Információbiztonsági gondolatok a home office körül

Dr. Horváth Zsolt

1. Bevezetés

A COVID-19 miatt 2020. március elején kialakult vészhelyzet majdnem minden vállalkozás eddigi működését felforgatta Magyarországon. A koronavírus miatti járványügyi intézkedések kikényszerítettek többek közt számos higiéniai szabályozást, az emberek mozgásának és egymással való érintkezésének drasztikus korlátozását, és elvárták, hogy aki csak teheti, „maradjon otthon”. Ennek támogatására a vállalatokat is arra ösztökélték, hogy – ahol ez megoldható – munkatársaikat engedjék haza, hogy inkább otthonról ún. „home office”-ban dolgozhassanak. Természetesen nem végezhető mindenfajta munka otthonról, de a home office így is szinte napok alatt ugrásszerűen elterjedt.

Ilyen nagy és gyors változásra azonban sem a vállalkozások, sem maguk az emberek nem voltak felkészülve, így a home office-ra való átállás az elején még sok cégnél döcögősen ment. Persze miután beindult a folyamat, a home office-működés számos olyan pozitív tapasztalata is szemmel láthatóvá vált, melyek valószínűleg a vészhelyzet visszavonása utáni időkben is éreztetik majd hatásukat. Ezekről a hatásokról és szempontokról a Magyar Minőség szakfolyóirat megelőző, 2020. júliusi számában több érdekes írás is megjelent [1],[2], amelyek több nézőpontból is bemutatták az ilyen típusú munkavégzés kialakításának szükséges feltételeit és hatékonysági szempontjait. Jelen írásban ezeket a gondolatokat szeretném a home office néhány információbiztonsági aspektusával kiegészíteni.

2. Mit is értünk a home office munkavégzés alatt?

Noha a home office újabban a COVID-19 vészhelyzet következtében került hirtelen a figyelem középpontjába, fokozatos térnyerése valójában már évek óta megfigyelhető volt, és a világ számos pontján vált a munkavégzés egyre elfogadottabb formájává. Ezt a paradigmaváltást nem a vírushelyzet generálta, hanem a telekommunikáció, a technika és az informatika fejlődésének hatásai gyűrűztek be a munkavégzési és életviteli szokásokba.

Azonban itt nem kizárólag a home office-ról beszélünk, hanem egy annál sokkal általánosabb fogalomról, a távmunkáról. „A távmunka egy munkaszervezési mód, melynek lényege, hogy a távmunkás számára biztosított a vállalati központtól eltérő helyen is egy olyan munkakörnyezet, ahol infokommunikációs eszközök segítségével egyes munkafeladatait teljes értékűen el tudja végezni.” [3] A hivatalos távmunka Magyarországon (ahogy sok más országban is) jogi keretek között szabályozott.

Ennek értelmezése és gyakorlata azonban nem egységes, az életben erre nagyon sok különböző példát találhatunk. Az egyik véglet az, amikor az irodai munkahelyen valaki épp „csak hazaviszi, és otthon fejezi be a sürgős munkát". Ekkor munkáját már részben otthon végzi anélkül, hogy erre bármilyen külön jogi megállapodása lenne a munkáltatójával. Egyre több vállalatnál megengedett és/vagy támogatott a munkavégzés egy meghatározott részét (pl. heti egy vagy két napot) home office-ról teljesíteni, ilyenkor pedig általában már írásos megállapodás is készül, melynek részeként az otthoni munkavégzés feltételei szabályozottak. Ugyanakkor látható, hogy az előző két eset között nagyon elmosódott a határ. A másik véglet ezzel szemben az az állapot, amikor a munkavégzés teljes mértékben otthon, azaz home office-ban történik.

A távmunka fenti definíciójából az is látszik, hogy nem köti a munkavégzés helyszínét a munkavállaló lakóhelyéhez, az lehet bármi más, nem a munkáltató által fixen biztosított helyszín is. Ilyen esetekre számos példát találhatunk az elmúlt időkben, hiszen egyre több az olyan munkakör, amit távolról is be lehet tölteni. A teljes értékű munkavégzéshez gyakran már elég egy internetkapcsolattal rendelkező infokommunikációs eszköz, valamint a munkáltató által biztosított (általában felhőszolgáltatásban lévő) alkalmazás. Ekkor a munkavállaló akár azt is megteheti, hogy szabadon utazik a világban, és ahol éppen van, onnan végzi munkáját. Ezt hívják „digitális nomád" munkavégzési formának, és egyben életmódnak is.

Látható tehát, hogy a távmunka sokféle lehet, és csak egy bizonyos fajtáját értjük otthoni munkavégzésnek, azaz „home office"-nak. Bár fontos megjegyezni, hogy a gyakorlatban ennek pontos meghatározása és értelmezése a különböző vállalatoknál még így sem egységes.

A továbbiakban azt az esetet vizsgáljuk, amikor a munkavégzés helye a munkavállaló lakhelye, ami lehet akár saját lakása, akár az albérlet ahol lakik. (A koronavírus miatti vészhelyzet is elsősorban ezt a home office formát kényszerítette ki.)

3. Információbiztonsági aspektusok a home office munkavégzés során

Érthető módon a home office első bevezetésének, illetve a koronavírus miatti vészhelyzet visszavonása után a home office teljes vagy részleges megtartásának megfontolásakor a vállalatvezetők elsődleges szempontja a munkavégzés hatékonyságának legalább azonos szinten tartása, esetleg annak növelése volt. Emellett még fontos szempont a munkavégzés során kezelt bizalmas adatok információbiztonsága is, erre azonban sokszor már nem fordítottak kellő figyelmet. Az ilyen biztonsági szempontok figyelmen kívül hagyása mindig nagy kockázatot jelent az adott vállalatnak. Különösen azért is, mert sajnos a COVID-19 következtében az egész világon bevezetett megszorítások alatt kiemelkedően megugrott az ezt kihasználó kibertámadások száma és fajtája.

Természetesen nem minden típusú munka vihető haza, számos munkavégzési tevékenység éppen annak jellege miatt kötött bizonyos eszközhöz vagy helyszínhez. Azonban sokféle munka végezhető otthonról is, elsősorban például az irodai adminisztratív tevékenységet vagy szellemi alkotó tevékenységet tartalmazó, tehát számítógéppel végezhető munkák nagy része. Továbbá a kommunikációs tevékenységek többsége is végezhető a megfelelő kommunikációs szoftverek és platformok alkalmazásával online. Ilyen tevékenységek lehetnek

bizonyos ügyfélszolgálati feladatok, de akár auditok és felülvizsgálati tevékenységek, oktatások és képzések, különféle csoportmunkát igénylő tevékenységek is.

A vállalat vezetője dönti el, hogy az adott tevékenység végezhető-e hatékonyan otthonról online. A home office engedélyezésekor mérlegeli a munkavégzés eszközeinek, hatékonyságának és a munkatársak otthoni munkavégzése kontrolljának szempontjait, majd itt kell(ene) kitérnie az otthoni munkavégzés információbiztonsági kockázataira, valamint az azok kezelését meghatározó szabályokra és feltételrendszer kialakítására is.

A home office információbiztonsági szempontjainak figyelembe vétele tulajdonképpen annak mérlegelését jelenti, hogy a vállalati irodai környezetben végzett munka során előforduló bizalmas, titkos adatok információbiztonsági szintje milyen mértékben tartható fenn, ha a munkatárs az irodai környezet helyett otthonról végzi a tevékenységét. Másképp megfogalmazva: ha a munkatárs a „védett" irodai környezetet a munkavégzés során otthoni környezetre cseréli fel, akkor milyen új információbiztonsági kockázatok lépnek fel, és ez milyen mértékben csökkenti a vállalat információinak biztonságát.

A téma fontosságát az is jól mutatja, hogy az információbiztonság öt gyakorlati területéből

- a terület- és objektumvédelem (fizikai biztonság),
- a személyvédelem (humánbiztonság),
- a hagyományos „alapú" adatok, módszerek, eszközök védelme (pl. iratkezelés biztonsága),
- az informatikai védelem (informatikai biztonság),
- a katasztrófák elleni védelem (megelőző céllal elemi károk, természeti csapások, társadalmi katasztrófák elleni védelem)

– részben vagy egészben, de – mind kikerülnek a vállalat közvetlen ellenőrzése alól.

A vállalatok működésük során sokféle adatot használnak, amelyek bizalmassági szintje (vagy másképp fogalmazva érzékenysége adatszivárgás esetén) különböző. Az adatok jellegüknél (adattartalmuknál) fogva is tartozhatnak különböző kategóriákba, melyekre így az egyes kategóriáknak megfelelő biztonsági szabályok lesznek érvényesek. Ilyen kategóriák lehetnek például – a teljesség igénye nélkül – a személyes adatok, az üzleti titkot képező, a banktitkot képező adatok vagy a nemzeti minősített adatok (ez utóbbi kategóriát régen államtitoknak hívták). Ezen adattípusok egy részét jogszabályok határozzák meg, és írják elő a kezelésükre vonatkozó követelményeket.

A vállalat belső (például irodai) munkavégzése során az adatok használatára, kezelésére jellemzően különböző biztonsági szabályokat határoznak meg, amelyek alapja az adott adatok bizalmassági szintje szerinti csoportosítás. Ezek csoportosíthatók például így: csak belső használatú adatok, bizalmas adatok vagy titkos adatok, ahol a besorolás során már figyelembe veszik az egyes adatok adattartalma szerinti jogszabályi követelményeket is. Ezek a szabályok jellemzően a munkahelyen történő munkavégzésre, annak körülményeire és feltételeire vonatkoznak.

Ez azt jelenti, hogy a vállalat által biztosított irodai környezetben kontrollált az adott munkahelyre belépők és ott tartózkodók köre, a papíralapú információkhoz és a számítógépes munkaállomáshoz hozzáférők köre. Így a munkavégzés helye is eleve egy „védett" környezet, amin belül vannak az érzékeny információk. Megfelelő szabályokkal kialakítható, hogy az adott információkhoz vagy információ-feldolgozó eszközökhöz csak azok férhessenek

hozzá, akiknek ez munkakörük miatt szükséges. Otthoni munkavégzés esetén a munkatárs lakásáról mindez viszont már csak korlátozottan mondható el, így minden esetben mérlegelni kell, hogy a hazavitt munka elvégzése során kezelt adatok biztonsága milyen mértékben és milyen megszorításokkal biztosítható, és ez a szint még elfogadható-e vagy sem.

Eddig még csak azokról az adatokról beszéltünk, amit a munkatárs a munkája során – akár munkahelyén, akár otthon – kezel, azaz amivel dolgozik. De sok esetben más is megjelenik itt. Az otthoni munkavégzés során, különösen ha számítógépes kommunikációs alkalmazást (pl. Skype, MS Teams, Google Meets vagy egyéb hasonló célú chatprogramot) használ, és az ügyféllel/partnerrel történő egyéni vagy csoportos kommunikáció során a kamera funkciót is használja, minden résztvevőnél megjelenik a többi résztvevő élő kameraképe is. Miután ő is, és a többi résztvevő is jellemzően home office-ban dolgozik, és onnan vesz részt a kommunikációban, a kamerafelvételen jellemzően láthatók a lakásának egy része és esetlegesen egyéb személyek is, akik ott tartózkodnak vagy épp bemennek a képbe. Ha ez a kommunikáció az adott eszközzel rögzítésre kerül, akkor már az érintett home office-ban dolgozó személy lakásrészletének illetve családtagjainak (vagy az egyéb ott tartózkodó személyek) rögzítésével olyan személyes adatok kezeléséről is beszélünk, amelyek egyébként nem is kapcsolódtak volna a munkavégzéshez. Ez további kellemetlen szituációkat és akár komoly jogi problémákat is eredményezhet.

A vállalati vezetőknek ezeket a szempontokat is figyelembe kell venni, amikor eldöntik, hogy mely tevékenységek végezhetők otthonról, azaz távmunkában. Nem csak az fontos szempont tehát, hogy az adott tevékenység végezhető-e egyáltalán és hatékonyan otthonról, hanem az is, hogy az adott tevékenység során használt, kezelt adatok biztonsága garantálható-e az otthoni, home office munkavégzés körülményei mellett. Vannak olyan tevékenységek, amelyeknél éppen ez a szempont – azaz a tevékenység során kezelt adatok bizalmassága – zárja ki a home office lehetőségét. Ezt a döntést minden esetben a vállalat vezetőjének kell meghoznia.

A home office kialakításakor fontos szempont a nyugodt munkakörülmények biztosítása. Ez nagyon fontos mind a munkavégzés folytonossága és hatékonysága szempontjából, de az adatokhoz való jogosulatlanok általi hozzáférés elkerülése szempontjából is. A nyugodt és zavartalan munkakörnyezet – legyen az egy munkasarok vagy egy külön szoba a lakásban – nem csak azért fontos, hogy a munkatárs otthon nyugodtan és zavartalanul tudjon dolgozni, hanem azért is, hogy amivel dolgozik, azokra az információkra másnak ne legyen rálátása. Ezt a gondolatot viszont azonnal kibővíthetjük: Ne csak az éppen a képernyőn vagy más adathordozón megjelenő információkra gondoljunk, hanem a telekonferencián lebonyolított munkamegbeszélésen szóban elhangzott információkra is. Hiszen a home office-ból folytatott telekonferencia megbeszélések tulajdonképpen a vállalati zárt tárgyalókban lefolytatott megbeszéléseket váltják ki. Míg azonban a vállalati zárt tárgyalók zavartalansága biztosított, addig a home office-ból telekonferenciára felcsatlakozó kollégák otthoni munkakörnyezetére ez nem mindig igaz.

A munkavégzéshez szükséges információk elhangozhatnak szóbeli megbeszéléseken, de lehetnek papíralapú iratokban vagy informatikai adathordozókon is.

Ha papíralapú iratokról, rajzokról vagy egyéb jegyzetekről beszélünk, akkor azokat célszerű

otthon mindig elzárva tartani, amikor éppen nem dolgozunk azokkal. Ha a kolléga hazaérve a munkaanyagait tartalmazó dossziét, iratokat vagy azok egy részét gyorsan leteszi az előszobában, a konyhában vagy a lakásban egy épp üres helyre, ahol utána ott felejti, akkor az könnyen elkeveredhet az egyéb családi iratok, reklámanyagok vagy kacatok közé. Ez kockázatot jelenthet mind az egyes iratok könnyű elvesztésében, mind pedig abban, hogy a lakásban véletlenül akár családtagok, akár vendégek kezébe kerülve azok érdeklődve kezdik olvasgatni. Persze nem minden munkaanyag tartalmaz olyan információt, amelybe való véletlenszerű illetéktelen beleolvasás komoly biztonsági problémákat okozna, de ennek a fordítottja sem igaz.

Ilyen esetekben – a munkavégzés szempontjából – illetéktelennek tekinthetők mind a családtagok, mind bármely egyéb személy, aki akkor a munkatárs lakhelyén tartózkodik.

Az informatikai eszközökön otthon tárolt adatok többnyire mobil számítógépeken (pl. notebookokon, tableteken, stb.), mobil passzív adathordozókon (pl. USB pendrive-okon, HDD-ken, SSD-ken, stb.) lehetnek elérhetők. Ezek védelme is fontos, hiszen ezek elvesztése vagy ellopása esetén ezek könnyen kerülhetnek idegen kezekbe, ahol a fájlok, információk útja már nem visszakövethető. A legcélszerűbb ezeket az eszközöket eleve titkosítással ellátni.

A home office munkavégzés biztonságát továbbá döntő mértékben a használt informatikai infrastruktúra és annak használati módja határozza meg. Ennek főbb elemei:

- az otthonról online dolgozó munkatárs végponti munkaállomása (notebook, tablet, és az esetlegesen kapcsolódó perifériák);
- az otthonról online dolgozó munkatárs otthoni internet szolgáltatása és annak beállításai;
- a központi (szerveroldali) eszköz vagy alkalmazás, ahová online csatlakozik;
- maga az internetes kapcsolat és kommunikáció, és annak eszközei.

Ezeknek egy része természetesen ugyanaz, mint amit a munkatárs a vállalati irodai környezetben amúgy is használna. Az irodai környezet home office-ra való leváltásakor azonban van, ami megváltozik, és van, aminek a használati módján kell változtatni az újonnan felmerülő esetleges kockázatok elkerülésére. Nézzük sorban a lehetséges nagyobb veszélyeket:

- **Az otthonról online dolgozó munkatárs végponti munkaállomása** általában valamilyen számítógép, ami lehet a munkahely által biztosított, de lehet a munkatárs saját otthoni számítógépe is.

Mindkét esetben kérdés, hogy ugyanazt a számítógépet, amin ő otthonról dolgozik, rajta kívül más is használja-e még, és ha igen, milyen célra. Elképzelhető, hogy a családtagok is használhatják szórakozásra, filmnézésre, chatelésre, egyéb munkára, távoktatásra, stb. Ekkor többféle kockázattal is lehet számolni. Egyrészt hogyha a különböző felhasználók adatai és géphasználata nem elkülönített egymástól (pl. eltérő felhasználói fiókokkal), akkor könnyen hozzáférhetnek egymás adataihoz, és ebből akár még véletlenszerűen is adódhatnak problémák. Másrészt a családtagok általi számítógép-használat során soha nem garantálható ugyanaz a tudatosság és a biztonsági szabályok (vállalati policy-k) betartása, amik az irodai munkakörnyezetet jellemzik, ezáltal pedig a számítógép vírusfertőzöttségének kockázata mindenképp megnő.

Vállalati tulajdonú számítógép (jellemzően notebook) esetén az alapvető biztonsági beállításokat a rendszergazda végzi, és úgy adja át használatra a gépet. Azonban, ha a munkatársnak az általa használt notebookon rendszergazdai jogosultsága van, akkor az otthoni használat során ezen beállításokból sok mindent meg tud változtatni. Különösen veszélyes ez akkor, ha otthon a munkavégzésen kívül odaenged a géphez másokat is. Vállalati notebook vírusfertőzésének további veszélye lehet, hogy a munkatárs visszatérve az irodai környezetbe a notebookját viszi magával, és amint rákapcsolja a vállalati lokális hálózatra, ott már a tűzfalon belül egyből elterjesztheti az otthon összeszedett kártékony programot.

Saját tulajdonú eszköz használata esetén a számítógép beállításait általában a gép tulajdonosa, azaz a munkatárs végzi, akinek (és családjának) a magáncélú használatot a vállalat még korlátozni sem tudja. Itt az előző kockázatok fokozottan lépnek fel. Ezen túlmenően további kockázatot jelenthet a számítógép kellő informatikai biztonsági védelmének (vírusellenes illetve internetes biztonsági szoftverek, tűzfalak, stb.), valamint a számítógépen használt szoftverek jogtisztaságának esetleges hiánya. Hiszen a vállalat felelős azért is, hogy minden üzleti tevékenységhez kapcsolódó munkavégzést legális, jogtiszta eszközzel, szoftverrel végezzen.

- **Az otthonról online dolgozó munkatárs otthoni internet szolgáltatása** általában valamelyik telekommunikációs szolgáltató által biztosított szolgáltatáscsomag internet-szolgáltatás része, jellemzően ADSL vagy kábelnet szolgáltatás. Az internet-szolgáltatáshoz sok esetben a szolgáltató biztosítja a routert, amit általában ő maga menedzsel, és amin keresztül jellemzően vezetékkel is és WiFi-n keresztül is lehet kapcsolódni az internetre.

Itt kockázatnak számít az internetkapcsolat biztonsága, a gyártó által a router beépített képességek (és sérülékenységek) illetve a szolgáltató általi beállítások, valamint a használt WiFi protokoll biztonsága, annak beállításai vagy esetleges gyengeségei. Sok esetben a munkatárs az otthoni munkahely kialakításakor csak WiFi-n keresztül tud csatlakozni az internetre, ami részint a közös használat miatti leterheltség következtében, részint pedig a WiFi kommunikációs stabilitásának problémái miatt gyengébb, megbízhatatlanabb internetkapcsolatot, kommunikációt eredményez. A WiFi további kockázatát jelenti a nem kellően erős védelem mellett a gyengébb protokoll relatív könnyű feltörhetősége, lehallgathatósága.

- **A központi (szerveroldali) eszköz vagy alkalmazás**, amire az otthonról dolgozó munkatárs online csatlakozik, az az eszköz vagy alkalmazás, amin a tulajdonképpeni munkavégzés történik, ugyanaz, amit a munkatárs a vállalati irodai környezetben is használ. Ez lehet például vállalati fájlszerver vagy alkalmazás-szerver, ami a vállalat telephelyén lévő szerverszobában érhető el, de lehet akár egy szerverfarmra kihelyezve is. Itt a munkatárs bejelentkezését, megbízható azonosítását és jogosultságainak menedzselését a vállalati rendszergazda végzi el, és ez nem különbözik a vállalati vagy az otthoni munkavégzés esetében egymástól. Amennyiben a munkatárs nem a vállalati, vezetékes lokális hálózatról csatlakozik a szerverhez, hanem interneten keresztüli távoli kapcsolattal, akkor a rendszergazda feladata a megfelelő biztonságos távoli kommunikáció beállítása.

Hasonlóan lehet ez a központi alkalmazás egy vállalat által használt felhő-tárhely szolgáltatás (pl. MS OneDrive, MS O365, Google Drive, stb.) vagy egy felhő alapú alkalmazás-szolgáltatás is. Ilyen esetekben a szolgáltatásra való

csatlakozás ugyanúgy történik mind az irodai munkahelyről, mind home office-ból, a biztonsági beállításoknak nem kell különbözniük egymástól.

- Az utolsó, de nagyon fontos pont **maga az internetes kapcsolatot biztosító kommunikációs szoftver**, és annak használata. Itt a munkavégzés jellegétől függően több mindenről is lehet szó.

Amennyiben az otthonról dolgozó munkatársnak vállalati szerverre (vagy egyéb vállalati számítógépre) kell kapcsolódnia, akkor a cél mindenképp egy biztonságos és titkosított kapcsolat kiépítése. Ezt általában különböző VPN kapcsolatokkal szokták megoldani. A VPN kapcsolat kiépítésében, beállításában sokféle lehetőség van, és ezek biztonsági szempontból is különböző szintű megoldásokat jelentenek. A munkavégzés megkívánt módja és az elérni kívánt biztonsági funkciók között sok átmenet figyelhető meg. Beállíthatók VPN kapcsolatokkal az autentikációk különböző szintjei, valamint beállíthatók a kapcsolati kommunikáció különböző szintjei is. Ez utóbbi alatt azt értjük, hogy a VPN-t használó notebook milyen szinten tud kommunikálni azzal a szerverrel/számítógéppel, amelyre csatlakozott. Az egyik véglet a teljes kommunikáció, a másik véglet pedig a gyakorlatilag egy vagy néhány IP protokollra szűkített kommunikáció. Ez utóbbi azt jelenti, hogy a munkatárs VPN-en keresztül, mintegy terminálmódban lép fel a szerverre vagy egy másik számítógépre, és dolgozik azon távolról. Ekkor saját notebookján ezen a kapcsolaton keresztül csak a billentyűzetet, egeret és monitort használja, és a saját notebookjának többi erőforrása elérhetetlen, azaz a szerverről nem tud lokálisan letölteni vagy kinyomtatni semmit. Ez a munkavégzés adatbiztonságát lényegesen megnöveli, de ugyanakkor nehézkessé is teszi bizonyos jellegű feladatok ellátását.

Ha az otthon dolgozó munkatársnak egy megbeszélésen kell távolról részt vennie, akkor ehhez szüksége van egy megfelelő csoportmunkát támogató alkalmazásra. Ezeknek minimális közös funkciói a chat-funkció, a hang- és videokapcsolati kommunikáció, valamint a képernyőmegosztás. Ilyen alkalmazásból elég sok van, mind ingyenesen használható, mind fizetős verzióban. Ezek vezérlése, illetve további funkciói és biztonsági tulajdonságai alkalmazásonként eltérhetnek. Az ilyen alkalmazások használatának információbiztonsági kockázatai lehetnek például: kommunikáció lehallgatása, illetéktelenek kéretlen becsatlakozása a megbeszélésbe, alkalmazás által mentett adatokhoz, információkhoz való illetéktelen hozzáférés lehetősége, kamerafelvételek jogosulatlan felhasználása vagy azokhoz való hozzáférés, illetve a nem kellően óvatos használat esetén a bekapcsolt kamerákon a megbeszéléshez nem tartozó személyek megjelenése, stb.

4. Összefoglalás

Az elmúlt években, évtizedekben a munkavégzési módok között folyamatosan egyre nagyobb életteret nyert a távmunka. Az idei év tavaszától a COVID-19 koronavírus elterjedése következtében kialakult vészhelyzet nyomán ugrásszerűen megnőtt az igény a távmunka egy bizonyos fajtájának, a home office-nak a kialakítására és használatára.

A home office kialakítása során elsődleges – és sokszor kizárólagos – szempont az otthoni munkavégzés kialakításának lehetősége és hatékonysága volt. Az ezekkel kapcsolatos információbiztonsági kockázatokra és azok kezelésére azonban a legtöbb esetben már nem került sor, erre a vállalatok vezetői általában nem is gondoltak.

Jelen írásban a home office kialakításával kapcsolatos legfontosabb információbiztonsági kockázatok közül mutattam be a teljesség igénye nélkül néhányat. Természetesen ezen kockázatok többségére van megoldás. Azonban ezekkel a kockázatokkal mindenképpen szükséges foglalkozni, ugyanis figyelmen kívül hagyásuk komoly biztonsági, és azon keresztül működési veszélyt jelenthet a vállalatok számára egy egyébként is kiélezett, a cégek fennmaradását is veszélyeztető szokatlan versenyhelyzetben.

5. Felhasznált források

[1] Rózsa András: Online Szakmai Szemináriumok válságos időszakban; Magyar Minőség XXIX. évfolyam 07. szám, p. 19-24.

[2] Torma Beáta: Home office vagy iroda? Magyar Minőség XXIX. évfolyam 07. szám, p. 25-29.

[3] Magyar Távmunka Szövetség honlapja, http://tavmunka.org/wp/tavmunka-fogalma/

Dr. Horváth Zsolt az INFOBIZ Informatikai, Információbiztonsági és Vezetési Tanácsadó Kft. társtulajdonosa és ügyvezetője 2006 óta. EOQ MNB által regisztrált minőségirányítási és információbiztonsági rendszermenedzser és auditor. Tíz évig látta el a SIEMENS magyarországi szoftverházának, a SIEMENS PSE Kft-nek a minőségirányítási igazgatói feladatait. Több, mint húsz éve dolgozik a minőségirányítás és az információbiztonsági irányítás területén több akkreditált tanúsító szervezet vezető auditoraként, valamint tanácsadóként és szakmai oktatóként. Számos szakmai konferencián elhangzott előadás és megjelent publikáció szerzője és társszerzője.

Egy máig ható filozófus

Georg Wilhelm Friedrich Hegel, az egyetemes filozófiatörténet egyik legnagyobb alakja, 250 évvel ezelőtt született, 1770. augusztus 27-én, Stuttgartban. Tübingenben diplomázott és védte meg doktori disszertációját. Munkásságának főbb korszakait azokról a városokról nevezték el, ahol éppen tevékenykedett. Csak felsorolva: Bern, Frankfurt, Jéna, Nürnberg és Berlin. Az átlagembernek Hegelről általában a dialektika hármas egysége jut az eszébe, a mennyiségi-minőségi változások ideáját már nem kapcsolják hozzá, pedig szintén az ő munkásságának eredménye. Életműve óriási, pedig mindössze négy könyvet írt. Az érdeklődők magyar nyelven is olvashatják, megjegyezzük nyelvezete elég nehéz az általa definiált új fogalmak és a sajátos megfogalmazási módja miatt. 1831. november 14-én hunyt el Berlinben, az ott tomboló kolerajárvány következtében.