Az információbiztonság időszerű kérdései a magyarországi kkv-k körében

Kiss Adrienn*, Kollár Csaba

Gábor Dénes Egyetem, Polgári adatbiztonság kutatócsoport, Budapest, Magyarország
*Levelező szerző, e-mail: adriennk73@gmail.com

Beérkezett: 2023. november 23.; elfogadva: 2023. december 6.; online megjelent: 2023. március 28.

Összefoglalás

A tanulmány célja az információbiztonság vizsgálata a magyarországi kis- és középvállalkozások (kkv-k) körében. Tanulmányunk aktualitását az adja, hogy az Európai Unió Bizottsága által évente kiadott Digitális Gazdaság és Társadalom Indexe szerint a magyarországi kkv-kat alacsony adat- és információbiztonsági szint jellemzi. Kutatásunk során egyaránt alkalmaztunk kvalitatív és kvantitatív módszereket. Az előbbinél dokumentumelemzéssel megvizsgáltuk, hogy a hazai szakirodalom milyen fontosabb információbiztonsági kihívásokat azonosít, illetve interjúk segítségével feltérképeztük a kkv-k információbiztonsági gyakorlatait és kihívásait, az utóbbinál pedig egy online, nagymintás kérdőív révén vizsgáltuk a szektor vezetőinek információbiztonsággal kapcsolatos véleményét, fejlettségét.

Kulcsszavak: információbiztonság, kkv, kiberbiztonság

Current issues of information security among SMEs in Hungary

Adrienn Kiss, Csaba Kollár

Gábor Dénes University, Civil Data Security Research Group, Budapest, Hungary

Summary

The aim of the study is to examine information security among small and medium-sized enterprises (SMEs) in Hungary. The relevance of our study is that, according to the Digital Economy and Society Index published annually by the Commission of the European Union, Hungarian SMEs are characterised by a low level of data and information security. In our research, we used both qualitative and quantitative methods. In the former, we conducted a document analysis to identify the main information security challenges identified in the domestic literature and mapped the information security practices and challenges of SMEs through interviews, while in the latter, we used an online, large-scale questionnaire to investigate the views and development of the sector's managers on information security. The findings of our study are based on the responses of 150 SME managers and 31 IT professionals working in the sector. We divided our questionnaire into six sections: demographics, business profile, device usage, digital habits, information security awareness survey based on the international HAIS-Q, information security awareness in daily practice. In the present research we deviated somewhat from the international model, firstly because we had to adapt the model to the domestic requirements and our research objectives, and secondly because this model was only a part of our questionnaire. During the research we have clearly identified the need to develop and implement practice-oriented training programmes that can help managers and IT professionals in the domestic SME sector to develop their information security awareness and even to make the transition to Industry 4.0. Based on the responses to the interview questions, it can be concluded that, overall, SME managers and their organisations are increasingly starting to build cybersecurity solutions and information security measures around their organisation. There is still a need to develop and share information security good practices that can reach SMEs, as there is a need for training and exchange of experiences, but not all companies are fully committed to the issue, so the actual need for action and organisation is ultimately lagging behind. A small proportion of the organisations surveyed have been victims of a cybersecurity incident and a good proportion of SME managers believe that until an incident has happened to an employee or the organisation, they will not learn from it. Basically, there is a growing demand for increased security

and the use of security tools and education in information security, but this is evolving as a slow process and not as fast as the world around us is changing, so it is questionable when an information security explosion will occur that may radically change the tools and attitudes of organisations.

Keywords: information security, SMEs, cybersecurity

Bevezetés

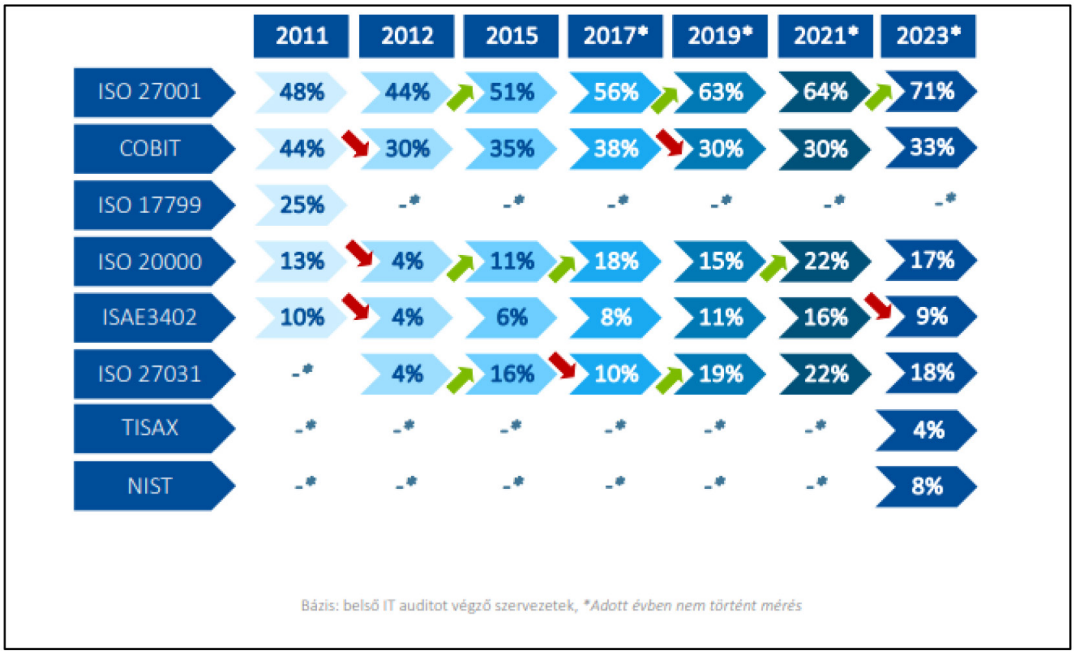
A KSH legfrissebb, 2022-ben megjelent kiadványa szerint Magyarországon 2021-ben 884 ezer vállalkozás tartozott a kkv-szektorba, s a szektorban foglalkoztatottak száma 3 millió fő fölött volt, ami azt jelenti, hogy tíz munkavállalóból hét ebben a szektorban dolgozott. Bár a kkv-k többségénél még nem lehet beszélni az ipar/mezőgazdaság 4.0-ra történő átállásáról, s ezzel párhuzamosan a kiber – tehát nem fizikai – rendszerek felértékelődéséről, de az elmúlt évtized ebben a szektorban is egyre inkább a fókuszba helyezte az informatikai eszközök és szoftverek használatát *(KSH 2022)*. A tulajdonosi szemléletmód is folyamatosan változik: már nemcsak a termelőeszközök, hanem az azokat működtető, a különböző adatokat feldolgozó, kimutatásokat, elemzéseket készítő, vagy legalábbis azok készítésében segítő szoftverek is egyre értékesebbé váltak. Az irodai és célalkalmazások, az online adatbázisok egyaránt megkövetelik, hogy az azokat használó munkavállalók megfelelő és modern szoftverismeretekkel rendelkezzenek, illetve hogy információbiztonság-tudatossági szintjük is fejlődjön. Ez utóbbi különösen fontos, mivel több olyan törvény/rendelet (pl. GDPR) jelent meg, amely komoly szankciókat helyez kilátásba a vállalkozásokkal szemben (is), ha azok a személyes adatokat hanyag módon kezelik, s ennek következtében ezekhez az adatokhoz illetéktelen személyek férhetnek hozzá: megismerve, megváltoztatva, letöltve, törölve azokat. Az információbiztonságot Magyarországon is egy összetett tevékenységnek tartjuk, amelyik magában foglalja az adat- és információvédelmet, a hálózati és fizikai biztonságot, az alkalmazások biztonságát, s természetesen a már említett információbiztonság-tudatosságot is. Jelen tanulmányunkban is ez utóbbi területre helyezzük a hangsúlyt.

Elméleti rész

Magyarországon címében nevesítetten a hazai kkv-k információbiztonságával az elmúlt időszakban két tanulmány foglalkozott, melyből egy *(Mike–Krén–Kecskeméti 2023)* érhető el. A szerzők alapvetően szekunder elemzést végeznek: a Digiméter 2020, 2021 és 2022-es kvantitatív kutatásának eredményét, az Európai Unió által biztosított DESI-index (Digital Economy and Society Index) és NCSI (National Cybersecurity Index) eredményeit mutatják be, illetve elemzik újra, kiemelve, hogy „[a]z Európai Unió (EU) tagállamai közül Magyarországon a helyzet különösen aggasztó: az információbiztonsági szint jelenleg még kiforratlan, ám a szükségességének jelei egyre nyilvánvalóbbak" *(Mike–Krén–Kecskeméti 2023: 44–45.)*.

Az információbiztonságot és szükségességét nem pusztán a sorra megjelenő, tudatosságot vizsgáló tanulmányok és az ezek végtermékét jelentő ajánlások jelzik, hanem azok a jogszabályok is, amelyek a szervezetek információbiztonsági kereteit hivatottak szabályozni. Ezek a jogszabályok és az általuk előírt kötelezettségek nem szabad, hogy csak egy kötelező érvényű előírás képében jelenjenek meg a munkavállalók szemében, hanem az minősülne előnyösnek, ha saját ügyüknek éreznék a szabályok betartását. Ez a fajta hozzáállás a szervezeti biztonsági kultúra alapja, amely képes jó hatással lenni a munkavállalók magatartására a biztonságtudatosság terén *(Lazányi 2016)*. A szabályok betartásával jó eséllyel elkerülhető, hogy a későbbiekben egy incidensből adódó anyagi, személyi kár vagy presztízsveszteség következzen be *(Póserné Oláh 2007)*.

Érdemes részletezni, hogy mely információbiztonsági, adatvédelmi vagy ezekhez kapcsolódó jogszabályok jöhetnek szóba magyarországi viszonylatban, amelybe akár az Európai Uniós irányelv és annak a hazai megfelelője is beletartozik. Egyrészről megemlítendő az Ibtv. *(2013. évi L. törvény az állami és önkormányzati szervek elektronikus információbiztonságáról)*, amely információbiztonsági kötelezettségeket határoz meg a hatálya alá tartozó szervezetek számára. Az Ibtv. követelményei írják elő többek között, hogy a jogszabály hatálya alá eső szerveknek kötelezően ki kell jelölni egy olyan felelőst, aki az informatikai biztonsági irányítási rendszer kialakításáért és működtetéséért felel. Ezenfelül a BM-rendelet *(41/2015. (VII. 15.) BM rendelet az állami és önkormányzati szervek elektronikus információbiztonságáról szóló 2013. évi L. törvényben meghatározott technológiai biztonsági, valamint a biztonságos információs eszközökre, termékekre, továbbá a biztonsági osztályba és biztonsági szintbe sorolásra vonatkozó követelményekről)* is besorolható az információbiztonság témakörébe, és olyan védelmi intézkedéskatalógust tartalmaz, amely megvalósítására az érintett vállalatoknak oda kell figyelniük. A BM-rendelet jó gyakorlatokkal és példákkal segíti az Ibtv.-ben definiált felelősöket. Adatvédelmi oldalról a biztonsági célkitűzéseket és követelményeket, a GDPR *(Általános adatvédelmi rendelet)*, mint Európai Uniós irányelv és hazai párja, az Infotv. *(2011. évi CXII. törvény az információs önrendelkezési jogról és az információszabadságról)* határoz meg. A GDPR részletes követelményeket tartalmaz a szervezetekre tekintettel, a személyes adatok gyűjtésére, kezelésére és tárolására vonatkozóan. Hazai viszonylatban pedig az Infotv. hatálya



1. ábra IT audit tevékenység végrehajtásához használt módszertanok és keretrendszerek

Megjegyzés: A fejlécben csillaggal jelölt években az alapsokaságok kis mértékben eltérnek egymástól.

Forrás: ISACA 2023

minden olyan adatkezelésre vonatkozik magyarországi viszonylatban, amely természetes személy adataira, közérdekből nyilvános vagy közérdekű adatra tartozik *(Bonnyai–Kiss–Tóth 2023)*.

A jogszabályok mellett nemzetközi szinten és hazai implementáció formájában a szabványok is kiemelt jelentőséggel bírnak. Magyarországi viszonylatban is kialakult eljárása, rendszere van a különféle szabványoknak, ezen belül is az információbiztonsági szabványok alkalmazásának és az információbiztonságot fenntartani kívánó szervezetek, vállalatok akkreditálásának és auditálásának. Tehát belső és külső auditálási rendszer működik arra vonatkozóan, hogy az érintett szervezeteknél a hivatalos szabványnak megfelelően valósuljon meg az információbiztonság *(ISACA 2023)*.

Elengedhetetlen a témához tartozó szabványoknak az átfogó ismerete, mint például:[1]

- az ISO 27001, amely a szervezetek által bevezetésre kerülő információbiztonsági irányítási rendszerének követelményhalmazát adja;
- az ISO 27002, az információbiztonsági vezetési és kockázatcsökkentő tanácsokat, illetve segítséget nyújt az információbiztonság gyakorlati megvalósításában;
- az ISO 18045 szabvány minimumkövetelményeket, -műveleteket határoz meg, amellyel az informatikai biztonság értékelését el lehet végezni;
- az ISO 27014 szabvány nyújt útmutatást az információbiztonság irányításának fogalmairól, célkitűzéseiről és folyamatairól, ezek segítségével tudják a szervezetek értékelni, irányítani és ellenőrizni a szervezeten belül megjelenő információbiztonsági folyamatokat;
- az ISO 27005, az információbiztonsági kockázatok menedzselésére vonatkozóan, a különböző alapelveket, elvárásokat és a hozzájuk tartozó módszerek kiválasztásában nyújt segítséget úgy, hogy bemutatja őket;
- az ISO 31000 egységes kockázatmenedzsment alapelveket tartalmaz;
- az ISO 15408 szabvány határozza meg az informatikai biztonság értékelésének általános fogalmait és elveit, illetve egy adott általános értékelési modellt.

Az ISACA – amely a nemzetközi ISACA (Information Systems Audit and Control Association) magyarországi szakmai szervezete – 2023-ban megjelent információbiztonsági felmérése alapján – Magyarország jelentős vállalatainak és intézményeire vonatkozóan – a nemzetközileg elismert IT audit módszertanok, szabványok, útmutatók közül a már korábban említett ISO 27001 volt a leginkább használt keretrendszer. Az *1. ábra* alapján is látható, hogy az évek során egyre inkább előtérbe kerülnek a különféle ajánlások, szabványok és ezek alkalmazása *(ISACA 2023)*.

Összességében számos jogszabály, szabvány, ajánlás és útmutató segíti a vállalatok mindennapi működését, és egyre inkább előtérbe kerül az információbiztonság fontossága. Ettől függetlenül ez egy olyan témakör, amellyel érdemes foglalkozni, és amely terület körében még bizonytalan mértékű fejlődés várható.

[1] https://www.iso.org/.

Módszertan

Tanulmányunk empirikus részében három módszerrel vizsgáltuk a magyarországi kkv-kat: dokumentumelemzés, kérdőív, interjúk. Az alábbiakban e három módszert ismertetjük röviden.

Dokumentumelemzés

A dokumentumelemzésünk módszertani alapját *Krippendorff (1995), Sántha (2022), Antal (1976), Babbie (2008)* munkái adták meg. Célként azt fogalmaztuk meg, hogy vizsgáljuk meg a hazai tudományos életben megjelenő, az információbiztonsággal foglalkozó tanulmányokat, kutatási jelentéseket, majd ennek alapján azonosítsuk be a kkv-kat is érintő fontosabb információbiztonsági kihívásokat. Dokumentumelemzésünkbe a Magyar Tudományos Művek Tárában rögzített tanulmányokat vontuk be, s a leválogatást az „információbiztonság" (274 találat), illetve a „kkv" (796 találat) kulcsszavak segítségével végeztük el. A két kulcsszó metszéspontjában összesen két találatot kaptunk. A kapott szövegkorpuszokat az Orange alkalmazás szövegbányászati lehetőségeinek a segítségével elemeztük úgy, hogy előzetesen nem határoztunk meg kulcsszavakat. A szövegmintázatok révén az „Eredmények" részben bemutatott hét fontosabb kihívást azonosítottunk.

Kérdőív

Online kérdőíves kutatásunk módszertani alapjait *Babbie (2008), Scipione (1994), Malhotra (2009)* és *Horváth (2004)* munkái adták meg. Az adatfelvételt 2023. június 16-án kezdtük az UniPoll rendszerén keresztül, és 2023. szeptember 8-án zártuk le. A tanulmányunkban szereplő megállapításainkat 150 kkv-vezető, valamint 31, a szektorban tevékenykedő informatikai munkatárs (IT szakember) válaszaira alapoztuk. Kérdőívünket hat fejezetre tagoltuk a következők szerint: demográfia, vállalkozások bemutatása, eszközhasználat, digitális szokások, információbiztonsági tudatosság felmérése a nemzetközi HAIS-Q mintájára, információbiztonsági tudatosság a napi gyakorlatban. A nemzetközi modellben eredetileg 63 állításon keresztül, hét területre vonatkozóan vizsgálják az információbiztonsági tudatossági szintet. Jelen kutatásunkban a nemzetközi modelltől némileg eltértünk, egyrészt mert a hazai elvárásokhoz és a kutatási céljainkhoz megfelelően kellett adaptálni a modellt, másrészt, mert ez a modell csak egy része volt a kérdőívünknek, így a 63 állítás a kérdőív hosszát jelentősen megnövelte volna, ami a kitöltési arányt negatívan befolyásolná.

Interjúk

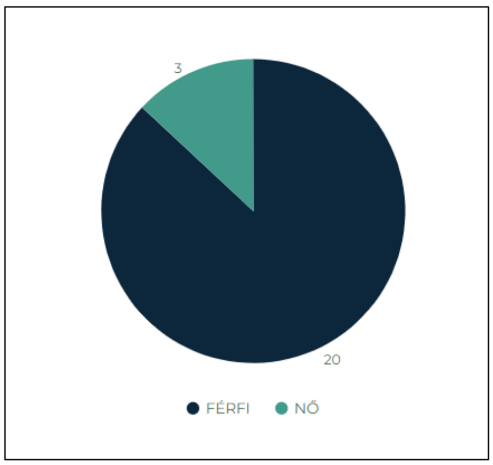
A felhasználók tudatossága általánosságban véve is jelentős kihívást jelent a biztonság területén, ugyanis az emberi tényező egy olyan kritikus elem, amelyet a támadók előszeretettel használnak ki. A munkahely meghatározó része az emberek életének, ebből kifolyólag a munkavállalók tudatosságának felmérésekor számos vállalat és számottevő mennyiségű személy körében lehet vizsgálódni. Az interjúk készítésekor módszertani kérdésekben *Babbie (2008)* munkája mellett *Seidman (2002)*, illetve *Sajtos–Mitev (2007)* írásaira támaszkodtunk. Az interjúalanyok kiválasztása a szakértői kiválasztás folyamatával zajlott le, ami azt takarja, hogy a kkv-vezetőnek rendelkeznie kellett a szakértőkre jellemző ismeretek/tulajdonságok többségével. Ilyen jellemző többek között a magas fokú szakmai ismeret, szakmai-tudományos közéleti aktivitás, szakmai tudományos szervezetek munkájában történő részvétel stb. *(Kollár 2018)*.

Az interjúkat 23 fő kkv-vezetővel készítettük el, akik számára a nemzetközileg is gyakorta alkalmazott információbiztonsági tudatossággal kapcsolatos ötlépcsős modell alapján kerültek összeállításra a kérdések. A modell a tudásra, attitűdre, a jogszabályok ismeretére, a szándékra és a viselkedésre összpontosít, amelyből tudunk következtetni a kkv-k és vezetőik általános információbiztonsági tudatossági szintjére. A napjainkban lezajló változásokra tekintettel a kérdések között helyet kaptak a mesterséges intelligenciára és a drónokra vonatkozó kérdések, a kkv-vezetők hozzáállásának vizsgálata is.

A 23 fő interjúalanyt elkülöníthetjük *(1. táblázat)* az alapján, hogy milyen típusú szervezethez tartoznak, így például az alanyok körében beszélhetünk 2–9 fős; 10–49 fős és 50–249 fős vállalatról.

1. táblázat | Interjúalanyok megoszlása a szervezet mérete alapján

Szervezet mérete	Interjúalanyok száma
2–9 fő	15 fő
10–49 fő	6 fő
50–249 fő	2 fő



2. ábra | Interjúalanyok megoszlása nem alapján

Forrás: saját szerkesztés

Ezen belül a férfi-nő megoszlási arányt is érdemes lehet megemlíteni, mely alapján 20 fő férfi és 3 fő nő kkv-vezetővel készültek el az interjúk. A megoszlási arányt a *2. ábra* szemlélteti.

Az interjúk lebonyolításához az interjúalanyokat e-mailes formában és mobiltelefonos megoldás segítségével kerestük fel, és a felkérés után az interjúk online körülmények között zajlottak. Alapvetően az információbiztonsági tudatossággal kapcsolatos ötlépcsős modellhez kapcsolódóan 26 db kérdést tettünk fel, illetve amennyiben felmerült még egyéb, pontosító és informatívnak minősülő kérdéseket is.

Eredmények

A dokumentumelemzés eredményei

A feldolgozott dokumentumok alapján a hazai kkv-szektor vonatkozásában az alábbi hét kritikus tényezőt azonosítottuk:

1. *Korlátozott erőforrások és költségvetés:* A kkv-k gyakran rendelkeznek korlátozott erőforrásokkal és költségvetéssel, ami megnehezíti az erős informatikai infrastruktúra kiépítését és fenntartását. Az esetlegesen hiányzó pénzügyi források és a szakértelem nélkül nehéz lehet hatékonyan kezelni az információbiztonsági kihívásokat.

2. *Tudatosság hiánya:* Sok kkv nem rendelkezik megfelelő információbiztonsági tudatossággal. A vállalkozások vezetői és alkalmazottai gyakran nincsenek eléggé tisztában az információbiztonság jelentőségével és az ezzel járó kockázatokkal. Ez vezethet a szabályozások figyelmen kívül hagyásához és a biztonsági gyakorlatok alacsony szintjéhez, valamint ezekből fakadóan hatósági bírságokhoz is.

3. *Személyes adatvédelem és szabályozások:* Az adatvédelemre vonatkozó szigorúbb jogi előírások, például az Európai Unió Általános Adatvédelmi Rendelete (GDPR), jelentősen megnövelték az információbiztonsági követelményeket. A kkv-knak komoly figyelmet kell szentelniük az adatvédelmi szabályozásoknak való megfelelésre, ami további erőforrásigényt jelent.

4. *Humán tényezők:* A fenyegetések jelentős része emberi eredetű, legyen szó szándékos vagy véletlen cselekedetekről. A kkv-knak így a technikai/informatikai és jogi megfelelőség mellett foglalkozniuk kell a külső/belső humán jellegű fenyegetésekkel is.

5. *Kiszervezett szolgáltatások biztonsága:* A kkv-k gyakran támaszkodnak kiszervezett IT-szolgáltatásokra, amelyek további biztonsági kockázatokkal járhatnak. A harmadik felek biztonsági intézkedéseinek monitorozása és a megfelelő szolgáltató kiválasztása létfontosságú az információbiztonság szempontjából.

6. *Fejlett kiberfenyegetések:* A kiberbűnözők és a rosszindulatú szereplők egyre fejlettebb támadásokat indítanak kisvállalkozások ellen is. A ransomware, phishing és egyéb támadási módszerek elterjedése miatt a kkv-knak szükségük van hatékony védelmi rendszerekre és azok folyamatos frissítésére.

7. *Mobilitás és távoli munkavégzés:* A mobil munkavégzés és a távoli hozzáférés növekvő trendje szintén kihívásokat vet fel az információbiztonság terén. Az eszközök, az adatok és a hálózatok biztonságának garantálása kulcsfontosságú, különösen a távoli munkavégzés széles körű elfogadásakor.

A kérdőívelemzés eredményei

A vizsgált minta általános leírása a következő. A kérdőívet értékelhető módon összesen 181 fő töltötte ki, akik 73%-a férfi, 27%-a nő volt. A vállalkozások települések szerinti megoszlásában a vármegyeszékhely vagy megyei jogú város (39%) szerepel leggyakrabban, ezt követi az egyéb város (33%), majd község, falu (18%), s végül a főváros (10%). A válaszadók közel fele (47%) 46–49 év közötti, közel harmada (30%) 60 éves vagy idősebb, és 23% 18–45 év közötti. A cégméret tekintetében 64% tartozik a 2–9 főt foglalkoztató mikrovállalkozások, 28% a 10–49 főt foglalkoztató kisvállalkozások, és 9% az 50–249 főt foglalkoztató középvállalkozások közé. A vizsgált vállalkozások elsődleges üzleti területei csökkenő arányban a következők: szolgáltatás (50%), ipar, mezőgazdaság (25%), kereskedelem (22%), közigazgatás, egészségügy, oktatás (3%).

Külön vizsgáltuk a válaszadók munkakörét, végzettségét. Ennek alapján a kkv-vezetők 92%-a ügyvezető, első számú vezető/helyettese, 5%-a pénzügyi vagy gazdasági vezető/helyettese, 3%-a operatív (műszaki, üzemeltetési, biztonsági) vezető/helyettese. Az IT szakemberek 61%-a informatikáért felelős első számú vezető/helyettese, 29%-a egyéb informatikai munkatárs, 10%-a IT-biztonságért felelős vezető/helyettese és 6%-a IT-biztonságért felelős munkatárs. Kíváncsiak voltunk, hogy az IT szakemberek milyen informatikai, információbiztonsági végzettséggel rendelkeznek. Sajnos a válaszadók több mint fele egyéb nem információbiztonsági végzettséggel rendelkezik, s csak elvétve találkoztunk elektronikus információbiztonsági vezetővel, ISO internal auditorral, illetve ISO lead auditorral. A vizsgált mintában senkinek sem volt CISA, CISM, CISSP, CRISC végzettsége, ahogy információbiztonsági szakjogász végzettsége sem.

Az általunk megkérdezett vállalkozások fele működik több mint 20 éve, csak üzleti ügyfeleknek 49%-uk, csak lakossági ügyfeleknek 12%-uk, míg mindkettőnek 39%-uk végez vállalkozói tevékenységet. A 2022. évi adózás utáni eredményét a többségük (56%) inkább pozitívnak értékeli. A 2023. évi (gazdasági) kilátásokkal kapcsolatban harmaduk (35%) stagnálást vár, míg fele-fele arányban (28%, illetve 24%) kismértékű fejlődést, növekedést, illetve enyhe visszaesést jósol.

A vállalkozások közel felében használ minden munkatárs számítógépet a munkavégzése során. Ezt alapvetően jónak ítéljük meg. A vállalkozások közel felében nincsen otthoni munkavégzés, s a válaszadók csupán 15%-a

mondta, hogy mindenki otthonról dolgozik. Azok a vállalkozások, amelyek részben/egészben otthonról (is) működnek, leggyakrabban a felhőalapú szolgáltatásokat használják (57%), ami a gyakorlatban rendszerint a Google Drive, vagy a Microsoft OneDrive szolgáltatását jelenti. Ezt követik használati gyakoriságban az online találkozók megszervezésére/lebonyolítására alkalmas alkalmazások (50%), majd a távoli asztali szolgáltatások (46%), illetve a VPN lehetősége (44%). Ezután egy viszonylagos törést láthatunk, mivel vállalatirányítási rendszert, illetve a teendők rendszerezésére és delegálására szolgáló eszközt 26-26%, projektmenedzsment-rendszert 25%, a hordozható eszközök végpontvédelméért felelős megoldást 23% használ. Megítélésünk szerint az említett alkalmazások használati aránya alacsony, ami egyértelműen kedvezőtlenül hat a szektor fejlődésére. Ilyen mintanagyság mellett nem volt értelme statisztikai relevancia mellett vizsgálni, hogy ez az arány milyen típusú vállalkozások esetében magasabb, de jelzésértékű, hogy azok a vállalkozások, amelyek partnerei üzleti ügyfelek (is), rendszerint magasabb arányban használják a megnevezett szolgáltatásokat. Sokunk számára ismeretes, hogy a COVID-korlátozások miatt meglehetősen sok vállalkozás választotta egy időben az otthoni munkavégzést. Ez a kényszerdöntés ugyan kedvezően hatott az informatikai eszközök és alkalmazások elterjedésére, ugyanakkor ezek nem megfelelően hatékony használata miatt csak meglehetősen korlátoltan tudták – különösen a kkv-k – azokat a hasznukra fordítani. A hatékonyság a COVID után is fontos szempont a vállalkozások számára, ahogy azt a válaszadóink is megerősítették az otthoni munkavégzés vonatkozásában mint a legfontosabb kihívást.

Egy másik kérdésben azt vizsgáltuk, hogy a magyarországi kkv-knál milyen alkalmazásokkal, munkakörökkel lehet találkozni, amelyek alapvetően az információbiztonsághoz kapcsolódnak. Saját weboldallal a megkérdezettek 78%-a, saját webshoppal pedig 20%-uk rendelkezik. Kevesebb mint harmaduknak (28%-28%) van adatvédelmi tisztviselője, illetve információbiztonsági felelőse, s elenyésző azok aránya (13%-13%), akik rendelkeznek üzletmenet-folytonossági tervvel, illetve információbiztonsági audittal. 10% alatt van azok aránya, akik használják a mesterséges intelligenciát, illetve a drón-technológiát. Ez megerősíti a bevezetésben tett azon megállapításunkat, hogy a hazai kkv-k még nem készültek fel az ipar/mezőgazdaság 4.0-ra történő átállásra.

Az informatikai eszközök esetében magától értetődik, hogy azokon operációs rendszer(ek), s egyéb szoftverek/alkalmazások futnak. Összehasonlítottuk, hogy a kkv-k által használt informatikai eszközökön kik végzik a karbantartást (telepítés, frissítés). Meglepő volt a számunkra, hogy a vállalkozás tulajdonosai és IT-területen foglalkoztatott munkatársai hasonló arányban válaszoltak, vagyis az az előzetes feltevésünk, hogy azoknál a vállalkozásoknál, ahol van IT-területen dolgozó kolléga, ott ez a kolléga végzi el ezeket a feladatokat, nem igazolódott. Az is meglepő volt, hogy közel minden ötödik (19%) IT munkatárs ezeket a feladatokat kiszervezi külsős cégnek. A vállalkozások csupán harmadának, felének nem volt még olyan informatikai problémája, amit ki kellett szervezni, hogy megoldják. A kkv IT szakemberek esetében a problémák ritkábban fordulnak elő, míg a vezetők esetében feltételezhetően ott fordul elő inkább a kiszervezés, ahol nincs a vállalkozásnak állandó IT szakembere.

Külön kérdéscsoportban vizsgáltuk meg, hogy a kkv-szektor képviselői milyen eszközöket és milyen gyakorisággal használnak (nyolc eszköz [kategória] használati gyakoriságát mértük). A vállalkozások alapadatai és az eszközhasználatuk kereszttábláinak elemzése során a következő megállapításokat tudjuk tenni. Átlagosan 4,39 eszközt használnak (gyakoriságtól függetlenül) a válaszadók. Napi eszközhasználati átlag 2,96. Nincs szignifikáns eltérés a teljes minta és az alcsoportok között. A hazai kkv-k valamelyest tükrözik azt a (nemzetközi) tendenciát, hogy az okostelefonok használata magasabb a laptopokhoz, a laptopok használata pedig magasabb az asztali számítógépekhez képest. Napi szinten okostelefont a válaszadók 92%-a használ, míg a legkevesebben okosotthon (domotika) rendszert, hangasszisztenst, illetve játékkonzolt használnak. A domotika rendszerek dinamikus elterjedése egyébként az elkövetkező évtizedben várható, így jelenlegi alacsony használata nemcsak a kkv-kra, hanem az egész lakosságra is jellemző.

Jelen tanulmányunkban többször utaltunk arra, hogy a hazai kkv-k nincsenek felkészülve az ipar/mezőgazdaság 4.0-ra történő átállásra, ugyanakkor a digitális munkahelyre *(Kollár–Poór 2018; Kollár 2015)* jellemző digitális szokások tekintetében a helyzet meglátásunk szerint elfogadható. Az e-mailek küldése és fogadása 100%-ban a napi rutin része lett. A válaszadók 99%-a használja a számítógépét online bankolásra, közel 40%-a ezt napi szinten teszi. 98% használja az internetet vásárlásra is, igaz, csak egytizedük teszi ezt napi rendszerességgel. A hírek olvasása, illetve a telefonálás és videóhívás a használat (96%-96%) és a napi használat (71%-78%) kimagaslónak mondható. Ugyan a közösségi médiát a válaszadók 86%-a használja, de napi rendszerességgel csak 39%-uk. Mivel a közösségi médiában való jelenlét rendszerint napi – akár többszöri – aktivitást kíván meg, így a kapott eredmények alapján úgy gondoljuk, hogy a hazai kkv-k még nem fedezték fel azokat az üzleti lehetőségeket, amelyeket a közösségi média platformjai kínálnak a számukra. Összességében alacsonynak tekinthető a mesterségesintelligencia-alapú tanulási és/vagy munkatevékenységeket támogató alkalmazások használata. Ezen véleményünk szerint a kkv-knak szóló képzéssel változtatni kellene. A kkv-k válaszait összevetettük a teljes magyar lakosságot reprezentáló 3000 fős mintánkkal, a napi rendszerességgel végzett internetes tevékenységek fókuszában *(2. táblázat)*.

2. táblázat | Internetes tevékenység – KKV vs. Polgári lakosság

Napi rendszerességgel végzett internetes tevékenységek (%)	Kkv-k (teljes minta)	Polgári lakosság (teljes minta)
Bázis	**181 fő**	**3000 fő**
E-mailek küldése/fogadása	96	68
Telefonálás vagy videóhívás	78	61
Hírek online olvasása	71	57
Közösségi médiában való részvétel	39	76
Internetes banki szolgáltatások használata számítógépen	38	24
Mobilbank használata	28	26
Streaming szolgáltatás	22	37
Tartalom letöltése/feltöltése	15	31
Internetes vásárlás	10	14
Online játékok	10	33
Digitális tanulás, távoktatás	10	19
Tanulás vagy munka mesterséges-intelligencia-alapú támogatása	7	17
Munkakeresés vagy munkára jelentkezés	6	17

Szignifikáns eltérés a polgári lakosság teljes mintájához képest: zöld színű mező: szignifikánsan nagyobb; narancsszínű mező: szignifikánsan alacsonyabb. A szignifikancia szintje ,05.

Fontosnak tartottuk megvizsgálni a vállalkozók szubjektív tudásszintjét. A tizenegy terület közül átlagosan 4,67 területre mondták azt a válaszadók, hogy rendelkeznek az adott tudással. Ez szignifikánsan magasabb, mint a polgári lakosság esetében (4,19). A kkv-minta esetében szignifikánsan alacsonyabb az átlagos tudásszint a nők, a 60 éves vagy idősebb, illetve a senki sem dolgozik home office-ban csoportok esetében. Több területen rendelkeznek tudással a 18–45 éves korosztály, az IT munkatársak és a home office-ban dolgozók. Az öt legtöbb pontot kapott ismeret csökkenő sorrendben a következő: szövegszerkesztő programok, táblázatkezelő programok, prezentációs programok, képszerkesztő programok, vállalatirányítási rendszerek.

Kérdőívünk információbiztonság-tudatossággal kapcsolatos része – ahogy arra már fentebb utaltunk – a nemzetközi HAIS-Q (Human Aspects of Information Security Questionnaire) mérésen alapul, mely a Tudás – Attitűd – Viselkedés modellen keresztül méri az Információbiztonsági Tudatosságot (ISA – Information Security Awareness). A kkv-vezetők esetében leginkább a közösségi média, a jelszóhasználat és a mobileszközök területén erős az információbiztonsági tudatosság. A közösségi média esetében a tudás, a jelszóhasználat esetében az attitűd, a mobileszközök esetében a viselkedés területe gyengébb némileg. A leggyengébb terület a mesterséges intelligencia használatához kapcsolódik. A kkv IT munkatársak esetében a mobileszközök mellett erős az információbiztonsági tudatosság az incidensek jelentése területén, ami rendkívül fontos az ilyen munkakörben dolgozók számára. A jelszóhasználattal kapcsolatos tudatosság is viszonylag erős, de itt a tudás elmarad az attitűd és a viselkedés szintjétől.

Kérdőívünk utolsó részében az információbiztonsági tudatosság további jellemzőit vizsgáltuk, s olyan kérdéseket tettünk fel, melyek az elmúlt eseményekre reflektálnak, azoknak a hatásait mérik, vagyis hogyan hatottak az emberek információbiztonsági tudatosságára. Az információbiztonsági képzéseken való részvétellel kapcsolatban szomorúan állapítjuk meg, hogy a válaszadók 83%-a nem szokott részt venni a munkahelyén minimum évenkénti rendszerességgel tartott információbiztonsági tudatosító képzésen. Még az IT szakembereknek is csak 23%-a mondta azt, hogy részt szokott venni ilyen képzésen. Ezen a helyzeten mihamarabb változtatni kellene. A kkv-vezetők és az IT munkatársak is hasonlóan vélekedtek a vállalkozások biztonsági érettségi szintjéről: közel 50%-uk szerint elfogadható szintű. A vállalkozások vezetői és IT munkatársai egyaránt egyetértenek abban, hogy az információbiztonsági kockázatokat azonosítani kell és a működési folyamatok során figyelembe kell venni – ezt pozitívan értékeljük. Ugyanakkor a többség nem, vagy nem kellő szakmaisággal méri fel a lehetséges incidensek kockázatát a vállalatra. Csak minden tizedik vállalkozásban tapasztaltak kiberbiztonsági incidenst az elmúlt egy év során, miközben a nemzetközi jelentések alapján ez a szám lényegesen magasabb. Vagyis: a hazai kkv-szektor fontosnak érzi az informatikai kockázatok azonosítását, de zömében nem rendelkezik olyan eszközökkel, megoldásokkal és humán intelligenciával, hogy a gyakorlatban is képes legyen ezt a tevékenységét eredményesen végezni. A válaszadók több mint fele (57%) alkalmaz olyan technikai megoldásokat, mint például szoftverfrissítések, biztonsági mentések készítése, kommunikáció titkosítása és a hálózati hozzáférésre vonatkozó szabályok alkalmazása – ami jó, de sajnos a többségnél ez jelenti egyelőre az információbiztonsági tudatosságot.

Interjúk eredményei

Ahhoz, hogy felmérhessük a célcsoport körében az információbiztonsági tudatosságot, segítségünkre van az információbiztonsági tudatosság felméréséhez kapcsolható, a korábbiakban már említett ötlépcsős modell. A modell összességében a releváns információbiztonsági tájékozottságot, az ismereteket, a szándékot és viselkedésmódot hivatott vizsgálni, tehát azt, hogy az információbiztonsági tudatosság milyen módon és mértékben van jelen a kutatócsoportunk által kijelölt célcsoportoknál. A 23 fővel lebonyolított interjúk kiértékelését és a kiértékelés eredményének összegzését kíséreljük meg bemutatni jelen fejezetrésznél.

Először is nézzük az első nyitott kérdést, hogy az interjúalanyok mit gondolnak arról, hogy mit jelent a kiberbiztonság mint kifejezés elméletben és gyakorlatban egyaránt. A kérdésre adott válaszokból – arról, hogy a kkv-vezetők szerint mit jelent a kiberbiztonság – összességében csoportokat képeztünk, mint például:

- információbiztonság,
- adatokhoz való hozzáférés korlátja,
- informatikai eszközhöz való hozzáférés korlátja,
- támadások és az ezek ellen való védekezés,
- biztonságtudat megléte.

Az interjúalanyok (kkv-vezetők) által irányított szervezetek többsége nem alkalmaz információbiztonságért felelős személyt és a szervezetek túlnyomó része nem rendelkezik semmilyen információbiztonsághoz kötődő tanúsítvánnyal. Az interjúk alapján a kkv-vezetők nagy része szerint adatvédelmi szempontból biztonságtudatosság jellemzi az adott szervezetnél dolgozó munkatársakat, és a kiberbiztonsághoz kötődő jogszabályok változását a megkérdezettek kicsit több mint a fele követi. Az interjúalanyok és a hozzájuk köthető szervezetek esetében zömében alkalmazzák a *„tiszta asztal, tiszta képernyő”*[2] politikát, és viszonylag kevés esetben engedett meg, hogy saját eszközt is alkalmazzanak munkavégzésre. Napjaink változására reagálva arra voltunk kíváncsiak, hogy a mesterséges intelligencia és a kiberbiztonság mennyire kötődik egymáshoz az interjúalanyok szerint. A nyilatkozatok alapján egy-két kivétellel, a többség szerint egyértelműen kötődik egymáshoz a két fogalom. Az esetek többségében pontosan nem tudták megmondani, hogy mennyire kötődnek egymáshoz, csekély mértékben pedig – a visszajelzések szerint – nagyon kötődik egymáshoz a mesterséges intelligencia és a kiberbiztonság. Az előbbi kapcsán mesterséges intelligenciát a megkérdezettek kevesebb mint fele használna humán munkaerő kiváltására, az alanyok javarészt pedig egyáltalán nem, vagy inkább csak a humán munkaerő segítésére, nem pedig kiváltására alkalmazná. Ezenfelül a drónok kapcsán nagyobb elhatárolódás figyelhető meg, ugyanis a kkv-vezetők nagyobb része nem alkalmazná a drónokat biztonságtechnikai eszközként. Ez talán abból is fakadhat, hogy a mesterséges intelligencia valamilyen formában elérhetőbb a felhasználók számára, mint például egy drón.

A szervezetnél már alkalmazott védelmi megoldásokat (pl. vírusirtó) a kkv-vezetők jobbára a mindennapok során is alkalmazzák, és a megkérdezett szervezetek pusztán kis része volt már áldozata kiberbiztonsági incidensnek. A kérdésre, amely arra vonatkozott, hogy az interjúalany mennyire érzi saját magát és szervezetét célpontnak a kibertérben, arra a válaszadók harmada válaszolta azt, hogy nagymértékben célpontnak érzi magát, minimális részük azt, hogy közepes mértékben érzi magát célpontnak, és a válaszadók valamennyivel több mint a fele egyáltalán nem érzi sem magát, sem pedig a szervezetet célpontnak. Az általános tendenciától eltekintve olyan válaszpár is megtalálható a kérdésekre adott válaszok között, ahol az interjúalany szervezete bár élt már át kiberbiztonsági incidenst/támadást, ettől függetlenül nem érzi magát célpontnak a kibertérben.

A kérdések során olyan válaszok is felmerültek, amelyek arra utaltak például, hogy adatvédelmi szempontból biztonságtudatosnak is tartja a kkv-vezető a munkatársait, meg nem is. Tehát a munkatársak igyekeznek betartani a szabályokat és tudatosan eljárni, azonban az érintett vezetők szerint még lenne hova fejlődni. A mesterséges intelligencia szabályozási kérdéskörében voltak olyan kkv-vezetők, akik nem tudták meghatározni azt, hogy szükséges-e szabályozni a mesterséges intelligencia használatát, főleg abból az okból kifolyólag, hogy számukra a munkaterületükön egyáltalán nem volt releváns a mesterséges intelligencia megjelenése, így a szabályozási kérdéseken sem gondolkodtak. Azzal kapcsolatban pedig, hogy a szervezetnél megengedett-e saját eszközt munkavégzésre használni, az érintett kkv-vezetők azt nyilatkozták, hogy bár összességében céges laptopot használnak, a munkahelyi levelezést, ügyintézést, vagyis bizonyos korlátozott munkahelyi funkciókat a munkavállalók a saját telefonjukról is elérnek.

A kkv-vezetők interjúkérdésekre adott válaszai alapján, a kiberbiztonsághoz kötődő védelmi megoldások esetében a *tűzfal* a leginkább alkalmazott védelmi megoldás, ezt követi a *jelszópolitika* mint a megfelelő erősségű jelszónak az előírása és alkalmazása, harmadik helyen a különféle *vírusvédelmi megoldások* állnak. Ezeken felül olyan kibervédelmi megoldások alkalmazása is elhangzott, mint a VPN[3], a biztonsági mentések és az authentikátor applikációk alkalmazása.

A munkavállalók biztonságtudatosságának hozzáállása és a hozzáállás megnyilvánulása – a kkv-vezetők válaszai alapján – *az adatok és informatikai eszközök gondos kezelésében, a szabályok betartásában és a tiszta asztal, tiszta képernyő politika alkalmazásában* látható. Abban, hogy a biztonságtudatos hozzáállás fenntartásának kérdésköre a megkérdezett szervezeteknél milyen módszerekben jelenik meg, a kapott válaszok alapján az *oktatás, a szimuláció és a tapasztalat(csere)* szerepel. Az interjúalanyok egy része szerint a *vezetői visszajelzés* is fontos szerepet tölt be a biztonságtudatos hozzáállás erősítésében. A lebonyolított interjúk egy részénél az oktatás kapcsán felmerült, hogy időhiányban szenvednek a szervezetek, nem pusztán pénzügyi erőforrásokat kell megteremteni, de időt is az efféle tevékenységre, amely már kiesett munkaerőt fog eredményezni.

Az interjúalanyok jellemezhették szervezeteik információbiztonsági érettségi szintjét is, ez alapján a meg-

[2] „Lényege, hogy a belső céges adatok ne kerüljenek a kezelésükre nem jogosult, ismeretlen vagy akár ártó szándékú felek kezébe.” *(Bonnyai–Kiss–Tóth 2023)*

[3] Virtual Private Network.

kérdezett kkv-vezetők több mint fele gondolja úgy, hogy magas szinten van a szervezete információbiztonsági érettségi szintje, egy kisebb részük szerint közepes szinten és az interjúalanyok legkisebb része érzi úgy, hogy a szervezete információbiztonsági szintje alacsony. Az interjú során a kérdésekre elvétve, de előfordult, hogy olyan válasz érkezett, amely a biztonságtudatosság és a kiberbiztonsági védelmi megoldások hiányát szemlélteti. Nagyrészt, aki azt nyilatkozta, hogy nincs a szervezetnél védelmi megoldás, vagy éppen a munkatársak biztonságtudatosságát tartotta alacsonynak, jellemzően ez a személy alacsonyra értékelte a szervezet információbiztonsági tudatossági szintjét. Azonban arra is van példa, hogy védelmi megoldása sincs a szervezetnek, a biztonságtudatosságot sem nevezte az interjúalany jellemzőnek a szervezetnél, azonban közepes szintűre értékelte a szervezet információbiztonsági érettségi szintjét. Így hát megállapítható, hogy elég szubjektív a vezetői szemszögből az, hogy mi minősül megfelelő biztonságtudatosságnak, és hogy a szervezetnek van-e szüksége kiberbiztonsági védelmi megoldásokra.

Összegezzük a feldolgozott interjúk alapján a hazai kkv-szektor vonatkozásában a korábban megállapított hét kritikus tényezőt:

1. *Korlátozott erőforrások és költségvetés:* Az interjúk során az derült ki, hogy erőforrás tekintetében az idő az egyik legkritikusabb tényező, hiszen a munkaidőben lebonyolított oktatások esetében munkaerőforrás esik ki.
2. *Tudatosság hiánya:* Az interjúk alapján az a tanulság a biztonságtudatosságra vonatkozóan, hogy bár folyamatosan egyre nagyobb az igény a szervezeteknél a biztonsági kultúra kiépítésére, azonban a legtöbb vállalat még viszonylag távol áll a teljes kialakítástól. Ez a tényező abból is fakadhat, hogy a kis méretű vállalatok túlnyomó többségénél úgy vélik, hogy a kis méretből adódóan nem képeznek célpontot a támadók számára. Ez a tény pedig azt eredményezi, hogy a biztonságtudatosságra és fokozására sem fordítanak elég erőforrást.
3. *Személyes adatvédelem és szabályozások:* A szabályozások és az adatvédelem területén a gyenge pontot a szabályozások változásainak a követése adta. A szervezetek rendszerint igyekeznek követni, ezt egy részük külsős szakértő vagy cég segítségével teszik meg.
4. *Humán tényezők:* Látható az interjúkérdésekre kapott válaszokból is, hogy egyrészről meglehetősen szubjektív értelmezésű a biztonságtudatosság az emberek szemében, illetve az ehhez tartozó fogalmak és a tevékenységek milyenségének megítélése is. Ezzel együtt megállapítható, hogy a biztonság fenntartása nem jelenti ugyanazt mindenki számára, így törékeny annak a biztosítása is. Egy rendszer lehet bármennyire biztonságos, ha nem tudatosak a rendszert használók.
5. *Kiszervezett szolgáltatások biztonsága:* Főleg az üzemeltetés és szabályozás terén az interjú során megkérdezett kkv-vezetők és szervezeteik körülbelül fele alkalmaz valamilyen, a szervezeten kívüli céget vagy szakértőt az információbiztonság, az üzemeltetés vagy az adatvédelem teljesülése érdekében.
6. *Fejlett kiberfenyegetések:* A szervezeti biztonsági kultúra kiépítése és fejlesztése nagy valószínűséggel lassabban valósul meg, mint ahogyan a támadók eszközkészlete és a kártevő programok fejlődnek. Az interjúkérdésekre kapott válaszok alapján a szervezetek nagy része az alapvető védelmi megoldásokkal rendelkezik, mint például a vírusirtó, tűzfal, alapvető jelszópolitika. Azonban a támadók felkészültségi oldala már nagy valószínűséggel sokkal előrehaladottabb, és nem akadályozzák meg őket a hagyományos védelmi eszközök.
7. *Mobilitás és távoli munkavégzés:* A szervezetek több mint a felénél működik a távoli munkavégzés is, egyikét szervezetnél pedig saját eszközt is lehet alkalmazni munkavégzésre. A távoli munkavégzésnek megvannak a kritikus pontjai, ilyen például az, hogy a munkaerőforrás az otthoni környezetben – ahol biztonságban éri magát – hajlamosabb szabadabban rákattintani, rákeresni a nem munkavégzéshez tartozó weboldalakra, fájlokra, ugyanis nem érzi magát ellenőrizve. Amennyiben ehhez még hozzávesszük az erősebbnek tartott védelmi megoldások hiányát és az amúgy is kritikus humán tényezőket, akkor láthatjuk, hogy érdemes odafigyelni a távoli munkavégzés sajátosságaira, és érdemes fejleszteni a biztonsági kultúra erre vonatkozó részeit is.

Következtetések, összefoglalás

A dokumentumelemzés során bemutatott hét kritikus tényező, valamint a kkv-szektor vezetői és IT munkatársai körében folytatott nagymintás, online kérdőív, illetve személyes interjúk egyaránt egy viszonylag kongruens képet mutatnak a szektor jelenlegi információbiztonsági helyzetéről. Mindenképpen pozitívan értékeljük, hogy a kkv-knál is számos informatikai eszköz és alkalmazás a napi/heti munkafolyamatok része lett. A vállalkozások többségénél lehet találkozni a digitális munkahelyekre jellemző digitális szokások elterjedésével, ugyanakkor meglátásunk szerint az eszközök, szoftverek, alkalmazások használatából eredő megannyi előnyből a vállalkozások zöme csak néhány – a magánéletében is gyakrabban használt – lehetőséggel él, vagyis az eszközök, szoftverek, alkalmazások vállalati környezetbe történő integrálása nem, vagy csak néhány területen történt meg.

Számunkra is kérdéses volt, hogy mennyire tekinthető egy 181 fő válaszát tartalmazó kérdőíves felmérés reprezentatívnak. Ha a kkv-szektor egészét nézzük, akkor meglehetősen szűk a mintánk. Másfelől: ezek a vállalkozásvezetők, illetve IT munkatársak voltak azok, akik számára fontos volt, hogy kifejezzék véleményüket, álláspontjukat az információbiztonság vonatkozásában, s a kérdéseinkre adott válaszaik lehetőséget adjanak a szá-

mukra egy kis információbiztonsági önreflexióra is. Ebből, illetve az interjúkból pedig egyértelműen megállapítottuk, hogy szükség van olyan gyakorlatorientált képzési programok kidolgozására és alkalmazására, amelyek segíthetik a hazai kkv-szektor vezetőit és IT szakembereit információbiztonsági tudatosságuk fejlődésében, s akár az ipar/mezőgazdaság 4.0-ra történő átállásban is.

Az interjúkérdésekre kapott válaszok alapján megállapítható, hogy összességében a kkv-vezetők és szervezeteik számosságban egyre inkább kezdik felépíteni a szervezetet övező kiberbiztonsági megoldásokat és információbiztonsági intézkedéseket. A 23 fővel készült interjú alapján elmondhatjuk, hogy a terület nagyságára tekintettel a teljes felméréshez szükséges további kutatások és felmérések elvégzéséről azonban már most is levonhatunk adott következtetéseket. A korábbiakban felvázoltak alapján jelenleg még szükséges lenne olyan információbiztonsági jó gyakorlatok kialakítása és megosztása, amely a kkv-kat is képes megfogni, ugyanis lenne igény oktatásokra és tapasztalatcserékre, de nem minden vállalat határozza el magát teljesen az ügyben, így a tényleges igény megfogalmazása és a cselekvés, szervezés már végső sorban elmarad. A megkérdezett szervezetek kis része volt már áldozata kiberbiztonsági incidensnek és a kkv-vezetők egy jó része gondolja úgy, hogy amíg nem történt meg egy incidens a munkavállalóval vagy a szervezettel, addig nem fog belőle tanulni az illető. A mesterséges intelligenciára és drónokra vonatkozóan egy általános, tartózkodó állapot figyelhető meg, de teljes elzárkózás nem, így a következő években fog várhatóan eldőlni, hogy mekkora szerepet fognak ezek az eszközök betölteni a szervezetek életében. Alapvetően az látható, hogy növekszik az igény a biztonság fokozására, és a biztonságot garantáló eszközök alkalmazására, illetve az információbiztonságot is érintő oktatásokra, azonban ez lassú folyamatként fejlődik, és nem olyan gyorsan, mint ahogyan a világ is változik körülöttünk, így kérdéses, hogy mikor fog bekövetkezni egy információbiztonsági robbanás, amely esetleg a szervezetek eszköztárát és hozzáállását gyökeresen megváltoztatja.

Köszönetnyilvánítás

A TKP2021-NVA-05 számú projekt a Kulturális és Innovációs Minisztérium Nemzeti Kutatási, Fejlesztési és Innovációs Alapból nyújtott támogatásával, a TKP 2021 pályázati program finanszírozásában valósult meg.

Irodalomjegyzék

Antal L. (1976) A tartalomelemzés alapjai. Budapest: Magvető

Babbie, E. (2008) A társadalomtudományi kutatás gyakorlata. Budapest: Balassi

Bonnyai T., Kiss A., & Tóth A. (2023) Nagyvállalati biztonságtudatosság és nyílt forrású információszerzés. Budapest: Nemzeti Közszolgálati Egyetem Ludovika Egyetemi Kiadó, pp. 15–29.

Horváth Gy. (2004) A kérdőíves módszer. Budapest: Műszaki Könyvkiadó

ISACA (2023) Információbiztonsági Helyzetkép 2023. 1–27. https://engage.isaca.org/budapestchapter/informaciobiztonsagi-helyzetkep (letöltve: 2023. 10. 30.)

Kollár Cs. (2015) Munkaadók és munkavállalók a digitális korban: Az intranettől a digitalizált munkahelyig. In: Futó Z. (szerk.) Tudomány és innováció a lokális és globális fejlődésért: nemzetközi tudományos konferencia előadásai. Szarvas: Szent István Egyetemi Kiadó, pp. 157–163.

Kollár Cs. (2018) A szakértővé válás, illetve a szakértők kiválasztásának és megkérdezésének módszertani kihívásai. Vezetéstudomány / Budapest Management Review, Vol. 2. pp. 63–75. https://doi.org/10.14267/VEZTUD.2018.02.07.

Kollár Cs., Poór J. (2018) Szervezetek a digitális korban – A digitális munkahely információbiztonsági aspektusa. In: Rajnai Z. (szerk.) Kiberbiztonság – Cyber Security: Tanulmánykötet a Biztonságtudományi Doktori Iskola kutatásaiból. Budapest: Óbudai Egyetem, Bánki Donát Gépész és Biztonságtechnikai Mérnöki Kar, pp. 95–107.

Krippendorff, K. (1995) A tartalomelemzés módszertanának alapjai. Budapest: Balassi

KSH (2022) https://www.ksh.hu/docs/hun/xftp/idoszaki/mosz/mosz_2022.pdf (letöltve: 2023. 10. 16.)

Lazányi K. (2016) A biztonsági kultúra szerepe a vezetői döntések támogatásában. The Role of Safety Culture in Supporting the Leaders' Decision Making. Taylor, Vol. 8. No. 1. pp. 143–150.

Malhotra, N. K. (2009) Marketingkutatás. Budapest: Akadémiai

Mike N., Krén E. & Kecskeméti T. (2023): Farkasbiztos téglaház? A KKV-k információbiztonsága Magyarországon. Vezetéstudomány, Vol. 54. No. 9. pp. 44–57.

Póserné Oláh. V. (2007) IT kockázatok, elemzésük, kezelésük. Hadmérnök, Vol. 2. No. 3. pp. 206–214. http://hadmernok.hu/archivum/2007/3/2007_3_poserne.html

Sajtos L., Mitev A. (2007) SPSS kutatási és adatelemzési kézikönyv. Budapest: Alinea

Sántha K. (2022) Kvalitatív tartalomelemzés. Budapest: Eötvös József Könyvkiadó

Scipione P. A. (1994) A piackutatás gyakorlata – Gyakorlati útmutató szakembereknek és hallgatóknak. Budapest: Springer Hungarica

Seidman, I. (2002) Az interjú, mint kvalitatív kutatási módszer. Budapest: Műszaki Könyvkiadó