MIKE NIMRÓD – KRÉN ENIKŐ – KECSKEMÉTI TAMÁS

# FARKASBIZTOS TÉGLAHÁZ? A KKV-K INFORMÁCIÓBIZTONSÁGA MAGYARORSZÁGON

# WOLF-PROOF BRICK HOUSE? INFORMATION SECURITY OF SMES IN HUNGARY

Az informatikai és információbiztonság olyan fontos a KKV-k életében, mint a sivatagban az oázis. A vállalatok versenyképességéhez nagyban hozzájárul a biztonság szintje, amely terület erősen alulreprezentált a KKV-szektorban. A tanulmány arra a kérdésre keresi a választ, miszerint valóban megfigyelhető-e, hogy a sürgetett digitalizáció negatív hatással van az információbiztonsági szintre nézve a KKV-k életében Magyarországon. Az elemzés főként az e-kereskedelemben aktívan részt vevő cégekre terjed ki. Magyarországon és az Európai Unióban összehasonlítva kimutathatók az információbiztonsággal és adatvédelemmel kapcsolatos trendek, amelyekből látható a területet érintő elmaradottság. A tanulmány a Digiméter 2020, 2021 és 2022-es kvantitatív kutatásának eredményét mutatja be, emellett az Európai Unió által biztosított DESI-index (Digital Economy and Society Index) és NCSI (National Cybersecurity Index) nyilvános adatait dolgozza fel. A kutatás várható eredménye igazolja, hogy Magyarországon jól látható az információbiztonság kiforratlansága.

Kulcsszavak: **információbiztonság, KKV, klaszteranalízis**

IT and information security are as important in the life of SMEs as an oasis in the desert. The level of security contributes greatly to the competitiveness of companies, an area that is strongly under-represented in the SME sector. The study seeks to answer the question of whether it can really be observed that urgent digitisation has a negative impact on the level of information security in the life of SMEs in Hungary. The trends related to information security and data protection can be compared in Hungary and the European Union, showing the backwardness of the area. The study presents the results of Digimeter's 2020, 2021 and 2022 quantitative research, and also processes public data from the Digital Economy and Society Index (DESI ) and other available indexes. The expected results of the research confirm that the immaturity of information security is clearly visible in Hungary.

Keywords: **information security, SME, cluster analysis**

**Finanszírozás/Funding:**
A szerzők a tanulmány elkészítésével összefüggésben nem részesültek pályázati vagy intézményi támogatásban.
The authors did not receive any grant or institutional support in relation with the preparation of the study.

**Szerzők/Authors:**
Dr. Mike Nimród[a] (nimrod.mike@librantis.hu) adatvédelmi szakértő; Krén Enikő[a] (eniko.kren@librantis.hu) vezető tanácsadó; Kecskeméti Tamás[a] (tamas.kecskemeti@librantis.hu) szoftverfejlesztő, adatelemző

[a] Budapesti Corvinus Egyetem/Librantis (Corvinus University of Budapest/ Librantis) Magyarország (Hungary)

A cikk beérkezett: 2022. 11. 25-én, javítva: 2023. 02. 28-án és 2023. 07. 20-án, elfogadva: 2023. 07. 21-én.
The article was received: 25. 11. 2022, revised: 28. 02. 2023, and 20. 07. 2023, accepted: 21. 07. 2023.

A legtöbben ismerjük a Három kismalac történetét, ahol a malacok okos stratégiával meg tudják leckéztetni az éhező farkast. Az infrastruktúra megszilárdítása és a fenyegetések kezelése alapvető tanulságai e mesének. A mesét összehasonlítva a valósággal, megállapítható, hogy a kis- és középvállalkozások (KKV-k) számára az erős infrastruktúra – ebben az esetben az információbiztonság – nélkülözhetetlen.

Az információbiztonság kérdése napjainkban kiemelt fontosságú, legyen szó bármely méretű vállalatról. Az adatok védelme, a kibertámadások elleni védekezés és a biztonságos digitális környezet fenntartása létfontosságú (Romanosky et al., 2011), és egyre több figyelmet kap nemcsak a nemzetközi, de a hazai szakirodalomban (Nemeslaki & Sasvári, 2014) is.

Ezen belül úgy tűnik azonban, hogy a KKV-k esetében az információbiztonság jelentősége gyakran alulreprezentált, holott ennek kiforratlansága komoly veszélyeket hordoz. Az Európai Unió (EU) tagállamai közül Magyarországon a helyzet különösen aggasztó: az információbiz-

tonsági szint jelenleg még kiforratlan, ám a szükségességének jelei egyre nyilvánvalóbbak.

A tanulmány célja, hogy betekintést nyújtson a magyarországi KKV-k információbiztonsági szintjébe, és feltárja a téma relevanciáját és fontosságát a vállalatok versenyképessége szempontjából. A kutatás során kvantitatív módszerekkel vizsgáljuk meg a KKV-k információbiztonsági szintjét befolyásoló tényezőket, és ennek alapján javaslatokat teszünk arra vonatkozóan, hogy milyen lépéseket tehetnek a vállalkozások a versenyképességük növelése érdekében. Kutatási eredményeink főleg a digitális marketinggel foglalkozó vállalkozások versenyelőnyét támasztják alá az egyéb szegmensekben tevékenykedő vállalkozásokkal szemben.

Az előzetes kutatások és az irodalmi háttér alapján feltételezhetjük, hogy a vállalkozások mérete, az alkalmazott technológiai eszközök, az információbiztonsági politikák, valamint a vezetők és alkalmazottak hozzáállása és tudatossága jelentősen befolyásolja az információbiztonsági szintet. Kutatásunk során e feltételezés mentén vizsgáljuk az információbiztonság és a vállalatok versenyképessége közötti összefüggéseket, hiszen meggyőződésünk, hogy az erős információbiztonság növeli a vállalkozások versenyképességét és hosszú távon a profitabilitását is.

Összességében kutatásunkkal szeretnénk hozzájárulni a KKV-k információbiztonsági felkészültségének növeléséhez, és elősegíteni a szükséges fejlesztések bevezetését ezen a területen.

## Szakirodalmi áttekintés

A téma mélyebb megértéséhez elengedhetetlen, hogy a fontosabb fogalmakhoz tartozó szakirodalmat áttekintsük, mint az információbiztonság, a kibervédelem vagy kiberbiztonság (cybersecurity), a biztonság tág körű fogalma a vállalatok szemszögéből és a KKV-k biztonsága. A biztonság megvitatására használt terminológia, a digitális eszközök és információk vonatkozásai jelentősen megváltoztak az elmúlt években. A század elején rendszeresen használt kifejezések ebben az összefüggésben a „számítógép-biztonság" „IT-biztonság" vagy „információs biztonság". Míg ezek a kifejezések árnyalatnyi eltéréseket mutatnak, az ebben dolgozó szakemberek értették, elég kézzelfoghatóak voltak ahhoz, hogy jelentőségteljessé váljanak szélesebb kör számára. Az első évtized vége felé új terminológia kezdett egyre népszerűbbé válni a „kiberbiztonság" kifejezés használata által (Schatz et al., 2017).

Az információbiztonság az információ védelmét jelenti azok létrehozása, feldolgozása, tárolása, továbbítása során. Az ártalmatlanítást olyan logikai, technikai, fizikai és szervezeti intézkedésekkel lehet véghezvinni, amelyek ellensúlyozzák a bizalmasság, integritás és elérhetőség elvesztésének lehetőségét (Ključnikov et al., 2019). Az információbiztonság irányítása az ISO/IEC 27001 szabványa szerint történik az egész világon. A vállalatoktól elvárt a szabványnak való megfelelőség, amely kitér a biztonsági menedzsment területekre, a vállalat eszközeinek biztonságára és az IT-biztonsági elvárásokra (ISO standards).

A szabvány részei kitérnek a kibervédelem témakörére, amely bizonyítja, hogy a vállalatoknak nincsen lehetőségük a téma elhanyagolására. Széles körben használják a kifejezést, változó definícióval alátámasztva. Nincsen egységesen meghatározott definíció, amely le tudná írni, hogy pontosan mit értünk kibervédelem alatt, mi tartozik ezen terület részeibe. A megértés függ a kontextustól, lehet szubjektív, esetenként informatív (Craigan et al., 2014).

A cikk megértését és alátámasztását szolgálja a szakirodalomban fellelhető kibervédelmi definíciók feldolgozása. A következő két definíció foglalja a legjobban össze, hogy a továbbiakban mi tartozik a kibervédelem fogalomkörébe. „Az a tevékenység vagy folyamat, képesség vagy készség, olyan állapot, amellyel az információs és kommunikációs rendszerek és a bennük lévő információk védve vannak a károsodástól, jogosulatlan használattól, módosítástól vagy kizsákmányolástól" (DHS, 2014).

„A kiberbiztonság olyan eszközök, irányelvek, biztonsági koncepciók, biztonsági biztosítékok, iránymutatások, kockázatkezelési megközelítések, intézkedések, képzések, legjobb gyakorlatok és technológiák gyűjteménye, amelyek felhasználhatók a kiberkörnyezet, valamint a szervezet és a felhasználó eszközeinek védelmére" (ITU, 2009). A feldolgozott indexek dimenziói megfelelnek a definíciókban leírtaknak. Emellett a fogalom komplexitása rávilágít, hogy széles körű ismeretekre van szükség a kibervédelem megértéséhez és a megfeleléshez (von Solms & von Solms, 2018).

Az információs rendszerek biztonsága kihívást jelent minden vállalat és kormányzati szervezet számára, a legnagyobbaktól kezdve a legkisebbig. A vállalatok, különösen a kis- és középvállalkozások kénytelenek az információ biztonságával foglalkozni. Üzleti működésük függ az információs technológiák és hálózati rendszerek használatától és elengedhetetlen a döntéshozatali folyamatok támogatása érdekében. Ez a függőség különösen sebezhetővé teheti őket az információs rendszerek biztonsági fenyegetéseivel szemben, korlátozott humán és technikai erőforrásaik, valamint az információs rendszerek sebezhetőségi problémáival kapcsolatos korlátozott lehetőségeik miatt (Sadok et al., 2020).

Magyarországon 2012-ben közel harmincezer vállalkozást számláltak az egyéni és mikrovállalkozásokat nem számolva. Nemzetközi és magyarországi felmérések egyaránt bizonyítják, hogy a vállalatok nem megfelelő súllyal foglalkoznak az információbiztonsággal. A KKV-k esetében különösen lehangoló a helyzet. A velük szemben támasztott elvárások gyorsan és nagymértékben változnak, az üzleti környezetükkel együtt. Habár az információbiztonsági tevékenységük vagy annak hiánya kisebb kockázatot rejt magában, mégis állandó felügyeletet és megújulást igényel. Számos lehetőség van az információbiztonság és a tudatosság növelésére. Az Európai Unió Hálózat- és Információbiztonsági Ügynöksége (European Union Agency for Cybersecurity – ENISA) külön kiadványt bocsátott ki annak érdekében, hogy segítse a vállalatoknak az információbiztonság kialakítását (Michelberger & Lábodi, 2012).

A kisvállalkozásoknak számítógépekre és internetre van szükségük az egyszerű feladatok elvégzéséhez, így a vírusok, rosszindulatú programok, hackerek, kémprogramok és adathalászat olyan biztonsági incidensek, amelyek leállíthatják az üzletet. Gyakran előfordul, hogy csak a biztonsági incidens bekövetkezte után érzékelik a probléma súlyát, és akkor kezdik a válaszintézkedéseket. Szükséges befektetni olyan biztonsági információs rendszerekbe, amelyek cserébe védelmet nyújtanak a biztonsági incidensekkel szemben (Simmonds, 2017).

Olyan információbiztonsági rendszerre van szükségük, amely megfizethető, könnyen megvalósítható, használható, és megakadályozza a biztonsági incidensek okozta károkat. A nem használt biztonsági rendszer olyan, mint egy zár a nyitva hagyott ajtón. Az a biztonsági rendszer, amely nem akadályozza meg a lopást, nem nyújt védelmet a biztonsági eseményekkel szemben. A biztonsági rendszernek olyan használatot kell ösztönöznie, amely pozitív élményt nyújt a felhasználó számára. A biztonsági rendszer használatának védelmet kell nyújtania a biztonsági incidensekkel szemben a felhasználó és a vállalkozás számára (Bryan, 2020).

## A webes biztonság

A webes biztonság több területből áll, ám a tanulmány terjedelmére való tekintettel a szerzők a legrelevánsabb területre, a biztonságos csatlakozó rétegre (Secure Sockets Layer/Transport Layer Security vagy SSL/TLS) koncentrálnak. A SSL-t 1999-ben egy új frissítés alkalmával TLS-re nevezték át. A TLS biztonságos összeköttetést hoz létre két csatlakozó között, és többek között a következő lehetőségeket kínálja: (a) paraméterek egyeztetése az ügyfél és a kiszolgáló között, (b) kölcsönös hitelesítés az ügyfél és a kiszolgáló között, (c) titkos kommunikáció, (d) az adatok sértetlenségének biztosítása (Tanenbaum & Wetherall, 2013).

A TLS gyakorlatilag egy új réteget jelent, mely az alkalmazási (Hyper Text Transfer Protocol vagy HTTP) és a szállítási (Transmission Control Protocol – TCP) réteg közé ékelődik be. A biztonságos összeköttetés kiépítése után a TLS fő feladata a tömörítés és a titkosítás kezelése (Tanenbaum & Wetherall, 2013). Gyakorlatilag, amikor a HTTP-t TLS fölött használják, akkor az HTTPS-nek (Secure HTTP – biztonságos HTTP) nevezik, még akkor is, ha maga a protokoll továbbra is csak a szabványos HTTP (Tanenbaum & Wetherall, 2013).

Eredetileg a weben az adatokat egyszerű szövegben továbbították vagy adatszinten kellett titkosítani. Az adatokat bárki elolvashatta, ha titkosítás hiányában elfogta az üzenetet. Ha például egy fogyasztó meglátogatott egy vásárlói weboldalt, megrendelést adott le, és a weboldalon megadta a hitelkártyaszámát, akkor ez a hitelkártyaszám az interneten keresztül egyszerű szövegként terjedt. Az TLS-t azért hozták létre, hogy orvosolja ezt a problémát és ezáltal megvédje a felhasználókat. A TLS a felhasználó és a webkiszolgáló közötti adatok titkosításával biztosítja, hogy bárki, aki elfogja az adatokat, csak egy titkosított karakter kavalkádot láthasson. A fogyasztó adatai így nagyobb biztonságban vannak, mivel azokat csak az a vállalkozás láthatja, amelynek oldalán a fogyasztó megadta azokat. Továbbá egy TLS-protokoll a kibertámadások bizonyos fajtáit is megállíthatja. Képes hitelesíteni a webkiszolgálókat, ami azért fontos, mert a támadók gyakran próbálnak hamis weboldalakat létrehozni adathalászat céljából.

A TLS széles elterjedésével a HTTPS kiterjesztésű weboldalak egyre inkább elterjedtek az interneten. 2014-ben publikált kutatásban a szerzők az "S" árát feltérképezve a "HTTPS"-ben, arra világítottak rá, hogy az akkor folyamatban lévő technológiai változások közvetve arra utaltak, hogy a HTTPS infrastrukturális költségei csökkentek (Naylor et al., 2014). A HTTPS azonban közvetlen és észrevehető protokollal kapcsolatos teljesítményköltségeket okozott, például jelentősen megnövelte a késleltetést, ami kritikus a mobilhálózatokban (Naylor et al., 2014). Mára ezek a teljesítményt okozó költségek tovább csökkentek. Egy átfogó képet a HTTPS adaptálásáról a weben (Felt et al., 2017) tettek közzé.

A szerzők meggyőződése, hogy minden weboldalnak, különösen azoknak, amelyek bejelentkezési adatokat igényelnek, HTTPS-t kellene használnia. A modern webböngészőkben (pl. a Google Chrome-ban), a HTTPS-t nem használó webhelyek másként vannak jelölve, mint azok, amelyek használják. Ilyen módon jelezve a felhasználónak, hogy a meglátogatott weboldal nem biztonságos, hiszen az ott közzétett adatok nincsenek titkosítva. A HTTPS alapvetően két különböző kulcsot használ a két fél közötti kommunikáció titkosításához: (a) privát kulcs – ezt a kulcsot a weboldal tulajdonosa ellenőrzi, és titokban tartja, és a nyilvános kulcs által titkosított információk visszafejtésére szolgál, (b) nyilvános kulcs – ez a kulcs mindenki számára elérhető, aki biztonságos módon kíván kapcsolatba lépni a szerverrel. A nyilvános kulccsal titkosított információkat csak a privát kulccsal lehet visszafejteni.

## A kommunikáció biztonsága

A kommunikáció biztonsága szintén több komponensből álló szakterület. A jelen tanulmányban a pragmatikusság elvét követve két komponenst emelünk ki: a tűzfalakat (Firewall) és a virtuális magánhálózatokat (VPN).

A gyakorlatban a tűzfal egy olyan tervezett védelmi komponens, amely egy vállalkozás ki és befelé irányuló forgalmát ellenőrzi. A tűzfal tehát csomagszűrőként viselkedik, mint egy virtuális felvonóhíd, amelyen keresztül minden adatot szállító csomagnak át kell haladnia, így a vállalkozás "kapuőrsége" ellenőrizheti a teljes adatforgalmat (Tanenbaum & Wetherall, 2013).

Egy alkalmazásszintű átjárót (Application-Level Gateway vagy ALG) megvalósító tűzfal beállításával konkrétan vizsgálható például a kimenő vagy bejövő forgalom tartalma, hogy megakadályozzák érzékeny dokumentumok kijuttatását a vállalattól (Tanenbaum & Wetherall, 2013). Ugyanakkor fontos megemlíteni, hogy bár a tűzfalak hasznosnak bizonyulhatnak külső támadások esetén, sajnálatos módon a tűzfalon belülről érkező támadások ellen nem annyira hatékonyak. Továbbá, a szolgáltatások elosztott megtagadására (Distributed Denial of Service

vagy DDoS) irányuló támadások esetén a tűzfalak aligha járulnak hozzá az információbiztonság védelméhez. Egy erre vonatkozó teljes taxonómiát Mirkovic és Reicher (2004) fogalmazott meg.

Ezzel szemben a virtuális magánhálózatok nagyon jól működnek és fokozottan biztonságosak is, mivel a VPN megkönnyíti az agilis IT-infrastruktúra kialakítását. Egy olyan komplex területről beszélünk, amely önmagában számos technikai vívmánynak és kutatásnak adott helyet. Átfogó tanulmányt a VPN-ek felépítéséről Lewis (2006) fogalmazott meg.

A globális VPN-ek a dedikált kapcsolatok költségének töredékéért lehetővé teszik a kapcsolódást a világ bármely pontjára (Venkateswaran, 2001). A VPN-szolgáltatások jelentősen alacsonyabb költséggel teszik lehetővé a távoli hozzáférést az "intranet"-hez, így lehetővé teszik a távolsági munkavégzést is (Venkateswaran, 2001). A VPN-szolgáltatások hatalmas népszerűségre tettek szert a kereskedelmi és védelmi szervezetek körében, mivel alacsonyabb költségek mellett képesek biztonságos kapcsolatot biztosítani (Khanvilkar & Khokhar, 2004). Kutatások igazolták, hogy a nyílt forráskódú, Linux-alapú VPN-alagutak átlagosan 50% alacsonyabb forgalomterheléssel (overhead), 80% nagyobb sávszélesség-kihasználtsággal és 40-60% alacsonyabb késleltetéssel/zavarral rendelkeznek, mint a TCP-alapú VPN-alagutak (Khanvilkar & Khokhar, 2004). A legnagyobb előnyük mégis az, hogy az alkalmazási szoftverek számára átlátszó, így a személyzetnek nem okoz gondot a VPN használata (Tanenbaum & Wetherall, 2013).

## A veszélyek megelőzése

Több veszély fenyegeti a KKV-szektor résztvevőit, mint azt elsőre gondolnánk. Már az indulás pillanatától kezdve számolniuk kell a vállalatoknak az őket érintő veszélyekkel. Amennyiben időben elkezdik a felkészülést, megelőzést, akkor jelentős mértékben csökkenthető a következmények mértéke (Kaila, 2018). A Cisco 2017-es biztonsági jelentése (Cisco, 2017) alapján az adathalászat, az e-mail átverések, illetve a saját eszközök használata a mindennapi munkában jelentette a legnagyobb problémát a KKV-k világában. Az adatok megszerzése érdekében számos lehetőség van arra, hogy a munkavállalókat fel tudják keresni az adathalászok. Elérhetőek telefonon, e-mailben vagy szöveges üzenetben is, amely lehetőségekkel a támadók könnyedén tudnak bizalmas és személyes adatokat gyűjteni.

A védekezés részeként fontos a munkavállalókat felkészíteni az esetleges megkeresésekre, gyanakvásra késztetni, illetve oktatni, hogy melyek a vállalatban elfogadott megkeresési formák, és mely gyakorlatok elkerülendők (Boletsis et al., 2021). A „phishing" e-mailekkel való átverés az egyik legelterjedtebb módja a munkavállalók megtévesztésének. A támadó általában különösebb erőfeszítés nélkül tud eljutni odáig, hogy felvegye a kapcsolatot a munkavállalóval. A kiküldött e-mailben gyakran kérik, hogy bizonyos összeget utaljanak el egy adott helyre, vagy az üzenetben megtalálható linkre kattintva tudnak adatot, így fontos információt szerezni a vállalatról (Abroshan et al., 2021). A vállalati e-mailek feladóját minden esetben ellenőrizni kell, különösen abban az esetben, ha az üzenet külső féltől érkezik. Tudatosságot növelő programokkal és oktatással nagymértékben megelőzhető az e-mail átverések megvalósulása (Pfeiffer, 2022).

Bring Your Own Device „BYOD" jelentése a saját eszköz használata a munkavégzés során, amely elterjedt munkavégzési forma a KKV-k viszonylatában. A munkával kapcsolatos tevékenységek gyakran zajlanak privát mobileszközön, vagy nyilvános Wi-Fi hálózaton, a vállalati tűzfalakat kikerülve. Az érkező és az elküldött adatokat ebben az esetben nem titkosítják, a vezeték nélküli hálózatokon könnyen hozzáférhetővé válnak. A probléma megvalósulása elkerülhető, ha a vállalati adatok eléréséhez minden esetben VPN-kapcsolat és tűzfal használata szükséges (Ratchford et al., 2022). A biztonságos internetes átjáró (Secure Internet Gateway vagy SIG) használata is hasznos, amely blokkolja, hogy a felhasználó nem biztonságos oldalakat elérjen. Munkavégzés során fontos, hogy csak olyan oldalakat látogassanak a munkavállalók, amelyek HTTPS sémával működnek, így biztosítva az internetes forgalomban részt vevő információk védelmét.

A KKV-szektorban megjelennek egyéb kockázatok is, amelyekre a kisebb vállalatok gyakran nem is gondolnak, vagy nem tudnak felkészülni rájuk. A jogosultságkezeléssel kapcsolatos veszélyek ebbe a csoportba tartoznak. Fontos az első pillanattól kezdve meghatározni, hogy a munkavállalók mely vállalati adatokhoz férnek hozzá. A használt szoftverek esetében, nemcsak a felhasználói csoportokat, de egyéni felhasználói szinten is ki kell alakítani a jogosultságokat. A felhasználók hozzáférésének közvetlen kezelése elősegíti a központi átláthatóságot és a tevékenységek egyszerűbb követését (Sharma et al., 2016).

A KKV-k világában is gyakran merül fel a „back-up" kifejezés, amely fizikai vagy virtuális file-oknak és adatbázisoknak a másodlagos tárhelyre való másolását jelenti annak érdekében, hogy ezeket meg lehessen védeni az esetleges hibáktól, megsemmisüléstől. Amennyiben az adatok visszaállítására van szükség, a back-up egy korábbi helyzet visszaállítását el tudja végezni, mivel meghatározott időközönként végez biztonsági mentést (Hemant et al., 2011).

Megvédi az információt az emberi hibáktól, a hardveres meghibásodástól, vírusoktól, természeti katasztrófáktól. A fizikai szervereken vagy a manapság egyre inkább elterjedt felhőben való tárolás biztosítja az adatok védelmét. Egyre több szolgáltatás található a piacon, amelyek az első dokumentumtól kezdve támogatják a vállalati információ biztonságos másolatát (Hemant et al., 2011).

A vállalatok életében a jelszóvédelem a kulcskérdések közé tartozik. Abban az esetben nyilvánítható egy jelszó erősnek, ha megfelelő hosszúságú, minimum 8 karakter, tartalmaz kis- és nagybetűt, speciális karaktert és számot. Elengedhetetlen a gyakori jelszóváltás szabályozása, amely megakadályozza a korábban már használt jelszó újbóli felhasználását. A vállalatnak szükséges rendelkeznie jelszavakat érintő szabályzattal, amelynek minden munkavállaló számára ismertnek kell lennie. Abban az esetben, ha plusz védelmet szeretnének a jelszavakat illetően,

a különböző jelszókezelő szoftverek használata megfelelő, amely titkosítja a jelszavakat, és minden alkalommal új jelszót generál a beállított fiókokhoz (Yildirim & Mackie, 2019).

## Kutatásmódszertan

A tanulmány arra a kérdésre keresi a választ, miszerint valóban megfigyelhető-e, hogy a sürgetett digitalizáció negatív hatással van az információbiztonsági szintre nézve a KKV-k életében Magyarországon. Az elemzés főként az e-kereskedelemben aktívan részt vevő vállalkozásokra terjed ki, azokat egyenként nem azonosítja. A kutatás esettanulmány-alapú, azonban a vizsgálatban résztvevők viselkedésének manipulálása nem cél és nem lehetőség (Baxter & Jack, 2008).

Az elérhető kutatási keretek közül a pragmatikus szemléletet alkalmaztuk (Mertens, 2005). Így valósul meg a kutatási kérdés hatékony fókuszálása (Mackanzie & Knipe, 2006; Creswell, 2003), annak többféle lencsén keresztül történő vizsgálata (Edmondson & McManus, 2007; Mullarkey & Hevner, 2018).

A kutatás az elméleti háttér megalapozását a szakirodalmi apparátus feldolgozásával nyitja. Ezt követően a vizsgálatban használt mutatókat mutatjuk be. Így jut az olvasó a kutatási eredményekhez és azok értékeléséhez. Az eredmények feldolgozása során több nemzetközi vagy nemzeti mutatót használtunk fel. Ezeknek az összetett mutatóknak az ismertetése azért szükséges, hogy az olvasó teljes képet kapjon az információbiztonság területét érintő átfogó indexekről. Az indexek bemutatása az általánostól a konkrét felé halad. Így az olvasó az általánosnak vélt információkon túl, amelyet az indexek alapján ismerhetünk, konkrét információhoz juthat a Digitális Gazdaság és Társadalom Index (DESI), valamint a Digiméter elemzései alapján.

Az empirikus kutatáshoz a Digiméter Index adatait használtuk fel. A minta nagysága évente változó: 2020-ban 777; 2021-ben 757 és 2022-ben 674 kérdőív kitöltéséből tevődik össze. Eltérő szignifikanciaszint nem figyelhető meg: a leginkább reprezentált csoport az 5-9 főt foglalkoztató vállalkozások válaszaiból áll, leginkább Budapest és Pest megyéből. Az eredmények statisztikai elemzéseket és klaszteranalízist (Simon, 2006) tartalmaznak. Az értekezés végül a kutatás korlátainak ismertetésével és konklúzióval zárul.

A kutatási eredmények alkalmazhatósága így széles körben demonstrálható. A magyarországi KKV-k vezetőségei részére egyértelműen figyelemfelkeltő és gondolatébresztő kutatási eredményeket tártunk fel. Továbbá, az információbiztonság területén aktívan tevékenykedő kutatókat kívánjuk elérni, azok visszajelzését befogadni.

A fejezet az információbiztonságot tárgyaló indexek rövid ismertetésével folytatódik.

### A Globális Kibervédelmi Index – Global Cybersecurity Index (GCI)

A GCI a Nemzetközi Távközlési Unió (ITU) által kifejlesztett összetett index, amely a világ országainak kiberbiztonsági felkészültségét méri. Az ITU biztosítja az ENSZ mellett a nemzetközi távközlési működést és a távközlési jogszabályok megalkotását. A GCI célja, hogy átfogó áttekintést nyújtson az országok kiberbiztonsági képességeiről, és segítsen azonosítani azokat a területeket, ahol fejlesztésre van szükség.

A GCI öt fő pilléren méri a kiberbiztonsági felkészültséget: jogi intézkedések, technikai intézkedések, szervezeti intézkedések, kapacitásépítés, együttműködés. Ezeket a pilléreket rész indikátorokra bontják, amelyek alapján az egyes országokhoz pontszámot rendelnek (Global Cybersecurity Index, 2020). A jogi intézkedések pillére az egyes országok jogi és szabályozási kereteit értékeli, beleértve a kiberbiztonsággal és adatvédelemmel kapcsolatos törvényeket és rendelkezéseket. A technikai intézkedések pillére az egyes országok műszaki infrastruktúráját és képességeit, a kiberbiztonsági technológiák elérhetőségét és használatát foglalja magába. A szervezeti intézkedések pillére felméri az egyes országok kapacitását a kiberbiztonsági intézkedések végrehajtására, a nemzeti kiberbiztonsági stratégiák meglétét és a nemzeti számítógépes vészhelyzeti reagálási csoportok (CERT-ek) létrehozását.

A kapacitásépítési pillér felméri az egyes országok erőfeszítéseit a kiberbiztonsági oktatás és tudatosság előmozdítása érdekében, a képzési programokat és a lakossági figyelemfelkeltő kampányokat. Az együttműködési pillér a kiberbiztonsági kérdésekben folytatott nemzetközi együttműködés szintjét értékeli, a két- és többoldalú megállapodások meglétét, valamint az egyes országok nemzetközi kiberbiztonsági kezdeményezésekben való részvételét (Bruggemann et al., 2022).

A GCI-t rendszeres időközönként frissítik, és hasznos a döntéshozók, az iparági vezetők és a nagyközönség számára a világ országainak kiberbiztonsági felkészültségének felméréséhez. A GCI segíthet a befektetési és politikai döntések meghozatalában a globális kiberbiztonsági erőfeszítések megerősítése és az országok kiberfenyegetésekkel szembeni ellenálló képességének javítása érdekében (Farahbod et al., 2020).

### A Nemzeti Kiberbiztonsági Index – National Cybersecurity Index (NCSI)

Az NCSI az országok általános kiberbiztonsági helyzetének mérőszáma, amely számos tényezőt figyelembe vesz: az ország jogi kereteit, műszaki infrastruktúráját, valamint a nyilvánosság kiberbiztonsági kérdésekkel kapcsolatos tudatosságát és megértését. Az index átfogóan mutatja be egy ország kiberbiztonsági környezetét, erőfeszítéseit. Segítségül szolgál az értékelésben és a javításban. Az NCSI és a GCI közötti legnagyobb különbségek az értékelési kritériumok, az adatforrások, az értékelési szintek és a célközönség.

Az NCSI jellemzően több különböző összetevőből áll. A jogi és szabályozási kereteket, a biztonsági technológiák elérhetőségét és használatát, a kiberbiztonsági oktatás és tudatosság általános szintjét, valamint a kiberbiztonsági kutatásba és fejlesztésbe történő befektetések általános szintjét is vizsgálja. Ezen összetevők mindegyikéhez súlyozás tartozik, amely tükrözi relatív jelentőségét az or-

ság általános kiberbiztonsági helyzetének meghatározásában (NCSI, 2023).

Az NCSI-t rendszeresen frissítik, jellemzően évente, hogy tükrözze a kiberbiztonsági fenyegetések változó környezetét, valamint a kiberbiztonsági technológiák és gyakorlatok fejlődő állapotát (Kravets, 2019). Ez lehetővé teszi az országoknak, hogy nyomon kövessék a kiberbiztonsági helyzetük javítása terén elért előrehaladást az idő múlásával, és azonosítsák azokat a területeket, ahol további erőfeszítésekre van szükség kiberbiztonsági környezetük megerősítéséhez (Nehrey et al., 2022).

### Digiméter

A Digiméter egy digitális érettséget mérő eszköz, amelyet a Smartcommerce Consulting, a Reacty Digital a Virgo és az eNET fejlesztett ki a magyarországi KKV-k digitális felkészültségének és képességeinek mérésére (Gerda & Regina, 2022). Az eszköz átfogó értékelést nyújt a vállalatok digitális érettségéről, amely számos területre kiterjed, mint a technológia átvétele, a digitális infrastruktúra, a digitális kultúra, valamint a digitális készségek.

Az értékelés célja, hogy a szervezetek átfogó képet kapjanak saját aktuális digitális érettségi szintjükről. Továbbá javaslatokat kapnak arra vonatkozóan, hogyan fejleszthetik digitális képességeiket, hogyan tudják jobban kihasználni a technológiát üzleti céljaik elérése érdekében.

A Digiméter Index hat alindexből tevődik össze: digitális jelenlét, digitális mindennapok, vállalkozásvezetés, értékesítés és marketing, digitális pénzügyek, informatikai biztonság (Smartcommerce Consulting et al., 2020). Az értékelést kérdőív alapján végzik, és a szervezet számos kérdést válaszol meg a digitális képességeiről az index által lefedett területek mindegyikén. A kérdéseket úgy alakították ki, hogy átfogóak legyenek, és a témák széles skáláját fedjék le, többek között olyan területeket, mint az IT-infrastruktúra, adatkezelés, e-kereskedelem, digitális marketing és ügyfél-elköteleződés.

A KKV-szektor résztvevőinek előrehaladását a digitalizációban évente két alkalommal mérik (Gerda & Regina, 2022). Az értékelés befejezése után a szervezet kap egy jelentést, amely általános pontszámot ad a digitális érettségre vonatkozóan, valamint részletes betekintést nyújt erősségeibe és gyengeségeibe az értékelés által lefedett egyes területeken (Digiméter jelentés, 2022).

### A Digitális Gazdaság és Társadalom Index – Digital Economy and Society Index (DESI)

A DESI egy összetett index, amely az uniós országok digitális gazdaságban és társadalomban elért előrehaladását méri. Az indexet az Európai Bizottság számítja ki, és a digitális gazdaság és társadalom korábban öt, jelenleg négy kulcsfontosságú dimenzióját fedi le: humán tőke, konnektivitás, digitális technológia integrációja, digitális közszolgáltatások (DESI, 2023).

Az első dimenzió, a humán tőke a munkaerő digitális készségeit és kompetenciáit, valamint az IKT (információs és kommunikációs) -szakértők arányát és a digitális alapkészségek szintjét méri a lakosság körében. Az második dimenzió, a hálózati összekapcsolhatóság, konnektivitás a szélessávú infrastruktúra kiépítését és a szélessávú szolgáltatások elterjedését méri. A harmadik dimenzió, a digitális technológia integrációja, a vállalkozások digitalizálását méri, például a számítási felhő, a közösségi média és a big data elemzések használatát. Ide tartozik az internetes szolgáltatások használata az online szolgáltatások, például az e-kereskedelem, a közösségi média. Végül a negyedik dimenzió, a digitális közszolgáltatások az online közszolgáltatások, például az e-kormányzati szolgáltatások és az e-egészségügyi szolgáltatások elérhetőségét és minőségét méri.

A dimenziókat további részdimenziókra és indikátorokra bontják fel (Csótó, 2019). A dimenziók mindegyike fontosságuk alapján súlyt kap, és az egyes dimenziókhoz tartozó pontszámokat kombinálva hozzák létre az egyes országok összpontszámát. Az index évente frissül, és magában foglalja az összes EU-tagállamot. A 2022-es adatokat feldolgozó riportok új fejlesztési irányoknak megfelelően készülnek el. Kitérnek új digitalizációt érintő témákra is (pl. a mesterséges intelligencia vagy a felhőtechnológiák elterjedése).

A DESI-index hasznos eszköz az uniós országok digitális gazdaságban és társadalomban elért előrehaladásának értékeléséhez. Kiemeli azokat a területeket, ahol az országok kiemelkedőek, vagy ahol javítás szükséges. Segíthet a politikai döntések meghozatalában és a digitális szektorba történő befektetésekben (Gergely, 2019). Az üzleti szféra digitális érettségének értékelésére alkalmas a mutató. A digitalizáció nemcsak országok, hanem iparágak szintjén is mérhető (Losonci et al., 2019).

A korábbi öt dimenzió eredményei alapján átfogó képet kaphatunk az országok digitalizációs helyzetéről, amely bemutatja, hogy az európai országok két nagy csoportba oszthatók. Az első csoportba 2016-ban 22 ország tartozik, amelyek esetében mind a gazdasági, mind a társadalmi digitális fejlettségi mutatók magasak. Többnyire fejlett országok tartoznak ebbe a csoportba, ahol nagy hangsúlyt fektetnek a gazdaságra, a szolgáltatások fejlesztésére és a technológiába történő befektetésre. A második csoportba 23 fejlődő ország tartozik, ahol megjelennek a törekvések a digitális érettségre, de nem minden tényező adott a hirtelen nagymértékű változáshoz. Magyarország is ebbe a csoportba tartozik (Bakumenko & Minina, 2020).

### Az indexek összevetése

Az indexek segítségével pontos képet kapunk Magyarország digitalizációs és kibervédelmi helyzetéről, és ezen belül a KKV-k digitális érettségi szintjéről és a fejlesztendő területekről. A kutatással kapcsolatos célunk, hogy a négy index adatainak feldolgozásával rávilágítsunk az információbiztonság fontosságára. A megadott mutatók dimenzióin és vizsgált területein túl további gondolkodásra alkalmasak az indexek.

Általánosságban elmondható, hogy vannak olyan szempontok, amelyekre nem térnek ki az elemzések során, vagy nem fedik le teljes mértékben az adott területet. Az információbiztonság mellett gyakran megjelenik az *adatvédelem* kérdése, amely kérdéskört az indexek nem vizsgálják teljeskörűen. Az egyre gyakoribb adatvédelmi

incidensek indokolttá teszik, hogy az adatvédelmi szempontokat hangsúlyosabbá tegyék az értékelésekben.

Elengedhetetlenné vált a *környezeti fenntarthatóság* figyelembevétele, amely szempont eddig az indexek értékeléseiből teljes mértékben kimaradtak, de a probléma kezelése egyre fontosabb. A digitális gazdaság növekedésével teret hódít a technológia átvételének negatív környezeti hatása. Ebbe a kategóriába tartozhat az adatközpontok jelentős mennyiségű energiafogyasztásának problémája, vagy az egyre termelődő elektronikai hulladék kérdése.

A digitális technológiák globális politikában betöltött szerepének növekedése miatt fontos lehet a *geopolitikai kérdések* figyelembevétele az értékelésekben. A nemzetközi kiberbiztonsági együttműködés, a kiberkémkedés, vagy a háborúk kibertérben történő aspektusa lehet új tényező.

*Társadalmi befogadás* szempontjából, bár a digitális gazdaság számos előnnyel járhat, mégis súlyosbíthatja az egyenlőtlenségeket, és hátrahagyhat egyes csoportokat. A digitális és kiberbiztonsági felkészültség értékelése során szükség lehet a társadalmi befogadás és a digitális megosztottság kérdéseinek átfogóbb kezelésére.

Az *etikai megfontolásokat* némelyik index érinti, de a mesterséges intelligencia (AI) és más fejlett technológiák növekvő hatása miatt egyre nagyobb szükség van a technológiaátvételek etikai vonatkozásainak ellenőrzésére. E szempont miatt különösen fontos, hogy az értékelés módszerét és magát az értékelést legalább évente felülvizsgálják.

A DESI-, Digiméter, NCSI- és GCI-indexek használhatósága a célközönségtől és a konkrét használati esettől függően változhat. Általában ezeket az indexeket úgy tervezték meg, hogy felhasználóbarátok, és az érintettek széles köre számára hozzáférhetőek legyenek. Az indexek amellett, hogy átfogó képet adnak a digitális és kiberbiztonsági felkészültségről, objektív adatokon és mérőszámokon alapulnak. Ezáltal biztosítható, hogy az értékelések függetlenek, megbízhatóak és adatvezérelt eszközökhöz kompatibilisek legyenek. Vizualizációk és egyéb eszközök biztosítják az adatok hozzáférhetőségét és értelmes megjelenítését. A DESI-index számos interaktív térképet és diagramot tartalmaz, amelyek segítenek a felhasználóknak megérteni, hogyan teljesítenek az országok a különböző területeken. A GCI tartalmaz egy irányítópultot, amely lehetővé teszi a felhasználók számára, hogy összehasonlítsák az országokat a különböző kiberbiztonsági mutatók alapján.

Digitális és kibervédelmi háttértudás nélkül nem minden esetben elérhetőek és értelmezhetőek az eredmények. Emellett előfordulhat, hogy az indexek nem mindig képesek megragadni a digitális környezet teljes komplexitását. Minden szempontot összevetve elmondható, hogy az indexek jól megtervezettek, hasznosak, könnyedén használhatók, felhívják a figyelmet a téma súlyosságára, a bennük foglalt tartalom fontosságára.

A tanulmány e fejezetében felvetjük a digitális átállás információbiztonságra gyakorolt hatásának részletes vizsgálatát egy specifikus kutatási módszertan segítségével. Gyakorlatiasság szempontjából a bemutatott indexek a vizsgált szakirodalmi háttérhez az 1. táblázat alapján viszonyulnak. A jelszóvédelem témakörét egyik index sem méri, de fontos kiegészítése több értékelt pontnak is, mint például a tudatosság vagy az oktatás.

1. táblázat

**Biztonsági intézkedések indexekben való megjelenése**

| | GCI | NCSI | Digiméter | DESI |
|---|---|---|---|---|
| Kiberbiztonság | X | X | | X |
| Kiberfenyegetések elemzése (adathalászat, identitáslopás) | X | X | | |
| Webes biztonság | | X | | |
| Személyzeti tudatosság | X | | X | |
| Oktatás és szakmai fejlődés | X | X | | X |
| Kommunikáció biztonsága | | | X | X |
| Jogosultságkezelés | | | X | |
| Biztonsági mentés | | | X | |
| Jelszóvédelem | | | | |
| Saját eszközhasználat | | | X | X |

*Forrás: saját szerkesztés*

## Eredmények bemutatása

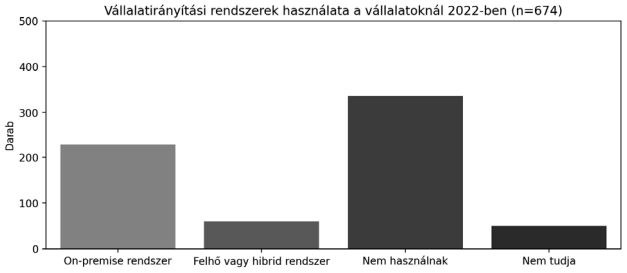
A Digiméter 2020-as, 2021-es és 2022-es eredményei alapján látható, hogy a koronavírus-lezárásokkal kapcsolatos digitalizációs törekvések változásokat értek el a KKV-k mindennapjaiban. Az új digitalizált módszerek, eszközök továbbra is megmaradtak a munkavégzés során, így csökkentve a lemaradást a nagyobb vállalatokhoz képest. Vannak olyan területek, ahol szinte elengedhetetlen, hogy a vállalat a digitalizációs lehetőségeket maximalizálja, mint például a marketingtevékenységek vagy ügyfélszerzés. A hosszú távú fennmaradás, a hatékonyság növelése és az általános növekedés érdekében minél hamarabb integrálniuk kell a KKV-knak a digitalizációs eszközöket és lehetőségeket. Néhány éven belül versenyelőnyre csak azok a vállalatok tehetnek szert, amelyek adatvezérelten, a biztonsági előírásoknak megfelelően, digitalizáltan működnek. Ennek egyik kulcsfontosságú eszköze a vállalatirányítási rendszerek használata a vállalatoknál. A 2022-es évben a 674 válaszadó alapján látható, hogy túlnyomó többségük, azaz 336 vállalat nem használ ilyen eszközt (*lásd 1. ábra*).

A kérdőív válaszai alapján továbbá egyértelműen látszik, hogy a 2020-as évben növekedett azon vállalatok aránya, amelyek valamilyen módon gondoskodtak az informatikai rendszerek működtetéséről, és személyzetet biztosítottak az informatikai feladatok lebonyolítására. A 2021-es évben némi visszaesés, átrendeződés látszik a területen, több vállalat rendelkezik informatikai felelőssel. A legtöbb KKV külső szakember segítségével oldja meg az IT-jellegű kérdéseket, illetve szerződésben állnak más szolgáltató vállalatokkal. A vállalatok közel egynegyede foglalkoztat önálló IT-munkakört betöltő vállalati munka-

társat, mint például rendszergazdát, amely munkakör az elmúlt két év eredményei alapján egyre elterjedtebb, viszont még mindig a vállalatok fele nem alkalmazott állandó jelleggel IT-munkatársat e feladatokra.

1. ábra

**Vállalatirányítási rendszerek használata a vállalatoknál**

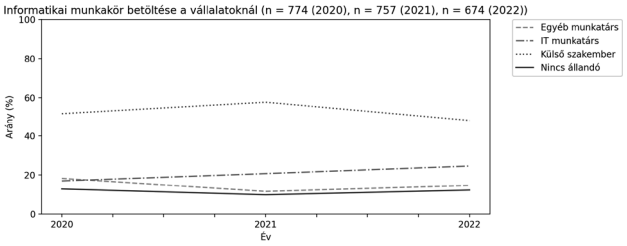



*Forrás: Digiméter jelentés (2022) alapján saját szerkesztés*

Gyakori megoldás a vállalatoknál, hogy olyan munkatársat bíznak meg az IT-jellegű feladatok ellátására, aki más jellegű munkakörrel is rendelkezik a vállalatnál. Habár azon KKV-k száma stagnál, ahol nincs jelenleg állandó IT-személyzet, mégis fontos lenne, hogy az információ- és adatvédelem érdekében minden vállalatnál legyen legalább egy fő, aki teljes mértékben az IT-val kapcsolatos kérdésekkel, feladatokkal foglalkozik (*lásd 2. ábra*).

2. ábra

**Informatikai munkakör betöltése a vállalatoknál**




*Forrás: Digiméter jelentés (2022) alapján saját szerkesztés*

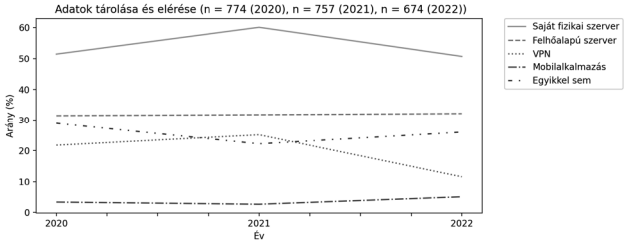
A 2020 és 2022 közötti időszak során a több, mint 2200 kitöltés alapján láthatjuk, hogy a vállalatok közel 80%-a rendelkezik saját honlappal, webáruházzal, vagy „My Business" – Google Cégem regisztrált fiókkal. E szolgáltatások védelme már nemcsak a vállalatra, hanem a felhasználókra is kiterjed. A webes védelem ilyen esetben érinti a vállalat egészét, a munkatársakat, és a felhasználók személyes adatait is. A webáruházak esetében különösen fontos szempont, hogy a külső féltől származó adatokat milyen módon titkosítják, hogyan tárolják. A honlapra látogatóknak tisztában kell lenniük azzal, hogy milyen módon kezelik az általuk megadott adatokat.

A közösségi médiában való megjelenésre nagymértékben megegyező szabályozások vonatkoznak, mint a honlapra és a webáruházra. Az elmúlt két év 1431 darab kitöltési eredményei alapján a közösségi média közkedvelt módja a felhasználók elérésének, bár az utóbbi egy évben minimális visszaesést mutat a platformok használata. A statisztika szerint minden negyedik vállalat rendelkezik Facebook-fiókkal vagy Youtube-csatornával, amelyek vagy kifejezetten a vállalathoz kötődnek, vagy egyes termékhez, szolgáltatáshoz. E platformok amellett, hogy lehetőséget biztosítanak a vállalat és a termékek bemutatására, számos veszélyforrást is jelentenek a KKV-kra nézve. A felhasználói fiókokhoz tartozó felhasználónév és jelszó védelme kiemelt fontosságú feladat. Emellett a tartalomnak minden esetben meg kell felelnie a törvényi előírásoknak és a vállalati irányelveknek. A platformokon megjelenő információ biztonságáról az erre kijelölt személyen kívül, a vállalat egészének is gondoskodnia kell.

Az információ védelméhez hozzátartozik a tárolás, amely a megkérdezett KKV-k esetében változatos eredményt hozott. A 2021-es eredmények alapján kijelenthető arányaiban a vállalatok több, mint fele rendelkezett saját, fizikai szerverrel és 2020-tól tovább nőtt ez az arány, viszont a 2022-es kérdőív eredményei már visszaesést mutatnak a 2020-as szintekre. Ennek hátterében az állhat, hogy vagy másmilyen módon oldják meg az adatok tárolását, vagy semmilyen szervert, rendszert nem vesznek igénybe. Az eredmények kismértékben azt mutatják, hogy a vállalatok inkább elhagyták a szervereket és a Virtual Private Network (VPN) szolgáltatást, mobilalkalmazást vagy más, felhőalapú megoldásokat választottak (*lásd 3. ábra*).

3. ábra

**Adatok tárolása és elérése**




*Forrás: Digiméter jelentés (2022) alapján saját szerkesztés*

A 2021-es évhez képest egyedül a saját céges mobilalkalmazások használati aránya növekedett. Számszerűsítve az arányuk közel 5%-kal nőtt. Ez a jelenség azért jelent problémát, mert míg azon vállalati információk, amelyek vagy fizikai szerveren, vagy a felhőben vannak tárolva, védve vannak. Addig azon adatok, amelyekről egyik helyen sem készülnek másolatok, könnyedén el tudnak veszni, visszaállításuk nehezen vagy semmilyen módon nem megoldható. Számos lehetőség lenne a felhőalapú szolgáltatások kihasználására (pl. Google Workspace, Microsoft OneDrive). Továbbá a VPN használata azért fontos, mert így az alkalmazottak biztonságosan tudják távolról is elérni a vállalati informatikai rendszereket.

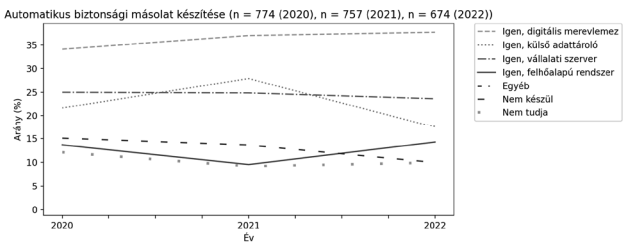
A jogosultságkezeléssel kapcsolatos eredmények elszomorító képet mutatnak. 2022-ben a 674 kitöltés alapján azt láthatjuk, hogy a megkérdezett vállalatok alig több, mint fele nyilatkozott úgy, hogy alkalmaznak többszintű jogosultsági rendszert, amely alapján egyes munkatársak

csak bizonyos elektronikus tartalmakhoz férhetnek hozzá. Habár kevesebb, mint 1% arányban voltak azon válaszadók, akik nem tudják, hogy az adott vállalatnál használnak-e ilyen rendszert, valószínűsíthetően ők is azok közé tartoznak, akik nem alkalmazzák ezt a megoldást. Nagy veszélyt jelent a vállalatra nézve, ha nincsenek meghatározva a felhasználói körök, és az információ mindenki számára azonos mértékben elérhető. A jogosultságkezelés hozzájárul a biztonságos és hatékony működéshez.

A 2021-es év eredményei azt mutatják, hogy hirtelen megemelkedett a digitálisan keletkező adatok mennyisége, ami a koronavírus által kialakult helyzet hozadéka. Az elmúlt évben kisebb visszaesés látható a digitális adatok és fájlok automatikus biztonsági másolatát illetően. Ez a szám a 674 kitöltő alapján közel 70 darab, azaz a vállalatok több, mint 10%-a nem használt automatikus biztonsági másolatot. A KKV-k közül nagyjából ugyanekkora arányban, a vállalatok 35%-a, adatainak biztonsági másolatát merevlemezen tartja (*lásd 4. ábra*), illetve 24%-uk vállalati szerveren, amely eredmény már korábban a tárolásnál is megmutatkozott. Holott az elmúlt évben egyre kevesebb válaszadó nyilatkozott úgy, hogy nem készítenek másolatot, nem gondoskodnak az adatok biztonságos meglétéről, a válaszadók 10%-a nem is tudja, hogy milyen módon kerülnek mentésre ezen adatok. Pozitívumként kiemelendő, hogy a 2021. évi eredményekhez képest, jelentős mértékben nőtt azon KKV-k aránya, amelyek felhőalapú rendszereket használnak az adatok automatikus biztonsági másolatának tárolásához. Ez az érték 10%-ról 15%-ra nőtt, vagyis 50%-kal nőtt e rendszerek aránya a kitöltők között. Fontos lenne, hogy mielőbb minden vállalat gondoskodjon a saját digitális adatainak és fájljainak biztonságos védelméről, így azok megfelelő helyen tárolt biztonsági másolatáról is.

4. ábra

**Automatikus biztonsági másolat készítése**




*Forrás: Digiméter jelentés (2022) alapján saját szerkesztés*

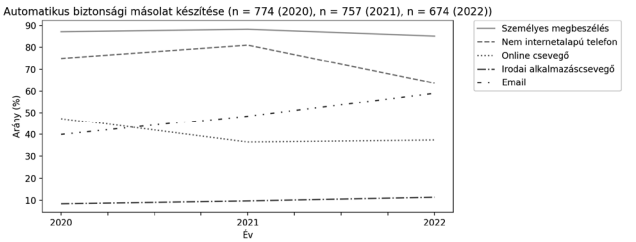
A felhasználói szintű egyedi azonosítás és jelszóvédelem eredményei további aggodalomra adnak okot. Habár 2022-ben a 674 megkérdezett KKV közül 540-en nyilatkoztak arról, hogy gondoskodnak arról, hogy a saját számítógépbe történő belépés során használjanak egyedi azonosítást és megfelelő módon védjék a jelszavakat. Ez a szám a vállalati szerverre történő belépés során sokkal kevesebb, számszerűleg 382 darab. Összefüggésben van ez az alacsony szám a korábbi eredménnyel, miszerint a vállalatok nagy része nem is használ szervert. A válaszadók közel kétharmada nyilatkozott úgy, hogy a szervereket is védik azonosítóval vagy jelszóval. A további kitöltők esetében elengedhetetlen, hogy a jövőben a szervereket is legalább annyira védjék, mint a számítógépeket, hiszen az információ mindegyik eszközről könnyedén és hasonló módon elérhető. A megfelelő azonosító és jelszó használatával megvédhetők a vállalat információi.

Mindeközben elmondható, hogy a fájlok vállalaton belüli megosztása és küldése leginkább e-mailen keresztül valósul meg, vagyis az fájlok több, mint háromnegyede ezen a csatornán keresztül vándorol. Mindezen túl a 2020-2022-es időszakban a teendők delegálására a KKV-k alig használnak digitális eszközöket (pl. Todoist, Trello, Asana). Ezen értékek az időszak során stagnáltak és minden évben 80% felett volt a nem használók aránya. Ezzel egyetemben a távoli asztali elérést biztosító eszközök használata sem elterjedt, habár a távmunka okozta változások miatt az értékek már fele-fele arányban jelentkeztek a használók – nem használók viszonylatában. Mindezeken túl a webinar és online találkozó megtartására alkalmas eszközök használatánál is csak 2021-től figyelhető meg lényegesebb, viszont ezen időszak során is csak 20%-os növekedés.

A kérdésekre érkezett válaszokból továbbá levonhatók olyan következtetések is, miszerint a digitális eszközt használó munkatársak még mindig a személyes megbeszéléseket jelölik meg preferált kommunikációs csatornának az irodai vagy online kollaboratív alkalmazások helyett. A 674 megkérdezett közül majdnem 600-an választották a személyes megbeszélést a legkedveltebb kommunikációs felületnek (*lásd 5. ábra*).

5. ábra

**Preferált kommunikációs csatornák**




*Forrás: Digiméter jelentés (2022) alapján saját szerkesztés*

A válaszokból szintén kiderül, hogy az elmúlt három évben a vállalkozások 60%-a leginkább tartózkodott az online ügyfélszerző eszközök alkalmazásától, ami nem is annyira meglepő, tekintve, hogy a válaszadók fele nem is használ semmilyen vállalatirányítási vagy ügyviteli rendszert. Alacsony kihasználtság mellett is, a kitöltők közel kétharmada nyilatkozza, hogy a döntéshozatal előkészítéseként figyelemmel kísérik a vállalati működés során keletkező adatokat.

A Digiméter kutatása alapján a vállalatokat négy különböző kategóriába soroltuk klaszterelemzés segítségével. A csoportok informatikai biztonsággal kapcsolatos különbözőségeit a 6. ábrán tekinthetjük meg. Látható, hogy az egyes kategóriák Informatikai Biztonság – mint az egyik fő Digiméter Index – pontszámainak eloszlása jól

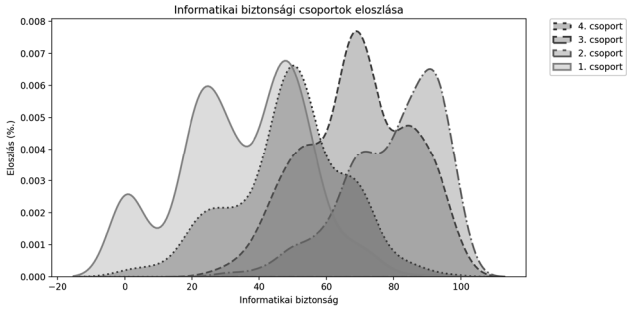
észlelhetően szétválik. Ennek egy egyszerű értelmezése, hogy a kialakított klaszterek, mint vállalatok egy-egy csoportja mind különböző informatikai biztonsági rendszerrel és stratégiával rendelkezik.

Az ábránál maradva még érdemes megjegyezni, hogy az eloszlásgörbék csúcsai mutatják az egyes kategóriák móduszát, tehát ezen értékek körül összpontosulnak az egyes kategóriák Informatikai Biztonság index pontszámai. Ezek pontos értékei az 1. csoportnál 45 pont, a 2. csoportnál 92 pont, a 3. csoportnál 67 pont és a 4. csoportnál 50 pont. Az átlag tekintetében pedig rendre így alakultak a pontszámok: 34, 80, 69, 49 pont. A számok alapján azt láthatjuk, hogy az egyes kialakított klaszterek átlagosan más-más információbiztonsági protokollokkal rendelkeznek, már ha léteznek ilyenek a vállalatoknál. Kézenfekvő kérdés lehet, hogy ha az általános informatikai biztonság index értékei során így különválnak a csoportok, akkor a többi szempont és tulajdonság alapján mekkora eltérések várhatók.

Fontos még megemlíteni, hogy a csoportok leggyakoribb értékei, azaz móduszai szinte kivétel nélkül 10-20 ponttal maradnak el a következő kategória móduszától. Ez azt mutatja, hogy következő klaszterbe történő átlépés csak valamilyen további komolyabb biztonsági intézkedéssel, fejlesztéssel érhető el, akár stratégiai szinten is. Ezt támasztja alá a 2. csoportnál látható nagyobb eltérés a többi csoporttól. Ámde érdemes észben tartani, hogy ennek a klaszternek az informatikai biztonsági átlagpontszáma 80 pont, amely azt mutatja, hogy – mint a többi – ez sem egy tökéletesen homogén csoport, tehát még ott is nagy tere van a fejlődésre az egyes átlagot "lehúzó" vállalatoknak.

6. ábra

**Informatikai biztonsági csoportok eloszlása**

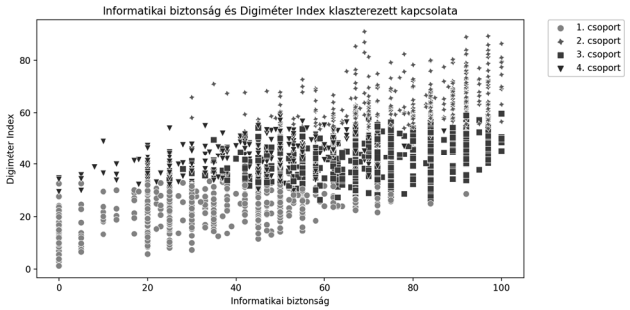



*Forrás: Digiméter jelentés (2022) alapján saját szerkesztés*

A feltételezés, miszerint az alacsonyabb digitalizáltsággal rendelkező vállalatok nem foglalkoznak oly mértékben az információbiztonsággal a további szempontokat megvizsgálva még nagyobb alátámasztást nyer. Az eddigi információk és a digitalizációt felmérő Digiméter Index megvizsgálása alapján látható (*lásd 7. ábra*), hogy az alacsonyabb indexszel rendelkező KKV-k az információt is vagy csekélyebb mértékben védik, vagy még nem is került az ilyes körű szempontrendszer a vállalatok fókuszába. Ehhez hozzátéve az elmúlt évek trendjeit még könnyebben kijelenthető, hogy ez a készültségi szint valószínűsíthetően már a közeljövőben a magasabb értékek felé fog elmozdulni.

7. ábra

**Informatikai biztonság és a Digiméter Index klaszterezett kapcsolata**

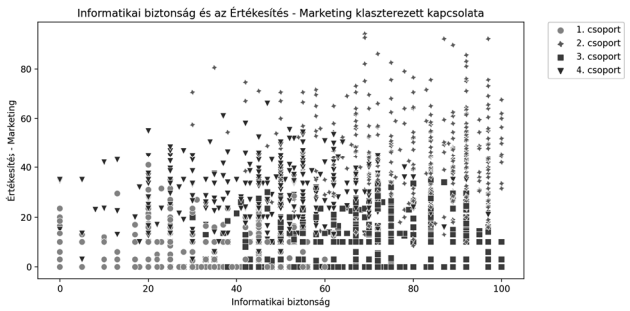



*Forrás: Digiméter jelentés (2022) alapján saját szerkesztés*

A kategóriák felosztása alapján az egyik legjobban értelmezhető kapcsolat az informatikai biztonság és az értékesítés, marketing között található meg (*lásd 8. ábra*). Tehát azon vállalatok, amelyek a digitalizációban előrébb járnak, nemcsak a különböző digitális jelenlét okán kerülnek ebbe a kategóriába, hanem az információs biztonságuk is jóval nagyobb figyelmet kap. Az értékesítés és marketing pedig pont ezt támasztja alá, hiszen az online térben gyakran hirdető és értékesítő vállalatoknak nagyon fontos szempont, hogy az információbiztonság és adatvédelem területén is naprakész tudással rendelkezzenek. Ennek hátterében az egyik fő okként az állhat, hogy a jogszabályoknak való megfelelés és a folyamatosan változó digitális jelenlét követelményrendszere a szüntelen adaptációt igényli. Az alkalmazkodási kényszert és naprakészséget viszont csak az erre a területre is vonatkozó kiemelt fókusszal lehet kivitelezni. Ennek hiányában pedig a vállalatok a további digitális terjeszkedésüket csak nagyon nehezen tudnák véghez vinni.

8. ábra

**Informatikai biztonság és az Értékesítés – Marketing klaszterezett kapcsolata**




*Forrás: Digiméter jelentés (2022) alapján saját szerkesztés*

Mindeközben a DESI-indexet 2014 óta minden évben mérik az Európai Unióban, így Magyarország helyzetével kapcsolatos változások folyamatosan figyelemmel kísérhetők. A mutató segítségével pontos képet kaphatunk a tagállamok digitális fejlődéséről, illetve mérik a meghatározott tervezetekhez kapcsolódó eredményeket. A korábbi pontszámokat és a rangsorolást évente újból kiszámítják, így tükrözve az alapadatok változását.

A 27 tagállam közül 2022-ben Magyarország a 22. helyezést érte el a DESI alapján (DESI, 2022). Négy különböző területen vizsgálják a tagállamokat: (a) humán tőke, (b) internet-hozzáférés, (c) digitális technológiák integráltsága, (d) digitális közszolgáltatások. Magyarország összpontszáma 43.8 pont, amely azt mutatja, hogy az ország az uniós átlagnak megfelelően fejlődött az elmúlt években, de még mindig jelentős lemaradásai vannak a vizsgált területeken.

A legelszomorítóbb eredmény a digitális technológiák integráltságát illetően született. Ezen a területen Magyarország a 25. helyen végzett, az EU-s átlagtól 14.5 ponttal lemaradva (DESI, 2022). A részeredmények tekintetében több területen láthatunk nagymértékű növekedést, mégis az eredmények azt mutatják, hogy még mindig nagyon sok magyar vállalkozás van, akik nem használják ki megfelelő mértékben a digitális technológiák lehetőségeit. Olyan erőforrás-tervezési rendszert, amelyeket az elektronikus információmegosztáshoz lehet használni, a vállalatok 21%-a használ (DESI, 2022). A vállalatok 13%-a van jelen valamilyen közösségi médián, ami azt mutatja, hogy ezeken a területeken jelentős mértékben az uniós átlag alatt teljesít Magyarország (DESI, 2022). A különböző rendszerek és platformok használata nem jelenti azt, hogy minden vállalat megfelelően és biztonságosan használja őket. A fejlett technológiák használata kismértékben elősegítené az információ védelmét, viszont a magyar vállalatok ezen a területen állnak a legrosszabbul. Fejlett technológia alatt értjük a mesterséges intelligenciát, amellyel a vállalatok 3%-a dolgozik, a Big Data-t, amivel 7% és a felhőtechnológiát, amely a legelterjedtebb, 21%-a használja a vállalatoknak (DESI, 2022).

A DESI-ben a KKV-kat három területen vizsgálják: (a) online kereskedő (18%), (b) e-kereskedelemből származó forgalom (12%), (c) határokon átnyúló online értékesítés (9%). Kismértékben érzékelhető növekedés jelenik meg mindhárom területen. Az eredményekből látható, hogy a magyar KKV-k jelentős lemaradásban vannak a digitalizációt tekintve. Alapszintű digitális intenzitással a vállalatok egyharmada rendelkezik, amely az EU-s 55%-os átlaghoz képest kimagaslóan rossz arányt mutat. A következő néhány évben elengedhetetlen, hogy a KKV-k minél közelebb kerüljenek digitalizáció szempontjából az uniós átlaghoz, amely szorosan összefügg az adatvédelem és az információbiztonság elterjedésével és előtérbe kerülésével.

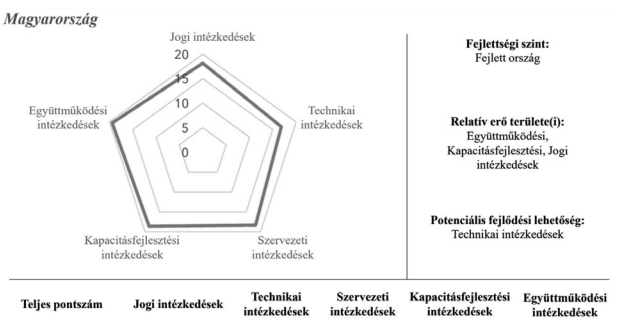
A Nemzeti Kiberbiztonsági Index szerint Magyarország a legutóbbi felülvizsgálat alapján, amely 2022. október 13-án történt, a világranglista 35. helyét foglalja el 65,53-as minősítéssel a maximálisan elérhető 100-ból (NCSI, 2022). A 2022-es méréseket megelőző adatokból, amelyek 2018 és 2019-ből származnak, egyértelműen kimutatható egy stagnáló helyzet. Ennek értelmében Magyarország információ- és kiberbiztonsága az elmúlt négy évben nem mutatott sem növekvő, sem csökkenő tendenciát. Bár az összkép többnyire kielégítő, három szektorban alapos felkészületlenség és kiaknázatlan növekedési potenciál figyelhető meg: (a) a kiber fenyegetettségek elemzése, különös tekintettel a weboldalakra, (b) az alapvető vagy kritikus szolgáltatásokra irányuló infrastruktúra védelme, valamint (c) a kiberválság kezelése (NCSI, 2022).

A fent említett 65,53-as értéket négy komponens adja, melyből a legkevésbé elfogadható az IKT-fejlettségi index. Ha az olvasó csak ezt az egy mutatót veszi irányadónak, akkor Magyarország a 48. helyre csúszik vissza (NCSI, 2022). Ez a megfigyelés összhangban van a DESI-indexben megfigyelt kijelentésekkel.

Hasonló módon, az International Telecommunication Union (ITU) 2020-as jelentése szerint Magyarország szintén a 35. helyet foglalta el a kutatók által vizsgált országok közül, és az európai országok között a 22. helyen zárt (GCI, 2020). Az ITU által végzett kutatások olyan Kiberbiztonsági Indexet állítanak fel, amely a kutatásban részt vevő államok öt alappillérre vonatkozó kötelezettségvállalásait értékelik egy 82 kérdésből álló kérdőívben. A felmérés szerint a *9. ábra* szemlélteti Magyarország erősségeit és fejlődési lehetőségeit. Összességében elmondható, hogy az öt pillérből négynél az intézkedések elégségesnek minősülnek, a technikai intézkedésekre vonatkozóan adott a lehetőség a további fejlődésre. Természetesen felmerül a kérdés, hogy mi motiválná a vállalkozásokat a technikai fejlesztésekre való kiadások fedezésére, ha ezekre vonatkozóan állami szinten nem kimagasló a teljesítmény. A válasz a kiberfenyegetések globális jellemzőjében rejlik, hiszen földrajzi elhelyezkedéstől függetlenül bármely vállalkozás lehet célpontja egy kibertámadásnak.

9. ábra

**Global Cybersecurity Index 2020 – Magyarország**




*Forrás: Global Cybersecurity Index 2020 (2021) alapján saját szerkesztés*

## Konklúzió

A kutatási paradigma, amely végigkísérte az eredmények kialakulását sikeresnek bizonyult. A különböző kérdőíves adatok feldolgozásával széles körben szerez az olvasó bepillantást a magyar KKV-k megvizsgálására digitalizáció, ezen belül információbiztonság szempontjából. Az eredmények pontos bemutatását és feldolgozását számos korlát nehezítette, amelyek az értelmezés során nem elkerülhetők. A kutatás egésze alatt három év adatait (2020, 2021 és 2022) dolgoztuk fel, amely adatok szűk rálátást nyújtanak a helyzetre. Ezen évek különösen kritikusak voltak a digitalizáció szempontjából, így ezek nemcsak korlátként, de sajátosságként is értelmezhetőek a kutatás szempontjából. A koronavírus terjedése 2020-ban magával hozta a gyors és nagymértékű digitalizációra való igényt, amellyel az

információbiztonság jelentősége is megnövekedett. Az eredmények mindegyikén kivehető az éles különbség a vírus kezdetekor és az utána következő időszakban megjelenő digitalizációt illetően.

A kérdőívek esetében minden évben változott a kitöltők száma, amelytől függ, hogy mennyire reprezentatív a kutatás eredménye a magyar KKV-k szempontjából. Emellett a vállalatoknál különböző szinten és mélységben ismeretes munkavállalók segítették a kitöltést. Mivel évről évre csökkent a kitöltők száma, ez befolyásolta, hogy milyen mértékben változott a vállalatok hozzáállása az információbiztonság területéhez. Általánosságban kijelenthető, hogy Magyarországon a digitalizációval kapcsolatban adathiány lép fel, amely egy minőségi kutatás elvégzéséhez komoly korlátot jelent. Az információbiztonság és kibervédelem, mint terület, Magyarországon kiforratlan és alulkutatott, kevés információja van róla a vállalatoknak, ezáltal nem érzékelik a téma súlyosságát.

A kutatás során számos területet érintve, korábbi eredményeket felhasználva hívtuk fel a figyelmet egy egyre égetőbb probléma és terület fontosságára. Az indexek összefüggései és ezek feldolgozása elősegítik a KKV-k helyzetének javulását. Az eredmények alátámasztják, hogy jelentős mértékű technológiai és biztonsági fejlődésre van szükség ahhoz, hogy a mindennapi információbiztonsági kihívások kezelhetővé váljanak.

Az elemzés záró gondolataiban ismét kerüljön említésre a bevezetésben tárgyalt történet. Az idillt megidéző végkifejlet szerint a farkast úgy móresre tanítják, hogy többé eszébe se jut a malacokra támadni. A valóságban természetesen semmi nem garantálja azt, hogy egy kivédett vagy elkerült kibertámadás után a KKV-k nem lesznek célpontjai több hasonló támadásnak.

A kutatási kérdés arra irányult, hogy bebizonyítsa a sürgetett digitalizáció valóban negatív hatással van az információbiztonsági szintre nézve a KKV-k életében Magyarországon. A kérdésre igenlő választ adunk. A klaszteranalízisben kimutatott összefüggések e tekintetben meggyőzőek.

A csoportosítás rávilágít arra, hogy az információbiztonsági szintet, mint spektrumot kell kezelni. Kisebb arányban megtalálhatók a területen kifejezetten jól teljesítő vállalkozások, ám a kritikus tömeg stagnál vagy felzárkózik. Ez az ún. kritikus tömeg jelképezi azokat a KKV-kat, amelyek az elmúlt két évben kezdtek el digitalizálni. Itt az információbiztonság háttérbe szorul. Erre számos intézkedés hiánya mutat rá a feldolgozott adatokból.

Az eredmények részletesen és több ízben támasztják alá, hogy egy, az információbiztonság tág területét a Magyarországon aktív KKV-k képtelenek lefedni. Ehhez sem elegendő idejük, lehetőségük, de leginkább szaktudásuk nincs. Az ezzel kapcsolatos költségekre a szerzőknek az adatokból nem volt rálátásuk.

Ugyanakkor kiemelendő, hogy nem tanácsos azzal mentegetőzni egy KKV-nak sem, hogy ő „kis cég" és nem jelent elsődleges célpontot a tanulmányban felsorolt fenyegetettségekre nézve. A sok területen megjelenő elmaradottság minden vállalkozást sebezhetővé tesz, és gyakran a támadók csupán szórakozásból teszik tönkre a vállalatok digitális infrastruktúráit.

Mindeközben tagállami szinten sem jobb a helyzet, hiszen a nemzetközi kutatásokból kimutatott eredmények alapján Magyarországon látható a területet érintő elmaradottság és annak kiforratlansága. Ez nemcsak az e-kereskedelemben aktívan részt vevő vállalkozásokra terjed ki, hanem a magyar KKV-k egészére.

Végül, a szerzők előszeretettel javasolják a kutatás újbóli elvégzését, hiszen várhatóan akár egy-két év alatt is nagy változások mehetnek végbe, az információbiztonság, mint szakterület gyorsan fejlődő jellegéből adódóan. Emellett további összehasonlító elemzéseket lenne érdemes elvégezni más országok piacain jelenlévő KKV-k között.

## Felhasznált irodalom


*A digitális gazdaság és társadalom fejlettségét mérő mutató, 2022 Magyarország.* https://hungary.representation.ec.europa.eu/digitalis-gazdasag-es-tarsadalom-fejlettseget-mero-mutato-2022-altalaban-veve-javult-helyzet-2022-07-28_hu

Abroshan, H., Devos, J., Poels, G., & Laermans, E. (2021). Phishing happens beyond technology: The effects of human behaviors and demographics on each step of a phishing process. *IEEE Access, 9,* 44928-44949. https://doi.org/10.1109/ACCESS.2021.3066383

Bakumenko, L. P., & Minina, E. A. (2020). International Index of Digital Economy and Society (I-DESI): Trends in the Development of Digital Technologies. *Statistics and Economics, 17*(2), 40-54. https://doi.org/10.21686/2500-3925-2020-2-40-54

Baxter, P., & Jack, S. (2008). Qualitative case study methodology: study design and implementation for novice researchers. *The Qualitative Report*, *13*(4), 544-559. https://doi.org/10.46743/2160-3715/2008.1573

Boletsis, C., Ragnhild, H., Pickering, J., Stephen, P., & Surridge, M. (2021). Cybersecurity for SMEs: Introducing the human element into socio-technical cybersecurity risk assessment. In Hurter, C., Purchase, H., Braz, J., & Bouatoch, K. (Eds.), *Proceedings of the 16th International Joint Conference on Computer Vision, Imaging and Computer Graphics Theory and Applications, SciTePress* (pp. 266-274). https://doi.org/10.5220/0010332902660274

Bruggemann, R., Koppatz, P., Scholl, M., & Schuktomow, R. (2022). Global Cybersecurity Index (GCI) and the Role of its 5 Pillars. *Social Indicators Research*, *159,* 125–143. https://doi.org/10.1007/s11205-021-02739-y

Bryan, L. L. (2020). Effective information security strategies for small business. *International Journal of Cyber Criminology, 14*(1), 341-360. http://doi.org/10.5281/zenodo.3760328

Cisco. (2017). *Annual CyberSecurity Report*. https://learningnetwork.cisco.com/s/contentdocument/0693i000001r6FtAAI

Craigen, D., Diakun-Thibault, N., & Purse, R. (2014). Defining Cybersecurity. T*echnology Innovation Management Review, 4*(10), 13-21. http://doi.org/10.22215/timreview/835

Creswell, J. W. (2003). *Research design: Qualitative, quantitative, and mixed methods approaches* (2nd ed.). Thousand Oaks: Sage. https://www.ucg.ac.me/skladiste/blog_609332/objava_105202/fajlovi/Creswell.pdf

Cseh G. (2019). *Digitális Gazdaság és Társadalom Index – Magyarország európai uniós teljesítménye a digitalizált világban*. https://www.researchgate.net/profile/Gergely-Cseh-Zelina/publication/338140204_Digitalis_Gazdasag_es_Tarsadalom_Index_-Magyarorszag_Europai_Unios_teljesitmenye_a_digitalizalt_vilagban_KEZIRAT_-_PREPRINT/links/5e01eeb74585159aa495de3f/Digitalis-Gazdasag-es-Tarsadalom-Index-Magyarorszag-Europai-Unios-teljesitmenye-a-digitalizalt-vilagban-KEZIRAT-PREPRINT.pdf

Csótó, M. (2019). Mérni annyi, mint tudni? Az elektronikus közigazgatás közösségi mérőszámairól. *Vezetéstudomány*, *50*(2), 14-31. https://doi.org/10.14267/VEZTUD.2019.02.02

Demeter K., Losonci, D., & Takács, O. (2019). Az ipar 4.0 hatásainak nyomában – a magyarországi járműipar elemzése. *Közgazdasági Szemle, 66*(2), 185-218. http://dx.doi.org/10.18414/KSZ.2019.2.185

DESI (2022). *A digitális gazdaság és társadalom indexe (DESI).* https://digital-strategy.ec.europa.eu/hu/policies/desi

DHS. (2014). A glossary of common cybersecurity terminology. *National Initiative for Cybersecurity Careers and Studies: Department of Homeland Security.* October 1. http://niccs.us-cert.gov/glossary#letter_c

Digiméter. (2023). *Digiméter jelentés 2022*. https://digimeter.hu/wp-content/uploads/2023/02/Digimeter-2022-jelentes.pdf

Edmondson, A., & McManus, S. (2007). Methodological fit in management field research. *Academy of Management Review, 32*(4), 1155-1179. https://doi.org/10.5465/AMR.2007.26586086

Farahbod, K., Shayo, C., & Varzandeh, J. (2020). Cybersecurity indices and cybercrime annual loss and economic impacts. *Journal of Business and Behavioral Sciences*, *32*(1), 63-71. http://asbbs.org/files/2020/JBBS_32.1_Spring_2020.pdf#page=63

Gerda, B., & Regina, R. (2022). A vállalkozások és a digitális fejlődés. In Baráth N. & Mezei J. (Eds.), *Rendészet – Tudomány – Aktualitások, A rendészettudomány a fiatal kutatók szemével, Konferenciakötet,* (pp. 82-97). Doktoranduszok Országos Szövetsége. https://tudasportal.uni-nke.hu/xmlui/bitstream/handle/20.500.12944/18611/RTA%202022.pdf?sequence=1&isAllowed=y

Global Cybersecurity Index 2020. (2021). *International Telecommunication Union* https://www.itu.int/epublications/publication/D-STR-GCI.01-2021-HTM-E?fbclid=IwAR0po3BCP_jjWUxMIOJCNK1Y4WxNAGWkIqbso_grf2zQ_1V2bA3tZssOoW4

Hemant, P., Chawande, N. P., Sonule, A., & Wani, H. (2011). Development of servers in cloud computing to solve issues related to security and backup. In *2011 IEEE International Conference on Cloud Computing and Intelligence Systems* (pp. 158-163). IEEE. https://doi.org/10.1109/CCIS.2011.6045052

International Organization for Standardization. (2020). *Information technology – Security techniques – Information security management systems – Requirements*. ISO/IEC 27001:2013. ISO. https://www.iso.org/standard/27001

ITU. (2009). *Overview of Cybersecurity. Recommendation ITU-T X.1205*. Geneva: International Telecommunication Union (ITU). http://www.itu.int/rec/T-REC-X.1205-200804-I/en

Kaila, U. (2018). Information security best practices: First steps for Startups and SMEs. *Technology Innovation Management Review, 8*(11), 32-42. https://doi.org/10.22215/timreview/1198

Khanvilkar, S., & Khokhar, A. (2004). Virtual private networks: an overview with performance evaluation. *IEEE Communications Magazine, 42*(10), 146-154. https://doi.org/10.1109/MCOM.2004.1341273

Ključnikov, A., Mura, L., & Sklenár, D. (2019). Information security management in SMEs: factors of success. *Entrepreneurship and Sustainability Issues, 6*(4), 2081-2094. https://doi.org/10.9770/jesi.2019.6.4(37)

Kravets, V. (2019). Comparative analysis of the cybersecurity indices and their applications. *Theoretical and Applied Cybersecurity, 1*(1), 97-102. https://doi.org/10.20535/tacs.2664-29132019.1.169090

Lewis, M. (2006). *Comparing, Designing, and Deploying VPNs*. Cisco Press.

Mackenzie, N., & Knipe, S. (2006). Research dilemmas: Paradigms, methods and methodology. *Issues in Educational Research, 16,* 193-205. http://www.iier.org.au/iier16/mackenzie.html

Mertens, D. M. (2005). *Research methods in education and psychology: Integrating diversity with quantitative and qualitative approaches* (2nd ed.). Sage.

Michelberger, P., & Lábodi, Cs. (2012). Vállalati információbiztonság szervezése. In *Vállalkozásfejlesztés a XXI. században II.* (pp. 241-302)., Óbuda University, Keleti Faculty of Business and Management. https://docplayer.hu/3431306-Vallalati-informaciobiztonsag-szervezese.html

Mirkovic, J., & Reiher, P. (2004). A taxonomy of DDoS attack and DDoS defense mechanisms. *ACM SIGCOMM Computer Communication Review, 34*(2), 39–53. https://doi.org/10.1145/997150.997156

Mullarkey, M. T., & Hevner, A. R. (2018). An elaborated action design research process model. *European Journal of Information Systems*, *28*(1). 6-20. https://doi.org/10.1080/0960085X.2018.1451811

*National Cyber Security Index* (2023). https://ncsi.ega.ee/indicators/

Naylor, D., Finamore, A., Leontiadis, I., Grunenberger, Y., Mellia, M., Munafò, M., Papagiannaki, K., & Steenk-

iste, P. (2014). The Cost of the „S" in HTTPS. In *Proceedings of the 10th ACM International on Conference on emerging Networking Experiments and Technologies (CoNEXT ,14)* (pp. 133–140). ACM. https://doi.org/10.1145/2674005.2674991

Nehrey, M., Voronenko, I., & Salem, A. B. M. (2022). Cybersecurity Assessment: World and Ukrainian Experience. In *2022 12th International Conference on Advanced Computer Information Technologies (ACIT)* (pp. 335-340). IEEE. https://doi.org/10.1109/ACIT54803.2022.9913081

Nemeslaki, A., & Sasvári, P. (2014). Az információbiztonság-tudatosság empirikus vizsgálata a magyar üzleti és közszférában. *Infokommunikáció és Jog, 60*(4), 169-177. https://infojog.hu/wp-content/uploads/pdf/201460_NemeslakiAndras_SasvariPeter.pdf

Pfeiffer, U. (2022). Eine starke Unternehmenskultur minimiert Cyberrisiken. *Digitale Welt, 6,* 24–27. https://doi.org/10.1007/s42354-022-0429-x

Porter Felt, A., Barnes, R., King, A., Palmer, C., Bentzel, C., & Tabriz, P. (2017). Measuring HTTPS adoption on the web. In *Proceedings of the 26th USENIX Conference on Security Symposium (SEC'17)* (pp. 1323–1338). ACM. https://www.usenix.org/system/files/conference/usenixsecurity17/sec17-felt.pdf

Ratchford, M., El-Gayar, O., Noteboom, C., & Wang, Y. (2022). BYOD security issues: A systematic literature review. *Information Security Journal: A Global Perspective*, *31*(3), 253–273. https://doi.org/10.1080/19393555.2021.1923873

Romanosky, S., Telang, R., & Acquisti, A. (2011). Do data breach disclosure laws reduce identity theft? *Journal of Policy Analysis and Management*, *30*(2), 256–286. http://www.jstor.org/stable/23018983

Sadok, M., Alter, S., & Bednar, P. (2020). It is not my job: exploring the disconnect between corporate security policies and actual security practices in SMEs. *Information and Computer Security*, *28*(3), 467-483. https://doi.org/10.1108/ICS-01-2019-0010

Schatz, D., Bashroush, R., & Wall, J. (2017). Towards a more representative definition of cyber security. *Journal of Digital Forensics, Security and Law, 12*(2), 53-74. https://doi.org/10.15394/jdfsl.2017.1476

Sharma, D. H., Dhote, C. A., & Potey, M. M. (2016). Identity and Access Management as Security-as-a-Service from Clouds. *Procedia Computer Science, 79,* 170–174. https://doi.org/10.1016/j.procs.2016.03.117

Simmonds, M. (2017). How businesses can navigate the growing tide of ransomware attacks. *Computer Fraud & Security*, (3), 9-12. https://doi.org/10.1016/S1361-3723(17)30023-4

Simon, J. (2006). A klaszterelemzés alkalmazási lehetőségei a marketingkutatásban. *Statiszikai Szemle*, *84*(7), 627-650. https://www.ksh.hu/statszemle_archive/2006/2006_07/2006_07_627.pdf

Smartcommerce Consulting, Reacty Digital, Virgo & Enet. (2020). *Digiméter* [Online]. https://digimeter.hu/

Tanenbaum, A. S., & Wetherall, D. J. (2013). *Számítógép-hálózatok*. Panem Kiadó.

Venkateswaran, R. (2001). Virtual private networks. *IEEE Potentials*, *20*(1), 11-15. https://doi.org/10.1109/45.913204

von Solms, B., & von Solms, R. (2018). Cybersecurity and information security – what goes where? *Information and Computer Security, 26*(1), 2-9. https://doi.org/10.1108/ICS-04-2017-0025

Yildirim, M., & Mackie, I. (2019). Encouraging users to improve password security and memorability. *International Journal of Information Security, 18*(12), 741-759. https://doi.org/10.1007/s10207-019-00429-y