, no. 1-2, pp. 406-412, 2015. ISSN:2062-1396
http://acta.bibl.u-szeged.hu/36354/1/vikek_018_019_406-412.pdf
[Utolsó megtekintés: 2023. február 7.]

11 MICHELBERGER Pál, LÁBODI Csaba, After Information Security – Before a Paradigm Change: A complex Enterprise Security Model, ACTA POLYTECHNICA HUNGARICA , vol. 9, no. 4, pp. 101-116, 2012. ISSN 1785-8860
http://acta.uni-obuda.hu//Michelberger_Labodi_36.pdf
[Utolsó megtekintés: 2022. december 29.]

12 MICHELBERGER Pál, KEMENDI Ágnes, Data, Information and IT Security - Software Support for Security Activities, Problems of Management in the 21st Century , pp. 108-124., 2020. ISSN 2029-6932
DOI:10.33225/pmc/20.15.108
[Utolsó megtekintés: 2023. február 8.]

13 GARETH James, Smartphone risk: Malicious threats to Smartphones, Network Security archive , vol. 2004, no. 8, pp. 5-7, 2004. ISSN:1353-4858
DOI:10.1016/S1353-4858(04)00115-1
[Utolsó megtekintés: 2023. február 8.]

14 RENN Ortwin: "Concepts of risk : a classification" in *Social theories of risk*, KRIMSKY Sheldon, Ed., 1992 , pp. 53-79 ISBN:0-275-94168-X.
DOI:10.18419/OPUS-7248
[Utolsó megtekintés: 2023. február 8.]

15 BAILLETTE Paméla, BARLETTE Yves, LECLERCQ-VANDELANNOITTE Aurélie, Bring your own device in organizations: Extending the reversed IT adoption logic to security paradoxes for CEOs and end users, International Journal of Information Management , vol. 43, pp. 76-84, 2018. ISSN:0268-4012
DOI:10.1016/J.IJINFOMGT.2018.07.007
[Utolsó megtekintés: 2023. február 8.]

16 KADENA Esmeralda, KOVÁCS Tibor, The need for BYOD security strategy, Hadmérnök , vol. 12 (4), pp. 138-145, 2017 december. ISSN:1788-1929
http://hadmernok.hu/174_14_kadena.pdf
[Utolsó megtekintés: 2023. február 8.]

17 WEBER U. Elke, BLAIS Renée Ann, BETZ E. Nancy, A Domain-Specific Risk-Attitude Scale: Measuring Risk Perceptions and Risk Behaviors, Journal of Behavioral Decision Making Volume , vol. 15, no. 4, pp. 263-290. ISSN:1099-0771
DOI:10.1002/BDM.414
[Utolsó megtekintés: 2023. február 8.]

18 BLAIS Ann-Renée, WEBER U. Elke, A Domain-Specific Risk-Taking (DOSPERT) Scale for Adult Populations, vol. 1, pp. 33-47, 2006. ISSN:1930-2975
http://journal.sjdm.org/06005/jdm06005.htm
[Utolsó megtekintés: 2023. február 8.]

19 NOBLE M. Stephanie, HAYTKO L. Diana, PHI Joanna, What drives college-age Generation Y consumers?, Journal of Business Research , vol. 62, no. 6, pp. 617-628, 2009. ISSN:0148-2963
DOI:10.1016/J.JBUSRES.2008.01.020
[Utolsó megtekintés: 2023. február 8.]

20 JONES L Jami. (2008) Who are Millennials? and what they Want from Libraries, Bookstores, and Librarians.
https://www.proquest.com/scholarly-journals/who-are-millennials-what-they-want-libraries/docview/236085193/se-2
[Utolsó megtekintés: 2022. december 28.]

21 PARDUE T. Karen, MORGAN Patricia, MILLENNIALS CONSIDERED: A NEW GENERATION New Approaches, and Implications for Nursing Education, Nursing education perspectives , vol. 29, no. 2, pp. 74-79, 2008. ISSN:1536-5026
DOI:10.1097/00024776-200803000-00007
[Utolsó megtekintés: 2023. február 8.]

22 LAZÁNYI Kornélia: "Study for nothing? Literature overview of labour market opportunities for individuals with tertiary education" in *Proceedings of FIKUSZ '12*, MICHELBERGER Pál, Ed., 2012 , pp. 37-46 ISBN:9786155018473.
http://kgk.uni-obuda.hu/sites/default/files/04_Lazanyi_Kornelia.pdf
[Utolsó megtekintés: 2023. február 8.]

23 LAZÁNYI Kornélia, What is the Role of Higher Educational Institutions in Managing their Students' Competencies?, Science journal of business management Special Issue: The Role of Knowledge and Management's Tasks in the Companies , vol. 3, no. 1, pp. 46-52., 2014. ISSN:331-0626
https://www.sciencepublishinggroup.com/journal/paperinfo?journalid=175&doi=10.11648/j.sjbm.s.2015030101.18
[Utolsó megtekintés: 2023. február 8.]

24 PRENSKY Marc, Digital Natives, Digital Immigrants, On the Horizon , vol. 9, no. 5, 2001. ISSN:1074-8121
DOI:10.1108/10748120110424816
[Utolsó megtekintés: 2023. február 8.]

25 PERILLO Suzanne, "Reaching Generation Y To Be or Not to Be – Relevant" , AASN Conference 2007 - The Wired Generation: Faith, Learning and Community with Generation Y.
https://web.archive.org/web/20080719195606/http://aasn.edu.au/zone_files/AASN_Conference_2007/dr_s_perillo_gen_y.pdf
[Utolsó megtekintés: 2023. február 8 (archive.org-on archívált változaton keresztül).]

26 BOLTON N. Ruth et al., Understanding Generation Y and their use of social media: a review and research agenda, Journal of Service Management , vol. 24, no. 3, pp. 245-267, 2013. ISSN:1757-5818
DOI:10.1108/09564231311326987
[Utolsó megtekintés: 2023. február 8.]

27 KOVÁCS Kármen, A divatterjedés és a divattermékek fogyasztását befolyásoló tényezők empirikus vizsgálata a hazai fiatalok körében, Marketing & Menedzsment , vol. 43, no. 1, pp. 62-71, 2009. ISSN:1219-0349
https://journals.lib.pte.hu/index.php/mm/article/view/769
[Utolsó megtekintés: 2023. február 8.]

28 PRZYBYLSKI K. Andrew, MURAYAMA Kou, DEHAAN R. Cody, GLADWELL Valerie, Motivational, emotional, and behavioral correlates of fear of missing out, Computers in Human Behavior , vol. 29, no. 4, pp. 1841-1848, 2013. ISSN: 1873-7692
DOI:10.1016/J.CHB.2013.02.014
[Utolsó megtekintés: 2023. február 8.]

29 SHAW R. Susan, FAIRHURST David, Engaging a new generation of graduates, Journal of Education and Training , vol. 50, no. 5, pp. 366-378, 2008. ISSN:2330-9709
DOI:10.1108/00400910810889057

30 TWENGE M. Jean: Generation Me: Why Today's Young Americans Are More Confident, Assertive, Entitled--and More Miserable Than Ever Before;. Free Press, 2007. ISBN:9780743276986

31 MI Jia, NESTA Frederick, Marketing library services to the Net Generation, Library Management , vol. 27, pp. 411-422, 2006. ISSN:0143-5124
DOI:10.1108/01435120610702404
[Utolsó megtekintés: 2023. február 8.]

32 LAZÁNYI Kornélia, A társas támogatás szerepe egy individualista társadalomban, A Virtuális Intézet Közép-Európa Kutatására közleményei , vol. 4, no. 2, pp. 51-58, 2012. ISSN:2062-1396
http://acta.bibl.u-szeged.hu/30184/
[Utolsó megtekintés: 2023. február 8.]

33 BROOKS Christopher D., "ECAR Study of Undergraduate Students and Information Technology, 2016," EDUCAUSE Center for Analysis and Research, Louisville, CO, 2016.
https://er.educause.edu/~/media/files/library/2016/10/ers1605.pdf
[Utolsó megtekintés: 2022. december 27.]

34 Pew Research Center. (2014. február) Emerging Nations Embrace Internet, Mobile Technology, Cell Phones Nearly Ubiquitous in Many Countries. https://www.pewresearch.org/global/2014/02/13/emerging-nations-embrace-internet-mobile-technology/ [Utolsó megtekintés: 2022. december 27.]

35 CHEN Baiyun, SEILHAMER Ryan, BENNETT Luke, BAUER Sue. (2015. június) Students' Mobile Learning Practices in Higher Education: A Multi-Year Study. https://er.educause.edu/articles/2015/6/students-mobile-learning-practices-in-higher-education-a-multiyear-study [Utolsó megtekintés: 2022. december 27.]

36 JOHNSON Larry et al.: NMC Horizon Report: 2016 Higher Education Edition;. The New Media Consortium, 2016. ISBN:978-0-9968527-5-3 https://www.learntechlib.org/p/171478/ [Utolsó megtekintés: 2023. február 8.]

37 SONG Yanjie, SUN Daner, JONG Siu-yung: "Enhancing students' science learning in a seamless inquiry-based learning environment leveraged by BYOD (Bring your own device)" in *Proceedings of the Workshop on Computer-Based Learning Environments for Deep Learning in Inquiry and Problem-Solving Contexts*. Singapore: The International Conference of the Learning Sciences (ICLS), 2016 , pp. 37 - 43. https://aims.cuhk.edu.hk/converis/portal/detail/Publication/35629123 [Utolsó megtekintés: 2017. szeptember 10.]

38 HAYWOOD D et al.: Student Mobility in a Digital World. Final Report of the Victorious Project;. European Commission E-Learning Programme, 2007. ISBN:9780955541414

39 Voxburner: UK Youth Trends Report;., 2016. http://www.voxburner.com/reports/ [Utolsó megtekintés: 2017. szeptember 1.]

40 Logicalis. (2015) The Shadow IT Phenomenon - CIOs respond with internal service provider transformation.
http://web.archive.org/web/20170622020039/https://www.logicalis.com/globalassets/group/cio-survey/cio-survey-2015_final3.pdf
[Utolsó megtekintés: 2023. február 8 (archive.org-on archivált változaton keresztül).]

41 VANDELANNOITTE Aurélie Leclercq, Managing BYOD: how do organizations incorporate user-driven IT innovations?, Information Technology & People , vol. 28, no. 1, pp. 2-33, 2015. ISSN: 0959-3845
DOI:10.1108/ITP-11-2012-0129
[Utolsó megtekintés: 2023. február 8.]

42 RAJNAI Zoltán, BLEIER Attila, Új generációs hálózati megoldások alkalmazása a Magyar Honvédség stacioner hálózatának modernizációjában, HADMÉRNÖK , vol. 4, no. 2, pp. 19-28, 2009. ISSN 1788-1929
http://hadmernok.hu/2009_2_bleier.pdf
[Utolsó megtekintés: 2023. február 8.]

43 eNET. (2015. március) BREAKTHROUGH IN MOBILE NET USAGE: HALF OF HUNGARIAN INTERNET USERS KEEP THE WEB IN THEIR POCKETS.
https://enet.hu/news/breakthrough-in-mobile-net-usage-half-of-hungarian-internet-users-keep-the-web-in-their-pockets/?lang=en
[Utolsó megtekintés: 2022. december 27.]

44 eNET. (2022. május) A PLAFONT SÚROLJA A HAZAI OKOSTELEFON-HASZNÁLAT.
https://enet.hu/a-plafont-surolja-a-hazai-okostelefon-hasznalat/
[Utolsó megtekintés: 2022. december 27.]

45 NetSafe. (2014) netsafe.org.nz.
https://web.archive.org/web/20160127015411/https://www.netsafe.org.nz/wp-content/uploads/2015/10/Smartphone-Security-Report-2014.pdf
[Utolsó megtekintés: 2022. december 27.]

46 European Network and Information Security Agency. (2013) Top Ten Smartphone Risks.
https://web.archive.org/web/20120527090937/http://www.enisa.europa.eu/activities/application-security/smartphone-security-1/top-ten-risks
[Utolsó megtekintés: 2022. december 27.]

47 DISTERER Georg, KLEINER Carsten, BYOD Bring Your Own Device, Procedia Technology , vol. 9, pp. 43-53, 2013. ISSN 2212-0173
DOI:10.1016/J.PROTCY.2013.12.005

48 ROSE Chris, BYOD: An Examination Of Bring Your Own Device In Business, Review of Business Information Systems (RBIS) , vol. 17, no. 2, pp. 65-70, 2013. ISSN:2157-9547
DOI:10.19030/RBIS.V17I2.7846

49 OLALERE Morufu, ABDULLAH Taufik Mohd, MAHMOD Ramlan, ABDULLAH Azizol, Bring your own device: security challenges and a theoretical framework for two-factor authentication, International Journal of Computer Networks and Communications Security , vol. 4, no. 1, pp. 21-32, 2016. ISSN 2410-0595
http://psasir.upm.edu.my/id/eprint/55224/

50 eNET. (2013. május) MÁR OKOSTELEFON-FELHASZNÁLÓ A MAGYAR LAKOSSÁG TÖBB MINT ¼-E.
http://www.enet.hu/hirek/mar-okostelefon-felhasznalo-a-magyar-lakossag-tobb-mint-%C2%BC-e/?lang=hu
[Utolsó megtekintés: 2022. december 27.]

51 Google. Think insights with Google.
https://www.thinkwithgoogle.com/
[Utolsó megtekintés: 2022. december 27.]

52 MOLNÁR Judit. (2013. december) Kütyükörkép 2013Q1.
https://nrc.hu/tavkozles-szektor/kutyukorkep-2013q1-lassan-mar-tobb-az-okos-mint-a-nem-okos/
[Utolsó megtekintés: 2022. december 27.]

53 eNET. (2015. december) OKOSTELEFONOK: MEGVAN A KÉTHARMAD!. https://enet.hu/okostelefonok-megvan-a-ketharmad/ [Utolsó megtekintés: 2022. december 27.]

54 IDC. (2020. december) Smartphone Market Share. http://www.idc.com/prodserv/smartphone-os-market-share.jsp [Utolsó megtekintés: 2020. december 15.]

55 GMBH Statista. (2022. december.) Mobile operating systems' market share worldwide from 1st quarter 2009 to 4th quarter 2022. https://www.statista.com/statistics/272698/global-market-share-held-by-mobile-operating-systems-since-2009/ [Utolsó megtekintés: 2022. december 28.]

56 Newzoo International. Top 50 countries/markets by smartphone users and penetration. https://newzoo.com/insights/rankings/top-50-countries-by-smartphone-penetration-and-users/ [Utolsó megtekintés: 2018. december 15.]

57 Google/TNS. (2017. november) Consumer Barometer Study 2017 - The Year of the Mobile Majority. https://www.thinkwithgoogle.com/intl/en-cee/marketing-strategies/app-and-mobile/consumer-barometer-study-2017-year-mobile-majority/ [Utolsó megtekintés: 2022. december 27.]

58 comScore Data Mine. (2013. március) Smartphones Reach Majority in all EU5 Countries. https://web.archive.org/web/20130320152641/http://www.comscoredatamine.com/2013/03/smartphones-reach-majority-in-all-eu5-countries/ [Utolsó megtekintés: 2022. december 27.]

59 Nemzeti Média és Hírközlési Hatóság. (2020. november) A Nemzeti Média és Hírközlési Hatóság mobilpiaci jelentése.
https://nmhh.hu/dokumentum/216281/NMHH_mobilpiaci_jelentes_2015Q42020Q2.pdf
[Utolsó megtekintés: 2022. november 16.]

60 PROTALINSKI Emil. (2014. március) F-Secure: Android accounted for 97% of all mobile malware in 2013, but only 0.1% of those were on Google Play.
http://thenextweb.com/google/2014/03/04/f-secure-android-accounted-97-mobile-malware-2013-0-1-google-play/
[Utolsó megtekintés: 2022. december 27.]

61 Kaspersky lab. (2014. április) IT threat evolution Q1 2014.
https://media.kasperskycontenthub.com/wp-content/uploads/sites/43/2018/03/08081202/q1-it-threats-en.pdf
[Utolsó megtekintés: 2022. december 27.]

62 CVE Details. Android Vulnerability Statistics.
https://www.cvedetails.com/product/19997/Google-Android.html?vendor_id=1224
[Utolsó megtekintés: 2022. december 27.]

63 SHINDER Littlejohn Debra. (2014. szeptember) iOS 8 fixes 53 security flaws in iPhone and iPad.
https://techtalk.gfi.com/ios-8-fixes-53-security-flaws-in-iphone-and-ipad/
[Utolsó megtekintés: 2022. december 27.]

64 CVE Details. Iphone Os Vulnerability Statistics.
https://www.cvedetails.com/product/15556/Apple-Iphone-Os.html?vendor_id=49
[Utolsó megtekintés: 2022. december 27.]

65 itsecurityguru.org. (2020. október) 8 Phones left in each London taxi each year, leads to security concerns.
https://www.itsecurityguru.org/2014/10/06/8-phones-left-london-taxi-year-leads-security-concerns/
[Utolsó megtekintés: 2022. november 16.]

66 PARSONS Kathryn, MCCORMAC Agata, BUTAVICIUS Marcus A., PATTINSON Malcolm Robert, JERRAM Cate, Determining employee awareness using the Human Aspects of Information Security Questionnaire (HAIS-Q), Computers & Security , vol. 42, pp. 165-176, 2014. ISSN:0167-4048 DOI:10.1016/J.COSE.2013.12.003

67 DHINGRA Madhavi, Legal Issues in Secure Implementation of Bring Your Own Device (BYOD), Procedia Computer Science , vol. 78, pp. 179-184, 2016. ISSN:1877-0509 DOI:10.1016/J.PROCS.2016.02.030

68 KEMENDI Ágnes, MICHELBERGER Pál, MESJASZ-LECH Agata, ICT security in businesses – efficiency analysis, ENTREPRENEURSHIP AND SUSTAINABILITY ISSUES , vol. 1, pp. 123-149, 2021. ISSN 2345-0282 (online) DOI:10.9770/jesi.2021.9.1(8) [Utolsó megtekintés: 2022. november 20.]

69 isBuzznews. (2016. február) Top 10 Hacking Methods. https://informationsecuritybuzz.com/study-research/top-10-hacking-methods/ [Utolsó megtekintés: 2022. december 27.]

70 HARRIS Mark A., PATTEN Karen P., Mobile device security considerations for small- and medium-sized enterprise business mobility, Information Management & Computer Security , vol. 22, no. 1, pp. 97-114, 2014. ISSN:0968-5227 DOI:10.1108/IMCS-03-2013-0019

71 KOH Eun Byol: "A Study on Security Threats and Dynamic Access Control Technology for BYOD, Smart-work Environment" in *Proceedings of the International Multi Conference of Engineers and Computer Scientists*. Hong Kong, 2014 , pp. 12–14 ISSN:2078-0966. http://www.iaeng.org/publication/IMECS2014/IMECS2014_pp634-639.pdf

72 HASSAN Mohammad Khaled Al, BYOD Technological: Next Generation Business Development Programs for Future Accelerations, Innovations and Employee Happiness, International Journal of Computer Applications , vol. 165, no. 10, pp. 4-14, 2017. ISSN:0975-8887
DOI:10.5120/ijca2017913929

73 TOPERESU B-Abee, BELLE Jean-Paul Van, Organisational Capabilities Required for Enabling Employee Mobility through Bring- Your-Own-Device Concept, Business Systems Research , vol. 8, no. 1, pp. 17-29, 2017. ISSN:1847-9375
DOI:10.1515/BSRJ-2017-0002

74 DAS Amit, KHAN Habib Ullah, Security behaviors of smartphone users, Information and Computer Security , vol. 24, no. 1, pp. 116-134, 2016. ISSN:2056-4961
DOI:10.1108/ICS-04-2015-0018

75 BLIZZARD Sonia, Coming full circle: are there benefits to BYOD?, Computer Fraud & Security , vol. 2015, no. 2, pp. 18-20, 2015. ISSN:1361-3723
DOI:10.1016/S1361-3723(15)30010-5

76 HOVAV Anat, PUTRI Frida Ferdani, This is my device! Why should I follow your rules? Employees' compliance with BYOD security policy, Pervasive and Mobile Computing , vol. 32, pp. 35-49, 2016. ISSN:1574-1192
DOI:10.1016/J.PMCJ.2016.06.007

77 ZAHADAT Nima, BLESSNER Paul, BLACKBURN Timothy, OLSON Bill A., BYOD security engineering, Computers & Security , vol. 55, pp. 81-99, 2015. ISSN:0167-4048
DOI:10.1016/J.COSE.2015.06.011

78 VIGNESH U., ASHA S., Modifying Security Policies Towards BYOD, Procedia Computer Science , vol. 50, pp. 511-516, 2015. ISSN:1877-0509
DOI:10.1016/J.PROCS.2015.04.023

79 DOWNER Kathleen, BHATTACHARYA Maumita, "BYOD Security: A New Business Challenge" in *2015 IEEE International Conference on Smart City/SocialCom/SustainCom (SmartCity)*, 2015 , pp. 1128-1133. ISBN:9781509018932 DOI:10.1109/SMARTCITY.2015.221

80 Macmillan Dictionary. BYOD ABBREVIATION. https://www.macmillandictionary.com/dictionary/british/byod [Utolsó megtekintés: 2022. december 27.]

81 BUDAI Balázs Benjámin: A közigazgatás újragondolása [Digitális kiadás.];. Budapest Akadémiai Kiadó, 2017. ISBN 978 963 454 065 6

82 BAILLETTE Paméla, BARLETTE Yves, BYOD-related innovations and organizational change for entrepreneurs and their employees in SMEs, Journal of Organizational Change Management , vol. 31, no. 4, pp. 839-851, 2018. ISSN:0953-4814 DOI:10.1108/JOCM-03-2017-0044 [Utolsó megtekintés: 2023. február 8.]

83 BALLAGAS Rafael, ROHS Michael, SHERIDAN G. Jennifer, BORCHERS Jan: "BYOD: bring your own device" in *Proceedings of the Workshop on Ubiquitous Display Environments*.: Ubicomp, 2004. http://www.vs.inf.ethz.ch/publ/papers/rohs-byod-2004.pdf

84 ROMAN Jeffrey. (2012. január) Bank Info Security. https://www.bankinfosecurity.com/byod-get-ahead-risk-a-4394 [Utolsó megtekintés: 2022. december 27.]

85 Bitport. (2014. január) A közép-európai cégek nem sietik el a BYOD trendek követését. https://bitport.hu/a-kozep-europai-cegek-nem-sietik-el-a-byod-trendek-koveteset [Utolsó megtekintés: 2022. november 17.]

86 Global Market Insights, Inc. (2016. március) Bring Your Own Device (BYOD) Market size worth USD 366.95 Billion by 2022: Global Market Insights Inc. https://www.globenewswire.com/news-release/2016/03/22/822021/0/en/Bring-Your-Own-Device-BYOD-Market-size-worth-USD-366-95-Billion-by-2022-Global-Market-Insights-Inc.html
[Utolsó megtekintés: 2022. december 27.]

87 KIS Endre. (2016. junius) Felhőben (lehetnének) jobbak a kkv-k. https://computerworld.hu/uzlet/felhoben-lehetnenek-jobbak-a-kkv-k-211561.html

88 BALCIK Chris. (2022. április) Smartphones and your employees: To BYOD or not to BYOD?. https://insights.samsung.com/2022/04/18/smartphones-and-your-employees-to-byod-or-not-to-byod/
[Utolsó megtekintés: 2022. december 27.]

89 Oxford Economics, SAMSUNG. (2022. április) Maximizing Mobile Value To BYOD or not to BYOD?. https://image-us.samsung.com/SamsungUS/samsungbusiness/short-form/maximizing-mobile-value-2022/Maximizing_Mobile_Value_2022-Final.pdf
[Utolsó megtekintés: 2022. december 27.]

90 TOKUYOSHI Brian, The security implications of BYOD, Network Security , vol. 2013, no. 4, pp. 12-13, 2013. ISSN:1353-4858
DOI:10.1016/S1353-4858(13)70050-3

91 LECLERCQ - VANDELANNOITTE Aurélie, Managing BYOD: how do organizations incorporate user-driven IT innovations?, Information Technology & People , vol. 28, no. 1, pp. 2-33, 2015. ISSN:0959-3845
DOI:10.1108/ITP-11-2012-0129

92 EM360 Tech. (2018. március) Top 10 companies supporting bring-your-own-device culture. https://em360tech.com/tech-news/top-ten/top-10-companies-supporting-bring-device-culture/
[Utolsó megtekintés: 2022. december 27.]

93 LAZÁNYI Kornélia: "Organisational Safety in Health-Care Setting – Literature Review" in *Proceedings- 11th International Conference on Management, Enterprise and Benchmarking (MEB 2015)*. Budapest: Óbuda University, Keleti Faculty of Business and Management, 2015 , pp. 111-122 ISBN:9786155460470. http://kgk.uni-obuda.hu/sites/default/files/08_Lazanyi-Kornelia.pdf [Utolsó megtekintés: 2023. február 8.]

94 MICHELBERGER Pál, HORVÁTH Zsolt, Biztonságorientált folyamatmenedzsment, INTERNATIONAL JOURNAL OF ENGINEERING AND MANAGEMENT SCIENCES / MŰSZAKI ÉS MENEDZSMENT TUDOMÁNYI KÖZLEMÉNYEK , pp. 344-364., 2017. ISSN: 2498-700X DOI:10.21791/IJEMS.2017.4.28.

95 LAZÁNYI Kornélia, A biztonsági kultúra, TAYLOR:GAZDÁLKODÁS- ÉS SZERVEZÉSTUDOMÁNYI FOLYÓIRAT: A VIRTUÁLIS INTÉZET KÖZÉP-EURÓPA KUTATÁSÁRA KÖZLEMÉNYEI , vol. 7, no. 1-2, pp. 398-405, 2015. ISSN:2064-4361 http://vikek.eu/wp-content/uploads/2015/10/TAYLOR_2015-nyomdai.pdf [Utolsó megtekintés: 2023. február 8.]

96 DOMBORA Sándor, MICHELBERGER Pál, Információbiztonság szerepe az üzleti folyamatokban, INTERNATIONAL JOURNAL OF ENGINEERING AND MANAGEMENT SCIENCES / MŰSZAKI ÉS MENEDZSMENT TUDOMÁNYI KÖZLEMÉNYEK , 2016. ISSN: 2498-700X DOI:10.21791/IJEMS.2016.1.17. https://ojs.lib.unideb.hu/IJEMS/article/view/4807/4540

97 MICHELBERGER Pál, DOMBORA Sándor, A felhasználói profil szerepe az információbiztonságban, PRO PUBLICO BONO: MAGYAR KÖZIGAZGATÁS; A NEMZETI KÖZSZOLGÁLATI EGYETEM KÖZIGAZGATÁS-TUDOMÁNYI SZAKMAI FOLYÓIRATA , vol. 3, no. 4, pp. 34-50, 2015. ISSN (online) 2786-0760 https://folyoirat.ludovika.hu/index.php/ppbmk/article/view/2640/1906

98 LAZÁNYI Kornélia, Szervezeti biztonság és a munkahelyi stress kapcsolata, TAYLOR: GAZDÁLKODÁS- ÉS SZERVEZÉSTUDOMÁNYI FOLYÓIRAT: A VIRTUÁLIS INTÉZET KÖZÉP-EURÓPA KUTATÁSÁRA KÖZLEMÉNYEI , vol. 8, no. 5, pp. 24-31, 2016. ISSN:2064-4361
http://vikek.eu/wp-content/uploads/2016/10/Taylor2016.5.sz%C3%A1mNo26.pdf
[Utolsó megtekintés: 2023. február 8.]

99 JOHNSON Steve, Bringing IT out of the shadows, Network Security , vol. 2013, no. 12, pp. 5-6, 2013. ISSN:1353-4858
DOI:10.1016/S1353-4858(13)70134-X

100 KESZTHELYI András, About passwords, Acta Polytechnica Hungarica , vol. 10, no. 6, pp. 99-118, 2013. ISSN:1785-8860
DOI:10.12700/APH.10.06.2013.6.6

101 WÓJTOWICZ Adam, JOACHIMIAK Krzysztof, Model for adaptable context-based biometric authentication for mobile devices, Personal and Ubiquitous Computing , vol. 20, no. 2, pp. 195-207, 2016. ISSN:1617-4909
DOI:10.1007/S00779-016-0905-0

102 BROOK Chris. (2020) The ultimate guide to BYOD security: overcoming challenges, creating effective policies, and mitigating risks to maximize benefits.
https://digitalguardian.com/blog/ultimate-guide-byod-security-overcoming-challenges-creating-effective-policies-and-mitigating
[Utolsó megtekintés: 2022. december 27.]

103 HOMER M. Pamela, KAHLE R. Lynn, A structural equation test of the value-attitude-behavior hierarchy, Journal of Personality and Social Psychology , vol. 54, no. 4, pp. 638-646, 1988. ISSN:0022-3514
DOI:10.1037/0022-3514.54.4.638

104 Frost & Sullivan. (2016) The Smartphone Productivity Effect: Quantitifying the Productive Gains of Smartphones in the Enterprise (White Paper). https://image-us.samsung.com/SamsungUS/samsungbusiness/short-form/the-smartphone-productivity-effect/20170727/WP_Smartphone_Productivity_AUG16FS_2.pdf [Utolsó megtekintés: 2022. december 27.]

105 KESZTHELYI András: "Some Special Fields of Data Security" in *Symposium for Young Researchers 2007: Proceedings*. Budapest: Óbudai Egyetem, 2007 , pp. 91-97 ISBN:9789637154645. https://kgk.uni-obuda.hu/sites/default/files/Keszthelyi_Andras.pdf

106 MICHELBERGER Pál: "Risk Management for Business Trust" in *MEB 2014 : Management, Enterprise and Benchmarking in the 21st Century*, MICHELBERGER Pál, Ed. Budapest, Magyarország: Óbudai Egyetem, Keleti Károly Gazdasági Kar, 2014 , pp. 401-413. ISBN:978-615-5460-06-7. http://kgk.uni-obuda.hu/sites/default/files/28_Michelberger.pdf

107 STAPOR Piotr Paweł, LASKOWSKI Dariusz Andrzej, Bring Your Own Device - providing reliable model of data access, Journal of Konbin , vol. 39, no. 1, pp. 41-56, 2016. ISSN:1895-8281 DOI:10.1515/JOK-2016-0031

108 HOLLÓ Dóra, Hol a határ? Magánszféra kontra munkahely a digitális korban, Detektor plusz , no. 3, p. 35, 2015. ISSN:1217-9175 http://hplaw.hu/wp-content/uploads/2015/07/Detektor_2015_3_Holloestsai.pdf [Utolsó megtekintés: 2022. december 27.]

109 FISHER Warren, ALLEN Charlotte, Road Warriors and Information Systems Security: Risks and Recommendations, Journal of Management Information and Decision Sciences , vol. 18, no. 1, p. 84, 2015. ISSN:1532-5806 http://faculty.sfasu.edu/fisherwarre/Road_Warrior_Fisher_Allen_JMIDS.pdf

110 KESZTHELYI András: "Netháborúk kora" in *Új kihívások a tudományban és az oktatásban - Gazdaságtudományi szekció : Zborník medzinárodnej vedeckej konferencie Univerzity J. Selyeho – 2013 "Nové výzvy vo vede a vo vzdelávaní" Sekcia ekonomických vied*, GYÖRGY Juhász et al., Eds. Komárom, Magyarország : Selye János Egyetem, 2013 , pp. 149-170 ISBN:978-80-8122-074-6.

111 RSA Security Inc. (2007. december) The Confessions Survey: Office Workers Reveal Everyday Behavior That Places Sensitive Information at Risk. https://web.archive.org/web/20081121114611/http://www.rsa.com/company/news/releases/pdfs/RSA-insider-confessions.pdf
[Utolsó megtekintés: 2022. december 27.]

112 NELSON Joanne. (2015. november) SHADOW IT IS A REALITY FOR 90% OF CIOS.
http://cxounplugged.com/2015/11/shadow-it-is-a-reality-for-most-cios/
[Utolsó megtekintés: 2020. november 17.]

113 STUART Andrew, The dangers of file sync and sharing services, Computer Fraud & Security , vol. 2016, no. 11, pp. 10-12, 2016. ISSN:1361-3723 DOI:10.1016/S1361-3723(16)30090-2

114 BROWNE Sean, LANG Michael, GOLDEN William, "Contextualising the insider threat: a mixed method study" , vol. WISP 2016 Proceedings, 13, 2016.
https://aisel.aisnet.org/wisp2016/13/
[Utolsó megtekintés: 2022. december 27.]

115 HANDEL Mark J., POLTROCK Steven, "Working around official applications: experiences from a large engineering project" in *Proceedings of the ACM 2011 conference on Computer supported cooperative work*, 2011 , pp. 309-312. ISBN:9781450305563
DOI:10.1145/1958824.1958870

116 GALLATTO Sara, CHEN Weifeng: "Security Management of Bring-Your-Own-Devices" in *Proceedings of the International Conference on Security and Management (SAM 2014)*, DAIMI Kevin, ARABNIA R. Hamid, Eds.: CSREA Press, 2015 , pp. 303-310 ISBN:978-1601322852. http://worldcomp-proceedings.com/proc/p2014/SAM9733.pdf

117 KOO Chulmo, CHUNG Namho, KIM Hee Woong, Examining explorative and exploitative uses of smartphones: a user competence perspective, Information Technology & People , vol. 28, no. 1, pp. 133-162, 2015. ISSN:0959-3845 DOI:10.1108/ITP-04-2013-0063

118 WALLI R. Stephen, The Arrival of the Mobile Internet Thanks to the Economics of Open Source Software, Open Source Business Resource , 2009 január. ISSN:1913-6102 http://timreview.ca/article/221

119 LAZANYI Kornelia: "Who do you trust? - Safety aspect of interpersonal trust among young adults with work experience" in *2016 IEEE 11th International Symposium on Applied Computational Intelligence and Informatics (SACI)*. Timisoara, Romania, 2016 , pp. 349-354 ISBN:9781509023790. DOI:10.1109/SACI.2016.7507400

120 JIA Yunhan Jack, CHEN Qi Alfred, LIN Yikai, KONG Chao, MAO Z. Morley: "Open Doors for Bob and Mallory: Open Port Usage in Android Apps and Security Implications" in *2nd IEEE European Symposium on Security and Privacy*.: University of Michigan, 2017 , pp. 190-203 ISBN:9781509057634. DOI:10.1109/EuroSP.2017.44

121 ELAHI Haroon, WANG Guojun, LI Xu: "Smartphone Bloatware: An Overlooked Privacy Problem" in *Security, Privacy, and Anonymity in Computation, Communication, and Storage. SpaCCS 2017. Lecture Notes in Computer Science*.: Springer, Cham, 2017 , pp. 169-185 ISBN:978-3-319-72389-1. DOI:10.1007/978-3-319-72389-1_15

122 Dr.Web. (2018. március) Doctor Web: over 40 models of Android devices delivered already infected from the manufacturers.
https://news.drweb.com/show/?i=11749
[Utolsó megtekintés: 2022. december 27.]

123 WALLS Jason, CHOO Kim-Kwang Raymond: "A Study of the Effectiveness Abs Reliability of Android Free Anti-Mobile Malware Apps" in *Mobile Security and Privacy*.: Syngress, 2017 , pp. 167-203 ISBN:978-0-12-804629-6.
DOI:10.1016/B978-0-12-804629-6.00008-0

124 Check Point Software Technologies Ltd. (2017. március) Preinstalled Malware Targeting Mobile Users.
https://blog.checkpoint.com/2017/03/10/preinstalled-malware-targeting-mobile-users/
[Utolsó megtekintés: 2022. december 27.]

125 FAQIRY Faiz Mohammad, SCRUTINIZING PERMISSION BASED ATTACK ON ANDROID OS PLATFORM DEVICES, International Journal of Advanced Research in Computer Science , vol. 8, no. 7, pp. 421-426, 2017. ISSN:0976-5697
DOI:10.26483/IJARCS.V8I7.4212

126 YUKSEL Asim S., ZAIM Abdul H., AYDIN Muhammed A., A Comprehensive Analysis of Android Security and Proposed Solutions, International Journal of Computer Network and Information Security , vol. 6, no. 12, pp. 9-20, 2014. ISSN:2074-9104
DOI:10.5815/IJCNIS.2014.12.02

127 Kaspersky. (2018) Skygofree: highly advanced, powerful Android surveillance software active since 2014.
https://www.kaspersky.com/about/press-releases/2018_skygofree-highly-advanced-powerful-android-surveillance-software-active-since-2014
[Utolsó megtekintés: 2022. december 27.]

128 BUCHKA Nikita, KIVVA Anton, GALOV Dmitry. (2017. december) Jack of all trades.
https://securelist.com/jack-of-all-trades/83470/
[Utolsó megtekintés: 2022. december 27.]

129 GIBBS Samuel. (2017. augusztus) Game of Thrones secrets revealed as HBO Twitter accounts hacked.
https://www.theguardian.com/media/2017/aug/17/game-of-thrones-secrets-revealed-as-hbo-twitter-accounts-hacked
[Utolsó megtekintés: 2022. december 27.]

130 LESWING Kif. (2017. Október) Apple gave Uber's app 'unprecedented' access to sensitive Apple features that can record iPhone screens.
https://www.businessinsider.com/uber-iphone-app-secret-access-sensitive-apple-features-2017-10
[Utolsó megtekintés: 2022. december 27.]

131 HERN Alex. (2018. január) Fitness tracking app Strava gives away location of secret US army bases.
https://www.theguardian.com/world/2018/jan/28/fitness-tracking-app-gives-away-location-of-secret-us-army-bases
[Utolsó megtekintés: 2022. december 27.]

132 PROSKE Sandra. (2017. február) Another Reason 99% of Mobile Malware Targets Androids.
https://blog.f-secure.com/another-reason-99-percent-of-mobile-malware-targets-androids/
[Utolsó megtekintés: 2022. december 27.]

133 LAIGNEE Barron. (2018. január) U.S. Soldiers are Accidentally Revealing Sensitive Locations by Mapping Their Exercise Routes.
https://time.com/5122495/strava-heatmap-military-bases/
[Utolsó megtekintés: 2022. december 27.]

134 RUSER Nathan. (2018. Január) Strava released their global heatmap.
https://twitter.com/Nrg8000/status/957318498102865920
[Utolsó megtekintés: 2022. december 27.]

135 SZOLDRA Paul. (2014. július) A Russian Soldier's Instagram Posts May Be The Clearest Indication Of Moscow's Involvement In East Ukraine.
https://www.businessinsider.com/russian-soldier-ukraine-2014-7
[Utolsó megtekintés: 2022. december 27.]

136 BODNÁR Ádám. (2011. május) Nem sokat törődtek az Android biztonságával.
https://www.hwsw.hu/hirek/46730/google-android-okostelefon-biztonsag-linux-dalvik.html
[Utolsó megtekintés: 2022. december 27.]

137 Computer Laboratory, University of Cambridge. (2015) AndroidVulnerabilities.org.
http://androidvulnerabilities.org/
[Utolsó megtekintés: 2022. december 27.]

138 PulseSecure. (2015) 2015 Mobile Threat Report.
https://www.pulsesecure.net/download/pages/2819/PulseSecure_MobilityReport.pdf
[Utolsó megtekintés: 2022. november 28.]

139 GAGANIS Chrysovalantis, HASAN Iftekhar, PAPADIMITRI Panagiota, TASIOU Menelaos, National culture and risk-taking: Evidence from the insurance industry, Journal of Business Research , vol. 97, pp. 104-116, 2019. ISSN:0148-2963
DOI:10.1016/J.JBUSRES.2018.12.037

140 LI Kai, GRIFFIN W. Dale, YUE Heng, ZHAO Longkai, How Does Culture Influence Corporate Risk-Taking?, Journal of Corporate Finance , vol. 23, pp. 1-22, 2013. ISSN:0929-1199
DOI:10.1016/J.JCORPFIN.2013.07.008

141 HOFSTEDE Geert, Insurance as a product of national values, The Geneva Papers on Risk and Insurance - Issues and Practice , vol. 20, no. 4, pp. 423-429, 1995. ISSN:1018-5895
DOI:10.1057/GPP.1995.36

142 HOFSTEDE Geert: Culture's Consequences: comparing values, behaviors, institutions, and organizations across nations (2nd ed.);. Thousand Oaks, CA SAGE Publications, 2001. ISBN:978-0-8039-7323-7

143 HOFSTEDE H. Geert, HOFSTEDE Jan Gert, MINKOV Michael: Cultures and Organizations, Software of the mind. Intercultural Cooperation and Its Importance for survival;. McGraw-Hill, 2010. ISBN:9780071664189

144 Hofstede Insights. WHAT ABOUT HUNGARY?
https://www.hofstede-insights.com/country/hungary/
[Utolsó megtekintés: 2022. december 27.]

145 DA VEIGA Adele, ELOFF Jan, A framework and assessment instrument for information security culture, Computers & Security , vol. 29, no. 2, pp. 196-207, 2010 március. ISSN:0167-4048
DOI:10.1016/j.cose.2009.09.002

146 LAZÁNYI Kornélia, A biztonsági kultúra szerepe a vezetői döntések támogatásában = THE ROLE OF SAFETY CULTURE IN SUPPORTING THE LEADERS' DECISION MAKING, TAYLOR: GAZDÁLKODÁS- ÉS SZERVEZÉSTUDOMÁNYI FOLYÓIRAT: A VIRTUÁLIS INTÉZET KÖZÉP-EURÓPA KUTATÁSÁRA KÖZLEMÉNYEI , vol. 8, no. 1, pp. 143-150, 2016. ISSN:2064-4361
https://ojs.bibl.u-szeged.hu/index.php/taylor/article/view/12993/12849
[Utolsó megtekintés: 2023. február 8.]

147 SZABÓ Attila, A biztonság szemüvegén keresztül, JövőKép , pp. 36-37, 2014. ISSN:2061-5035
http://docplayer.hu/docview/25/5700143/#file=/storage/25/5700143/5700143.pdf

148 KRISTÓF Csaba. (2013. szeptember) A BYOD jogi útvesztői.
http://bitport.hu/vezinfo/a-byod-jogi-utvesztoi
[Utolsó megtekintés: 2022. december 27.]

149 KRISTÓF Csaba. (2013. június) A britek a biztonságtudatosság növelésére költenek.
http://bitport.hu/biztonsag/a-britek-koeltenek-biztonsagtudatossag-noevelesere
[Utolsó megtekintés: 2022. december 27.]

150 SCHOPP Attila, VASVÁRI György. (2012. február) Tudatos biztonság.
https://itbusiness.hu/technology/aktualis-lapszam/focus/tudatos-biztonsag/
[Utolsó megtekintés: 2022. december 27.]

151 International Organization for Standardization, Information technology — Security techniques — Information security management systems — Requirements (ISO/IEC 27001:2013),2013.

152 International Organization for Standardization, Risk management — Guidelines (ISO 31000:2018),2018.

153 FORD Glenn. (2014. január) BYOD Demand and Information Security.
http://cybersecurity-hq.blogspot.com/2014/02/byod-consumer-demand-and-information.html
[Utolsó megtekintés: 2022. december 27.]

154 HOLLÓ Dóra. (2014. február) BYOD: céges és privát adatok egy dobozban.
https://computerworld.hu/uzlet/byod-ceges-es-privat-adatok-egy-dobozban-144359.html
[Utolsó megtekintés: 2022. december 27.]

155 MICHELBERGER Pál, BEKE Éva, Stratégiai döntéseknél alkalmazható összesített kockázati mutatószámok meghatározása: Egy döntéstámogató módszer alkalmazási feltételei, BELÜGYI SZEMLE: A BELÜGYMINISZTÉRIUM SZAKMAI TUDOMÁNYOS FOLYÓIRATA , pp. 13-24., 2020. ISSN 2677-1632
http://real.mtak.hu/112744/1/Michelberger-BekeBelugyiSzemle2020.evi7.szam13-24.pdf

156 BRODIN Martin, Mobile Device Strategy : From a Management Point of View, Journal of Mobile Technologies, Knowledge and Society , 2017. ISSN:2155-4811 http://www.diva-portal.org/smash/get/diva2:1069979/FULLTEXT01.pdf

157 MICHELBERGER Pál: "Információvédelmi képzés - egy próbát megér (?)" in *Informatika a felsőoktatásban 2014*, KUNKLI Roland, PAPP Ildikó, RUTKOVSZKY Edéné, Eds. Debrecen, Magyarország: Debreceni Egyetem Informatikai Kar, 2014 , pp. 724-729 ISBN 978-963-473-712-4. http://www.sze.hu/~erdosf/publikaciok/IF2014_kiadvany.pdf

158 RAJNAI Zoltán, MÓGOR Tamásné, Elektronikus adatkezelő rendszerek kockázatelemzése, a kockázati módszerek bemutatása, Bolyai Szemle , vol. 4, no. 2, pp. 43-59, 2014. ISSN:1416-1443 https://www.uni-nke.hu/document/uni-nke-hu/bolyai-szemle-2014_-ev-2_-szam.original.pdf

159 MAYNARD Bright Harold: Industrial Engineering Handbook;. New York McGraw-Hill, 1971. ISBN:9780704108448

160 BRAUNSTEIN Christopher J, Mobile Device Management, Army Communicator , vol. 37, no. 2, pp. 28-30, 2012. ISSN:0362-5745 https://cybercoe.army.mil/AC/2012/Vol37/No2/Summer_2012_Edition.pdf

161 BRADLEY Loucks, J., Macaulay, J., Medcalf, R., Buckalew, L., J.. BYOD: A Global Perspective, Harnessing Employee-Led Innovation. http://www.cisco.com/web/about/ac79/docs/re/BYOD_Horizons-Global.pdf [Utolsó megtekintés: 2022. december 27.]

162 HERSEY Blanchard, Ken Paul,: Management of Organizational Behavior: Utilizing Human Resources;. New Jersey, Amerikai Egyesült Államok Prentice Hall, 1977. ISBN 978-0132617697

163 Behavioral Science for Policy Lab, Andlinger Center for Energy and the Environment, Princeton University. Scoring Instruction. https://sites.google.com/decisionsciences.columbia.edu/dospert/scoring-instructions?authuser=0 [Utolsó megtekintés: 2022. december 27.]

PUBLIKÁCIÓK

A doktori értekezéshez kapcsolódó publikációk

[P1] Fehér-Polgár, Pál ; Michelberger, Pál: *A sajáttulajdonú mobil eszközök információbiztonsági kockázatai: The information security risks of the BYOD,* INTERNATIONAL JOURNAL OF ENGINEERING AND MANAGEMENT SCIENCES / MŰSZAKI ÉS MENEDZSMENT TUDOMÁNYI KÖZLEMÉNYEK 3 : 4 pp. 176-185. , 10 p. ISSN: 2498-700X (2018) DOI: 10.21791/IJEMS.2018.4.16.

[P2] Fehér-Polgár, Pál: BYOD, hozd magaddal a saját biztonsági kockázataid In: Fehér-Polgár Pál (szerk.) Kutatók éjszakája – Fiatal kutatók előadásai 2018 Budapest, Óbudai Egyetem Keleti Károly Gazdasági Kar, ISBN 9789634491026.pdf pp.9 1p.

[P3] Fehér-Polgár, Pál ; Németh, Zsolt: *Safety Consciousness of the Mobile Phone Users pp. 345-348. 4 p.* In: Szakál, Anikó (szerk.) Proceedings of the11th IEEE International Symposium on Applied Computational Intelligence and Informatics SACI 2016 Budapest, Magyarország : IEEE, (2016) p. 412 ISBN:978-1-5090-2380-6 DOI:10.1109/SACI.2016.7507399

[P4] Fehér-Polgár, Pál: *Felsőoktatásban Tanuló Hallgatók Biztonságtudatossága* TAYLOR: GAZDÁLKODÁS- ÉS SZERVEZÉSTUDOMÁNYI FOLYÓIRAT: A VIRTUÁLIS INTÉZET KÖZÉP-EURÓPA KUTATÁSÁRA KÖZLEMÉNYEI 7 : 3-4 pp. 15-21. , 7 p. (2015) ISSN 2676-8917

[P5] Fehér-Polgár, Pál: *A biztonságot veszélyeztető tényezőkkel kapcsolatos attitűdök vizsgálata egyetemi hallgatókon* TAYLOR: GAZDÁLKODÁS- ÉS SZERVEZÉSTUDOMÁNYI FOLYÓIRAT: A VIRTUÁLIS INTÉZET KÖZÉP-EURÓPA KUTATÁSÁRA KÖZLEMÉNYEI 7 : 1-2 pp. 413-419. , 7 p. (2015) ISSN 2676-8917

[P6] Fehér-Polgár, Pál: *Safety conscious of the students in higher education* In: Gabriela, Kristová; Peter, Schmidt; Janette, Brixová; Mária, Szivosová (szerk.) Trends and Innovations in E- business, Education and Security : PROCEEDINGS Fourth International Scientific Videoconference of Scientists and PhD. students or candidates Pozsony, Szlovákia : Ekonomická Univerzita v Bratislave, (2015) pp. 8-16. , 9 p. ISBN 978-80-225-3987-6

[P7] Fehér-Polgár, Pál: *Saját tulajdonú mobilinformatikai eszközök vállalati használatának jogi kérdései* In: Rácz, Pál (szerk.) IESB 2014 : Nemzetközi Gépész és Biztonságtechnikai Szimpózium Budapest, Magyarország : Óbudai Egyetem, Bánki Donát Gépész és Biztonságtechnikai Mérnöki Kar, (2014) ISBN 978615546008-1

[P8] Fehér-Polgár, Pál: *Data Security of Mobile Phones , from the Aspect of University Students* In: Michelberger, Pál (szerk.) MEB 2014 : Management, Enterprise and Benchmarking in the 21st Century Budapest, Magyarország : Óbudai Egyetem Keleti Károly Gazdasági Kar, (2014) pp. 393-400. , 8 p. ISBN: 9786155460067

[P9] Michelberger, Pál ; Fehér-Polgár, Pál Byod Security Strategy (Aspects of a managerial decision) JOURNAL OF SECURITY AND SUSTAINABILITY ISSUES 9 : 4 pp. 1135-1143. , 9 p. (2020) ISSN 2029-7025 DOI:10.9770/jssi.2020.9.4(1)

[P10] Pál Fehér-Polgár, Pál Michelberger, The Information Security Risks of the BYOD, from Theoretical Point of View, Interdisciplinary Description of Complex Systems ISSN 1334-4676, 2019 DOI: 10.1109/SISY47553.2019.9111514

[P11] Pál, Fehér-Polgár, Managerial decision options about BYOD with the consideration of shadow IT In: Szikora, Péter; Fehér-Polgár, Pál (szerk.) 17th International Conference on Management, Enterprise, Benchmarking. Proceedings (MEB 2019) Budapest, Magyarország : Keleti Károly Faculty of Business and Management, Óbuda University (2019) 194 p. pp. 28-34. , 7 p. ISBN 978-963-449-127-9

[P12] Pál, Fehér-Polgár Examination of IT risk-taking with modified DOSPERT questionnaire among university students In: Keszthelyi, András; Szikora, Péter; Fehér-Polgár, Pál (szerk.) 18th International Conference on Management, Enterprise, Benchmarking. Proceedings (MEB 2020) Budapest, Óbudai Egyetem Keleti Károly Gazdasági Kar (2020) 231 p. pp. 48-56. , 9 p. ISBN 978-963-449-223-8

[P13] Pál, Fehér-Polgár, Measuring Safetyconsciousness In: Aniko, Kelemen-Erdos; Pal, Feher-Polgar; Anett, Popovics (szerk.) FIKUSZ 2021 XVI. International Conference Proceedings Budapest, Magyarország : Óbudai Egyetem, Keleti Károly Gazdasági Kar (2021) 251 p. pp. 22-27. , 6 p. ISBN 978-963-449-274-0

[P14] Pál, Fehér-Polgár, Can be the DOSPERT questioner used for measuring IT risk taking in Agnes Csiszarik-Kocsir (Szerk.), Anett Popovics (Szerk.), Pal Feher-Polgar (Szerk.) FIKUSZ 2022 XVII. International Conference Proceedings (pdf) : Óbudai Egyetem (2022) , 637-645 pp. 654 p. ISBN: 978-963-449-305-1

[P15] Pál, Fehér-Polgár, Results upon two samples of university students on safety consciosness in smartphone usage in Agnes Csiszarik-Kocsir (Szerk.), Anett Popovics (Szerk.), Pal Feher-Polgar (Szerk.) FIKUSZ 2022 XVII. International Conference Proceedings (pdf) : Óbudai Egyetem (2022) , 123-128 pp. 654 p. ISBN: 978-963-449-305-1

További tudományos közlemények

[P16] Holicza, Péter ; Fehér-Polgár, Pál: The Role of IT in International Student Mobility: The Y-Generation Case pp. 147-150. , 4 p. In: Szakál, Anikó (szerk.) IEEE 15th International Symposium on Intelligent Systems and Informatics : SISY 2017 New York, Amerikai Egyesült Államok : IEEE, (2017) ISSN: 1949-0488 DOI: 10.1109/SISY.2017.8080542

[P17] Duong Van Thinh ; Fehér-Polgár Pál: (2016) CULTURE AND ENVIRONMENTAL AWARENESS, A STUDY ON HUNGARIAN HIGHER EDUCATION STUDENTS in Ivan Mihajlović et al. (szerk) "Environmental awareness as a universal European Value", University of Belgrade, Technical Faculty in Bor, Engineering Management Department (EMD) Bor, 2016 ISBN: 978866305044-0 http://media.sjm06.com/2016/02/Monograph-Environmental-awareness-as-a-universal-European-Value.pdf

[P18] Roque, João ; de Miranda, João Luís ; Fehér-Polgár, Pál, Risk Mitigation and Preventing Medicines Shortages In: de Miranda, João Luís; Jenzer, Helena; Barbosa-Povoa, Ana Paula (szerk.) Pharmaceutical Supply Chains - Medicines Shortages Springer International Publishing (2019) pp. 103-109. Paper: Chapter 6 , 7 p. ISBN: 978-3-030-15398-4 DOI: 10.1007/978-3-030-15398-4_6

[P19] György, Eisemann; Pál, Fehér-Polgár Safety consciousness in future employees MACROTHEME REVIEW: A MULTIDISCIPLINARY JOURNAL OF GLOBAL MACRO TRENDS 9 : 1 pp. 74-84. , 11 p. (2020) ISSN 2379-9765

[P20] Kornélia, Lazányi ; Pál, Fehér-Polgár ; Imre, Vida Identification of the most important european productivity factors through the dimension reduction EKONOMICKO-MANAZERSKE SPEKTRUM / ECONOMIC AND MANAGERIAL SPECTRUM 14 : 1 pp. 77-86. , 10 p. (2020) ISSN: 2585-7258 DOI: 10.26552/ems.2020.1.77-86

[P21] Nóra Fodor, Pál Fehér-Polgár E-document, or the human factor in the security of electronic storage of personal documents in Agnes Csiszarik-Kocsir (Szerk.), Anett Popovics (Szerk.), Pal Feher-Polgar (Szerk.) FIKUSZ 2022 XVII. International Conference Proceedings (pdf) : Óbudai Egyetem (2022) , 637-645 pp. 654 p. ISBN: 978-963-449-305-1

Oktatási művek

[P22] Fehér-Polgár, Pál, A magyar B2C e-kereskedelem jelene In: Fehér-Polgár, Pál Esettanulmány kötet Budapest, Magyarország : Óbudai Egyetem, Keleti Károly Gazdasági Kar, (2019) pp. 27-36. , 10 p. ISBN: 9789634491552

TÁBLÁZATJEGYZÉK

ÁBRAJEGYZÉK

KÖSZÖNETNYILVÁNÍTÁS

Szeretném megköszönni témavezetőm, Prof. Dr. Michelberger Pál iránymutatásait a kutatási munka és az értekezés elkészítése során is és kitartó segítségét a teljes folyamat alatt!

Köszönöm az Óbudai Egyetem Biztonságtudományi Doktori Iskolájának és a Keleti Károly Gazdasági Kar és az Egyetemi Könyvtár minden munkatársának támogatását és szakmai segítségét a kutatásaimmal kapcsolatban. Prof. Dr. Lazányi Kornéliának az UNKP kutatásom témavezetését.

Külön köszönöm Daragó Anitának, hogy nem csak az életben más területein támogat és mellettem áll, de a doktori kutatásom során és az értekezés elkészítése közben is folyamatosan segítette munkámat.