

A KKV-K VÁLLALATMENEZSMENTJÉNEK „ÚJKELETŰ” KIHÍVÁSAI ÉS LEHETŐSÉGEI – A KIBERBÜNÖZÉSTŐL AZ ONLINE VÁLLALKOZÁSTÁMOGATÁSIG

GULYÁS Krisztina

PhD-hallgató, Széchenyi István Egyetem Regionális- és
Gazdaságtudományi Doktori Iskola

*PhD student, Széchenyi István University Doctoral School of Regional-
and Business Administration Sciences*

krisguphd@gmail.com

ORCID: 0009-0004-5411-2283

ABSTRACT

The recent years have been marked by a series of tumultuous events, including cyber pandemics, armed conflicts, the digital revolution, and a surge in cyber threats. These developments have profoundly impacted the operations of small and medium-sized enterprises (SMEs), leaving them reeling. The European Family Business Barometer and international CSV reviews have consistently identified that the same challenges and dilemmas are faced in all countries. One of the most concerning aspects of business operations is the potential for external actors to compromise the security of a company's digital assets. This can take the form of unauthorized access to financial accounts or the complete disruption of a company's digital infrastructure, including servers and databases. The threat of cybercrime is becoming increasingly acute for small and medium-sized enterprises (SMEs). These businesses form the backbone of the Hungarian economy, representing the biggest part of domestic enterprises and providing employment for over 3 million individuals. However, many SMEs lack adequate cybersecurity protection, while hackers are constantly developing new ways to steal, destroy or extort money from corporate assets. Virtual assistants (VAs) represent a potential solution to the challenges associated with digitalization and the shortage of skilled workers in small and medium-sized enterprises. In my own questionnaire survey, I demonstrated that SME managers initially perceive delegation as a significant challenge. However, they subsequently demonstrate a preference for delegation, including the delegation of complete projects, due to the success, efficiency gains, and cost reductions that they observe. Those lacking sufficient IT knowledge and skills are particularly vulnerable to fraudsters. It is impractical for a small business to provide ongoing training to its employees in all areas, so it is advisable to engage the services of other specialists for all but the core activity (e.g., woodworking in a joinery workshop). In this regard, it is worth noting

the increasing prevalence of professional, highly skilled digital business support providers who work on a project or hourly basis. Such professionals are sufficiently qualified and sufficiently small to undertake the work of a small company for a few hours a week at a fair price. The range of services is extensive, encompassing areas such as cyber security, administration, legal assistance, marketing, and graphics. There are already qualified and available virtual assistants (VAs) on the market for all these services.

Keywords: SMEs, management challenges, cyber security, online business support services, virtual assistants

Kulcsszavak: kkv, menedzsmentkihívások, kiberbiztonság, online vállalkozástámogatás, virtuális asszisztensek

Bevezetés

Az utóbbi évek turbulens eseményei (covid pandémia, háborúk, a digitalizáció berobbanása, a kiberfenyegetettség drasztikus növekedése) alapjaiban rengették meg a kkv-k életét. A European Family Business barométer és nemzetközi CSV review-k évek óta megállapítják, hogy ugyanazok a dilemmák és a kihívások minden országban. Az elmúlt évek viharos eseményei, amelyek magukban foglalják a kiberjárványokat, a geopolitikai konfliktusokat, a digitális robbanást és a kiberfenyegetések drámai növekedését, mélyen érintették a kis- és középvállalkozások életét. Ezek a kihívások paradigmaváltást tettek szükségessé az üzletviteli gyakorlatokban, kiemelve az innovatív üzletvitel kritikus szerepét a kkv-k ellenálló képességének és fenntarthatóságának biztosításában. Ezek mind hozzátevődnek természetesen az alapvető, hosszú évek óta húzódó szakképzett munkaerőhiány problematikájához, illetve a felsorolt válságok következményeként jelentkező magas inflációhoz, mint például hazánkban is. A vállalati stratégiai tervezés főként a környezeti erőkkel való kölcsönhatások kezelésére összpontosít: a korábban lassúbb és kiszámíthatóbb környezet 2020 tavasza óta gyorsan változó és bizonytalan üzleti környezetté vált. Reaktív vezető helyett a proaktív típusú vezetés a túlélés záloga, de legalábbis a villámgyors alkalmazkodási képesség.

1. Újkeletű kihívások a vállalatmenedzsmentben, a kiberbűnözés megjelenése

A KSH adatai⁷⁰ szerint közel kilencszázezer vállalkozás működik Magyarországon, amelyek 99,9%-a minősül mikro-, kis- vagy középvállalkozásnak, vagyis ők a hazai gazdaság gerince, tartópillérei. A kkv-k biztosítják a magyar munkavállalók kétharmadának a foglalkoztatását és ezáltal számos család egzisztenciáját is.

⁷⁰ Magyarország, 2022 (ksh.hu)

A KSH 2022-es adatai szerint a magyar kkv-k a hazai foglalkoztatottak 72 %át alkalmazták, a nettó árbevétel és a bruttó hozzáadott érték 55%-át képviselték a magyar gazdaságban. A KSH adatsoriából az is kiderül, hogy a kkv-k termelékenysége a pandémiás évek hatásainak ellenére 2022-ben javult, azonban továbbra is elmaradást mutatott az uniós átlaghoz képest. Az alacsony termelékenység egyik oka, hogy az innovációk (digitalizáció, új technológiák, zöld megoldások) kis mértékben hasznosulnak a kkv-knál. 2020 óta globális, EU-s és nemzeti szinten is több válsághelyzet alakult ki (Covid-19 járvány, orosz-ukrán háború, energiaválság, alap- és nyersanyag hiány, infláció, szabályozási változások, értékláncokon lefutó sokkhatások, a szakképzett munkaerő hiánya, digitalizációs és kiberbiztonsági kihívások), amely a gazdasági helyzet jelentős átalakulását eredményezték és számottevően kihatottak a magyar kkv-kra.

A „kiberpandémia”⁷¹ kifejezés a digitális infrastruktúrát világszerte megzavaró kibertámadások széles körű és egyidejű előfordulására utal. A kkv-k, amelyek gyakran nem rendelkeznek szilárd kiberbiztonsági keretekkel, különösen sebezhetőek. Az innovatív vállalatirányítás magában foglalja a fejlett kiberbiztonsági intézkedések és a proaktív fenyegetés-felderítés elfogadását. A mesterséges intelligencia (AI) és a gépi tanulási (ML) technológiák bevezetése javíthatja a kiberfenyegetések észlelését és az azokra való reagálást. Meglátásom szerint alapvető fontosságú a kiberbiztonsági tudatosság kultúrájának előmozdítása az alkalmazottak – és általánosságban a diákok és a lakosság - körében. Rendszeres képzések és gyakorlatok biztosíthatják, hogy a személyzet felkészült legyen a kiberfenyegetések felismerésére és az azokra való reagálásra. A kkv-knak, saját belső kompetencia hiánya esetén fontolóra kell venniük a kiberbiztonsági cégekkel való partnerséget is, hogy olyan szakértelemhez és erőforrásokhoz jussanak hozzá, amelyek máskülönben esetleg elérhetetlenek lennének, s már előre kell gondolkodniuk, egy incidens kellős közepén vagy megtörténte után már sokkal nehezebb lesz jó megoldást találniuk.

Az innovatív üzleti menedzsment rugalmas ellátási lánc stratégiákat kell, hogy kidolgozzon. A beszállítók diverzifikálása, a velük szemben támasztott elvárások és a megfelelő vészhelyzeti tervek kidolgozása és végrehajtása kritikus fontosságú.

Kevés aggasztóbb dolog van egy vállalkozás életében, mint amikor idegenek próbálják feltörni a cég vagy a tulajdonos bankszámláját és leemelni az ott lévő forrásokat vagy hozzáférhetetlenné tenni a teljes digitális céges adatbázist, komplett szervereket. A kiberbűnözés már a kis- és középvállalkozások számára is egyre akutabb veszélyt jelent. Hiszen amellet, hogy ők a gazdaság gerince, több millió munkahelyet biztosítanak-, a kkv-k gyakran nem rendelkeznek megfelelő kiberbiztonsági védelemmel, míg a hackerek folyamatosan új módszereket fejlesztenek ki, hogy ellopjanak, megsemmisítsenek vállalati tulajdont, vagy pénzszerzési céllal zsaroljanak. Az anyagi károkozás mellett a kiberbűnözők súlyosan ronthatják a

71 Biztonságportál - IT-biztonság: nem sikerült lépést tartani a világjárvánnyal (biztonsagportal.hu)

kkv-k hírnevét és versenyképességét. Egy súlyosabb, nem megfelelően kezelt eset pedig akár az érintett vállalkozás csődjéhez is vezethet. Eupában már 2020-ban is több kiberbiztonsági incidens történt, mint azt megelőző 15 évben összesen. A NIS2 Európai Unió szintű kiberbiztonsági irányelv életbe lépésével a megfelelés már kötelező lesz sok középvállalat számára.

A „Digitális Évtized Magyarország” 2023-as országjelentése⁷² szerint a magyar vállalkozások 95%-a használ valamilyen IKT eszközt a napi működése során. Ez az utóbbi években javuló tendenciát mutatott, de a mikro- és kisvállalkozások körében ez egyértelműen kényszerpálya volt. A pandémia alatti fizikai kapcsolattartási korlátozások sok kisvállalkozót kényszerítettek bele a digitalizációba; amiket korábban például nem elektronikus kapcsolattartással oldottak meg (pl fogyasztói árajánlatok, megrendelői kapcsolattartás, könyvelővel és más szervezetekkel való elektronikus kapcsolattartás), már egy vidéki mikrovállalkozás is digitálisan kényszerült lebonyolítani. A jelentés szerint a hazai kkv-k csupán 34%-a rendelkezik legalább alapszintű digitális intenzitással (uniós átlag: 55%). A felmérésben megállapítottakkal egyetértek, az uniós átlagtól való elmaradás oka a humán tőke alacsonyabb digitális képzettségi szintjének, az IKT szakemberek alacsonyabb arányában és a vállalkozások digitalizáltságának alacsonyabb fokában keresendő. A legszélesebb körben elterjedt digitális, informatikai megoldás a hazai vállalatok körében az elektronikus számlázó rendszer (80,4%). A magyar vállalkozások alacsony hányada rendelkezik közösségi médiafelülettel (13%), és csak kis hányadban használnak fejlett technológiákat: mesterséges intelligenciát a tavalyi válaszadók csupán 3%-a felhőalapú szolgáltatást 21%-uk, big data-t pedig 7% használt. A felmérés azt is megállapította, hogy a magyar kkv-k teljesítménye csak az online kereskedelemmel foglalkozók arányában, valamint az e-kereskedelemből származó forgalom arányában éri el az uniós átlagot. Kiberbiztonsági szemmel nézve szomorú és leginkább aggodalomra okot adó adat a felmérésből az lehet, hogy a növekvő trend ellenére a kisvállalkozások csupán közel negyede, míg a középvállalkozások valamivel több mint fele alkalmaz informatikai szakembert.

A KSH adatai⁷³ szerint 2021 óta Magyarországon a bankkártyás csalások: 50%-kal, az átutalási csalások elkövetési értéke 200%-kal nőtt, s már 2020-ban is több kiberbiztonsági incidens történt, mint az előző 15 évben összesen. Tudjuk, hogy ezek a visszaélések a „kiberbűnözők piacának növekedésével”, a kiberbűnözők számának növekedésével és módszereik, alkalmazott technológiájuk fejlődésével vált lehetségessé. A „piacnövekedés” alatt pontosan azt értem, hogy az elmúlt években szinten minden 14+ korú lakos (sok esetben akár ennél is fiatalabb), 80+ illetve „szépkorúakig” bezárólag, belépett a kibertérbe, önszántából vagy kény-

72 Az Európai Bizottság 2023. évi jelentése a digitális évtized helyzetéről (háttéranyagokkal) – eGov Hírlevél

73 Magyarország, 2022 (ksh.hu)

szerből. A mikro- és kisvállalkozásoknál ez a magánemberkénti és vállalatkénti kibertérbe történő belépés „összeér”, mely halmozott veszélyeztetettséghez vezetett. Az ilyen kisvállalatok tőkéje, javai nagymértékben összeolvadnak a tulajdonos és az ő családjának a vagyonával. S nem csupán. Nagyon sok esetben sajnos nem csupán pénzügyi értelemben vett „közösködésről” van szó, hanem IT szempontú „közösködésről” is beszélünk. Pl. egy vidéki egyéni vállalkozó egy és ugyanazon IT eszközről intézi privát és céges ügyeit, kezeli esetenként a céges és a privát online bankját, de arról használja a közösségi médiát (stb.) is. A legtöbb „egyszerű” IT user nem használ még egy alap vírusvédelmet sem, legtöbbjük a jelszóhasználat és a szoftverupdate-ek fontosságát sem ismeri. Nem végeznek karbantartást, nem csinálnak rendszeresen biztonsági mentéseket, stb. A kiberbiztonsági irányelvek - például a jelszókezelés, a jogosultságalapú hozzáférés, valamint az adatmentési és helyreállítási eljárások - létrehozása és végrehajtása segíthet az üzleti kommunikáció, az üzleti adatok védelmében.

Volumenében így ez a sokkal kevésbé óvatos, kevésbé tudatos és alig felkészült „csoport” komoly érdeklődésre tart számot a kiberbűnözők körében, hiszen sokkal nagyobb eséllyel és sokszor sokkal „egyszerűbben” (vagyis akár kevésbé „jól kvalifikált” kiberbűnözők által is) tudnak anyagi kárt okozni. A mikro- és kisvállalatok estében véleményem szerint hatványozottan igaz tehát, hogy a leggyengébb láncszem az egyén -tulajdonos, ügyvezető, alkalmazott(ak). Hiányzik az ismeret, képzések, megfelelő eszközök beleértve a szoftvereket, szabályzatok. Ez nem feltétlenül tőkeigényesség, hanem inkább felhasználói naïvitásra vezethető vissza. Például sok kisvállalkozó ismerősöm ugyanazon az eszközön tárolja a vevői adatokat, a könyvelést, amin a családi fotókat is (esetenként beleértve Sharenting⁷⁴-et is a közösségi médiákban). S a gyermeke esetleg ugyanerről az eszközről szörföl a darkneten torrentfájlokat letöltve/megosztva. Az eszközök egyidejű használata a személyes és az üzleti adatok szétválasztásának hiányát eredményezheti, ami növeli a jogosulatlan hozzáférés vagy az érzékeny információk elvesztésének kockázatát. Ha az eszközöket személyes és üzleti célokra is használják, kihívást jelenthet a hozzáférés-ellenőrzési irányelvek végrehajtása és az üzleti adatokhoz való hozzáférés korlátozása csak azokra, akiknek erre szükségük van.

Így a kkv-k kibertámadásoknak való kitettsége jelentősen megnő (adathalászat, rosszindulatú programok és a zsarolóprogramok), s a veszélyekről néha sejtelmük sincs, a veszélyforrásokat képtelenek beazonosítani, amíg meg nem történik a baj. A sokak által feltételezett „életkor-digitális felkészültség” korreláció véleményem szerint nem általánosítható teljesen és számos tényezőtől függ: iskolai végzettség, munkatapasztalat, a digitális technológiák iránti személyes érdeklődés, a vállalkozás profilja, működési mechanizmusok, tőkeerősség, vállalati profil és méret, stb. Anaív felhasználók veszélyeztethetik a személyes és az üzleti adatokat, akár teljes vagyonukat, s könnyen komoly adatvédelmi incidensbe is keve-

74 <https://www.kamaszpanasz.hu/hirek/lelek/8446/sharenting>

redhetnek. Véleményem szerint a NIS2 által nem érintett kkv-kat és az oktatási rendszerből már kikerült internetfogyasztó magánszemélyeket is szenzibilizálni kellene. A vírusirtó szoftverekbe, tűzfalakba, behatolásjelző rendszerekbe és más információbiztonsági megoldásokba való befektetés segíthet megvédeni a vállalati rendszereket a rosszindulatú szoftverektől és más kibertámadásoktól. Az operációs rendszerek, alkalmazások és egyéb üzleti szoftverek naprakészen tartása a legújabb biztonsági frissítésekkel és javításokkal csökkentheti a sebezhetőségeket és a kibertámadások kockázatát. A rendszeres adatmentési eljárások végrehajtása és az üzletmenet-folytonossági tervek kidolgozása segítheti a kis- és középvállalkozásokat és a családi vállalkozásokat a működés helyreállításában adatvesztés vagy kompromittálódás esetén, amelyek jelentős pénzügyi és hírnévbeli károkat okozhatnak. Kockázattudatossággal és megfelelő védelmi stratégiák elfogadásával azonban ezek a szervezetek jelentősen csökkenthetik a kibertámadásoknak való kitettségüket, és megvédhetik üzleti kommunikációjukat.

Az Európai Unió Kiberbiztonsági Ügynökségének (ENISA) tanulmánya⁷⁵ szerint az európai KKV-k közel 60%-a a költségvetési korlátokat tartja a robusztus kiberbiztonsági intézkedések végrehajtásának legfőbb akadályának. Emellett a képzett kiberbiztonsági szakemberek hiánya is tovább súlyosbítja az európai kkv-k előtt álló kihívásokat. A nagyvállalatokkal ellentétben, amelyek megengedhetik maguknak, hogy külön kiberbiztonsági csapatokkal dolgozzanak, a kkv-k gyakran nem rendelkeznek a kiberkockázatok hatékony csökkentéséhez szükséges belső szakértelemmel. Az Európai Bizottság kutatása⁷⁶ szerint Európa-szerte jelentős a kiberbiztonsági készséghiány, továbbá a kkv-k küzdenek a szakképzett munkaerő felvételével és megtartásával. Itt most nem feltétlenül arra kell gondolnunk, hogy minden kis vállalkozásnak a saját állománybeli kiberbiztonsági és IT szakember felvételével van a gondja, hiszen legtöbb helyen ez nem is egy „főállásnyi” munkamennyiség, hanem arról van szó, hogy a kkv-k nehezen vesznek fel mapaság „egyszerűbb” munkakörökbe is olyan munkaerőt (ügyintéző, stb.) aki szabálykövető, tudatos felhasználó. S ha találnak is ilyen jó dolgozókat, megtartani nehéz őket.

„A ma ismert támadások 99%-át vissza lehetne verni egyszerű, gyakran díjtalanul elérhető módszerekkel, mégis, az ügyfelek kevesebb mint 20 %a használ olyan jól bevált védekezési eszközt, mint a többtényezős hitelesítés” – derül ki a Microsoft legfrissebb, 2023 éves Digital Defense Report⁷⁷ jelentéséből. A vírusirtó szoftverek előnyei jól ismertek, de kevesebb információ áll rendelkezésre azzal kapcsolatban, hogy milyen egyéb védelmi vonalra van még szükség. A kisvállalkozások 30%-a nem rendelkezik kiberbiztonsági tudással és stratégiával. Egy vírusirtó ma

75 Studies — ENISA (europa.eu)

76 Az Európai Bizottság 2023. évi jelentése a digitális évtized helyzetéről (háttéranyagok) – eGov Hírlevél

77 Microsoft Digital Defense Report 2023 (MDDR)

már nem elég. A megfelelő szoftverek beszerzése mellett az összes alkalmazott mindennapi munkájának szerves része kell legyen a kiberbiztonsági tudatosság. Nem költséges képzésekben kell gondolkodni, elég, ha egy jól átgondolt útmutatót készítünk, átadjuk a tudást a munkavállalóknak, és megbizonyosodunk róla, hogy elsajátították az ismereteket, megértették a szabályokat.

2. Újkeletű megoldások a vállalatmenedzsmentben, az online vállalkozástámogatás avagy a virtuális asszisztencia (VA) megjelenése

Míg a globális trendek itt is más képet mutatnak, hiszen az USA-ban már 20 éve komolyan vették ezt a szektort, kutatni is kezdték, cikkek⁷⁸ jelentek meg a VA hozzáadott értékeiről, addig hazánkban a 2020 tavaszán kezdődő pandémiás időszak adott lendületet a kereslet és a kínálat találkozásának a VA szektor és családi KKV-k kapcsolatában. Ennek alapvető tere az online tér, a digitális kommunikáció, s feltétele az innovatív vállaltmenedzsment. Itt nem chatrobotokról és mesterséges intelligenciáról van szó, hanem húsvér emberekről, akik (egyéni) vállalkozóként más vállalkozások munkáját segítik online, vagyis nem fizikális jelenlét keretében végezve tevékenységüket. A pandémiával berobbant az „online” tér a munkavállalók életén keresztül minden munkaadó életébe is (homeschooling, homeoffice, e-commerce, elektronikus ügyintézés a könyvelőtől az ügyfélen át a hatóságokig, betegápolás). Lehetőség teremtdött (vagy rákényszerülés történt) sok, a pandémia miatt munkahelyét elvesztő, vagy a családi kötelezettségeket máshogyan nehezen teljesítő (gyermekek otthoni oktatása, folyamatos karanténok stb.), kiválóan képzett, nagyrészt vidéken élő nők számára az alternatív és sikeres karrierépítésre, az önmegvalósításra, komoly értékteremtés mellett: megjelent az online vállalkozástámogatás, mint szolgáltatás. Magyarország egyik legnagyobb VA szakmai csoportjának- (Szabó Ágnes Virtuális Irodaház⁷⁹) segítségével sikerült egy 100 fős VA közösséget elérnem, s körükben egy kérdőíves felmérést készítenem, illetve nekik köszönhetően anonim módon az ő megrendelőik bevonásával a megrendelői KKV oldal hozzáállását, véleményét is megismernem (54 beérkezett, kiértékelhető online kérdőív válaszait kielemezve).

A válaszadó VA-k: 97,4%-a nő; 68,4% 36-45 éves; 21,1%-uk 26-36 éves; 10,5%-uk 46-55 év közötti. Legmagasabb iskolai végzettségüket tekintve 16% többdiplomás, 36,8% egy diplomás, a többiek mind okj-s vagy nemzetközi felsőfokú szakképesítéssel rendelkeznek. Csupán 16%-uk gyermektelen, 16%-uknak 1; 42% -uknak 2; 18% -uknak 3; 5%-uknak 4 és 3%-uknak több, mint 4 gyermeke van. A gyermekek 95%-a 16 év alatti, kimagasló volt az általános iskolás életkor (homeschooling érintettség annak idején!). 53%-uk egyből teljesállásban kezdett

78 „Real work in virtual offices” 2002. International Journal of Productivity and Performance Management 51 (4/5), 266–268. o. ISSN 1741-0401

79 Bemutakozom - Virtuális Irodaház (virtualisirodahaz.hu)

neki a munkának, nem mellékállásban. 15,8%-uk 2019-ben, 23,7%-uk 2020-ban, 42,1%-uk 2021-ben, míg 18,4%-uk 2022-ben kezdte meg a VA munkáját hivatalosan. 80%-ukat a rugalmasabb és a családi logisztikai kihívások mellett otthonról végezhető munkalehetőség, míg 20%-ukat a munkanélküliség vagy egyéb nyomós ok (eü-i problémák, túl kicsi kereset) motivált. 64%-uk (!) idegennyelven is rendszeresen dolgozik, legtöbbjük angolul, németül, franciául, spanyolul, olaszul, de van aki japánul is! A válaszadók több, mint 55%-ának Pest megyében (29%-nak konkrétan Budapesten) van a székhelye „home office”-ban, a többi válaszadó pedig országos szinten inkább a nyugati megyékre koncentrálódik, de minden megyében megtalálhatóak, sőt, még Máltán is! Ügyfeleik székhelye: Magyarország, Amerikai Egyesült Államok, Németország, Svájc, Bulgária, Spanyolország, Málta, Kína, Olaszország, Portugália, Kanada, Ciprus, Svédország, Románia, Oroszország, Tajföld.

Mely tényezők okoztak nehézséget a saját virtuális asszisztens vállalkozás elindításban? Saját bevallásuk szerint a következők:

- Csupán 68%-ukat támogatta a család, környezet a saját VA vállalkozás indításának az ötletében
- Csupán 55%-uknak nem okozott nehézséget az indulótőke előteremtése. Ezt azért is fontos kiemelni, mert ez a típusú saját vállalkozás az egyik lehető legkisebb beruházásigényű tevékenységek közé tartozik.
- Mivel több éves szakmai tapasztalattal rendelkező emberekről van szó, így 47% válaszolta azt, hogy egyáltalán nem tartott az új, speciális szoftverek használatától, és 34% jelezte, hogy nem okozott neki problémát az ügyfelekkel való kommunikáció és a vállalkozás elindításához szükséges döntéshozatal sem.
- nehézséget okozó tényezőnek az ügyfélszerzés nehézségét (29%), illetve a bizonytalanságot (lesz- e elég ügyfél, bevétel?) (29%) jelölték meg.

65%-uk határozatlan idejű megbízással dolgozik (esetenként havi óraminimummal partnerenként, pl könyvelés, adminisztráció, asszisztencia, fordítások, online marketing, árajánlatok készítése, hírlevelek készítése, IT szolgáltatások), 35%-uk eseti vagy projektjellegű megbízásban dolgozik (ezutóbbinak tipikus esete volt a válaszokban egy honlap vagy egy webshop létrehozása, piackutatás, projektmenedzsment, marketing- és PR anyagok készítése, szövegírás). Az ügyfeleik 10%-a magánszemély, 25,6%-a egyéni vállalkozó, 36,6%-a mikrovállalkozás (2-10 fő), 25,3%-a kisvállalkozás (11-50 fő), 2,5%-a nagyvállalkozás (51-250 fő). Szektor szerint a megbízók a kis- és nagykereskedelemből, a tanácsadásból, a szolgáltatóiparból, az építő- és oktató iparból, az egészségügyből, a turizmusból, az ingatlan és a biztosítási szektorból kerülnek ki főként. De igazából úgy fogalmazhatunk, hogy a helyi asztalostól és műkőrmöstől át a legnagyobb online kereskedésig vagy nagy ügyvédi irodáig és magánkórházig mindekinek dolgoznak. A válaszok szerint a legtöbb ügyfél kezdetben azon aggódott, hogy nem ismerte ezt a szolgáltatást és

félt, hogy nem fog működni, hiszen nem is fognak személyesen találkozni, bizalmatlanok voltak és sokan drágálták az elején az óra- vagy a projektbért, főként idegennyelvű szolgáltatás esetén. (Megjegyzés: 2023-ban átlagosan 5000 forint órabér körül mozgott egy magyar nyelvű asszisztensi szolgáltatás ára.) A szabad élet hátrányaira is rákérdeztem a VA-k körében: 42%-a ismerte be, hogy a kezdetekben a megfelelési kényszer és az anyagi szükséglet miatt még sokkal többet dolgozott, mint alkalmazottként, és ugyanennyien szenvednek a vállalkozói magánytól. 37%-uk szenved egészségügyi panaszoktól a mozgásszegény életforma miatt (sok monitorozás, nem megfelelő testtartás stb.). Az ügyfélszerzés módjával kapcsolatban rengetegféle válasz érkezett, de a legtöbben a saját ismeretségi körön keresztül (ajánlással), Facebook és LinkedIn-es kapcsolatépítéssel, tematikus rendezvények során ismerték meg leendő megrendelőiket. A válaszadó VA-k soha, egyetlen egy alkalommal sem találkoztak személyesen az eddigi összes -valaha volt és jelenlegi- megbízójuk 89%-ával (!), 5%-ukkal pedig csak egyetlen egyszer az elején megismerkedni az ügyfél kérésére. A VA-k szolgáltatási spektrumuk szerint használnak szoftvereket, legtöbbjük a Microsoft 365-öt jelelte meg, mint „must have”, időmérő szoftverként legtöbbjük a Toogl-t használja, rengeteg a Canva előfizető közöttük, továbbá mindennapos a számlázó, feladatkezelő, videó vágó és szerkesztő szoftverek használata, gyakori a webshop és honlapszerkesztő programok, videokonferencia alkalmazások használata, de az SAP sem ritka. A megbízók arra kérdésre, hogy miért fordultak VA-hoz, a következő válaszokat adták (sorrendben multiple choice válaszok): nem győzték egyedül ellátni az adminisztrációs feladatokat a kkv-ben; eseti jellegű vagy projekt feladatokra nem volt vagy kapacitás vagy szaktudás a cégnél; olcsóbb így, mint saját alkalmazottal; gyors és komoly szaktudást kap így óradíj alapon elszámolva; olyan feladatokat tudott kiszervezni amiket nem szeretett csinálni de muszáj volt (pl. könyvelés előkészítése, webshopfeltöltés); nincs irodám ahova valakit leültethetnék egyéni vállalkozó vagyok és segítségre volt szükségem. Az elvárásokkal kapcsolatban a legtöbb megbízó a következő elvárásokat tartotta fontosnak (szintén a legtöbb szavazatot kapott válaszokat előre sorolva): megbízhatóság, precíz munkavégzés, szakértelem, önállóság, rugalmasság, gyorsaság. Meglepő lehet ugyan, de az olcsó ár és a geográfiai közelség a megbízók 6%-át érdekelt csupán. A megbízókról azt is igyekeztem kideríteni, mennyire „digitális” a vállalkozásuk. A legtöbb válaszadó közülük rendelkezik honlappal (75%), sokuknak van webshopja, 70%-uk a vállalati profillal is jelen van pl a FB-on, 70%-uk használ hírlevelet, 13%-uknak saját szervere van, míg 18,8%-uk bérlő a szervert, közel 20%-uknak van digitális adatvédelmi szabályzata és kiberbiztonsági incidensek esetére szabályozott folyamataik. S hogy mennyit fizetnek a megbízók átlagosan a VA-juknak havonta? Havi szinten 5-20.000 Ft (38%), 20-40.000 Ft (25%), 40-60.000 Ft (6%), 60-80.000 Ft (6%), míg 100.000 Ft felett is 6%-uk. A VA-k munkájának köszönhetően a válaszadó megbízó kkv-k vezetőinek bevallása szerint saját munkájuk így havonta a következő mértékben csökkent: 1-5 óra (31%), 5-10 óra (19%), 10-15 óra (25%), 15-20

óra (19%), 20 óránál több (6%). Egyértelmű, hogy egy egyéni vállalkozó nem ltrhet mindenhez. Biztosan remek a szakmájában, de egy hírlevél avgy egy honlap elkészítése egy szakértő VA-nak sokkal kevesebb idejében kerül. Arra is kíváncsi voltam, mivel töltik a megbízók az így felszabadult idejüket. A válaszok magukért beszélnek (multiple choice, csökkenő sorrendben): 81,3%-uk jelölte, hogy a felszabaduló időben meg többek között üzletfejlesztéssel is foglalkozik, a válaszadók 50%-a ügyfélszerzésre is tud így időt fordítani, s szintén 50%-uk így bővíteni tudta a vállalkozást. Ezenkívül 31,3%-uk jelölte meg, hogy családra, hobbira és pihe- nésre, feltöltődésre fordítja a felszabauló idő egy részét, míg szintén közel 30%-uk továbbképi magát ez idő alatt. Ezeken túlmenően olyan pozitív visszajelzéseket is kaptam, mint

- a megbízó vállalkozó ezáltal kevésbé fáradt,
- rengeteg időt spórol, főleg mert több területhez nem ért a felsorolt tevékeny- ségek közül,
- visszavezettek egy szolgáltatást, amit kapacitáshiány miatt eddig nem tudtak elvégezni,
- rend van a vállalkozásában, mert mindenki azt tudja csinálni, amihez ért,
- van ideje az értékteremtő, kreatív munkára, ami a szakmája, mert az admi- nisztrációs teendők csökkentek,
- több ügyfelet tud vállalni,
- kiegyensúlyozottabb lett,
- szereti, hogy együtt tudnak gondolkodni a VA-val.

3. Összegzés

Őszintén remélem, mint érintett kkv-s vezető, hogy az adat-, és általánosságban a kibervédelem komolyabb figyelmet és támogatottságot kap, állami szintről is. Ehhez attól tartok még sok időre lesz szükség, hiszen a hírek szerint⁸⁰ a Külügy- minisztériumban is csak „mostantól” veszik komolyabban a témát, az incidens után. Az, hogy kkv-k finanszírozott tanácsadásban s egyéb kibervédelmet szol- gáló lehetőségekben részesülhessenek, viszonylag bárki számára előrhető szinten, attól még sokáig nagyon messze lesz Magyarország, sajnos. És sajnos attól is, hogy a magyar közoktatásban, akár egy szakmunkásképzésben vagy egy ügyin- tézői OKJ-s tanfolyamon is kötelező tananyag legyen a kibervédelem, vagy hogy „vállalkozásmenedzsment” tananyagokba bekerüljön a felsőoktatási intézmények- ben. Bár őszintén, már az alapszintű (8 általános) oktatásban helye lenne a tudatos internetfelhasználás és a kiberveszélyek -hiszen sokan már okostelefonnal és oko- sórával, tablettel látják el az alsótagozatos gyermekeket is-, illetve az adatvédelem oktatásának, hiszen sok kiskorú már most nem csupán veszélyeztetett, de a jövő munkavállalójaként potenciális veszélyforrás is, naív felhasználói attitűdje miatt

80 Itthon: Nem cáfolták, hogy hiteles a külügy informatikai rendszerét ért orosz hack- értámadásokról szóló levél | hvg.hu

(rengeteg adatot maga vagy a szülei osztanak meg az egész világgal – lsd. Sharenting).

Az elmúlt évek viharos eseményei aláhúzták a kkv-k innovatív üzleti irányításának szükségességét. A fejlett kiberbiztonsági intézkedések elfogadásával, az ellátási láncok diverzifikálásával, a digitális technológiák integrálásával és átfogó kockázatkezelési stratégiák végrehajtásával a kkv-k eligazodhatnak a modern üzleti környezet összetettségében. Ezek az innovatív gyakorlatok nem csak az ellenálló képességet növelik, hanem a kkv-kat a fenntartható növekedés és siker érdekében is helyzetbe hozzák az egyre inkább digitális és összekapcsolt világban. A kkv-k tulajdonosainak, vezetőinek marad tehát az önképzés, az öngondoskodás, a bölcs előrelátás. A figyelem és a fegyelem lehet a legfőbb erényük ebben az aránytalan küzdelemben.

FELHASZNÁLT IRODALOM / REFERENCES

Az Európai Bizottság 2023. évi jelentése a digitális évtized helyzetéről (háttéranyagokkal)
– eGov Hirlevél

<https://www.kamaszpanasz.hu/hirek/lelek/8446/sharenting>

Bemutakozom - Virtuális Irodaház (virtualisirodahaz.hu)

Biztonságportál - IT-biztonság: nem sikerült lépést tartani a világjárvánnyal (biztonsagportal.hu)

Itthon: Nem cáfolták, hogy hiteles a külügy informatikai rendszerét ért orosz hackertámadásokról szóló levél | hvg.hu

Magyarország, 2022 (ksh.hu)

Microsoft Digital Defense Report 2023 (MDDR)

„Real work in virtual offices” 2002. International Journal of Productivity and Performance Management 51 (4/5), 266–268. o. ISSN 1741-0401

Studies — ENISA (europa.eu)