Home office – hosszú távú megoldás vagy átmeneti probléma?

Jelen értekezésben arra keressük a választ, hogy a digitális átalakulási hullám közepén reális lehetőségként kell-e tekintenünk a home office intézményére és rendelkezésünkre áll-e a megfelelő jogi és informatikai eszköztár, ha ennek megfelelően átszervezzük a céges működésünket.

A szokásaink rabjai vagyunk. Felnőtt életünk során a legtöbbünk, ahogy a szüleink is, minden munkanap reggelén elindul munkába. Egyszerűen megszoktuk, hogy a munkahelyünk egy másik utcában, egy másik környezetben van és utazunk kell miatta. Ingázunk a lakhelyünk és a munkahelyünk között. Egy átlagos munkavállaló évente 251 alkalommal megy be a munkahelyére, majd tér onnan haza. Fél órás utazási idővel számolva ez évente 10 és fél napot jelent. Érthető, hogy egy kicsit idegenkedve, furcsán tekintünk a home office jelenségre. Az otthoni környezetből történő munkavégzés nem újkeletű dolog. Számos nagyvállalat alkalmazta ezt a módszert már évekre visszamenőleg. Bizonyos munkahelyeken stabilan 3-4 napra szűkítették az irodai jelenlétet, de találkozhatunk dinamikusan szabályozott munkarenddel is. A motiváció tiszta és világos, a magas irodabérleti árak és az ezzel járó rezsiköltségek miatt költséghatékonyabb volt így szervezni a munkát és a munkatársak rengeteg időt spórolhattak meg a napi ingázás hiányában. A hazai kkv szektorban számos cég otthonról végzi az adminisztratív feladatait, egyáltalán nem tart fent irodát. Ugyanakkor léteznek olyan munkák, amelyeket egyáltalán nem lehetséges otthoni környezetből elvégezni.

A COVID-19 vírus miatt kialakult járvány óvintézkedései hozták el a home office tömeges megjelenését hazánkban és számos más országban, hiszen logikus és kényszerű döntésként így lehetett a leginkább csökkenteni a vírus terjedésének elsődleges módját, az emberi kontaktusok számát. Ugyanakkor, nemcsak a cégek, hanem az oktatási intézmények is kénytelenek voltak bezárni kapuikat, ezzel jelentős többlet terhet róva az aktív korú szülőkre. A teljes képhez figyelembe kell venni, hogy a járványhelyzet a digitális transzformáció közepére érkezett meg, mely számos lehetőséget biztosított számunkra a járvány időszak átvészelésére. Jelenleg a már bevált és megbízható analóg módszereket, eszközöket még nem tudjuk elengedni, még jelentősen függünk tőlük és támaszkodunk rájuk, mindeközben érezzük a folytonos javulási, megújulási kényszert, amely a hatékonyságnövelés és az átláthatóság irányába terel. Ezt a transzformációs időszakot gyorsította fel tulajdonképpen a COVID-19-es válság. Szerencsére mára már mindenki számára elérhető a digitális aláírás, a prompt utalás, a NAV adatszolgáltatása, E-papír, arc alapján történő azonosítás, mobilbankolás és hasonló innovatív technológiai megoldások. A tech cégek évről évre új megoldásokkal ismertetnek meg bennünket, amelyeket a hadiipar, a hírszerzés vagy az űrkutatás területéről „szelídítenek” meg a polgári felhasználás számára. Folyton keressük, tanuljuk és részben már alkalmazzuk az új és hatékony digitális technológiára építő megoldásokat. Nehezíti az együttműködést és a kommunikációt, hogy jelentős eltérések azonosíthatók az egyes szervezetek digitális érettségi szintje között. A nem technológiaorientált nagyvállalatok, tehetetlenségüknél fogva lassabban képesek követni a változásokat, míg a megjelenő informatikai startup-ok (LogMeIn, Prezi) elképesztő világsikereket könyvelhetnek el.
A digitális transzformációval párhuzamosan említést kell tennünk az „ipari forradalom 4.0”-nak nevezett jelenségről, amelyet a hatékonyságnövelés, kontrollálhatóság és automatizálás motivációja mentén hívtak életre az iparági szereplők. Az ipari eszközök 20–30 éves életciklussal működnek, ami előre vetíti, hogy a jelenleg használt gépek között találni nemritkán 10–15 évnél is idősebbet. A „forradalom” fő célja, hogy az ipari környezetben

használt termelésirányító eszközök valós időben szolgáltassanak adatokat működésükről, ilyen módon a megalapozott információkra támaszkodva születhetnek meg az irányítással kapcsolatos döntések. Nem túlzó azt állítani, hogy két világ összekapcsolásának lehetünk tanúi, ami komoly kihívás elé állítja a szakembereket.
A digitális transzformáció az ipar 4.0 és IOT[1] eszközök elterjedése a szakemberek oldaláról is szorosabb együttműködést követel meg. A jogi és pénzügyi terület folyamatait egyre inkább informatikai rendszereken keresztül bonyolítják a szakemberek, digitális aláírás segítségével már távolról is lehetséges a szerződéskötés, a számlákat már elektronikus úton továbbítják, a NAV rendszere fogadja a kibocsátott számlák adatait. Az erősödő interdiszciplináris együttműködés igénye új szakmákat fog teremteni, melynek szakértői képesek lesznek átlátni a folyamatok egészét és illeszteni tudják az üzleti igényekhez a modern technológiákat. A BI[2] elemzők, a SOC operátorok és a robotika szakértői testesítik meg az ily módon létrejövő új tudományágak első szereplőit.
Az ilyen horderejű átalakulások közben a rendszerek kevésbé képesek tolerálni a nem várt változásokat (COVID-19), mint amikor kiforrott, nyugvóponton lévő folyamatok mentén működnek. A járvány egyvalamivel nagyon könyörtelenül bánik és ez nem más, mint az idő. Nem lehet még két hónap haladékot kérni, nincs türelmi zóna, nem lehet még további teszteket és ellenőrzéseket futtatni, kész tények vannak, amelyekhez mindenkinek alkalmazkodnia kell, válogatás nélkül, azonnal. A járvány azonban nem tarthat örökké, hamarosan a gyógyszercégek megalkotják a megfelelő védőoltást és megszűnik a kitettség, de a digitalizációs átállásnak folytatódnia kell tovább.

1. Home office informatikai szemszögből

Az informatikai rendszerek felkészültek a helyfüggetlen munkavégzés lebonyolítására. Napjaink igényeit teljesítő védelmi rendszerek már több éve rendelkezésre állnak, maximum a használatuk vált egyszerűbbé, gördülékenyebbé. Ilyen megoldás például a VPN is, amelynek a segítségével biztonságos kapcsolat építhető ki a központ infrastruktúrájával. A végponti eszközökön kezelt adatok ma már számos módon védhetőek meg, például helyi titkosítással, jogosultságkezeléssel és adatszivárgás megelőző rendszerekkel. Az anyagi tényezők jelenthetnek valamelyest akadályt, hiszen a jól megtervezett védelmi rendszer komoly szakértelmet és folyamatos figyelmet igényel, aminek jelentős költségvonzata van. Ezért fontos, hogy a védelem kockázatarányosan kerüljön kidolgozásra, hogy ne jelentsen felesleges költségeket. Az ISO 27001 szabvány alapján felépített biztonsági rendszerek például mindig a kockázatarányos védelem megvalósítására törekszenek, ezzel is észszerű keretek közé szorítva az intézményre háruló pénzügyi terheket. Költségvetési oldalról szemlélve, jó megoldást nyújthatnak az egyre népszerűbb felhő alapú megoldások. Adatvédelmi oldalról jelentkezhetnek további biztonsági igények a felhő alapú adatkezeléssel kapcsolatban, lévén, hogy a legnagyobb szolgáltatók amerikai cégek és nincs egyenszilárd jogi kontroll a két kontinens között.

2. Üzleti folyamatok

[1] IOT – Internet of things – Hálózatba kötött szenzorokat jelent, amelyek adatokat szolgáltatnak kiterjedt, heterogén rendszerek működéséről, ezzel támogatva az automatizálási és felügyeleti törekvéseket.
[2] Business Intelligence – üzleti intelligencia. Döntéstámogató, hatékonyságnövelő módszereket és eszközöket tömörítő gyűjtőnév. Az új technológia a nagy mennyiségű adatok feldolgozásában és célzott elemzésében jelenik meg (Big Data).

Az informatikai rendszerek fő feladata, hogy az üzleti tevékenységeket támogassák, tehát ún. kiszolgáló szerepet töltenek be. Természetesen részben kivételt képeznek ez alól azok az informatikai vállalkozások, ahol maga a termék vagy szolgáltatás szorosan kapcsolódik az informatikához. Azért csak részben számítanak kivételnek, mert ezen cégeknél is informatikai rendszer támogatja a klasszikus területeket, mint a pénzügy, a munkaügy, a jogi adminisztráció, a kereskedelem, a beszállítói kapcsolattartás, a beszerzés, így a biztonságos és stabil IT szolgáltatás nekik is kiemelt fontosságú.
Az otthoni munkavégzéssel kapcsolatos kérdések alapos vizsgálatához első körben egy picit el kell távolodni az informatikától. Az üzleti folyamatok és tulajdonságaik, illetve a velük szemben támasztott elvárások oldaláról kell megfogni a kérdést. Minden cég tudatosan vagy szokásjog alapján, de folyamatok mentén működik. Egy érett és felkészült szervezet képes felmutatni az átgondolt és dokumentált folyamatait, amelyeknek felelőse, eleje, vége, eredményterméke, célja, határideje, kezelt adatköre, tisztázott függési viszonyai és erőforrásigényei vannak. Első pillantásra túlzónak tűnhet egy tevékenységhez fűződő ilyen méretű dokumentációs igény, ám az első komolyabb incidens vagy működési anomália esetén, minden befektetett munka busásan megtérül. *A dokumentált üzleti folyamatok jelentik az alapját minden további lépésnek.*
A home office-szal járó érdemi változások alapos áttekintéséhez vizsgáljuk meg az irodai környezetben történő munkavégzést és az ahhoz kapcsolódó feltételeket, majd mindezt áthelyezve az otthoni környezetbe egyértelművé válik, hogy mely feltételeket szükséges módosítani, fejleszteni.
A tevékenységgel kapcsolatban meghatározható azon erőforrásigények összessége, amelyek elengedhetetlenek a zavartalan működés biztosításához. Egy irodai környezetben végzett könyvelési tevékenységet alapul véve, szükséges maga az iroda, amely biztosítja az időjárás viszontagságaitól mentes környezetet, továbbá helyet ad íróasztalnak, széknek, amelyek biztosítják a munkatárs ergonomikus munkakörülményeit. Szükséges egy iratszekrény, amely a még nem digitalizált tevékenységgel járó papírok tárolását biztosítja. Az asztalon elhelyezhető egy számítógép, amely futtat egy operációs rendszert, egy levelező klienst és egy könyvelő alkalmazást, mindemellett csatlakozik a világhálóra, hogy biztosítsa az elektronikus levelezést és weboldalak segítségével lekérdezhessenek adatokat vagy ezen keresztül vegyenek igénybe szolgáltatásokat. A legfontosabb erőforrás maga a munkatárs, aki szakmai ismeretei birtokában, képes a rendszerek segítségével előállítani az üzleti értékeket.
A fenti példát informatikai, IT biztonsági szemmel megvizsgálva az alábbi erőforrásigények azonosíthatók:
– Az irodai beléptető rendszer távol tartja a jogosulatlan embereket, így csökkenti az adathalászat és a lopás lehetőségét. Nyomon követhetők a munkatársak, hogy mikor tartózkodnak az irodában.
– Az épülethez tartozó erőforrásigényként merülhet fel a szünetmentes áramellátás és a klimatizált levegő igénye is.
– Az iratszekrény és az iroda együttesen tudja szavatolni a tűzvédelmet és az üzletileg kritikus papírok fizikai védelmét.
– Az irodai infrastruktúra biztosítja az internetelérést, amely megfelelő hálózati védelmet és szeparációt biztosít a kliensek számára. Igény lehet a folyamatos internetelérésre, ezért alternatív kapcsolatok (4G modem) kiépítése lehet indokolt. Ajánlott szeparálni az eltérő munkaterületeket és a vendég wifi szegmenst.
– Szükség lehet az incidens detektáló képességre, amely log elemzéssel, monitoring rendszerekkel és adatszivárgás megelőző eszközökkel valósítható meg.
– A számítógép rendelkezésre állása megfelelő támogatási szerződésekkel vagy csereeszközök raktározásával biztosítható.

– Az operációs rendszer működését helyes jogosultságkezeléssel, rendszeres gyártói frissítéssel, vírusirtó telepítésével és rendszeres mentés-archiválással tudjuk szavatolni.
– A helyben telepített alkalmazásokat (pl. könyvelő program) gyártói frissítések rendszeres telepítésével, indokolt esetben tesztkörnyezetben elvégzett előzetes vizsgálatokkal és napi mentés-archiválás segítségével tudjuk biztonságosan üzemben tartani.
– A munkatársakat folyamatosan képezve lehet fenntartani a tudatos, biztonságos és hatékony munkavégzést.
A fenti példát üzleti szemmel vizsgálva az alábbi igények fogalmazhatók meg:
– A munkának folyamatosnak kell lennie, minden leállás pénzben kifejezhető veszteséget okoz.
– Az ágazati jogszabályokban meghatározott határidőket mindenáron tartani kell, mert a késések büntetést vonnak maguk után és az ügyfelek elpártolhatnak.
– Maradéktalanul eleget kell tenni az adatvédelmi elvárásoknak, a szenzitív adatokat meg kell védeni.
– A valós immunitást valósítsuk meg a cybertámadásokkal szemben.
– Meg kell lovagolni a modern technológiák által nyújtott előnyöket (adatelemzés, gépi tanulás, digitális aláírás, folyamatvezérlés, automatizálás).
– Folyamatosan optimalizált költségstruktúrával kell megvalósítani a feladatokat.
– Minden tevékenységnek legyen egyértelmű felelőse.
A fenti két nézőpont metszeteként kirajzolódik egy hármas kritériumrendszer, amelyek a bizalmasság, a sértetlenség és a rendelkezésre állás köré csoportosulnak (angolul a három szót leírva a „CIA” mozaikszót kapjuk: Confidentiality, Integrity, Availability). Ez a három paraméter jellemezhet egy rendszert, egy konkrét információt vagy akár egy folyamatot is. A nemzetközi ajánlások és szabványok 5 szintű skálával dolgoznak, ahol az 5-ös érték a legerősebb védelmet jelenti, az 1-es érték pedig a leggyengébbet.
A *bizalmasság értéke* határozza meg, mennyire kell védeni az illetéktelen betekintésektől az adatokat. Nehezíti a dolgot, hogy az adatok sértetlensége az időben mozogva más-más értéket vehet fel. Egy versenytárgyalás során leadott árajánlat tartalma az eredményhirdetésig a legmagasabb értéken szerepel, azaz szigorúan titkos, majd az eredményhirdetést követően, akár publikálásra is kerülhet ezzel a legalacsonyabb bizalmassági értéket magára öltve.
A *sértetlenségi-integritási érték* tekintetében a véletlen vagy szándékos adatmódosítással szembeni védelem erősségét határozzuk meg. Például az egészségügyi rendszer nyilvántartja a betegek adatait, köztük a vércsoportjukat is, amennyiben ez az adat „megsérül”, esetleg valaki véletlenül átírja, az a páciens életébe is kerülhet. A könyvvizsgálati tevékenység egy pénzügyi integritás vizsgálat, amely a számviteli adtok nem kívánt „kozmetikázását” hivatottak felderíteni.
Rendelkezésre állási érték meghatározása során az adat elérhetőségének fontosságát rangsoroljuk. A havi áfabevallás elkészítése nem valósulhat meg a számviteli bizonylatok hiányában (rendelkezésre állása nélkül). Informatikai szemszögből például a zsarolóvírusok az adatok rendelkezésre állását támadják, így akarnak váltságdíjat kikényszeríteni.
Le kell szögezni, hogy a fenti védelmi elvárások szintjét az üzleti terület határozza meg, amelyeket az informatikai rendszernek kell megvalósítania, biztosítania technológiai megoldásokkal. Az informatikai terület – ismerve saját képességeit és szolgáltatási lehetőségeit – igyekszik eleget tenni az elvárásoknak, de a legtöbb esetben alulmúlja az igényeket. Magas pénzügyi terhek, a tudatos fejlesztések és szakmai ismeretek hiánya húzódhat meg az eltérések mögött.

3. Kockázatarányos védelem

Korábban már említésre került a *kockázatarányos védelem*. Ezen elv mögött az a tudatos döntés-előkészítő munka húzódik meg, amely a fentiek szerint azonosítja az üzleti igényeket, majd feltárja az informatikai rendszer aktuális képességeit és számba veszi azon fenyegetettségeket, és hiányosságokat, amelyek esetében fennáll a lehetőség, hogy kárt okozhatnak a működésben.
Az informatikai külső és belső fenyegetések feltárására sérülékenység vizsgálatokat lehet végezni. Az ellenőrzés célja, hogy azonosítsa azokat a gyenge pontokat, amelyeket támadva rendellenes működés, szolgáltatáskiesés idézhető elő. A tesztek történhetnek technológiai síkon, etikus hacker-ek bevonásával vagy emberi oldalról, amikor a munkatársak jóhiszeműségére hatva kísérelnek meg adatokat vagy információkat szerezni. Az informatikai vizsgálatokat érdemes minimum évente elvégeztetni, mert a technológia fejlődése és a heti rendszerességgel publikált szoftverhibák, valamint a szervezeten belüli változások indokolttá teszik. A sérülékenységvizsgálatok során javasolt figyelmet fordítani a következőkre:
– A rendszereket alkotó komponensek a legfrissebb szoftververzióval működnek.
– A rendszerek biztonsági beállításai csak a legszükségesebb funkciókat, kapcsolatokat engedélyezik.
– A rendszerekhez csak a munkavégzéshez elengedhetetlen munkatársaknak van hozzáférése.
– A felhasználói jelszavak elég hosszúak (8–12 karakter) és komplikáltak (kis betű, nagy betű, szám, speciális karakter) és megfelelő időközönként változtatva vannak (max. 3 havonta).
– Minden felhasználó egyedi bejelentkezési – autentikációs paraméterekkel bír.
– Az előző vizsgálat óta bekövetkezett változások megfelelően lettek kezelve.
– Detektált incidensek kivizsgálása, hasonló esetekkel szemben felkészült a rendszer.
– Adathalász leveleket és gyanús igényeket képesek a munkatársak azonosítani.
Az előbbiekben említett szempontok szerint elvégzett vizsgálatoknak köszönhetően minden adat a rendelkezésre áll, hogy elvégezhető legyen a *kockázatelemzés*.
Az adott fenyegetés előfordulási valószínűsége és bekövetkezése esetén, annak károkozási képessége adja meg a kár értéket. Mindkét paramétert egy 5-ös skálán elhelyezve értékkel ruházhatok fel, majd a kapott értékek szorzata adja az eredményt. Tehát egy ritkán előforduló esemény, amely kis károkozással bír, várhatóan 1–2-es értéket fog felvenni, ám egy ritkán bekövetkező esemény, amely kiemelkedő kárt képes okozni a rendszerekben, már 5–10-es értékkel fog szerepelni az elemzésben.
A felmért kockázati értékek birtokában el tudjuk dönteni, melyek a legsúlyosabb kockázatok, amelyek elhárítására mielőbbi védelmi intézkedéseket kell bevezetni.

4. Védelmi intézkedések

A fenyegetések sokszínűsége indokolja, hogy minden felületen képes legyen megvédeni magát a szervezet. Az ajánlások három fő csoportba sorolják a védelmi intézkedéseket:
– Fizikai – beléptetés, betörésvédelem, látogató kezelés, zavartalan áramellátás, tűzvédelem, vízbetörés, karbantartás.
– Adminisztratív – szabályozás, kockázatelemzés, beszerzés, üzletmenet-folytonosság, incidens kezelése, személybiztonság, tudatosítás.
– Logikai – Tervezés, tesztelés, konfigurációkezelés, karbantartás, adathordozók védelme, azonosítás, hozzáféréskontroll, rendszerfelügyelet, naplózás.

Az állami és önkormányzati szervekre már 2015-ben megalkotta a törvényalkotó a 41/2015. (VII. 15.) BM rendeletet,[3] amelynek a 4. mellékletében található a védelmi intézkedés katalógus, ami háromszáznál is több intézkedést definiál. Természetesen csak azon védelmek kiépítése javasolt, amelyeket az adott szervezet méretei és tevékenysége indokol.
Az otthoni munkavégzéssel kapcsolatban a leghasznosabb védelmi technológiák:
– PKI – Public key infrastructure és Digitális aláírás, hitelesített időbélyeg
A digitális világ legnehezebb feladata azonosítani valakit, akivel csak elektronikus úton érintkezünk. Hitelesítésszolgáltatók segítségével orvosolható a probléma. A rendszer úgy épül fel, hogy egy személyes találkozó alkalmával meggyőződik a szolgáltató az ügyfél személyazonosságáról, majd kibocsát egy tanúsítványt, amelyben garantálja a személy digitális azonosságát. Az időbélyeg-szolgáltatás pedig az egyes tranzakciók időbeliségét igazolja.
– VPN – Virtual Private Network – virtuális magánhálózat
Egy hálózati technológia, ami biztonságos kapcsolatot létesít egy nyilvános hálózaton (mint az internet) keresztül. Titkosítás segítségével sérthetetlen adatátvitelt biztosít két rendszer között. Kiépíthető ilyen kapcsolat egy mobiltelefon, egy notebook, egy telephely és a cég központi rendszere között. Az internetszolgáltatók is kínálnak ilyen kapcsolatokat, ám azok merőben eltérő technológián alapszanak, de az elv ugyanaz. A titkosított kapcsolatok működtetése jelentős számítási kapacitást emészt fel, ezért az egyidejűleg nagy számú kapcsolat, céleszköz beszerzését igényelheti, VPN koncentrátorként hivatkoznak rá a szakemberek.
– MDM – Mobile Device Management – mobilflotta menedzsment
Mobiltelefonokra, tabletekre és PC-kre is telepíthető védelmi szoftver, amely technológiai megoldásokkal biztosítja a magán és a céges tevékenységek elkülönítését, méghozzá úgy, hogy külön azonosítással enged hozzáférést a céges védett adatokhoz, illetve támogatja az adatok titkosított tárolását.
– HTTPS – Titkosított webszolgáltatás
Web felületen egyre gyakrabban kommunikálunk szenzitív adatokat, ahol elvárás a kommunikáció titkosítása, ilyen esetekben használandó a https protokoll. A pénzintézetek által működtetett oldalak ma már kivétel nélkül így nyújtják a szolgáltatásaikat.
– Erős azonosítás
Három faktor alapján lehetséges azonosítani egy természetes személyt a digitális világban:
= Vagyok valaki – biometrikus adatok, ujjlenyomat, arc, írisz, érhálózat, hang.
= Van valamim – egyszer használatos jelszavak, belépőkártya.
= Tudok valamit – pin kód, felhasználói név/jelszó.
Legalább két faktor kombinált használata esetén beszélhetünk erős azonosításról. A netbank felületre történő bejelentkezéskor, első faktorként név/jelszó párost helyesen megadva, sms-ben érkezik a második faktor, amelyet begépelve a megfelelő helyre megtörténik az azonosítás. Indokolt több kommunikációs csatornán végezni az azonosítást, mert az egyik lehallgatása révén még nem lehetséges ellopni a bejelentkezést.
– DLP – Data Loss Prevention – Adatszivárgás-megelőzés
Két nagy csoportja ismert: a tartalom alapján és a tárhely alapján védelmező megoldások. A tartalom alapú megoldások jellemzően a vírusirtó gyártók kínálatában találhatóak meg, mivel nagyon hasonló „motorok” segítségével detektálják a keresett tartalmakat. Nagyon drága megoldások, és robosztus háttértámogatást és erőforrásokat igényelnek. Minden

[3]Az állami és önkormányzati szervek elektronikus információbiztonságáról szóló 2013. évi L. törvényben meghatározott technológiai biztonsági, valamint a biztonságos információs eszközökre, termékekre, továbbá a biztonsági osztályba és biztonsági szintbe sorolásra vonatkozó követelményekről szóló 41/2015. (VII. 15.) BM rendelet.

dokumentumot feldolgoznak, komplex logika alapján lenyomatokat készítve belőle, hogy képesek legyenek megállítani igény esetén a védendő adatokat. A tárhely alapú megoldások ezzel szemben sokkal egyszerűbb döntéshozatali logika alapján működnek: melyik mappából, milyen fájlt, melyik felhasználó, mikor, milyen művelettel (olvasás, törlés, módosítás, másolás), milyen célterülethez szeretne hozzáférni. Az ilyen rendszerek olcsóbbak és jelentősen kisebb erőforrást igényelnek, hiszen a védelmi mechanizmusuk sokkal takarékosabb elv szerint működik.

– Log elemzés

Minden rendszerkomponens (operációs rendszer, adatbázis, alkalmazás) saját naplórendszere segítségével rögzíti működésének minden pillanatában a bekövetkezett események adatait. A keletkezett napló adatok összegyűjtése és kielemzése segítségével lehetséges biztonsági incidenseket detektálni. Napló adatokra támaszkodva mutatható ki például, ha egy munkatárs nincs az irodában a beléptető rendszer adatai alapján, de a belső rendszerbe belépési kísérlet történik az adott kolléga fiókjába, akkor arról egyértelműen értesíteni kell a biztonsági részleg munkatársait és természetesen blokkolni kell az adott kliens belépését.

– SOC – Security Operations Center – Kiberbiztonsági műveleti központ

Szolgáltatásként elérhető biztonsági incidensdetektáló képesség, amely azonosítani tudja a szervezetben bekövetkezett működési anomáliákat és értesíteni tudja az illetékes szakembereket. Fejlettebb megoldások esetén automatikusan képes válaszlépések megtételére. Jellemző, hogy preventív módon képesek jelezni a várható fenyegetéseket, hogy fel lehessen rájuk készülni.

– Personal Firewall – Személyes tűzfal

Az operációs rendszerre telepített speciális biztonsági alkalmazás, amely többlettudással (VPN kliens, vírusirtó, központi felügyelet és menedzsment) ruházza fel az eredeti védelmi képességeket. Jellemzően a vírusirtógyártók együtt kínálják virológiai és határvédelmi megoldásként.

– Háttértár titkosítása

Minden számítógép futtatható operációs rendszerének a részét képezi egy beépített háttértér-titkosítási képesség, amelyet érdemes alkalmazni. A kliensek véletlen elvesztése, szándékos eltulajdonítása vagy szervizbe adás esetén ez megvédi az eszközön tárolt adatokat. Indokolt esetben lehetőség van további titkosítás alapú védelemre, amikor egy könyvtárat egyedi kulcs segítségével extra védelemmel ruházunk fel. Ennél az eljárásnál kiemelt figyelmet kell fordítani a kulcskezelésre, mert a titkosított állományok visszaállítása nem lehetséges a megfelelő kulcs hiányában.

– Titkosított külső adathordozó

A szenzitív adatok továbbítása esetén jelenthet megoldást ez a speciális eszköz. Elérhető pendrive és külső HDD formájában. Minden rámásolt adat titkosítva tárolódik és feltörés esetén képesek fizikailag is megsemmisíteni a tárolt adatokat.

– Vírusirtó

Kémprogramok, zsaroló vírusok, erőforrástolvajok elleni védelmet valósítanak meg gyártói terjesztésű minták segítségével. Az ilyen működési modellek esetén a vírusirtó csak azokat a káros programokat képes megállítani, amiről van leírása, ezért nagyon fontos, hogy a vírusirtónkra mindig töltsük le a legújabb frissítéseket. A zsarolóvírusok megjelenésekor egy-két hetes késéssel tudtak csak reagálni a gyártók, addig nem tudtak valós védelmet biztosítani. A fejlettebb vírusirtók viselkedés alapú vizsgálatokat is képesek elvégezni, viszont az nagyobb erőforrást is emészt fel.

5. Home office előkészítése

Üzleti síkon megragadva a kérdést azonosítani kell azon feladatokat, folyamatokat, amelyek végezhetők részben vagy akár teljes mértékben otthoni környezetből. A vizsgálatnak ki kell térnie rá, hogy képes az otthoni környezet eleget tenni az előzetesen meghatározott bizalmassági, sértetlenségi és rendelkezésre állási kritériumoknak. Abban az esetben, ha eltérések mutatkoznak, mert a kommunikációs kapcsolat nem kielégítő, a fizikai biztonsági követelmények csak részlegesen teljesülnek vagy a logikai védelmek nem valósulhatnak meg maradéktalanul, akkor kompenzáló kontrollok kiépítésével lehetséges fokozni a védelem szintjét. Az otthoni környezetben javasolt nagyobb hangsúlyt fektetni a logikai és adminisztratív védelmekre, mert azok távolról jobban felügyelhetők, kikényszeríthetők. Érdemes megvizsgálni az átszervezést költség-haszon elemzés oldaláról is, hiszen a kompenzáló kontrollok kialakítása és működtetése akár magasabb költséggel is járhat, mint az eredeti állapot fenntartása. Figyelembe kell venni, hogy a távoli munkavégzés indokolhatja videó kommunikációs, fájlmegosztó rendszerek fejlesztését is, ami növelheti a költségeket.

6. Az ideális home office környezet

A megalapozott üzleti döntést követően megvalósítható az otthoni munkavégzés előkészítése. A következő cselekvési terv egy ajánlás, amely törekszik a legteljesebb kontrollt és védelmet megvalósítani az informatikai és IT biztonsági eszközök felhasználásával. Valós körülmények között a szervezetre értelmezhető és kockázatarányos védelmek megvalósítása javasolt.
A távmunka *infrastrukturális feltételeit* az alábbi kritériumok mentén elő kell készíteni:
– A központi informatika rendszerét fel kell készíteni a megnövekedett külső kapcsolatok fogadására.
– A távmunkában érintett üzleti folyamatok rendelkezésre állási elvárását teljesíteni kell a kiszolgáló rendszereknek is és gondoskodni kell ezen rendszerek felügyeletéről.
– Elő kell készíteni a távmunka technikai feltételeit mindkét oldalon, titkosított kapcsolat, erős azonosítás, határvédelem, felügyelet.
– Amennyiben az otthoni tevékenység ellátása igényli a publikus felhő szolgáltatások használatát (videókonferencia, fájlmegosztás és csoportmunkatámogatás), törekedni kell az egyenszilárd védelmek fenntartására. Javasolt a központi rendszeren keresztül igénybe venni az ilyen szolgáltatásokat.
A szervezet működési és biztonsági *szabályzatait* ki kell egészíteni az új helyzetet lefedő fejezetekkel, amelyekben meghatározásra kerülnek a következők:
– a távmunkavégzést hogy értelmezi a szervezet, milyen feltételeket támaszt a megvalósulásához;
– a távmunkában elvégezhető tevékenységek körét;
– a kívülről elérhető rendszereket és az azokon kezelt adattípusokat;
– mely szerepkört ellátó munkatársak végezhetnek távmunkát;
– távmunka igénylésének/visszavonásának folyamata, felelőse, módja;
– távmunka adminisztráció módja, helye, felelőse;
– távmunka során indokolt kiegészítő kontrollok mibenléte eszköztípusonként, erős azonosítás, adatkezelési eljárások, tevékenység felügyelet, titkosítás, MDM;
– jóváhagyott eszközök listája;
– eszközök igénylése és nyilvántartásának módja, helye, felelőse;
– otthoni környezettel szembeni elvárások;
– munkatárstól elvárt viselkedési norma;
– tartós távmunka esetén az eszközök meghibásodásának, karbantartásának kezelése;
– eszközök elvesztésének kezelése;
– papír alapú ügykezelés, tiltása-engedélyezése, feltételei.

A biztonsági elvárásokat kizárólag saját felügyelet alatt álló eszközökön lehet megvalósítani. Az elmúlt években kezdett el terjedni a BYOD[4] szemlélet, mely felkínálja azt a lehetőséget, hogy a munkatárs a magán eszközén keresztül (telefon, laptop stb.) végezheti a munkáját, fér hozzá a munkahelyi adatokhoz, rendszerekhez, anyagokhoz. Ez a megoldás biztosan gördülékenyebbé teszi az ügykezelést, de komoly áldozatot és kockázatot jelent a biztonság oltárán. Természetesen a fent már említett MDM megoldásokkal kiegészítve fokozható a biztonság, de figyelembe kell venni, hogy ez további költségekkel járhat.
Távmunka során *használható eszközökkel kapcsolatban figyelni kell a következőkre*:
– A munkavégzéshez használt eszköz legyen a cég tulajdonában és képes legyen a cég teljes mértékben felügyelni, menedzselni azt. Az ellátott tevékenység biztonsági elvárásaival párhuzamosan bevonható a dolgozó eszköze is a munkavégzésbe, azonban ilyen esetekben javasolt MDM-rendszer használata. Az eszköz kompromittálódása esetén a munkatárssal tisztázni érdemes, hogy a cég távolról blokkolhatja vagy akár le is törölheti az eszközön tárolt adatokat. Itt fontos megemlíteni, hogy csak a fejlettebb (és drágább) MDM-rendszerek képesek a védendő adatok célzott megsemmisítésére úgy, hogy nem teszik használhatatlanná a készülékeket.
– Az eszköz legyen képes biztonságos kapcsolat kiépítésére a céges rendszerrel. Indokolt esetben, technikailag és szabályzatba foglalva meg kell akadályozni, hogy más kapcsolatokat is kiépíthessen az eszköz (internetkávézók, egyéb publikusan elérhető hálózatok). A nem otthoni környezetből történő kapcsolódási igény esetén a cég által biztosított mobil adatátviteli eszköz használata javasolt.
– Ki kell kényszeríteni a rendszer használata során a felhasználó azonosítását, ideális esetben a céges jogosultságkezelő rendszerrel szinkronban.
– Az adatok helyben történő tárolását (lokálisan magán a számítógépen és adattárolókon) lehetőség szerint kerülni kell, amennyiben ez nem lehetséges, a tárolási titkosításról gondoskodni kell.
– Az eszközökön csökkentett jogosultságú felhasználói profillal tudjon dolgozni a munkatárs. Kerülendő az adminisztrátori jogosultság.
– Csak a cég által jóváhagyott szoftverek legyenek telepíthetők az eszközökre, blokkolni kell minden további nem engedélyezett alkalmazás telepítését és futtatását egyaránt.
– Gondoskodni kell az összes szoftverkomponens (operációs rendszer, alkalmazások, driverek, védelmi rendszerek adatbázisa) folyamatos frissítéséről.
– Az eszközökre helyi tűzfalszoftvert javasolt telepíteni, amely kikényszeríti az előzetesen beállított hálózati védelmeket.
– Adatszivárgás megelőző funkciót javasolt kialakítani az eszközökön, amely a titkosítással védett területről nem engedi kimozgatni a szenzitív adatokat. Blokkolni képes a nyomtatást, a külső adathordozóra való másolást vagy a cégen kívüli levelezésbe illesztést.
– A külső adathordozók csatlakoztatását lehetőség szerint blokkolni kell már az operációs rendszer szintjén. Indokolt esetben a cég által jóváhagyott, lehetőleg titkosított adathordozó használata javasolt.
– A felügyelet hatékonysága miatt gondoskodni kell az eszközök idejének szinkronizálásáról.
– Blokkolni kell a közösségi média oldalakat, a webmail szolgáltatókat, fájlmegosztó oldalakat, mert fokozott adatszivárgási kockázatot jelentenek.
A technológiai felkészülésen túl, kiemelt figyelmet kell fordítani az otthoni fizikai környezet kialakítására a következők szerint:

[4] Bring Your Own Device – a dolgozó saját eszközei segítségével eléri a céges erőforrásokat, levelezés, filemegosztás.

– Tevékenység kockázatától függően, az otthoni munkavégzés zárható helyiségben történjen, a munkaterületre történő közvetlen rálátás akadályozásával, telefonbeszélgetés kihallgatásának védelmével.
– Az eszközök nem hagyhatók őrizetlenül (autóban, hotelszobában), azonnal zárolni kell, amint a személyes felügyelet megszűnik. Nem szabad átengedni a használatot a családtagoknak sem.
– Az erős azonosításhoz használt eszköz(öke)t szeparáltan kell tárolni, biztonságos helyen.
– Az otthoni hálózat biztonságát a lehetőségekhez képest meg kell erősíteni.
– Az adathordozók védelméről használaton kívül is gondoskodni kell, el kell zárni a biztonsági előírásoknak megfelelően.
– Tájékoztatni és képezni kell a felhasználót a megváltozott körülményekről, és az abban alkalmazandó speciális szabályokról, elvárásokról.
– A bekövetkezett incidenseket haladéktalanul jelenteni kell.

7. A távmunkavégzés jogi aspektusai

2020. március 11. napján megváltozott az élet körülöttünk a vészhelyzet kihirdetéséről szóló 40/2020. Korm. rendelettel, amit rövidesen kijárási korlátozások követtek, majd megjelentek a veszélyhelyzethez történő alkalmazkodást célzó kormányrendeletek, amelyek változtattak a munkajogi, adatvédelmi szabályokon is. Ezen gyors ütemben jelentkező változások, illetve maga a szokatlan élethelyzet váratlan, és sok esetben megoldhatatlan kihívások elé állították a vállalkozásokat, s más foglalkoztatókat. Sejteni lehetett azt is, hogy a szabályok nem csupán átmeneti jellegűek, lehetséges, hogy évekig együtt kell tudnunk élni a folyamatosan változó szabályokkal és problémákkal. Az alábbiakban a téma aspektusait mutatjuk be azzal, hogy rövidesen e területtel összefüggésben újabb változása várható a Munka Törvénykönyvéről szóló 2012. évi I. törvénynek (a továbbiakban: Mt.), az adatbiztonság területéhez kapcsolódóan pedig a Magyar Nemzeti Bank is ajánlással készül. Mindennek tetejében az sem zárható ki, hogy időközben a romló járványügyi adatok a kormányzatot újabb, egyoldalú változtatásokra is fogja ösztönözni. Lássuk akkor a helyzetet most:

7.1. A távmunkavégzés alapvetően munkaszerződés-módosítást igényel

Az Mt. 196. § (1) bekezdése szerint a távmunkavégzés a munkáltató telephelyétől elkülönült helyen rendszeresen folytatott olyan tevékenység, amelyet számítástechnikai eszközzel végeznek és eredményét elektronikusan továbbítják. Fontos tehát leszögeznünk, hogy a távmunkavégzés és az otthoni munkavégzés (home office) nem azonos fogalmak. Távmunkavégzés esetében a feleknek a munkaszerződésben meg kell állapodni a munkavállaló távmunkavégzés keretében történő foglalkoztatásában. A munkaviszony létesítésekor a munkavállaló számára nyújtott foglalkoztatói tájékoztatást pedig ki kell egészíteni azzal, hogy hogyan történik a munkáltató általi ellenőrzés, melyek a számítástechnikai vagy elektronikus eszköz használata korlátozásának szabályai, továbbá meg kell nevezni azt a szervezeti egységet, amelyhez a munkavállaló munkája kapcsolódik. A munkáltató a távmunkát végző munkavállalónak minden olyan tájékoztatást köteles megadni, amelyet más munkavállalónak biztosít. Az Mt. azt is rögzíti, hogy a munkáltató utasítási joga – eltérő megállapodás hiányában – kizárólag a munkavállaló által ellátandó feladatok meghatározására terjed ki. Ami a munkáltató ellenőrzésének módját illeti, a munkáltató jogosult megállapítani az ellenőrzés módját és a munkavégzés helyeként szolgáló ingatlan területén történő ellenőrzés esetén annak bejelentése és megkezdése közötti legrövidebb tartamot. Az ellenőrzés ugyanakkor nem jelenthet a munkavállaló, valamint a munkavégzés helyeként szolgáló ingatlant használó más személy számára aránytalan terhet.

7.2. Fő szabályként a munkarend kötetlen

Az Mt. alapvető szabálya, hogy a munkaidő-beosztás szabályait (munkarend) a munkáltató állapítja meg. A munkáltató a munkaidő beosztásának jogát – a munkavégzés önálló megszervezésére tekintettel – a munkavállaló számára írásban átengedheti (kötetlen munkarend). A munkarend kötetlen jellegét nem érinti, ha a munkavállaló a munkaköri feladatok egy részét sajátos jellegüknél fogva meghatározott időpontban vagy időszakban teljesítheti. Távmunkavégzés esetében az Mt. 196. § (5) bekezdése alapján a munkavállaló munkarendje kötetlen. Ez azonban csak abban az esetben áll fenn, amennyiben a munkáltató a munkaidő-beosztás kereteit egyáltalán nem határozza meg. Az Mfv.II.10086/2016. számú döntésében a Kúria rámutatott arra, hogy amennyiben a munkavállalók a munkájukat az áruház nyitvatartási idejében voltak kötelesek ellátni, nem valósul meg a kötetlen munkaidő-beosztás. Ezt erősíti az is, ha az érintett munkavállaló feladata szorosan kapcsolódik a többi munkavállaló munkavégzéséhez, vagy például az áruház nyitvatartási idejéhez (munkáltató üzemidejéhez). Nem tekinthető a munkavégzés önálló megszervezésének az a körülmény sem, hogy az egyes munkavállalók szabadon állapodhattak meg egymás között abban, hogy a napi nyolc órás munkavégzésüket – a nyitvatartási idő tükrében – mikor kezdjék meg.

7.3. A munkáltató munkavédelmi felelősségének terjedelme vitatott

A távmunkavégzés munkavédelmi aspektusairól a munkavédelemről szóló 1993. évi XCIII. törvény (a továbbiakban: Mvt.) 86/A. §-a rendelkezik. Távmunkavégzés esetén munkahelynek azt a munkaszerződésben a felek által meghatározott helyiséget kell tekinteni, ahol a munkavállaló az információtechnológiai vagy számítástechnikai eszközzel rendszeresen a munkáját végzi. Az Mvt. nem túl életszerűen rögzíti, hogy a munkahelyen, azaz a munkavállaló szobájában a munkavállaló a munkáltató hozzájárulása nélkül nem változtathatja meg a munkakörülményeket. A munkakörülményeket (mozgástér, megvilágítás, külső zavaró körülmények, biztonságosság) a munkáltató és a munkaügyi felügyelet ellenőrizni is jogosult. A munkáltató vagy megbízottja kockázatértékelés elvégzése, balesetvizsgálat lefolytatása, valamint a munkakörülmények ellenőrzése céljából beléphet és tartózkodhat a munkavégzési helyként szolgáló ingatlan területén. Felmerül azonban a kérdés, hogy a munkavédelmi szempontból megfelelő munkakörülményekért a munkáltató felelősséggel tartozik-e. Ahogyan arra a Magyar Munkajogi Társaság 2020. március 11. napján kelt állásfoglalása rámutat, kétféle álláspont létezik. Az egyik álláspont szerint a munkáltató felelőssége kizárólag az általa biztosított munkaeszköz kockázati megfelelőségének biztosítására, illetve egy általános jellegű, a veszélyforrásokra és azok kezelésére irányuló tájékoztatási kötelezettség terheli. A másik álláspont szerint a munkáltató felelőssége változatlan, azaz teljes mértékben megegyezik a munkahelyen végzett munkavégzésért való felelősség szabályaival. Az első álláspont ugyanakkor véleményem szerint teljes mértékben alátámasztható. Lehetőség szerint a munkavállalónak a munkáltató biztosítsa a munkavégzéshez szükséges, munkavédelmi szempontból is megfelelő eszközt, melynek munkavédelmi megfelelősége érdemi problémát nem vethet fel. Emellett biztosítsuk számára mind a munkavédelmi, mind pedig az adatvédelmi kérdésekre vonatkozó munkáltatói tájékoztatást. A megfelelés alapja pedig a munkahelyi adatkezelésre vonatkozó belső szabályozás megléte.

7.4. A távmunkavégzés adatvédelmi keretei szigorúak

A távmunkavégzés azonban adatvédelmi kérdéseket is felvet. A munkáltató ugyanis köteles gondoskodni mind az üzleti titok megőrzéséről, mind pedig arról, hogy a személyes adatok kezelése a 95/46/EK rendelet hatályon kívül helyezéséről szóló 2016. április 27-i 2016/679 európai parlamenti és tanácsi rendelet (a továbbiakban: GDPR) szabályainak betartásával történjék. Ezeket tehát ellenőrizni is köteles még abban az esetben is, amennyiben a

munkavégzéshez a munkavállaló saját eszközét használja. Az Mt. 11/A. §-a szerint ugyanakkor a munkavállaló kizárólag a munkaviszonnyal összefüggő magatartása körében ellenőrizhető, ami azt jelenti, hogy az ellenőrzésre még a munkáltató általa biztosított eszköz vonatkozásában sem kerülhet sor korlátozás nélkül. A munkáltató ennek figyelembevételével a munkaeszközön (pl. laptop) található levelezést kizárólag a fokozatosság elvének megtartásával, s a munkavállaló jelenlétében ellenőrizheti. Első lépésben a beérkezés időpontját, majd a feladót, a tárgysort, s végül – a relevancia beazonosítását követően – a tartalmat is megtekintheti. Tekintettel arra, hogy a magánéletre vonatkozó adat munkáltató által nem kezelhető, illetve, hogy ilyen adat még a magánhasználat kizárása esetén is előfordulhat (korlátozás munkavállaló általi megszegése, harmadik személy munkavállalóval történő adatközlése), az ellenőrzésnek a munkavállaló jelenlétében kell történnie. A munkáltató részéről pedig adatvédelmi szempontból feltétlenül ajánlott a munkáltató tulajdonában álló eszköz biztosítása, illetve a tekintetben a magánhasználat teljes körű kizárása, amely megoldást az Mt. 11/A. § (2) bekezdése már alaphelyzetnek tekint. Amennyiben pedig a magáncélú használatot lehetővé tesszük, a munkavállalóval a GDPR 26. cikke alapján közös adatkezelői megállapodást kell kötnünk. Fontos, hogy kötelezzük a munkavállalót arra, hogy a munkáltatóval, ügyfelekkel történő kommunikációra kizárólag a céges eszközöket és e-mail-címet használja. Ellenkező esetben a személyes adatokat, üzleti titkot később „magával viheti". Állapítsuk meg továbbá mind a használat, mind pedig az ellenőrzés szabályait. Ezen szabályok betartására azért is kell fokozottan ügyelni, mert nem zárható ki, hogy munkaviszony megszüntetése esetén a munkavállaló panasza a felügyeleti hatóságnál fog kikötni. A munkahelyi adatkezeléssel kapcsolatosan közzétett, bírság szankciót is tartalmazó hatósági döntések között egyetlen példát sem találunk ennek ellenkezőjére, azaz valamennyi panaszt elbocsátott dolgozó nyújtotta be.

7.5. Hatósági ajánlások születnek a távmunkavégzés szabályaival összefüggésben

Az angol felügyeleti hatóság (Information Commissioner's Office, a továbbiakban: ICO) ajánlást fogalmazott meg a vállalkozások részére a távmunkavégzés adatvédelmi aspektusait illetően, melyet várhatóan más hatóságok is követni fognak. Az ajánlásban a figyelmet a következőkre hívják fel:

A vállalkozások kötelezettsége megfelelő eljárásrendek, szabályzatok kialakítása. Gondoskodniuk kell a távoli hozzáférés megfelelőségének a biztosításáról, az adatszivárgás megakadályozásáról, szigorú jelszókövetelmények alkalmazásáról. Az ICO a felhőalapú adattárolást javasolja azzal, hogy minden munkavállaló számára egyedi hozzáférési szintet kell meghatározni. A saját adathordozó használhatóságát, vállalati rendszereken kívüli kommunikációt tiltani szükséges. Tiltja továbbá a privát e-mail-címek használatát, valamint korlátozásokat lát szükségesnek a hivatali emailek külsős e-mail-címekre történő továbbítása tekintetében.

Az ICO nem tiltja általánosságban a saját eszköz használatát, ennek adatvédelmi kockázataira figyelmeztet. A saját eszköz megfelelő informatikai védelme jellemzően nem megoldott, illetve nem biztosított, hogy a legújabb biztonsági frissítések is telepítésre kerüljenek. Problémaként jelenik meg az is, hogy a munkavégzés közben családtagok vagy más jelenlévő személyek számára is hozzáférhetővé válhatnak személyes adatok, illetve az eszköz el is veszhet. Ezek potenciális következményeire, illetve a követendő eljárásrendre (adatvédelmi incidens) fel kell hívni a munkavállalók figyelmét. Külön fel kell arra hívni a figyelmüket, hogy az adatvédelmi incidens kiemelt jelentőségű, annak bejelentése a munkáltató kötelezettsége. A nem megfelelő incidenskezelésnek pedig bírságkockázata is lehet. Biztosítani kell továbbá azt, hogy a céges, illetve a magánjellegű adatok a munkaeszközön ne keveredjenek.

Külön felhívja a figyelmet arra is, hogy szigorú szabályokat kell alkalmazni a dokumentumok nyomtatására, illetve azok tárolására vonatkozóan. A tiszta asztal politikát otthon is meg kell a munkavállalóktól követelni.
Arra is fel kell hívni a munkavállalók figyelmét, hogy ismeretlen eredetű, gyanús emailek mellékleteit ne nyissák meg, hiszen így külsős személyek számára a személyes adatok, üzleti titkok potenciálisan hozzáférhetővé válhatnak.

8. Összegzés

Mára már a home office intézménye valós megoldást jelenthet a járványhelyzet során a digitális technológiának köszönhetően. A vírus okozta váratlan helyzet gyors megoldásért kiáltva elősegítette a távmunka és a digitális transzformáció fejlődését. Felfogható mindez a rugalmas, távoli munkavégzés és a kikényszerített digitalizáció egy éles tesztjeként, melynek eredményét és hatékonyságát az elkövetkező időszakban fogjuk csak megismerni. Lesznek olyan szervezetek, amelyek pozitív és előremutató megoldásként tekintenek a távmunka lehetőségeire és lesznek, akik még nem látják elérkezettnek rá az időt.
Ahogy fentebb összefoglaltuk, jogi és informatikai oldalról is rendelkezésünkre állhat minden eszköz, módszertan, amellyel kockázatarányosan és biztonságosan kidolgozhatjuk az otthoni munkavégzést, csak alaposan fel kell mérnünk az intézmény, a folyamatok és a dolgozók kockázatait és szükségleteit. A legfontosabb, hogy megfelelően előkészített, tudatos döntés eredménye legyen az átszervezés minden esetben.

Hivatkozott jogszabályhelyek:
– GDPR 26. cikke
– Mt. 11/A. §
– Mt. 196. § (1) bekezdése
– Mt. 196. § (5) bekezdése
– Mvt. 86/A. §
– 41/2015. (VII. 15.) BM rendelet 4. melléklet

Kancsal Tamás

Dr. Kéri Ádám
ügyvéd