Mobil eszközök hivatali használata

(Mobil Devices in Government Environment)

A tanulmány a KÖFOP-2.2.2-VEKOP-16-2016-00001

„KÖFOP keretében megvalósuló fejlesztések IT biztonságának növelése, ezáltal rendszerekkel összefüggő korrupciós lehetőségek és kockázatok csökkentése”

című projekt keretében készült.

Tartalomjegyzék

Absztrakt

Napjainkban a mobil eszközök (mobiltelefon, tablet, hordozható számítógép) használata magánéletünk szerves része. Nemcsak magánéletünkben, hanem munkahelyünkön is használunk ilyen eszközöket, melyet a munkáltató is biztosíthat. Az eszközök használata során biztonsági események történhetnek, melyek információ- és adatbiztonsági incidenst okozhatnak, ezért alkalmazásuk esetében a hatályos jogi szabályozás alapján megfelelő szabályokat, ellenőrzési rendszereket kell létrehozni, és nagy hangsúlyt kell fektetni a munkavállalók biztonságtudatosságának növelésére. A bevezetés előfeltétele a jogi környezet vizsgálata, azért, hogy a hatályos jogi, valamint a szervezet belső szabályozásnak és a hivatali gyakorlatnak megfelelően történjen a bevezetés, az üzemeltetés, a megfelelő védelmi rendszerek kialakítása és az ellenőrzés.

Abstract

Nowadays the use of our mobile devices (mobile phone, tablet and laptop) is an essential part of our lives. However, these devices can also be provided by our employers, so they can be used for work. While using these devices, events can happen that can affect the security of our personal data. That is why, according to the current legal framework, proper regulations and checking systems must be established, while also putting emphasis on improving the employees' awareness of such danger factors. In order for the installation, the operation, the establishment of proper security and checking systems to be executed according to the current legal, inner organisational regulation and the governmental practise, the precondition of the installation is the examination of the legal framework.

Kulcsszavak

mobileszköz, mobiltelefon, tablet, hordozható számítógép, magán és hivatali felhasználás, biztonsági esemény, információbiztonság, információbiztonsági szabályzat, adatvédelem, adatbiztonság, eszközfunkciók, BYOD, CYOD, COBO, COPE, bevezetési stratégia, jogi környezet

1. Bevezetés

„Csak egészség legyen és térerő”, tartja az egyre népszerűbb, legújabb keletű mondás, ami napjaink társadalmának talán legfontosabb szükségleteit fogalmazza meg. Az egészség szükségessége abszolút nem szorul magyarázatra, de lassan a térerő is abba a kategóriába kerül, amikor nemléte, hiánya komoly problémákat okozhat a mindennapi életünk során.

Mi az a térerő, és miért is van szükségünk rá? A térerő a mikrohullámú kommunikációs hálózat által generált tér, melyhez csatlakozva lehet működtetni és használni azokat az eszközeinket, amelyek lévén kommunikációnk nem helyhez, vezetékhez kötött, hanem mobilis.[1]

Ezen eszközeinket összefoglaló néven mobil eszközöknek[2] nevezzük, és ide sorolunk a hordozható számítógéptől elkezdve, a mobiltelefonon („hagyományos” és okos) és táblagépen (a továbbiakban: tablet) át, az okosórán keresztül minden olyan elektronikus eszközt, amely vezeték nélküli működésre képes. Ezek az eszközök számítástechnikai eszközként funkcionálnak, még ha nem is feltétlenül így gondolunk rájuk a mindennapokban. A különböző mobil eszközök és a működésük alapját biztosító hálózatok fajtáinak és típusainak fejlődése rövid időn belül, nagyon gyorsan történt meg, és napjainkban még nagyobb tempóban folytatódik.

A mobil eszközök közé tartozik a már fentebb említett hordozható számítógép is, mely az asztali számítógépek teljes értékű hordozható változata. Ezeket a számítógépeket a ’80-as évektől kezdték el fejleszteni és gyártani, napjainkra pedig több ilyen hordozható számítógépet adnak el világszerte, mint asztali számítógépet. Méretük és hardver felszereltségük alapján több kategóriába sorolhatók:netbook, laptop/notebook, ultrabook

A hordozható számítógépek egyik egyre jobban elkülönülő változata a tablet, mely szintén a mobil eszközök közé tartozik. A tablet előfutárai először a ’90-es években jelentek meg, de átütő sikert csak a 2010-es évekre értek el vele a fejlesztők, ezt követően hamar elterjedt, és népszerű eszközzé vált a felhasználók körében. A tablet hordozható számítógép, melynek formája egy táblára hasonlít, nagy kijelzője van, fizikailag megjelenő billentyűzet nélkül. Informatikai tudása egyre jobban hasonlít a számítógépekére, de tárolási és számítási kapacitásában vannak korlátai, ezért legfőbb felhasználási területe a tartalomfogyasztás (hírek, képek, videók, játékok), akár olyan helyeken is, amelyek kívül esnek az otthonunkon és az munkehelyünkön. A tablet a megfelelő technikai felszereltség és kiegészítők megléte esetén önállóan vagy más eszközökön keresztül is képes az internetre csatlakozni.

A mobiltelefon[3] a számítógéppel párhuzamosan fejlődött, a XX. század közepétől kezdődött meg kísérleti alkalmazása, majd a ’80-as évektől kezdett elterjedni használata. A technológia fejlődésének köszönhetően az eszközök és a szolgáltatások ára csökkenni kezdett, és a ’90-es évek végére, a 2000-es évek elejére széles körben elérhetővé vált a lakosság körében. A mobiltelefon először csak hanghívások kezdeményezésére és fogadására volt alkalmas, majd a GSM rendszer megjelenésével már szöveges üzenetek továbbítására is alkalmas volt, azután a technológia fejlődése lehetővé tette, hogy később már kép- és videoüzenetek továbbítása is megvalósítható legyen, illetve sok kényelmi funkció (naptár, ébresztőóra stb.) épült be az eszközökbe. Napjainkban a hagyományos nyomógombos mobiltelefonokat már felváltotta az úgynevezett okostelefon (smartphone), ami azt jelenti, hogy a

[1] Ekler Péter – Forstner Bertalan – Kelényi Imre: *Bevezetés a mobilprogramozásba.* 2008. http://www.szak.hu/konyvek_htm/sample_chapters/mobilprog/chap1.pdf

[2] Előházi János: *Mobil eszközök biztonsági problémái.* Robothadviselés 7. Tudományos szakmai konferencia, 2007. november 27. http://hadmernok.hu/kulonszamok/robothadviseles7/elohazi_rw7.html

[3] Fei Yu: *Mobile Device Security.* 2011. https://www.cse.wustl.edu/~jain/cse571-11/ftp/mobiles/index.html

mobiltelefonok alkalmasak arra, hogy internetre kapcsolódva böngészhessünk is rajtuk, vagy akár e-maileket küldjünk és fogadjunk.

Mind a hordozható számítógéphez, mind a tablethez és mobiltelefonhoz is van már lehetőség különböző okos eszközöket – pl. okosóra, okoskarkötő, fényképezőgép, tévékészülék, hangrendszerek, gépkocsik elektronikus rendszere – csatlakoztatni, és azokat egymást kiegészítő eszközökként alkalmazni, melyek között az adatok áramlása különböző technológiák (pl. bluetooth, internet) segítségével történik.

A mobil eszközök használatakor meg kell említeni az IoT (Internet of Things) fogalmát is, amely azt jelenti, hogy különböző, egyértelműen azonosítható elektronikai eszközök képesek felismerni valamilyen lényeges információt, és azt egy internet alapú hálózaton egy másik eszközzel kommunikálni, megosztani. Jellemző példa a mobil eszközök, okosotthonok, okosautók, egészségügyi eszközök kommunikációja. Az IoT rohamosan terjed és fejlődik.

A mobil eszközök és használatuk már mindennapi életünk részét képezik a gyermekkortól egészen idős korunkig, jelenlétük annyira általánossá vált, hogy már észre sem vesszük, hogy használjuk őket, azonban hiányuk egyik pillanatról a másikra komoly problémát okozhat még egyszerűbb helyzetekben is. Például lemerül a mobiltelefonunk, nincs nálunk töltő, de sürgősen fel kellene hívnunk egy személyt, akinek a száma a telefonunk névjegyzékében van, így nem tudjuk a számot, és az illetőt sem felhívni.

A mobil eszközök használata nemcsak magánéletünk része, hanem ma már egyre több munkáltató is ilyen eszközöket biztosít munkavállalóinak munkavégzésükhöz.

A munkáltatóknak minden esetben végig kell gondolniuk és mérlegelniük kell, hogy milyen mobil eszköz politikát folytatnak, illetve azt milyen stratégia mentén valósítják meg, mert ezek mind kihatással lehetnek gazdasági tevékenységükre, nemcsak költséghatékonyság szempontjából, hanem vállalati biztonsági, információbiztonsági és adatvédelmi vonatkozásokban is, mely kockázatoknak, az anyagi veszteségen túl, komoly reputációs vetülete is lehet.[4]

Az eszközök nagy száma és mindennapi jelenléte, a „tőlük való függőség", valamint a magán és a hivatali felhasználás miatt is szükséges ezen eszközök, a rajtuk tárolt és segítségükkel továbbított információk védelme, melyet információbiztonsági, valamint adatbiztonsági intézkedésekkel lehet elérni.

A tanulmány célja annak bemutatása, hogyan lehet hivatali környezetben a mobil eszközöket biztonságos módon alkalmazni. Példákon keresztül bemutatjuk a mobil eszközök magán és hivatali használatának veszélyeit, továbbá, hogy milyen biztonsági intézkedésekkel lehet a hivatali használat kockázatait csökkenteni.[5] A hivatali mobil eszköz használatának eseteit külön fejezetben fejtjük ki részletesen. A tanulmány kitér a hivatali mobil eszközök biztosításának módjaira is, valamint külön fejezet szól a hivatali mobil eszközök használatának bevezetéséhez kapcsolódó stratégiákról is. Nemcsak a gyakorlati megvalósítás fontos a mobil eszközök hivatali használata során, hanem a jogi háttér vizsgálata, elemzése is, mely önálló fejezetet kapott a hatályos jogi szabályozás információbiztonsági, adatvédelmi és egyéb releváns területein keresztül. A tanulmány végén, az összegzésben összehasonlítjuk az egyes használati módok előnyeit és hátrányait, valamint a bevezetési stratégia fontosabb lépései is teret kapnak.

---

[4] Kassai Károly: *A mobil kommunikációs eszközök használatának és védelmi rendszabályainak szabályozása.* Hadmérnök, V. évfolyam, 3. szám, 2010. szeptember. http://hadmernok.hu/2010_3_kassai.pdf

[5] *Guidelines for Managing the Security of Mobile Devices in the Enterprise.* NIST Special Publication 800-124, Revision 1, 2013. https://nvlpubs.nist.gov/nistpubs/specialpublications/nist.sp.800-124r1.pdf

A tanulmány – adott keretek között – törekszik a mobil eszközök hivatali bevezetésének legszélesebb és legmélyebb aspektusait bemutatniarra is figyelemmel, hogy a téma gyorsan változik, folyamatosan bővülnek a rendelkezésre álló információk, és látnak napvilágot az alkalmazást befolyásoló biztonsági események és az arra adott válaszok. Figyelembe kell azt is venni, hogy az elemzés eredményeit egy konkrét szervezetnél történő bevezetéskor a szervezet sajátosságaira tekintettel kell felhasználni.

2. A mobil eszközök használatából fakadó biztonsági események[6]

A mobil eszközök használatának nemcsak előnyei vannak, hanem lehetnek negatív hatásai, amikor olyan nem kívánt vagy várt események történnek, melyek az eszközök használatát megnehezítik vagy ellehetetlenítik. Az ilyen eseményeket biztonsági vagy információbiztonsági incidensnek, illetve ha az esemény során személyes adatok is érintettek, akkor adatvédelmi incidensnek nevezzük.

Biztonsági esemény az a nem kívánt vagy nem várt egyedi esemény vagy eseménysorozat, amely az elektronikus információs rendszerben kedvezőtlen változást vagy egy előzőleg ismeretlen helyzetet idéz elő, és amelynek hatására az elektronikus információs rendszer által hordozott információ bizalmassága, sértetlensége, hitelessége, funkcionalitása vagy rendelkezésre állása elvész, illetve megsérül.[7] E fogalom-meghatározás alkalmazható az információbiztonsági incidens meghatározására is. Például, illetéktelen személy jogosulatlanul hozzáfér a hivatali adatokhoz, egy munkavállaló elveszti a mobil eszközét, melyen hivatali adatok voltak tárolva.

Adatvédelmi incidens a biztonság olyan sérülése, amely a továbbított, tárolt vagy más módon kezelt személyes adatok véletlen vagy jogellenes megsemmisítését, elvesztését, megváltoztatását, jogosulatlan közlését vagy az azokhoz való jogosulatlan hozzáférést eredményezi.[8] Hasonló esetek tartozhatnak ide, mint az információbiztonsági incidensek esetében, azzal kiegészítve, hogy ezen esetekben személyes adatok is vannak az adatok között, és ezek kerülnek veszélybe.

A különböző biztonsági események alapja, háttere és megvalósítása többféle lehet, de a leggyakoribbak a következők:

- **Fizikai alapú** az esemény például, amikor valaki elveszíti a mobil eszközét, vagy eltulajdonítják tőle. Ilyenkor az ismeretlen személy, aki az eszközt megszerzi, közvetlenül hozzá tud férni az eszközhöz mint hardverhez, és szinte korlátlan lehetősége (idő, tudás és eszköz kérdése) van az eszközön tárolt adatokhoz történő jogosulatlan hozzáférésre. De ide tartozik az is, amikor valaki nem megbízható mobil eszközön keresztül akarja igénybe venni az informatikai szolgáltatásokat.
- **A web alapú** esemény az esetek többségében észrevétlenül történik meg, a kifinomult mechanizmusok alkalmazásának köszönhetően. Internetes böngészés közben, a tartalom felkeresésekor és megtekintésekor, az elsődleges felület hátterében a rosszindulatú tartalom automatikusan letöltődik az eszközre, és általában aktivizálódik is.
- **Alkalmazás alapú** esemény akkor fordul elő, amikor a felhasználó alkalmazást tölt le, amely legálisnak, valósnak és hitelesnek tűnik, de valójában nem az, és a telepítést követően jogosulatlanul megszerzi és továbbítja az eszközön tárolt adatainkat. Ilyenek például a kém- és a rosszindulatú programok, amelyek „ellopják” az adatainkat, anélkül, hogy azt észlelnénk.
- **Hálózati alapú** az esemény, ha olyan hálózatot használunk, mely számunkra és eszközünk számára ismeretlen, például szállodai wi-fi, mert ezeknek a hálózatoknak a titkosítása nem valószínű, hogy megfelelő, ezért ezek használata során nagyobb lehet a valószínűsége annak, hogy arra nem jogosult személy hozzáférhet a kommunikációnkhoz, adatainkhoz.

A felsoroltak önállóan és egymást kiegészítve is alapot adhatnak egy biztonsági esemény bekövetkezésére.

[6] www.auth0.com - https://auth0.com/blog/ten-mobile-security-threats-and-what-you-can-do-to-fight-back/
[7] Ibtv. – Az állami és önkormányzati szervek elektronikus információbiztonságáról szóló 2013. évi L. törvény 1. § (1) bekezdés 9. pont
[8] GDPR – az Európai Parlament és a Tanács (EU) 2016/679 rendelete 4. cikk 12. pont

2.1. A magánhasználatból fakadó biztonsági események[9]

A mobil eszközök magáncélú használata során a következőkben felsorolt események is bekövetkezhetnek, ezek megelőzése, esetleges bekövetkezésük esetén szükség van a keletkezett kár csökkentésére és az incidens kezelésére. A felsorolás nem lehet teljes körű, mert az élet olyan kiszámíthatatlan, hogy az emberi elme néha kigondolni sem képes olyan dolgokat, amelyek a való életben végül megtörténnek, bekövetkeznek, ezért most a leggyakrabban előforduló és legnagyobb kárt okozó eseményeket emeljük ki.

2.1.1. Elveszett vagy eltulajdonított mobil eszköz[10]

Mindennapos eset a mobil eszköz felhasználók körében, hogy eszközüket elveszítik, vagy eltulajdonítják tőlük azt. Az eszközhöz így közvetlen hozzáférés nyílik fizikailag, így akár megfelelő tudás és eszköz nélkül is megismerhető a rajta tárolt tartalom (tárolt nevek, telefonszámok, SMS-ek, híváselőzmények, jegyzetek, fényképek és videók, dokumentumok, böngészési előzmények stb.), és jogosulatlanul használhatóvá válnak a különböző szolgáltatások (hívásokat lehet kezdeményezni, SMS-t küldeni vagy internetezni), ami további anyagi kárt okozhat az eszköz valódi birtokosának.

Nemcsak az eszközön tárolt adatokhoz lehet így hozzáférni, hanem az eszközön levő alkalmazásokhoz is, melyek akár felhasználói neveket, jelszavakat, különböző azonosítókat is tartalmazhatnak, melyekkel a továbbiakban vissza lehet élni. Legtöbbször a mobil eszközökön található alkalmazások megnyitásához nem is szükséges a felhasználói nevek és jelszavak ismerete, mert azokba már korábban bejelentkezett a felhasználó, és így a folyamatos belépés miatt egyszerűbb azok további jogosulatlan használata.

Az esetleges elvesztésből vagy eltulajdonításból fakadó károkat úgy lehet mérsékelni, hogy az eszköz feloldásához vagy a belépéshez erős jelszavakat, jelkódokat használunk, nem tárolunk olyan tartalmakat az eszközön, amelyek bizalmas jellegűek, illetve ha ez elkerülhetetlen, azokat erős védelemmel látjuk el. Fontos az is, hogy ha észrevesszük, hogy az eszköz birtokunkon kívül került, akkor lehetőség szerint a kapcsolódó szolgáltatásokat haladéktalanul le kell tiltani, illetve mivel egyre több alkalmazás, eszköz képes arra, hogy abból távolról ki lehessen lépni, vagy törölni lehessen, ezt szintén meg kell tenni. Bizonyos eszközök esetében van olyan funkció, amelynek segítségével – ha előzetesen beállítjuk – lokalizálni lehet a fizikális fellelhetőséget, és így meg lehet próbálni az eszközt megtalálni és visszaszerezni.

2.1.2. Ismeretlen eszköz használata

Előfordulhatnak olyan élethelyzetek, melyek során sürgősen mobil eszköz használata lenne szükséges, azonban a sajátunk nem áll rendelkezésünkre. Ilyen esetben előfordulhat, hogy kölcsönkérjük valakinek az eszközét, akár ismeretlen személyét is, és azt használjuk. Ezekben az esetekben előfordulhat, hogy az ismeretlen eszközön bejelentkezve maradunk egy alkalmazásban, esetleg az általunk begépelt adatok rögzítődhetnek is, s később ezekkel visszaélhet az eszköz birtokosa. Tekintettel erre, idegen eszközön ne használjunk olyan alkalmazásokat, amelyekbe bejelentkezésünk vagy adataink megadása szükséges.

2.1.3. A mobil eszköz kiegészítő funkcióival történő visszaélés

A legtöbb mobil eszköz beépített kamerái és hangszórói, mikrofonjai alkalmas lehet arra, hogy ne csak akkor közvetítsen képet és hangot, amikor a felhasználó tudatosan ezt szeretné. Előfordulhatnak olyan

[9] www.auth0.com - https://auth0.com/blog/ten-mobile-security-threats-and-what-you-can-do-to-fight-back/
[10] Kitteringham, Glen: *Lost Laptops = Lost Data – Measuring Costs, Managing Threats.* 2008. https://www.asisonline.org/globalassets/foundation/documents/crisp-reports/crisp-lost-laptops-lost-data.pdf

események, amikor illetéktelen személyek az eszköz ezen kiegészítőit visszafelé használják, és megfigyelik a felhasználót a kamerán keresztül, illetve a hangszórón, mikrofonon keresztül hallják a hangokat. Az ilyen visszaélések megelőzhetőek például a kamera letakarásával, az eszköz teljes energiaforrásának kiszerelésével, illetve ha olyan beszélgetés hangzik el, akkor az eszközt olyan helyre tesszük, ahol a hang már nem érzékelhető.

2.1.4. Jelszó hiánya vagy nem megfelelősége

Meglepő módon a felhasználók egy része nem használ jelszót vagy jelkódot eszközeinek védelme érdekében. Az is meglepő, hogy akik használnak, azok olyan gyengének minősítetteket mint például: 0000, 1234, 1111, jelszo, password, qwertz vagy ehhez hasonlók, melyek viszonylag egyszerűen kitalálhatóak, feltörhetőek, és ezzel megkönnyítik a jogosulatlan felhasználó azon törekvéseit, hogy az eszközön tárolt adatokhoz hozzáférjen. Elkerülhetőek az ebből fakadó biztonsági események, ha megfelelő jelszavas, jelkódos védelemmel látjuk el eszközeinket, megfelelő felépítettségű, hosszúságú és többféle betűt, számot és karaktert tartalmazó jelszavakat, jelkódokat használunk. A megfelelően kialakított jelszón és jelkódon kívül fontos az is, hogy azokat bizonyos időközönként, kb. három havonta megváltoztassuk, ne használjuk legalább az előző 5 változatot, illetve a különböző eszközökön más és más védelmet alkalmazzunk.

2.1.5. Téves hívás, üzenet- és e-mail küldés

A mobil eszköz használata során előfordulhat olyan helyzet, amikor véletlenül nem a megfelelő telefonszámot hívjuk, vagy nem a megfelelő telefonszámra küldünk SMS vagy MMS üzenetet, illetve nem a megfelelő e-mail címre küldünk e-mail-t. Ilyen eset bárkivel előfordulhat, melynek oka legtöbbször figyelmetlenség, viszont olykor kellemetlen helyzeteket is okozhatnak. Leginkább a tévesen küldött üzenetek, e-mailek lehetnek kockázatosak, mert azokban olyan adatokat oszthatunk meg, melyekkel kárt okozhatunk magunknak és másoknak is. Előfordulhat olyan eset is, például e-mail küldés esetén, hogy a levelező program automatikusan elkezdi beírni, hozzáadni az e-mail címet, mi pedig csak rákattintunk az első lehetőségre, de nem győződünk meg a helyességéről, és csak elküldés után derül ki a hiba. Az ilyen eseteket nagyobb odafigyeléssel, tudatosabb felhasználói magatartással elkerülhetjük, illetve ha például rossz e-mail címre küldtük levelünket, és azt még időben észleljük, van lehetőség a visszahívására.

2.1.6. Pszichológiai manipuláció (Social engineering)

Pszichológiai manipulációnak nevezzük azt a módszert, amikor egy jogosulatlan személy megtévesztéssel szerez meg adatokat. Ilyen esetekben nem technikai jellegű biztonsági eseményről beszélünk, hanem emberi interakciókon alapulóról, melynek lényege, hogy az emberi magatartás rosszhiszemű befolyásolásával lehet hozzáférni az adatokhoz.

A rosszhiszemű megtévesztés megjelenési formája a telefonos adathalászat, a farmolás vagy az adatok kifigyelése, kilesése is, de legelterjedtebb és talán leginkább anonim módszere az adathalász támadás.

A telefonos adathalászat során a felhasználót telefonon éri el a csaló, és hamis történetet előadva, az emberi jóhiszeműségre apellálva szerzi meg az adatot.

Farmolás során a felhasználót olyan weboldalakra navigálják, melyeket előzetesen manipuláltak, hamisítottak, majd ott különböző adatok megadását kérik. Az adatok kifigyelése vagy kilesése során a csaló a felhasználó nyíltságát, figyelmetlenségét kihasználva vagy például a billentyűzethez kapcsolódó program segítségével látja meg az adatokat, amelyekkel azt követően visszaél.

Ezen módszerek ellen úgy védekezhetünk a leghatékonyabban, hogy telefonon nem adjuk meg adatainkat senkinek, csak abban az esetben, ha meggyőződtünk arról, hogy az illető az, akinek mondja

magát, illetve különböző adataink kezelésekor figyelmet fordítunk arra, hogy azokat ki láthatja, észlelheti a tudtunkon kívül.

Az internetes adathalászat esetében előfordulhat olyan helyzet is, hogy elektronikus levelezés közben olyan e-mail-t kapunk, melyben arra kérnek minket, hogy egy az e-mail-ben található linkre kattintsunk rá, és a megnyíló webhelyen adjuk meg különböző adatainkat, pl. felhasználói név, jelszó, személyes vagy akár bankkártya adatainkat is. Az e-mail küldője ránézésre olyan személy vagy szervezet, melyet ismerünk és megbízhatónak tartunk. Ilyen e-mailek esetében sokan első reakcióként megteszik, hogy megnyitják a linket, majd a megnyíló weboldalon megadják a kért adatokat. Ezzel azonban hibát követünk el, és valószínű, hogy adatainkkal hamarosan visszaélnek, melyből akár közvetlen anyagi kárunk is származhat. A hamis e-mailek és weboldalak a legtöbb esetben felismerhetőek, például mert az e-mail vagy weboldal címe eltér a valóditól, a tartalmak szövegezése sok esetben helytelen nyelvtanilag. Fontos kiemelni azt is, hogy pénzintézetek, hivatalok sosem kérik e-mail vagy weboldalas adatközlés útján az adataink megadását.

Napjainkban szerencsére a legtöbb elektronikus levelezőrendszer és böngészőprogram rendelkezik úgynevezett spam és adathalász weboldal szűrővel, amelyek a folyamatos fejlesztés és beállítás esetén nagy részben képesek arra, hogy az adathalász jellegű e-maileket és weboldalakat kiszűrjék, vagy annak esetleges voltát jelezzék. A rendszerszintű szűrés önmagában nem működhet, és nem is elégséges, a biztonság megőrzéséhez szükséges a felhasználó tudatos magatartása is: példáulha ilyen jellegű e-mail-t kap, akkor azt felismerje, ne kattintson a benne található linkre, és ne adja meg az adatait, illetve másoknak ne továbbítsa azt, csak akkor, ha erre konkrétan kérik.

2.1.7. Rosszindulatú szoftver (malware)

A rosszindulatú szoftver célja, hogy kárt okozzon a mobil eszközben, információkat gyűjtsön, amelynek alapján az eszközön tárolt vagy felhasznált adatokhoz juthat hozzá arra jogosulatlan személy. A rosszindulatú szoftver gyűjtőfogalom, magában foglalja az összes kártevő szoftvert, mint például a vírust, a férget, a trójai programot, a kémprogramot (spyware), a rootkit-et.. Ezek ellen a rosszindulatú szoftverek ellen vírusvédelmi programmal, rendszeres szoftverfrissítésekkel és tudatos eszközhasználattal védekezhetünk, például nem nyitunk és töltünk le ismeretlen tartalmakat az eszközünkre.

2.1.8. Rosszindulatú és inaktív alkalmazás

A mobil eszközök használata és a felhasználói élmény maximalizálása érdekében többféle alkalmazás letöltésére van lehetőség különböző tartalomszolgáltatóktól (pl. Google Play, App Store). Vannak azonban olyanok, amelyeket kifejezetten azért fejlesztettek, hogy a letöltést követően az eszközön tárolt adatokat megszerezzék, és azokkal visszaéljenek. A leggyakoribb megoldás, hogy az alkalmazás hozzáférést kér különböző, az eszközön tárolt adathoz (pl. névjegyek, kamera, fotók, mikrofon stb.). Ezeket az engedélyeket vagy az általános szerződési feltételekben, vagy a felugró ablakok engedélykéréseiben szokták elhelyezni, amelyeket a felhasználók általában gondosabb elolvasás nélkül jóváhagynak, elfogadnak.

A tartalomszolgáltatók folyamatosan ellenőrzik az alkalmazásokat, és a károsakat törlik. Előfordulhat azonban, hogy ezt nem észleljük, és olyanokat használunk, melyek így inaktívak lesznek ugyan, de a háttérben továbbra is károkat okoznak. Ezek az alkalmazások, nem is feltétlenül közvetlenül, hanem a háttérben futva, az eszköz erőforrásait kihasználva okozhatnak károkat, például csökkentik az eszköz terhelhetőségét, rendelkezésre álló tárhelyét.

Ezek ellen az alkalmazások ellen a felhasználók tudatos magatartásukkal tudnak védekezni: csak megbízható alkalmazást szabad letölteni, folyamatosan frissíteni kell őket, illetve a különböző engedélykérések alkalmával mindig el kell olvasni, hogy mit is hagyunk jóvá.

2.1.9. Botnet

Vannak olyan rosszindulatú szoftverek, amelyek a mobil eszközt megfertőzve egy hálózat részévé teszik azt, így távolról irányíthatóvá válik, melynek elsősorban az a veszélye, hogy a valódi felhasználás során az eszköz teljesítménye lecsökken, mert a távoli vezérlés az erőforrásokat más célra használja. A botnetbe kerülés másik veszélye lehet, hogy mivel rosszindulatú szoftver alapján kapcsolódik egy hálózathoz, más rosszindulatú szoftverek is települhetnek az eszközre, így az eszközön tárolt adataink veszélybe kerülhetnek. A botnet kialakulása ellen a felhasználó ugyanazokat a védelmi lépéseket teheti meg, mint a rosszindulatú szoftverek ellen.

2.1.10. Mobil eszközök közötti vezeték nélküli kommunikáció használata

Ha a mobil eszközünkön aktiváljuk a bluetooth vagy airdrop funkciókat, veszélynek tehetjük ki az eszközön tárolt adatainkat. A rendszerek sérülékenységét kihasználva illetéktelen személyek megfigyelhetik a készülékek közötti kommunikációt, az egyes készüléken végzett tevékenységet, és megszerezhetik adatainkat. Az ilyen támadás ellen úgy védekezhetünk, ha ezeket a funkciókat kikapcsoljuk, alapvetően nem használjuk, de ha mégis szükséges alkalmazni, akkor csak rövid ideig tesszük, és közben nem használunk olyan alkalmazásokat, amelyek esetében érzékeny adatokat (pl. felhasználói név és jelszó) kell abban az időben megadnunk.

2.1.11. Mobil eszközök töltése nyilvános helyen

A mobil eszközöketrendszeresen tölteni kell. A mobiltelefon és a tablet esetében ugyanazt a kábelt használjuk az eszköz töltésére, mint az adatátvitelre, ami azt jelenti, hogy a kábel nemcsak az áram továbbítására, hanem az eszközön lévő adatok továbbítására is képes. Ezt használhatják ki illetéktelen személyek úgy, hogy a nyilvános, már meglévő töltési pontokat manipulálják, vagy ilyen manipulált pontokat helyeznek ki ezekre a helyekre. A töltés közben a kábelen keresztül rosszindulatú kódot küldhetnek az eszközünkre, amelyen keresztül ellophatják adatainkat. Az eszközgyártók is ismerik ezt a visszaélési módszert, ezért folyamatosan fejlesztik az eszközeiket és a kiegészítőket, hogy biztonságossá tegyék a töltést. Ezt a módszert „juice jacking”-nek hívják, ami ellen úgy lehet védekezni, hogy nyilvános helyeken nem töltjük az eszközünket, csak megbízható helyen (pl. otthon, irodában), illetve külső akkumulátort (power bank) használunk, amikor az eszközt tölteni szükséges. Az is megoldás lehet, ha olyan kábelt, USB adaptert használunk, amely csak az áram felvételére képes.

2.1.12. Nyilvános Wi-Fi használata

Egyre több helyen (pl. étterem, söröző, szálláshely, irodaház, repülőtér stb.) van már lehetőségük a felhasználóknak, hogy ha internetkapcsolatra van szükségük, akkor ne a saját erőforrásukat használják, hanem az ingyenesen igénybe vehetőeket. Mivel ezen hálózatok igénybevétele naponta több felhasználó által, egy időben is történhet, a csatlakozás vagy jelszó nélkül, vagy igen egyszerű formát használva történik meg. Jellemző ezekre a szolgáltatásokra, hogy általában a szolgáltatás nyújtók további biztonsági intézkedéseket sem tesznek, mert csak az igényt akarják kiszolgálni, a felhasználók esetleges biztonsági kockázataival nem foglalkoznak. Az ilyen nyilvános hálózatok lehetnek valódiak, de lehetnek kreáltak, amelyeket egy jogosulatlan személy kifejezetten azért hoz létre, hogy ott a felhasználók adatait szerezze meg. A valódi nyilvános hálózatok fentebb is említett biztonsági hiányosságait használják ki jogosulatlan személyek arra, hogy a rendszer sérülékenységén keresztül megszerezzék a felhasználók különböző adatait. Lehetőség szerint érdemes mellőzni a nyilvános Wi-

Fi-k használatát, azonban ha mégis szükséges, akkor célszerű csak olyan dolgokra használni, amelyek nem járnak adatok megadásával.

2.1.13. A végponttól végpontig terjedő titkosítás hiánya

Ahhoz, hogy kommunikációnk megfelelően biztonságos lehessen, figyelmet kell fordítani arra, hogy a két felhasználó közötti kapcsolat teljes egészében, végponttól végpontig zárt legyen, ahhoz külső, jogosulatlan személy ne férhessen hozzá. Ezen biztonsági esemény megelőzése érdekében a felhasználók olyan kommunikációs alkalmazásokat tudnak használni, melyek titkosítják az adatátvitelt.

2.1.14. IoT biztonsági fenyegetések

Az Internet of Things (IoT) terjedése folyamatos, különböző mobil eszközeinket újabb és újabb okoseszközökkel köthetjük össze, így jelentősen megkönnyíthetjük mindennapi életünket. Azonban ennek nagy kockázata is van, hiszen az eszközök összekötéséből és azok kommunikációjából számos biztonsági esemény keletkezhet, ha nem vagyunk felkészültek és tudatosak. A jogosulatlan személyek rendszereink sérülékenységét kihasználva eljuthatnak olyan mobil eszközeinkhez is, ahol adatainkat nagyobb számban tároljuk, megszerezhetik azokat, és visszaélhetnek velük. A különböző eszközök biztonságos használatához elengedhetetlen a megfelelő védelmi rendszerek használata, az alkalmazások folyamatos frissítése és a felhasználók biztonságtudatos magatartása.

2.2. Hivatali használatból fakadó biztonsági események

A hivatali használatból fakadó biztonsági események nem mutatnak szignifikáns különbséget a magánhasználatból fakadóaktól, ugyanazok az esetek fordulhatnak elő. Eltérés azonban közöttük az, hogy amíg magánhasználat során leginkább saját adataink sérülhetnek, és azokkal élhetnek vissza, addig a hivatali felhasználás során olyan adatok is illetéktelenek kezébe kerülhetnek, amelyek egy adott szervezet nem nyilvános tevékenységére, működésére vonatkoznak, melyek jogosulatlan megszerzése jelentős reputációs és anyagi kárral, de akár élet és testi épség vagy más egyéb érdekek veszélyeztetésével is járhat. Kiemelten magas kockázatú például a minősített adatok tárolása, továbbítása mobil eszközökön. A minősített adat és a mobil eszköz kapcsolatát a tanulmány 6.4. pontja mutatja be részletesebben.

A hivatali használatból eredő magas kockázatok miatt ezen eszközök alkalmazása még nagyobb odafigyelést, rendszeres fejlesztést, valamint a felhasználók biztonságtudatosságának növelését és gyakori ellenőrzését igényli. A hivatali használatból fakadó biztonsági események kezelésénél minden esetben a belső szabályozást kell figyelembe venni, betartani és a szükséges lépéseket megtenni, például az előírt személynek a megfelelő formában és időn belül jelezni, ha ilyen esemény történik.

3. A mobil eszközök biztonsága

Az előző fejezet bemutatta a magán- és hivatali használat során valószínűsíthetően leggyakrabban bekövetkező biztonsági eseményeket, illetve gyakorlati tanácsokat fogalmazott meg a megelőzésük, elhárításuk érdekében. A biztonsági események hivatali vagy vegyes használat (magán és hivatali) esetén ugyanígy előfordulnak, így a magánhasználat során elsajátított védelmi fogásokat tudjuk alkalmazni a hivatali használat során is, illetve fordítva.

A hivatali használat esetében azonban még nagyobb figyelmet kell fordítani a védelmi intézkedésekre, mert olyan adatokat tárolhatnak az eszközökön, melyek kompromittálódása esetén hatalmas kár keletkezhet. Azt is figyelembe kell venni, hogy előre meghatározott szabályokat kell követni, nemcsak ad hoc jelleggel, hanem folyamatosan, egészen a munkavállaló birtoklási ideje alatt a mobil eszköz teljes életciklusa folyamán. Nem elég azonban alkalmanként betartani és alkalmazni ezeket a szabályokat, hanem tudatosan, több oldalról megközelítve szükséges a mobil eszközök biztonságáról gondoskodni. Ezeket a védelmi intézkedéseket célszerű írásba foglalni, és minden olyan munkavállalóval dokumentáltan megismertetni, akik mobil eszközt használnak hivatali munkájuk során, függetlenül attól, hogy az eszköznek ki a tulajdonosa.

Állami és önkormányzati szervek esetében a szabályozást az állami és önkormányzati szervek elektronikus információbiztonságáról szóló 2013. évi L. törvény (a továbbiakban: Ibtv.) és a törvény végrehajtását szabályozó rendeletek figyelembevételével kell kialakítani.

3.1. Adminisztratív védelmi intézkedések

Adminisztratív védelemnek nevezzük a védelem érdekében hozott szervezési, szabályozási, ellenőrzési intézkedéseket, továbbá a védelemre vonatkozó oktatást.[11] Az adminisztratív intézkedések elsősorban szabályozási oldalról tartalmaznak előírásokat a különböző tevékenységekre, melyeket egységesen, valamennyi mobil eszközre vonatkozóan kell végrehajtani.

- Információbiztonsági politika és stratégia

A szervezetnek saját magára szabottan ki kell dolgozni információbiztonsági politikáját és megvalósítása érdekében a hozzá kapcsolódó információbiztonsági stratégiáját. Mind az információbiztonsági politikának, mind a stratégiának tartalmazni kell a mobil eszközökkel kapcsolatos elképzeléseket és az azok megvalósítására és végrehajtására utaló rendelkezéseket.

- Információbiztonsági szabályzat

Ahogy fentebb megfogalmaztuk, a szervezetnek rendelkezni kell informatikai biztonsági szabályzattal, amely intézkedik az összes elektronikus rendszerrel, eszközzel kapcsolatos teendőről, többek között a mobil eszközökről és azok használatáról is.

- Személyi vonatkozású intézkedések

A szabályozásnak ki kell terjednie a témáért felelős személyek kijelölésére és a hozzájuk kapcsolódó feladatok megfogalmazására is. Nemcsak a szervezet vezetőjének van felelőssége az információbiztonság területén, hanem a fentebb már említett Ibtv. alapján a szervezetnek ki kell jelölnie egy információbiztonságért felelős személyt is, aki a jogszabályokban meghatározott feladatok végrehajtásáért felel.

[11] Ibtv. 1. § 6. pont

- Intézkedési terv

Az információbiztonsági politika figyelembevételével kidolgozott stratégia alapján intézkedési terv készítése szükséges, hogy látható legyen, az információbiztonsági tevékenységeket hogyan, milyen formában, kinek a felelősségében, milyen határidővel kell megvalósítani.

- Nyilvántartások vezetése

Az elektronikus rendszerekről, a rendszerekhez kapcsolódó hardver elemekről és a rendszerek működtetéséhez szükséges szoftverekről nyilvántartást szükséges vezetni. Ebben a nyilvántartásban szerepeltetni kell a mobil eszközöket, illetve kapcsolódó alkalmazásaikat és szoftvereiket is.

- Biztonsági osztály és szint

Az elektronikus rendszereket biztonsági osztályba, míg a szervezetet biztonsági szintbe kell besorolni.

- Kockázatelemzés

Az információbiztonsági szabályzat része a kockázatelemzés, melyet a mobil eszközök vonatkozásában is el kell készíteni.

- Üzletmenet folytonosság

Az üzletmenet folytonosság leírása is részét képezi a szabályozásnak, mert meg kell fogalmaznia a szervezetnek azt, hogy milyen teendői vannak, ha bizonyos folyamatai nem megfelelően működnek, hogyan lehet azokat a normális működési szintre hozni. Biztonsági események

Ha biztonsági esemény történik, akkor arra reagálni kell és a szükséges lépéseket meg kell tenni, ezért célszerű ennek is írásban történő rögzítése, hogy előre kidolgozott protokoll alapján lehessen kezelni ezeket az eseményeket a bekövetkeztüktől egészen a folyamatjavító, helyesbítő intézkedések lezárásáig.

- Személyi biztonság

Az elektronikus rendszerekhez, eszközökhöz hozzáférő és azokat használó személyek ellenőrzését szabályozni kell, adott esetben, a szervezet sajátos előírásai szerint.

- A biztonságtudatosság fokozása, képzés

Az elektronikus rendszerekhez, eszközökhöz hozzáférő és azokat használó munkavállalók biztonságtudatosságának szintjére mindig figyelemmel kell lenni, és az eszközök magabiztosabb használata, valamint a biztonsági események megelőzése érdekében, rendszeresen vagy akár ad hoc módon is fejleszteni, emelni kell.

- Eszköz- és szolgáltatás-beszerzés

A különböző elektronikus rendszerekhez kapcsolódó hardver és szoftver, valamint a szolgáltatási elemek (pl. internet, karbantartás, javítás) beszerzésekor kellő körültekintéssel kell eljárni, ennek lépéseit és részleteit szabályozni szükséges. A mobil eszközök vonatkozásban fontos látni azt, hogy az eszközök és a kapcsolódó szolgáltatások hogyan szerezhetők, üzemeltethetők be vagy vehetők igénybe.

3.2. Fizikai védelmi intézkedések

A fizikai térben megvalósuló fenyegetések elleni védelem fontosabb részei a természeti csapás elleni védelem, a mechanikai védelem, az elektronikai jelzőrendszer, az élőerős védelem, a

beléptetőrendszer, a megfigyelőrendszer, a tápáramellátás, a sugárzott és vezetett zavarvédelem, a klimatizálás és a tűzvédelem.[12] A belépések kontrollállása

Bár a mobil eszközök nevében benne van, hogy azok elsősorban nem helyhez kötöttek, de természetesen ezek tárolására és időszakonkénti elhelyezésére is szükség van, ezért azokban az objektumokban, ahol ez megtörténik, ott mind az állandó, mind pedig az alkalmi jelleggel történő belépéseket a kockázatoknak megfelelően ellenőrizni és dokumentálni kell.

- A fizikai hozzáférések ellenőrzése

A belépéseken túl azt is kontrollálni szükséges, hogy a különböző rendszerekhez, eszközökhöz ki, hogyan férhet hozzá. A mobil eszközök esetében is szükséges ennek előírása és ellenőrzése.

- Szállítás, tárolás

A mobil eszközök, elnevezésükből adódóan is, szállíthatóak, ezért meg kell fogalmazni azokat a szabályokat, hogy ez, illetve tárolásuk hogyan, milyen állapotban és körülmények között történhet. Külön kell szabályozni, amikor ezeket az eszközöket beüzemelés előtt a szervezethez szállítják, vagy szükség esetén karbantartásuk, javításuk szükséges, amely nem a szervezet objektumában történik. Karbantartás, javítás

Gondolni kell a karbantartásra és javításra is, szabályozni kell, hogy ki, mikor, hogyan, milyen felhatalmazás alapján végezhet ilyen tevékenységet.

3.3. Logikai védelmi intézkedések

Logikai védelemnek nevezzük az elektronikus információs rendszerben információtechnológiai eszközökkel és eljárásokkal (programokkal, protokollokkal) kialakított védelmet.[13] Fontos területe a védelmi intézkedésnek a logikai szekció tekintettel arra, hogy habára fizikai kontrollokat kialakították és működnek, ezek a rendszerek, így a mobil eszközök is egy kibertérben működnek, a szükséges védelmet e vonatkózásban is kell alakítani.

- Engedélyezés

A rendszerekhez és eszközökhöz való hozzáféréseket engedélyezni szükséges, melynek részleteit az információbiztonsági szabályzatban szükséges lefektetni.

[12] Ibtv. 1. § 20. pont
[13] Ibtv. 1. § 34. pont

- Tervezés

Az elektronikus információs rendszereket meg kell tervezni, a szervezet felépítésével összhangban lévő rendszerbiztonsági tervet kell készíteni.

- Konfigurációkezelés

A konfigurációkezelés célja az informatikai infrastruktúra adatainak kézben tartása, az egyes komponensek beazonosítása, figyelemmel követése és karbantartása. Idetartozik az elektronikus rendszerelem leltár, melynek része a mobil eszközök nyilvántartása is, de ide sorolható a szoftverek, alkalmazások nyilvántartása is, illetve ezek bizonyos elemeinek korlátozása.

- Karbantartás

A karbantartás célja, hogy a szervezet biztosítani tudja a hivatali munkához szükséges eszközök és szolgáltatások zavartalan működését, esetleges hiba észlelésekor pedig azokat időben észlelhesse és javíthassa. Rendszeres karbantartás során az arra jogosultaknak szükséges ellenőrizni minden hardver és szoftver állapotát, és az esetlegesen észlelt hibák kijavításáról intézkedni kell. A karbantartás távoli eléréssel is megvalósítható.

- Adathordozók védelme

Rögzíteni kell az adathordozók védelmével kapcsolatos szabályokat, irányelveket is, köztük a mobil eszközökre mint adathordozókra vonatkozókat is. Itt kell rendelkezni többek között az adathordozók konkrét védelmi rendszeréről (pl. hardver titkosítás), hozzáférésükről, szállításukról, törlésükről.

- Azonosítás és hitelesítés

Azonosítási és hitelesítési eljárásrend kidolgozása is szükséges, melynek célja, hogy a munkavállalók, akik mobil eszközöket alkalmaznak mint felhasználók, minden esetben egyedileg legyenek azonosítva és hitelesítve. Meg kell különböztetni a tudás és a birtoklás alapú hitelesítést, és ezeket lehetőség szerint többlépcsős formában kell alkalmazni.

- A hozzáférés ellenőrzése

A különböző rendszerekhez, eszközökhöz és az azokban vagy azokon tárolt adatok vonatkozásában hozzáférési, jogosultságkezelési rendet kell kidolgozni, mely szabályozza az igényléstől annak törléséig a hozzáférés teljes életciklusát. A hozzáférés adása mindig szakmai alapon történik, figyelembevéve a szervezeti sajátosságokat és a munkakör adottságait is.

- Rendszer- és információ sértetlenség

Szükséges szabályozni a rendszerekhez történő hozzáféréseket, hogy a külső, belső kommunikáció ellenőrizhető legyen, csak az arra jogosultak ismerhessék meg az adatokat, ezért megfelelő tűzfalvédelem, kártékony kódok elleni védekezés kialakítása és szabályozása szükséges.

- Naplózás és elszámoltathatóság

A rendszerekben és eszközökön történő események hiteles naplózásnak kialakítása azért elengedhetetlen, hogy nyomon követhető és ellenőrizhető legyen a felhasználók tevékenysége.

A különböző védelmi intézkedéseket nem általánosságban vagy véletlenszerűen kell alkalmazni, hanem minden esetben a meghatározott biztonsági osztályba sorolt elektronikus információs rendszerek védelme érdekében kötelező alkalmazni.

4. A mobil eszközök hivatali használatának esetei

A különböző mobil eszközöket a munkavállalók széles körben alkalmazhatják hivatali tevékenységük, munkájuk során. Az eszközök felhasználási területét meghatározza, hogy milyen eszközzel és esetlegesen kiegészítőkkel rendelkezik a munkavállaló, illetve hogy az eszközzel milyen kapcsolódó szolgáltatást tud igénybe venni (pl. internet). A mobil eszközök lehetővé teszik, hogy a munkavállalók szinte helytől és időtől függetlenül tudjanak munkát végezni, kapcsolatot tartani kollégáikkal és külsős partnereikkel, valamint olyan dokumentációkat is elkészíteni, melyekkel időt és erőforrásokat tudnak megtakarítani.

A tanulmány ezen fejezetében a leggyakrabban előforduló felhasználási területek kapnak teret olyan formában, hogy meghatározzuk az eszközt, annak használható funkcióját, általánosságban a munkakört, valamint a felhasználási területet.

Az, hogy egy szervezeten belül kinek, milyen mobil eszköz, milyen kiegészítővel és szolgáltatással szükséges, minden esetben egyedileg eldöntendő, figyelembevéve a munkakör sajátosságait. Nemcsak az irodai, szellemi munkát végző munkavállalók láthatók el a különböző mobil eszközökkel, a fizikai munkavállalók elérhetősége (pl. ügyelet, karbantartás, szállítás, posta stb.) ugyanígy indokolt és szükséges lehet.

4.1. A mobiltelefonhoz kapcsolódó funkciók használata

A mobiltelefonok közül az okostelefon használata javasolt hivatali környezetben, mert azok tudása szinte egy kisebb kézi számítógépnek felel meg, nagyméretű színes érintőkijelzővel, kamerával, internetcsatlakozással és sok más kiegészítővel rendelkeznek, amelyeket maximálisan ki lehet használni munkavégzés közben. Az okostelefonhoz megfelelő mennyiségű mobilinternet szükséges, hogy funkciói rendeltetésszerűen használhatóak legyenek.

A mobiltelefon egyre gyakrabban váltja ki az asztali telefonokat, ma már szinte csak központi elérhetőségként adunk meg a külvilágnak vonalas asztali telefonszámot, pl. ügyfélszolgálatok, titkárságok, recepciók esetében.

Fontos szem előtt tartani, hogy a mobiltelefonok használhatóságának korlátot szab az akkumulátor üzemideje, ezért gondoskodni kell arról, hogy a készülékek minden esetben megfelelő töltöttségűek legyenek, vagy ha szükséges, kéznél legyen a töltéshez szükséges eszköz, akár irodai környezetben, akár például gépkocsiban utazva. Ha van rá lehetőség, külső akkumulátor (power bank) használatát is biztosítani érdemes.

Az okostelefonoknak a kijelző a legfőbb eleme, mert ezen keresztül lehet érdemben, funkcióinak megfelelően használni, ezért célszerű hivatali alkalmazásakor a munkavállalóknak olyan tokot vagy kijelzővédő fóliát, üveget biztosítani, amelyek legalább a közepes erőbehatásoktól megvédik, így jelentősen csökkenthetők a károk és a javításra fordított kiadások.

Mobiltelefonok esetében célszerű azt is felmérni, hogy milyen környezetben történik a használatuk, mert olyan helyen, ahol nagyobb igénybevételnek vannak kitéve, a külső környezet szennyezettebb lehet, érdemesebb olyan készüléket választani, amely bizonyos határig csepp-, por- és ütésálló. A funkciók használata során előfordulhatnak biztonsági események – melyeket a tanulmány 1. fejezetében fejtettünk ki –, de ezek megelőzhetők az egyes pontoknál felsorolt alapvető szabályok betartásával.

4.1.1. Híváskezdeményezés és -fogadás, SMS/MMS küldés és fogadás

A mobiltelefon alapfunkciói a hívás kezdeményezés és -fogadás, valamint az SMS és MMS (kép vagy videó küldése üzenet formájában) küldése és fogadása. A munkavállalók bármikor elérhetőek, függetlenül attól, hogy a szervezet objektumában tartózkodnak vagy sem, illetve ők is bárkit képesek elérni

Az előlapi kamera használatával bizonyos eszközök önmagukban, más eszközök alkalmazások telepítése után alkalmasak arra, hogy konferenciahívásokat lehessen tartani, egy időben több személy is egyszerre legyen vonalban, illetve, hogy videóhívásokat lehessen rajtuk lebonyolítani. Ez a funkció alkalmas lehet arra is, hogy a felhasználó a videohívás közben a környezetét bemutassa annak, akivel beszél, így akár élőképet is tud közvetíteni bizonyos tevékenységek közben. Ezen funkciókat minden munkakörben alkalmazni lehet, ahol szükséges az időtől és helytől független, telefonon történő, gyors kapcsolattartás, akár szervezeten belül, akár kívül is, például vezetők, asszisztensek, irodai alkalmazottak, területi munkát végzők, karbantartók, ügyeletesek, őrzés-védelmet ellátók, sofőrök, futárok esetében is.

A mobiltelefonon kezdeményezett hívásokkal kapcsolatban fel kell hívni a figyelmet arra, hogy bizonyos, például a szervezet objektumain kívül végzett területi munkák során, amikor a több személynek szükséges rövid időn belül, gyorsan kommunikálnia, akkor nem ez az eszköz a legmegfelelőbb hosszú távon, mert a hívások kezdeményezése és az egyes konkrét hívások szolgáltató általi felépítése időigényes, így értékes idő veszhet el olyan szituációkban, ahol minden pillanat számít. Ilyen esetekben más eszközt kell használni fő kommunikációs vonalként.

Ezen funkciók használata során felmerülő biztonsági eseményeket elkerülhetjük, ha

- mindig tudjuk, hogy hol a készülékünk;
- nem adjuk kölcsön másnak, és nem használjuk más készülékét;
- figyelemmel vagyunk a hívott és fogadott telefonszámokra, tudjuk, hogy kivel beszélünk;
- mielőtt bármit elküldünk üzenetben, ellenőrizzük a fogadó fél személyét és telefonszámát.

4.1.2. Internetes böngészés

A mobiltelefonokon található böngésző segítségével különböző weboldalak felkeresésére nyílik lehetőség, szükség szerint hírek olvasása, különböző információk beszerzése és keresések oldhatóak meg, helytől és időtől függetlenül. Ez a funkció jelentősen megkönnyítheti az irodai környezeten kívül, területen munkát végzők tevékenységét, például olyan esetben is, amikor hirtelen információra van szükség egy adott helyzetben, de nincs más lehetőség annak beszerzésére, különböző címek, telefonszámok, arcfényképek, menetrendek, nyitva tartások megtekintése stb.

A funkció minden okostelefonon megtalálható, tehát az a munkavállaló, akit munkaköre miatt ilyen eszközzel látnak el, ezt használni tudja. Az internetes böngészővel e-mailezésre is van lehetőség, melynek részletes kifejtése a következő pontban történik meg.

Az internet használata során felmerülő biztonsági eseményeket elkerülhetjük, ha

- ismert és biztonságos weboldalakat keresünk fel,
- figyeljük a biztonsági tanúsítványokat, és csak megfelelő oldal esetében adunk meg személyes adatot.

4.1.3. E-mail küldés és fogadás

Az okostelefonok képesek elektronikus levelezőrendszer kezelésére is, akár internetböngészőn vagy alkalmazáson keresztül is. A munkavállaló a részére küldött e-maileket bárhol és bármikor az eszközön elolvashatja és megválaszolhatja.

E-mailezés során elkerülhetjük a felmerülő biztonsági eseményeket, ha

- ismert e-mail címekre küldünk e-mail-t;
- megbízható mobil eszközökön használjuk a funkciót;
- ismeretlen feladótól származó e-mailre nem reagálunk, nem kattintunk a benne levő linkre, és nem töltjük le a mellékletét.

4.1.4. A dokumentumok megtekintése

A mobiltelefonokon lehetőség van különböző dokumentumok , például, Word, Excel, prezentáció, kép-, videó- és hangfájlok megtekintésére is. A dokumentumok megtekintése, adott esetekben a rájuk történő reagálás azon munkakörökben dolgozó munkavállalók részére hasznos például, akik jogosultak dokumentumok jóváhagyására, vagy irodai környezetben dolgoznak, és e-mailjeiket rendszeresen megtekintik mobiltelefonjukon.

Az ezen funkció alkalmazása során előforduló biztonsági eseményeket elkerülhetjük, ha

- csak olyan dokumentumokat tekintünk meg, melyek biztonságos forrásból származnak,
- illetve odafigyelünk arra, hogy a megtekintés során illetéktelen személyek ne lássák a kijelzőt.

4.1.5. Fénykép, videó- és hangfelvétel készítése

Az okostelefonok fel vannak szerelve olyan kamerákkal és mikrofonokkal, melyek fényképek, videók, hangfelvételek készítésére alkalmasak. Ezeknek a képeknek, videóknak és hangfelvételeknek, akárcsak korábban a hagyományos vagy digitális fényképezőgépekkel, videó kamerával készített felvételeknek a minősége változó lehet, a kamera felbontásától, a fényviszonyoktól, a mikrofon elhelyezkedésétől és a felhasználó ügyességétől függően.

A mobiltelefon használata gyorsabb lehet bizonyos élethelyzetekben, ezenkívül nem kelt feltűnést, valamint az elkészített felvétel – ha szükséges – rögtön továbbítható, például MMS-ként, e-mailben vagy más alkalmazáson keresztül. Ezen funkciók a hivatali munka során hasznosak lehetnek, ha meg kell örökíteni valamilyen tevékenységet folyamatában vagy annak végeredményét, illetve ha dokumentálni kell bizonyos történéseket, de megkönnyítheti a tárgyalások dokumentálását is. Jól használható ez a funkció például területen dolgozó munkavállalók esetében, ha meg kell örökíteni egy adott helyzetet, de például gépkocsihasználóknak is célszerű lehet egy esetleges forgalmi, baleseti helyzetben, illetve futárok is alkalmazhatják például küldemények sérülésének dokumentálására.

Biztonsági esemény ezen funkciók használata során is előfordulhat, a rögzített felvételek az eszközről kikerülhetnek illetéktelen személyekhez, illetve a munkavállalók esetleg visszaélhetnek ezzel, és olyan történéseket rögzíthetnek, melyet később felhasználhatnak a munkaáltató ellen. Az adatok kikerülése nagyfokú odafigyeléssel, biztonságtudatossággal elkerülhető, illetve az illegális használatot bizonyos környezetben történő korlátozással el lehet kerülni, így csökkentve a kockázatokat.

4.1.6. Alkalmazások használata

Az okostelefonokon különböző alkalmazásokat használhatunk, melyek egyszerűbbé tehetik a mindennapos munkavégzést, elősegíthetik például a kommunikációt, dokumentumok szerkesztését, de akár tájékozódásunkat is. A kommunikációt – akár belső, akár külső – könnyítheti különböző

csevegő vagy akár videókonferencia alkalmazások használata, melyekkel helytől és időtől függetlenül le lehet bonyolítani a szükséges megbeszéléseket, tárgyalásokat. A munkavállalók tájékozódását, közlekedését például navigációs alkalmazások segíthetik.

Az alkalmazások használata során elkerülhetjük a felmerülő biztonsági eseményeket, ha

- csak ellenőrzött, biztonságos alkalmazásokat használunk, és
- azokat rendszeresen frissítjük.

4.1.7. Távoli rendszerekhez, alkalmazásokhoz történő csatlakozás

A hivatali mobiltelefon alkalmas lehet arra, hogy olyan távoli rendszerekhez, alkalmazásokhoz kapcsolódjon, melyeket leggyakrabban irodai környezetből lehet elérni. Ehhez az szükséges, hogy a hivatali mobiltelefonra telepítve legyen a rendszer, illetve az alkalmazás, mely azonosítás után elérhetővé válhat, nemcsak az irodából, hanem távolról, hely- és időkorlát nélkül. Az ilyen elérések előnye lehet, hogy bizonyos események, történések azonnal rögzíthetőek egy rendszerben, és például a berögzített adatok így mások számára megismerhetők, feldolgozhatók.

Azon munkakörökben dolgozók mobiltelefonjára érdemes ilyen eléréseket telepíteni, akik sok időt töltenek az irodától távol, de szükséges, hogy a tevékenységükhöz kapcsolódó adatokat haladéktalanul vagy rövid időn belül rögzíteni tudják egyes rendszerekbe, illetve olyan személyeknek is hasznos lehet az ilyen elérés, akik a rendszerbe bevitt adatok alapján döntéseket hoznak, vagy ezeket az adatokat a továbbiakban feldolgozzák.

Távoli rendszerekhez, alkalmazásokhoz történő csatlakozás során is előfordulhatnak biztonsági események, de ezeket megelőzhetjük, ha

- mindig biztonságos módon csatlakozunk a rendszerekhez, alkalmazásokhoz, és
- megfelelő azonosítást és jelszót használunk a csatlakozáskor.

4.1.8. Helymeghatározás

A mobiltelefonon beállítható olyan funkció, mely alkalmas arra, hogy az eszköz földrajzi helyzetét meghatározhassuk. Az eszköz ilyenkor GPS jeladóként viselkedik, és ez alapján lehet megállapítani a helyzetét.

A helymeghatározási funkció hasznos lehet mind az eszköz, mind a birtokos helyzetének azonosítása szempontjából. Érdemes lehet használni több esetben is, például amikor a mobiltelefon kikerül a birtokos tulajdonából, és meg kell találni az eszközt, de abban az esetben is fontos lehet, amikor a birtokos felkutatása érdekében szükséges a helyzet meghatározása. Célszerű lehet olyan munkakörök esetében ezt a funkciót alkalmazni, amikor szükséges azt tudni és online látni, hogy az eszköz és annak használója hol tartózkodik. Ilyen munkakör lehet a területen dolgozóké, továbbá például ügyeleti vagy őrszolgálati tevékenységet végzőké.A helymeghatározás funkció alkalmazása során is történhetnek biztonsági események, de ezek kivédhetőek, ha csak olyan alkalmazás használata során alkalmazzuk, amely csak azokkal osztja meg ezt az információt, akikkel mi akarjuk.

4.1.9. Különböző funkciók összekapcsolása

A fentebb felsorolt funkciók közül több össze is kapcsolható, és olyan tevékenységek végezhetőek, amikor szükséges pontosan tudni, hogy ki, mikor, mit és hogyan csinált. Létrehozhatóak és üzemeltethetőek olyan rendszerek, amelyek egy mobiltelefonon keresztül elérhetőek, a birtokos vagy felhasználó egyedileg azonosítható, tevékenysége, fényképpel, videó- vagy hangfelvétellel

dokumentálható, majd a készített felvétel a rendszerbe betölthető, hozzáadva a tevékenység és a feltöltés idejét, valamint a helymeghatározás segítségével a tartózkodás és az esemény helyét.

Az így létrejövő dokumentumegység bizonyos feltételek fennállta esetén hiteles lesz, mások által is elérhető, kereshető, viszont megfelelő beállítások esetén módosíthatatlan. Az ilyen jellegű eszköz használat hasznos lehet a területen dolgozók munkaköreiben, de például alkalmazható sofőrök, futárok, ügyleti rendszerben dolgozók, továbbá őrzés-védelmi feladatokat ellátók esetében is.

4.2. Tablethez kapcsolódó funkciók használata

Napjainkban egyre jobban terjed a tabletek hivatali felhasználása bizonyos munkakörökben.

A tablet önállóan is képes internetkapcsolatra, de Wi-Fi-hez kapcsolódva vagy mobiltelefonról megosztott internettel is lehet működtetni. A tabletekhez kiegészítő eszközök csatlakoztathatóak, például billentyűzet vagy érintő ceruza, fül- és fejhallgató.

A tablet hivatali alkalmazásakor azt kell megvizsgálni, hogy van-e olyan munkakör a szervezetben, ahol nem elegendő vagy nem eléggé praktikus a mobiltelefon és a hordozható számítógép használata, hanem esetlegesen a tablet gyorsasága, könnyen kezelhetősége szükséges lehet, mert könnyíti és elősegíti a munkavégzést, vagy esetleg olyan pozitív képet közvetíthet a szervezetről, hogy innovatív megoldásokat alkalmazó, ezért reputációs értéke nőhet. A legtöbb esetben olyan munkakörökben érdemes tabletet alkalmazni, ahol idejük többségét irodán kívül töltik, de nem konkrétan egy másik, például egy ügyfél, partner irodájában, hanem esetleg a szabadban, gépjárműben vagy olyan objektumokban, ahol nincs konkrét helyhez kötött munkavégzés, viszont szükség van adminisztrálásra, dokumentálásra. Gyakran használnak tabletet az ügyfelekkel kapcsolattartó munkavállalók (pl. értékesítők, futárok), de lehetnek olyan munkakörök is, például tervezési, kivitelezési stb., ahol előnyös lehet egy ilyen eszköz használata. A sokat utazó munkavállalóknak, köztük a vezetőknek is érdemes lehet ilyen eszközt biztosítani, mert bizonyos esetekben egyszerűbb, gyorsabb és kényelmesebb a használata, például e-mailezésre, dokumentumok megtekintésére és alkalmazások használatára.

A mobiltelefonhoz hasonlóan szükséges gondoskodni a megfelelő akkumulátortöltésről és az eszköz fizikai védelméről.

A tablet használata során hasonló biztonsági események történhetnek, mint a mobiltelefon használata közben, amelyeket fentebb részletesen taglaltunk.

4.3. Hordozható számítógéphez kapcsolódó funkciók használata

A munkáltatók egyre gyakrabban látják el munkavállalóikat asztali számítógép helyett laptoppalA laptopok nemcsak alkalmazásokat, hanem szoftvereket is képesek futtatni, ezért felhasználási lehetőségük szélesebb, mint egy mobiltelefoné vagy tableté. Mára egyre kevesebb olyan munkakör van, ahol ne lenne elegendő egy megfelelő hardveres felszereltségű laptop, ezért a munkakörök nagy részében használható és kiváltható vele az asztali gép. A laptop ezért remekül alkalmazható a legtöbb munkakörben, mert nemcsak az irodában, de akár otthonról is folytatható vele munkavégzés, illetve a területen dolgozó munkavállalók akár utazás közben is használhatnak egy erős számítási kapacitással rendelkező eszközt. Jellemzően azokban a munkakörökben célszerű meghagyni vagy párhuzamosan alkalmazni az asztali gépet a laptoppal, ahol állandó bekapcsolt állapot szükséges, vagy nagy teljesítményre van szükség, például informatikusi, biztonsági, ügyfélszolgálati, tervezői munkakörökben, vagy kép-, videó- és hanganyagokkal dolgozók esetében.

A laptop önállóan képes internetkapcsolatra, de mobil internet stick-kel vagy Wi-Fi-hez kapcsolódva, továbbá mobiltelefonról megosztott internettel is lehet működtetni.

A mobiltelefonhoz hasonlóan szükséges a megfelelő akkumulátortöltésről és az eszköz fizikai védelméről gondoskodni.

A laptop használata során hasonló biztonsági események történhetnek, mint a mobiltelefon vagy a tablet használata közben.

5. A mobil eszközök hivatali biztosításának módjai[14]

A hivatali munka során meghatározott munkakörökben mobil eszközök használata válhat szükségessé. A munkavállalók többsége általában már rendelkezik egy vagy több mobil eszközzel, és ilyenkor a munkáltatónak döntenie kell, hogyan történjen az eszközök hivatali alkalmazása: a munkavállaló a saját eszközeit használja, vagy a munkáltató biztosítson eszközt a munkavégzéshez, vagy ezek valamilyen kombinációjával.

A munkáltató többféle lehetőség közül választhat, de minden esetben szem előtt kell tartani a megvalósítandó feladatot, az elérni kívánt célt, a költséghatékonyságot, az eszközök biztonságát információbiztonsági és adatbiztonsági szempontból, illetve a munkavállalók elégedettségéről sem feledkezhet meg.

A fejezet következő pontjai bemutatják, hogy a különböző mobil eszközök hivatali biztosításának milyen alternatívái vannak, hogy a munkáltató milyen módon biztosíthat mobil eszközöket a munkavállalóinak. SWOT (**S**trengths – Erősségek, **W**eaknesses – Gyengeségek, **O**pportunities – Lehetőségek, **T**hreats – Veszélyek) analízisen keresztül elemzem, milyen előnyei, hátrányai, lehetőségei és veszélyei vannak a különböző lehetőségeknek.

A hivatali mobil eszközök biztosításának lehetőségei a következők:

- **Implicit BYOD (Bring Your Own Device)**: Implicit „Hozd a saját eszközöd”, vagyis a munkavállaló a saját mobil eszközét használja hivatali munkavégzése során, de az eszközök semmilyen módon nincsenek integrálva a hivatali informatikai struktúrába.
- **Explicit BYOD (Bring Your Own Device)**: Explicit „Hozd a saját eszközöd”, vagyis a munkavállaló a saját mobil eszközét használja hivatali munkavégzése során, de az eszközök részben integrálva vannak a hivatali informatikai struktúrába (részben elérhető a hivatali belső hálózat, és az eszközön keresztül használható).
- **CYOD (Choose Your Own Device)**: A „Válassza ki saját készülékét” elv azt jelenti, hogy a szervezet meghatározza, hogy milyen típusú, márkájú eszközök használatát engedélyezi, és a munkavállalók ezek közül az eszközök közül választhatnak, és azokat használhatják hivatali munkájukhoz. Az eszköz lehet a munkavállaló sajátja is, de a szervezeté is, vagy a szervezet biztosíthatja valamilyen formában az eszközt, amely a munkavállaló tulajdonába kerül. Ebben az esetben az eszközök legalább részben integrálva vannak a hivatali informatikai struktúrába.
- **COPE (Corporate Owned, Personally Enabled)**: A „Vállalati tulajdonú, magánhasználat megengedett” lehetőség alkalmával az eszközök a szervezet tulajdonában vannak, a munkavállaló a munkavégzéséhez kapja azokat, de a hivatali használat mellett a magánhasználat is engedélyezett. Az eszközök integrálva vannak a hivatali informatikai struktúrába.
- **COBO (Corporate Owned, Business Only)**: A „Vállalati tulajdonú, csak üzleti célra” használt eszközök a szervezet tulajdonában vannak, a munkavállaló a munkavégzéséhez kapja azokat, és csak hivatali célra használhatja, a magánhasználat nem engedélyezett. Az eszközök integrálva vannak a hivatali informatikai struktúrába.

[14] Bizarro, Pascal A. PhD – Garcia, Andy PhD – Nix, Jacob: *Using Personal Mobile Devices in a Business Setting.* 2013. https://www.isaca.org/Journal/archives/2013/Volume-1/Pages/Using-Personal-Mobile-Devices-in-a-Business-Setting.aspx

5.1. Implicit BYOD (Bring Your Own Device)[15]

Az Implicit BYOD (Bring Your Own Device – Hozd a saját eszközöd) esetében a munkavállaló a saját mobil eszközét használja hivatali munkavégzése során, de az eszközök semmilyen módon nincsenek integrálva a hivatali informatikai struktúrába. Ez azt jelenti, hogy a munkavállaló rendelkezik saját mobil eszközzel, amit a munkáltatója kérésére a hivatali munkája során használni fog, ilyenkor a munkavállaló üzemelteti a saját eszközét. Ebben az esetben a munkáltatók mobil eszközei sokféle márkájú, típusú készülékek lesznek, melyek ezért különböző rendszerűek is lesznek. Ehhez hozzá kell venni, hogy a munkáltató is rendelkezik már valamilyen informatikai infrastruktúrával, amellyel ez a heterogén eszközhalmaz az esetek többségében nem biztos, hogy minden ponton kompatibilis lesz.

Az ezen típusú eszköz használat azt is jelenti, hogy a munkavállalók eszközei nincsenek a hivatal informatikai környezetével integrálva, tehát az eszközök hatékony együttműködése így nincs biztosítva. Az a lehetőség sem biztosított a munkáltatónak, hogy valóban nyomon tudja követni az eszközök és az azokon található alkalmazások, szoftverek naprakészségét, mely komoly információbiztonsági kockázatot jelent. Az ilyen jellegű eszközhasználat során a munkavállalók magánjellegű eszköz használata egyértelmű, mert a saját eszközét használja, amely mellé társul a hivatali használat is.

A munkáltatói oldalról ennek a modellnek a működése azt az előnyt biztosan jelenti, hogy kevesebb anyagi erőforrást kell azok beszerzésére fordítani, illetve megtakaríthatóak az adminisztrációval, üzemeltetéssel, karbantartással és javítással kapcsolatos költségek. A modell előnye lehet még a munkáltató számára, hogy a munkavállalók ismerik az eszközeiket, így azok használatával elégedettebbek lehetnek, ami növelheti a termelékenységet, a jobb és hasznosabb munkavégzést.

A hátrányok vizsgálatakor felmerülő kérdés a munkáltatói oldalról, hogyan használhatják a munkavállalók a hivatal rendszereit, hogyan csatlakozhatnak azokhoz biztonságosan, milyen adatok kerülhetnek az eszközökre, hogyan lehet az információbiztonsági, adatbiztonsági elveket érvényesíteni. Kérdés továbbá, hogyan lehet az eszközöket ellenőrizni, milyen lépéseket és ki tesz meg, ha valamilyen biztonsági esemény következik be, valamint mi a teendő abban az esetben, amikor a munkavállaló munkaviszonya megszűnik, mi történik az eszközén tárolt adatokkal.

A felelősség minden esetben a munkáltatóé, neki kell biztosítania azt, hogy a munkavállalók eszközei biztonságosan tudjanak csatlakozni a hivatali rendszerekhez, ki kell dolgozni a különböző adatok kezelésének rendjét, és azt be kell tartatnia. Ezenkívül fokozott figyelmet kell fordítania az információbiztonsági és adatbiztonsági tudatosság növelésére. Biztonsági esemény bekövetkeztekor haladéktalanul teljes támogatást kell nyújtania a munkavállalónak, és segítenie kell a károk minimalizálásában. Az ellenőrzési lehetőség minimálisra csökken ebben az esetben, szigorú adatvédelmi szabályokat kell betartania a munkáltatónak, melyek érdekes helyzeteket teremtethetnek ebben az alá-fölé rendelt jogviszonyban: a munkavállaló védettebb helyzetben lesz, a munkáltató saját adatainak viszonylatában kiszolgáltatottabbá válik. A munkaviszony megszűnésekor is nehéz helyzetben van a munkáltató, hogy hivatali adatainak sorsát megfelelően tudja rendezni a szervezettől távozó munkavállalóval. További problémát jelenthet, nehézkes lehet, illetve plusz adminisztrációval járhat a munkavállalókkal történő mobil eszköz használatból fakadó díjak és költségek elszámolása, kezdve például a telefonszámla, az internet csomagdíj kérdéskörétől az eszköz karbantartásán és javításán át, egy esetleges új eszköz beszerzésével bezárólag.

[15] Priyadarshi, Gaurav: *Leveraging and Securing the Bring Your Own Device and Technology Approach.* 2013. https://www.isaca.org/Journal/archives/2013/Volume-4/Pages/Leveraging-and-Securing-the-Bring-Your-Own-Device-and-Technology-Approach.aspx

S – Erősségek • A hardver és szoftver beszerzési költség csökkenése • A biztonságtudatosság növelése a munkavállalók körében • Elégedettebb munkavállaló • Hatékonyabb munkavégzés	**W – Gyengeségek** • Kompatibilitás hiánya • Sérülékeny informatikai rendszer • Az eszközök és adatok feletti kontroll hiánya • Munka és magélet egyensúlyának megbomlása a munkavállalók esetében
O – Lehetőségek • Informatikai rendszer fejlesztése • Más eszköz használati modell választása	**T – Veszélyek** • A szervezet elveszti a kontrollt az adatai felett • Kilépő munkavállalók könnyen elvihetik az adatokat • Információ- és adatbiztonsági incidensek számának növekedése

1. táblázat: Az implicit BYOD modell SWOT elemzése

A fenti elemzés alapján megállapítható, hogy olyan szervezetek esetében, ahol a munkavállalók száma magas, ezért több eszköz alkalmazása szükséges, illetve a szervezet komolyabb informatikai infrastruktúrával rendelkezik, nem jelent valódi és hatékony megoldást az implicit BYOD mobil eszköz használati modell alkalmazása.

Magas kockázatot jelent, ha nagy számban kezelnek adatokat, melyeket a munkavállalók rendelkezésére kell bocsátani, illetve olyan adatokat is kezelnek, melyek adott esetben minősítettnek vagy személyes, esetleg különleges személyes adatnak minősülnek, mert az adatok kikerülhetnek a szervezet hatóköréből, és biztonsági esemény alakulhat ki.

5.2. Explicit BYOD (Bring Your Own Device)[16]

Az Explicit BYOD rendszer (Bring Your Own Device – Hozd a saját eszközöd) esetében a munkavállaló a saját mobil eszközét használja hivatali munkavégzése során, de az eszközök részben integrálva vannak a hivatali informatikai struktúrába. Ez továbbra is azt jelenti, hogy a munkavállaló rendelkezik saját mobil eszközzel, amit a munkáltatója kérésére a hivatali munkája során használni fog.

Az explicit BYOD modell ugyanolyan alapról indul, mint az implicit BYOD, tehát a munkavállaló a saját mobil eszközét használja hivatali munkavégzése során, de az eszközök ebben az esetben legalább részben integrálásra kerülnek a hivatali informatikai struktúrába.

Alapjaiban ugyanazok az előnyök és hátrányok jellemzik az implicit és az explicit BYOD modellt is:

- A mobil eszközök sokféle márkájúak, típusúak, ezért különböző rendszerűek is. A munkáltató informatikai infrastruktúrája eltérő lehet, ami miatt kompatibilitási problémák adódhatnak.
- Magán célú használat továbbra is fennáll.
- A munkavállalók ebben az esetben is ismerik az eszközeiket, ezért elégedettebbek lehetnek, a jobb és hasznosabb munkavégzést.
- A munkáltatónak kevesebb költsége keletkezik a hardver és szoftver beszerzés során.

[16] Priyadarshi, Gaurav: *Leveraging and Securing the Bring Your Own Device and Technology Approach.* 2013. https://www.isaca.org/Journal/archives/2013/Volume-4/Pages/Leveraging-and-Securing-the-Bring-Your-Own-Device-and-Technology-Approach.aspx

Az eltérés a kettő között az, hogy az explicit BYOD alkalmazása esetén a munkavállaló saját mobil eszközét legalább részben integrálják a hivatali informatikai struktúrával, ezáltal megjelenik a munkáltató kontrollállási lehetősége, ebből kifolyólag csökkenteni tudja kockázatait.

Az eszközök integrációja azt jelenti, hogy a munkáltató egy mobil eszköz menedzsment rendszert (Mobile Device Management, a továbbiakban: MDM) működtet, melyekkel össze tudja fogni és hangolni a különböző mobil eszközök működését és használatát egy informatikai rendszeren belül. Az így felügyelt mobil eszközök biztonságosan tudnak csatlakozni, például VPN-en keresztül a hivatali hálózathoz, lehetővé téve például a biztonságos elektronikus levelezőrendszer vagy a belső hálózaton található alkalmazás használatát.

Az MDM rendszer, mobil applikáció menedzsment (Mobile Application Management, a továbbiakban: MAM) és mobil tartalom menedzsment (Mobile Content Management, a továbbiakban: MCM) rendszerekkel kiegészítve még erősebb kontroll kifejtésére tudja alkalmassá tenni a hivatali informatikai rendszert. Az MDM, az MAM és az MCM rendszerek használata lehetővé teszi a munkáltatónak, hogy csökkentse azokat a kockázatokat, amelyeket a munkavállalók a saját mobil eszköz használata miatt magukban hordoznak.

A rendszerek alkalmazása lehetővé teszi, hogy az eszközök távolról is elérhetőek legyenek, azokon szabályokat állítsanak be, védelmi rendszereket telepítsenek, a frissítések megtörténjenek, a használat kontrollálható legyen, beavatkozási lehetőség, akár törlés vagy zárolás távolról is megoldható legyen. Érvényesíthető és ellenőrizhető így például az eszközök szoftvereinek, alkalmazásainak frissítése vagy a jelszavak és jelkódok beállítása, továbbá észlelhetőek a biztonsági események, de lehetőség van hibaelhárításra is, és még a biztonsági mentések is megvalósíthatóak. A hivatali adatok védelme így már fokozottabban valósul meg, mert van lehetőség arra, hogy a munkáltató az adataihoz hozzáférjen, és adott esetben rendelkezzen felettük.

A munkáltatónak a fenti rendszerek használata mellett továbbra is nagy hangsúlyt kell fektetnie a munkavállalók biztonságtudatosságának fejlesztésére. A rendszerek használta sok kérdést megnyugtatóan tud rendezni, azonban nagy figyelmet kell fordítani az adatvédelmi jogszabályok betartására, mert a munkavállaló saját eszközére egy hivatali rendszert telepítenek, amely képes az eszköz használatát befolyásolni, illetve olyan adatokat gyűjteni, amely sértheti a magánéletéhez való jogát. A rendszereknek képeseknek kell lenniük arra, hogy elkülöníthető legyen a magán- és hivatali használat és az ezekből származó adatok.

Ebben az esetben is problémát jelenthet, nehézkes lehet, illetve plusz adminisztrációval járhat a munkavállalókkal történő mobil eszköz használatból fakadó díjak és költségek elszámolása.

S – Erősségek	**W – Gyengeségek**
• A hardver- és szoftver-beszerzési költség csökkenése • Nagyobb kontroll az eszközök és az adatok felett • A biztonságtudatosság növelése a munkavállalók körében • Elégedettebb munkavállaló • Hatékonyabb munkavégzés	• Részleges kompatibilitás • Sérülékenyebb informatikai rendszer • Menedzsment rendszerek költsége • Adatvédelmi szabályozás szükséges • A munka és a magánélet egyensúlyának megbomlása a munkavállalók esetében

O – Lehetőségek	T – Veszélyek
• Az informatikai rendszer fejlesztése • Más eszköz használati modell választása	• A kilépő munkavállalók elvihetik az adatokat • Növekedhet az információ- és adatbiztonsági incidensek száma

2. táblázat: Az explicit BYOD modell SWOT elemzése

A fentiek alapján összefoglalásként elmondható, hogy az explicit BYOD modell alkalmazása során már nagyobb kontroll alakítható ki az eszközök és az adatok felett, de továbbra sincs teljes kompatibilitás, ezért az informatikai rendszer sérülékenyebb marad, illetve a nagyobb kontroll mellett jelentős szerepet kap az adatvédelmi szabályok kialakítása és betartása, illetve továbbra is fennállhat a biztonsági események veszélye.

5.3. CYOD (Choose Your Own Device)

A CYOD modell (Choose Your Own Device – Válassza ki saját készülékét) azt jelenti, hogy a szervezet meghatározza, milyen típusú, márkájú mobil eszközök használatát engedélyezi, és a munkavállalók ezek közül az eszközök közül választhatnak, és azokat használhatják hivatali munkájukhoz. Az eszköz lehet a munkavállaló sajátja is, vagy a szervezet biztosíthatja valamilyen formában az eszközt, amely a munkavállaló tulajdonába kerül. Ebben az esetben az eszközök legalább részben integrálva vannak a hivatali informatikai struktúrába. Ez a modell átmenet a BYOD és a később ismertetendő COPE és COBO modellek között.

A BYOD modellhez képest előrelépés, hogy a szervezet meghatároz egy mobil eszköz márkát, típust, amely kompatibilis informatikai rendszerével, és ezek használatát engedélyezi a munkavállalóknak, akik ezek közül választhatnak, és használhatják hivatali munkájuk során. Ez az eszközmeghatározás a CYOD rendszer előnye, mert így biztosítható a szervezet informatikai struktúrájának és a munkavállalók által használt mobil eszközöknek a teljes kompatibilitása. Az eszközök a CYOD modellben is a munkavállalók tulajdonában vannak. A tulajdonba kerülés formája többféle lehet, például

- már a munkavállaló tulajdonában volt a készülék, és azt kezdi el használni;
- a munkavállaló saját maga szerzi be az eszközt, és kezdi el használni;
- az eszközt a munkáltató szerzi be és adja át valamilyen formájú juttatás vagy térítés ellenében a munkáltatónak, ami így a tulajdonába kerül, és ezt követően kezdődik meg a használat.

Az eszközmeghatározás és a beszerzési forma hátrányos lehet a munkavállalóra nézve, mert kényszerhelyzetben van az eszköz beszerzését illetően, nincs meg a szabadsága abban, hogy maga válassza ki az eszközt, és előfordulhat olyan eset, hogy olyan terméket kell vásárolni és használnia, amely számára nem komfortos, vagy a beszerzése jelentősebb anyagi terhet ró rá. A CYOD modell alkalmazása során is fontos kiemelni azt, hogy az ebben a formában üzemeltetett és használt mobil eszközöket legalább részben integrálják a hivatali informatikai struktúrával, ezáltal megjelenik a munkáltató kontrollállási lehetősége, ebből kifolyólag a kockázatok csökkenthetőek.

A megjelenő munkáltatói kontroll ugyanolyan elvek mentén épül fel és működik, mint az explicit BYOD modell alkalmazása esetén:

- MDM rendszer működtetése, melyekkel össze tudja fogni és hangolni a különböző mobil eszközök használatát egy informatikai rendszeren belül.

- Biztonságos csatlakozás például VPN-en keresztül a hivatali hálózathoz, lehetővé téve többek között a biztonságos elektronikus levelezőrendszer vagy a belső hálózaton található alkalmazás használatát.
- Az MDM rendszer kiegészíthető MAM és MCM rendszerekkel a hatékonyabb kontroll elérése érdekében, ez lehetővé teszi a munkáltatónak azt, hogy csökkentse azokat a kockázatokat, amelyeket a munkavállalók a saját mobil eszköz használat miatt magukban hordoznak.
- A rendszerek alkalmazása lehetővé teszi, hogy az eszközök távolról is szabályozottan elérhetők legyenek, így a hivatali adatok védelme már fokozottabban valósul meg, mert lehetőség van arra, hogy a munkáltató az adataihoz hozzáférjen, és adott esetben rendelkezzen felettük.
- A munkáltatónak a menedzsment rendszerek használata mellett továbbra is nagy hangsúlyt kell fektetnie a munkavállalók biztonságtudatosságának fejlesztésére.
- Ebben az esetben is lehetőség van az eszköz magáncélú használatára.

Ahogy az explicit BYOD esetében, a CYOD alkalmazásakor is a rendszerek használta sok kérdést megnyugtatóan tud rendezni, azonban itt is nagy figyelmet kell fordítani az adatvédelmi jogszabályok betartására, ahogy az előző pontban megfogalmaztuk. A rendszereknek képeseknek kell lenniük arra, hogy elkülöníthető legyen a magán- és hivatali használat és az ezekből származó adatok.

Ebben az esetben is problémát jelenthet és nehézkes lehet, illetve plusz adminisztrációval járhat a munkavállalókkal történő mobil eszköz használatból fakadó díjak és költségek elszámolása.

S – Erősségek	**W – Gyengeségek**
• Teljes kompatibilitás • A hardver- és szoftver-beszerzési költség csökkenése • Nagyobb kontroll az eszközök és az adatok felett • A biztonságtudatosság növelése a munkavállalók körében	• Menedzsment rendszerek költsége • Elégedetlenebb munkavállaló • A munkavégzési hatékonyság csökkenése • Adatvédelmi szabályozás szükséges • A munka és a magánélet egyensúlyának megbomlása a munkavállalók esetében
O – Lehetőségek	**T – Veszélyek**
• Az informatikai rendszer fejlesztése • Más eszközhasználati modell választása	• Az információ- és adatbiztonsági incidensek száma növekedhet

3. táblázat: A CYOD modell SWOT elemzése

A fentiek alapján megállapítható, hogy a CYOD modell alkalmasabb lehet az eszközök menedzselésére és üzemeltetésére, mint a BYOD modellek, de még mindig vannak olyan negatív tényezők, például adatvédelemi, elszámolási kérdések, amelyek folyamatos kockázatot jelenthetnek a szervezet részére, illetve figyelembe kell venni azt is, hogy a munkavállalók szinte kényszerpályára kerülnek az eszközök beszerzésekor.

5.4. COPE (Corporate Owned, Personally Enabled)

A COPE rendszer (Corporate Owned, Personally Enabled – Vállalati tulajdonú, magánhasználat megengedett) alkalmazásának esetében a mobil eszköz a szervezet tulajdonában van, a munkavállaló a munkavégzéséhez kapja azt, de a hivatali használat mellett, a magánhasználat is engedélyezett. Az eszközök teljesen integrálva vannak a hivatali informatikai struktúrába. Ennél a modellnél a szervezet biztosítja a mobil eszközöket a munkavállalói számára, a munkavállalók saját eszközének használatára nincs elehetőség a rendszerben. Ez azzal az előnnyel jár, hogy a hivatali informatikai struktúra teljesen

kompatibilis a mobil eszközökkel, így a biztonsági események száma csökkenthető. Ebben az esetben is szükséges a különböző menedzsment rendszerek (MDM, MAM, MCM) alkalmazása, hogy az informatikai infrastruktúra működése optimális lehessen.

A COPE rendszer előnye a szervezet számára az is, hogy a teljes kompatibilitásból kifolyólag az eszközök és az azokon tárolt adatok felett teljes kontroll kialakítására van lehetőség a mobil eszköz teljes életciklusa alatt. Ellenőrizhető például a használat, a szabályok betartása, a mindenkori frissítések, karbantartások elvégezhetőek, és szükség esetén távolról is törölhető, zárolható az eszköz vagy annak tartalma. Ennek ellenére a biztonságtudatosság fokozása ezen esetben is elengedhetetlen, mert szükséges az, hogy a munkavállalók mindig tudatosan használják eszközeiket, és ismerjék azokat a szabályokat, amelyeket be kell tartaniuk.

A munkavállalók is elégedettebbek lehetnek, mert korszerű, a rendszerrel kompatibilis mobil eszközöket kapnak használatba, melynek magánhasználata előre lefektetett és kialakított szabályok szerint lehetséges. További előny számukra, hogy alapvetően semmilyen költség nem jelentkezik az eszközökkel kapcsolatos beszerzéskor, üzemeltetéskor, karbantartáskor vagy javítás alkalmával.

Mivel a mobil eszközök magánhasználata is engedélyezett a szervezet által biztosított mobil eszközökön, de természetesen annak igénybevétele nem kötelező, bizonyos eszközök vonatkozásában méltányos lehet a felmerülő költségek megosztása valamilyen, akár az adó és számviteli szempontokat is figyelembe vevő költségtérítés formájában. Leggyakrabban egy havi költségkeretet állapítanak meg, amelynek túllépése esetén megvizsgálják, hogy az hivatali vagy magánhasználatból ered, és ha magánhasználatból, akkor azt a részt a munkavállaló megtéríti.

Leggyakrabban a mobiltelefon használatához, hanghívásokhoz, SMS-ek küldéséhez kapcsolódó keret-túllépések fordulnak elő, míg általában a mobil eszközök internethasználatával kapcsolatban nem szoktak költségtérítést alkalmazni, csak kivételes, például kiugróan magas külföldi roamingdíjak esetében.

A magánhasználat miatt azonban ennek a modellnek az alkalmazásakor is figyelemmel kell lenni a személyes adatok védelmére, és a hivatali használat ellenőrzésekor számolni kell vele. A hatályos adatvédelmi szabályok szerint ki kell alakítani az ellenőrzés szabályait, és aszerint kell eljárni minden esetben.

S – Erősségek	**W – Gyengeségek**
• Teljes kompatibilitás és kontroll az eszközök és az adatok felett • A biztonságtudatosság növelése a munkavállalók körében • Elégedett munkavállalók • Hatékony munkavégzés	• A hardver- és szoftver-költségek magasabbak • Menedzsment rendszerek költsége • Az informatikai rendszer fejlesztése • A költségtérítési modell kidolgozása • Adatvédelmi szabályozás szükséges
O – Lehetőségek	**T – Veszélyek**
	• Előfordulhatnak információ- és adatbiztonsági incidensek

4. táblázat: A COPE modell SWOT elemzése

A COPE modell alkalmas lehet olyan szervezetek számára, ahol nagyobb munkavállalói kört látnak el mobil eszközökkel, mert bár a beszerzés, üzemeltetési, karbantartási, és javítási költségek a szervezet számára többletkiadásként jelentkeznek, de ugyanakkor egységes, jól menedzselhető rendszer alakul ki, melynek sokkal nagyobb előnye, hogy a szervezet adatai nagyobb biztonságban vannak, és a biztonsági események száma így csökkenthető.

5.5. COBO (Corporate Owned, Business Only)

A COBO modell (Corporate Owned, Business Only – Vállalati tulajdonú, csak üzleti célra) alkalmazása esetén a használt mobil eszköz a szervezet tulajdonában vannak, a munkavállaló a munkavégzéséhez kapja azt, és csak hivatali célra használhatja, a magánhasználat nem engedélyezett. Az eszközök integrálva vannak a hivatali informatikai struktúrába. A COBO modell alapvetései, szabályai, alkalmazása megegyezik az előző pontban kifejtett COPE modellel, annyi különbséggel, hogy ebben az esetben a mobil eszközök magánhasználata nem engedélyezett, csak a hivatali ügyek intézéshez vehetők igénybe.

Mivel napjaink gyakorlatában nem feltétlenül lenne életszerű, hogy a mobil eszközök magánhasználata teljes tilalom alá essen, célszerű lehet a rendszert úgy felépíteni és működtetni, hogy a magáncélú használat alapvetően tilos, de annak megszegése bizonyos, például költségkeretek között, nem szankcionálandó. Azért szükséges ez a kitétel, mert adatvédelmi szabályok miatt nem mindegy, hogy magáncélra engedélyezett vagy sem az eszköz használata. Ha engedélyezett, akkor például egy azonnali hatályú felmondás esetén az eszközt nem lehet azonnal elvenni a munkavállalótól, mert lehetőséget kell számára biztosítani, hogy személyes adatait lementhesse az eszközről, és csak a hivatali adatokat hagyja rajta.

Ha viszont tilos a magáncélú használat, akkor elméletileg nem lehet az eszközön olyan tartalom, amely személyes adatot tartalmazhatna, ezért az eszköz azonnal elvehető, maximum a munkáltató jóindulatán múlik, hogy biztosít-e lementési lehetőséget a munkavállalónak, ha mégis lennének személyes adatai az eszközön. Az elvételt követően sem lehet viszont a munkáltató célja az, hogy a munkavállaló személyes adatait megismerje, ilyenkor a hatályos adatvédelmi szabályozás betartásával ezeket az adatokat dokumentáltan, lehetőleg törekedve a megismerés mellőzésére, törölni kell, és csak a hivatali adatokkal lehet a továbbiakban a megfelelő intézkedéseket megtenni.

Hasznos lehet ennek a modellnek az alkalmazása esetében is költségkeretrendszer kialakítása azért, hogy egy esetleges kerettúllépés esetén látható lehessen, hogy a szervezet meddig tolerálja az esetlegesen mégis előforduló magánhasználatot. Ez a tolerancia a munkavállalók elégedettségét jellemzően pozitív irányba befolyásolja.

S – Erősségek	**W – Gyengeségek**
• Teljes kompatibilitás és kontroll az eszközök és az adatok felett • A biztonságtudatosság növelése a munkavállalók körében • Elégedett munkavállalók • Hatékony munkavégzés	• Az informatikai rendszer fejlesztése • Hardver- és szoftver-költségek magasabbak • Menedzsment rendszerek költsége • Adatvédelmi szabályozás szükséges • Szükség esetén költségtérítési és szankciós modell kidolgozása
O – Lehetőségek	**T – Veszélyek**
	• Előfordulhatnak információ- és adatbiztonsági incidensek

5. táblázat: A COBO modell SWOT elemzése

A COBO modell alkalmazása szintén megfelelő lehet olyan szervezetek számára, ahol nagyobb munkavállalói kört látnak el mobil eszközökkel, és ebben az esetben is sokkal nagyobb előny – az anyagi ráfordítással szemben – egy egységes, jól menedzselhető rendszer kialakítása, melynek működtetésével a szervezet adatai nagyobb biztonságban vannak, és így csökkenthető a biztonsági események száma.

6. A mobil eszközök hivatali bevezetésének stratégiái[17]

Az előző fejezetben bemutattuk azokat a modelleket, amelyek alkalmazásával biztosítani lehet a munkavállalóknak a mobil eszközök hivatali használatát. Miután a szervezet kiválasztja, hogy melyik az a rendszer, amely alapján a leghatékonyabban, a legkisebb kockázatokkal tudja biztosítani a mobil eszközök hivatali használatát munkavállalóinak, meg kell vizsgálni, hogyan lehet ezeket bevezetni, a szervezet működésének részévé tenni.

6.1. Implicit BYOD (Bring Your Own Device)[18]

Az implicit BYOD modell alkalmazása esetén a következő lépéseket kell megtenni, hogy működőképesen bevezethető és alkalmazható legyen a rendszer.

- Kezdésként ki kell jelölni a bevezetésért felelős személyt, aki összeállítja a megfelelő támogatói csapatot, meghatározza a stratégiát, és kijelöli a határidőket.
- Az első lépés a felmérés, meg kell vizsgálni és el kell dönteni, hogy az implicit BYOD modell üzemeltetése-e a legmegfelelőbb a szervezet számára.
- Ha igen, meg kell határozni a stratégia megvalósítását lehetővé tevő feladatokat, majd felelősöket és határidőket kell hozzá rendelni.
- Meg kell határozni, hogy mely munkakörökben milyen mobil eszköz használata szükséges, és ezekről listát kell készíteni.
- Meg kell vizsgálni, hogy ha szükséges, a szervezet jelenlegi informatikai struktúrájához hogyan lehet illeszteni a használni kívánt eszközöket, de figyelemmel kell lenni arra is, hogy ebben az esetben a mobil eszközök nem kapcsolódnak a szervezet informatikai rendszereihez.
- Ki kell dolgozni a rendszer szabályozási hátterét is, hogyan történik az eszközök hivatali használatba történő bevonása, hogyan történik a költségek elszámolása stb.
- A szabályozás részévé kell tenni az információbiztonsági és adatvédelmi elvárásokat, irányelveket is.
- Ha szükséges, a munkavállalók munkaszerződését és munkaköri leírását is módosítani kell.
- A munkavállalókat megfelelő módon tájékoztatni kell, és a rendszer üzemeltetését meg kell kezdeni.
- Nem lehet megfeledkezni a biztonságtudatosság növeléséről sem, ezért a munkavállalóknak kötelező képzéseket kell szervezni.
- Mint minden rendszer bevezetését követően, az első időszakban folyamatosan felügyelni kell a működést, és ha szükséges, korrigálni kell a nem megfelelően működő területeket.

[17] Kassai Károly: *A mobil kommunikációs eszközök használatának és védelmi rendszabályainak szabályozása.* Hadmérnök, V. évfolyam, 3. szám, 2010. szeptember. http://hadmernok.hu/2010_3_kassai.pdf

[18] *Guidelines for Managing the Security of Mobile Devices in the Enterprise.* NIST Special Publication 800-124, Revision 1, 2013. https://nvlpubs.nist.gov/nistpubs/specialpublications/nist.sp.800-124r1.pdf

S – Erősségek	W – Gyengeségek
• Nincs hardver és szoftver beszerzési költség • A munkavállalóknál azonnal rendelkezésre állnak az eszközök • Biztonságtudatosság növelése a munkavállalók körében	• Növekszik az adminisztráció • Legalább 1 főnek részben az üzemeltetéssel kell foglalkoznia • Informatikai és biztonsági rendszerek fejlesztése • Nagyobb figyelmet kell fordítani az adatok biztonságára • Nincs kompatibilitás • Nem működik megfelelően a bevezetett modell
O – Lehetőségek	**T – Veszélyek**

6. táblázat: Az implicit BYOD modell bevezetésének SWOT elemzése

6.2. Explicit BYOD (Bring Your Own Device)[19]

Az explicit BYOD modell bevezetése esetén hasonlóan kell eljárni, mint az implicit változat esetében, egy dolog kivételével. Ez az eltérés az, hogy a mobil eszközök legalább részben csatlakoznak a szervezet már meglévő informatikai struktúrájához. Emiatt a különbség miatt a bevezetési stratégiába be kell építeni a már meglévő informatikai rendszerek felülvizsgálatát, meg kell vizsgálni, hogy a munkavállalók milyen eszközökkel akarnak csatlakozni a rendszerekhez. Az eredmény függvényében a már meglévő rendszerek fejlesztésére lehet, informatikai protokollok kidolgozása válhat szükségessé, melyek a csatlakozás menetét írják le.

Az informatikai rendszerek felülvizsgálata és esetleges fejlesztése még azelőtt időszerű, mielőtt az első mobil eszköz csatlakozása megtörténik, hogy megelőzhető legyen egy esetleges biztonsági esemény. A csatlakozás miatt ki kell dolgozni ennek nemcsak informatikai, de adminisztratív miként jét is és a vonatkozó szabályrendszert is.

S – Erősségek	W – Gyengeségek
• Nincs hardver- és szoftver-beszerzési költség • A munkavállalóknál azonnal rendelkezésre állnak az eszközök • A biztonságtudatosság növelése a munkavállalók körében	• Növekszik az adminisztráció • Legalább 1 főnek részben az üzemeltetéssel kell foglalkoznia • Nagyobb figyelmet kell fordítani az adatok biztonságára • Nagyobb figyelmet kell fordítani az informatikai rendszer védelmére • Nem működik megfelelően a bevezetett modell • Informatikai és biztonsági rendszerek fejlesztése • A kompatibilitás növelése
O – Lehetőségek	**T – Veszélyek** • Az információ- és adatbiztonsági incidensek száma növekedhet

7. táblázat: Az explicit BYOD modell bevezetésének SWOT elemzése

[19] *Guidelines for Managing the Security of Mobile Devices in the Enterprise.* NIST Special Publication 800-124, Revision 1, 2013. https://nvlpubs.nist.gov/nistpubs/specialpublications/nist.sp.800-124r1.pdf

6.3. CYOD (Choose Your Own Device)

A CYOD modell bevezetése esetén is hasonlóan kell eljárni, mint az explicit BYOD modell alkalmazásakor, de itt is van egy különbség, amelyre figyelemmel kell lenni a CYOD rendszer használatakor. A CYOD rendszerben is ugyanazokat a lépéseket kell megtenni, mint az előző pontban vázolt esetben, de azzal a különbséggel, hogy itt szükséges egy olyan mobil eszköz lista összeállítása, melyet a munkáltató hivatali használatra engedélyez a munkavállalói számára.
A lista összeállítását követően ki kell dolgozni azt is, hogy a munkavállalók hogyan jutnak hozzá az eszközhöz, saját maguknak kell beszerezniük, vagy a szervezet teszi ezt meg. Ha a szervezet szerzi be az eszközt, akkor meg kell határozni, hogy az milyen formában, honnan történjen meg, majd azt is részletezni kell, hogyan kerül a munkavállalók birtokába, tulajdonába. A szervezet eszközbeszerzése annyiból lehet költséghatékonyabb, hogy a nagyobb mennyiség miatt jobb áron tudja azt megtenni, így utána a munkavállalók is kedvezményesebb áron kaphatják meg. Az is megoldás lehet, hogy a munkavállalók vagy saját maguk szerzik be az eszközöket, és a forrásuk nem lényeges, de a munkáltató meghatározhatja azt is, hogy egy megbízható, minősített forrásból lehet csak az eszközöket beszerezni, de ezúton például kedvezményes árat biztosít a munkavállalóinak.

S – Erősségek	**W – Gyengeségek**
• Teljes kompatibilitás • A munkavállalói elégedettség nő • A biztonságtudatosság növelése a munkavállalók körében	• Ki kell dolgozni egy eszköz listát • Növekszik az adminisztráció • Legalább 1 főnek részben az üzemeltetéssel kell foglalkoznia • Esetlegesen van hardver- és szoftverköltség • Időlegesen lehet hardver- és szoftverköltség • Nem működik megfelelően a bevezetett modell • Informatikai és biztonsági rendszerek fejlesztése
O – Lehetőségek	**T – Veszélyek**

8. táblázat: A CYOD modell bevezetésének SWOT elemzése

6.4. COPE (Corporate Owned, Personally Enabled)

Ugyanúgy, ahogy a BYOD modellnél, itt is ugyanazokat az alapvető lépéseket kell megtenni, a következő különbségekkel: A mobil eszközöket a szervezet szerzi be és készíti fel a hivatali használatra, és ezzel egy időben ki kell alakítani az üzemeltetési, karbantartási és javítási infrastruktúrát is.

Ki kell dolgozni a rendszer szabályozási hátterét is: hogyan történik az eszközök kiosztása, használata, visszavétele, törlése, rendszerből történő kivonása stb. A szabályozás részévé kell tenni az információbiztonsági és adatvédelmi elvárásokat, irányelveket is, valamint az ellenőrzéssel kapcsolatos szabályokat is. Meg kell határozni a magánhasználat módját és határait is, valamint a kapcsolódó költségek viselésének alapjait is.

S – Erősségek	W – Gyengeségek
• Teljes kompatibilitás • Teljes kontroll • A biztonságtudatosság növelése a munkavállalók körében • A munkavállalói elégedettség nő	• Hardver- és szoftver-költség • Növekszik az adminisztráció • Legalább 1 főnek részben az üzemeltetéssel kell foglalkoznia • Nem működik megfelelően a bevezetett modell • Informatikai és biztonsági rendszerek fejlesztése
O – Lehetőségek	**T – Veszélyek**

9. táblázat: A COPE modell bevezetésének SWOT elemzése

6.5. COBO (Corporate Owned, Business Only)

A COBO modell bevezetése hasonló stratégia mentén történik, mint a COPE modellé, annyi különbséggel, hogy itt külön rendelkezni kell a magánhasználat tiltásáról és esetleges szankcionálásáról.

S – Erősségek	W – Gyengeségek
• Teljes kompatibilitás • Teljes kontroll az eszközök és az adatok felett • Elégedett munkavállalók • Hatékony munkavégzés • A biztonságtudatosság növelése a munkavállalók körében	• Hardver- és szoftver-költségek magasabbak • Menedzsment rendszerek költsége • Adatvédelmi szabályozás szükséges • Informatikai rendszer fejlesztése • Szükség esetén költségtérítési és szankciós modell kidolgozása
O – Lehetőségek	**T – Veszélyek** • Előfordulhatnak információ- és adatbiztonsági incidensek

10. táblázat: A COBO modell bevezetésének SWOT elemzése

Az egyes modellek vegyítése és ilyen módon való bevezetése nem előnyös, mert a különböző módokon használt eszközök adminisztrálása bonyolulttá válhat, illetve a munkavállalók között feszültséget okozhat, ha valamelyik modell előnyösebb lehet az egyik csoportnak a többi munkavállalóval szemben.

Célszerű a modelleket magukban, tisztán alkalmazni, azzal a kikötéssel, hogy ha a felhasználási rendszert megváltoztatják, akkor teljes átállást hajtanak végre, melyre alaposan felkészül a szervezet, hogy gyors és zökkenőmentes lehessen.

7. A mobil eszközök hivatali használatának jogi vetületei

A mobil eszközök hivatali használatának eseteiben nemcsak az informatikai, információbiztonsági szabályok vizsgálata elengedhetetlen, hanem a hatályos jogi szabályozás feltárása, vizsgálata és bemutatása is. Szükségessége azért indokolt, mert tisztázni kell azt, hogy a hatályos jogi szabályozás tartalmaz-e olyan jogi előírásokat, amelyekre tekintettel kell lenni az eszközök hivatali alkalmazásának bevezetése, használata során, akár személyügyi, akár információbiztonsági, vagy adatvédelmi, esetleg a minősített adatok kezelésével kapcsolatos területeken. Jelen fejezetben ezeket a területeket elemzem a jogi szempontok alapján.

7.1. Személyügy

A személyügyi kérdések tisztázása elengedhetetlen abból a szempontból, hogy van-e jogszabályi előírás a munkavállalók mobil eszköz használatával kapcsolatosan.

- Közalkalmazottak

A közalkalmazottak jogállásáról szóló 1992. évi XXXIII. törvény (a továbbiakban: Kjt.) nem rendelkezik ezen munkavállalói csoport mobil eszköz használatáról.

- Közszolgálati tisztviselők

A közszolgálati tisztviselőkről szóló 2011. évi CXCIX. törvény (a továbbiakban: Kttv.) nem tartalmaz rendelkezést ezen foglalkoztatotti csoport mobil eszköz használatáról.

- Rendvédelmi feladatokat ellátó szervek hivatásos állománya

A rendvédelmi feladatokat ellátó szervek hivatásos állományának szolgálati jogviszonyáról szóló 2015. évi XLII. törvény (a továbbiakban: Hszt.) 30. §-a a tulajdonjog gyakorlásának korlátozásával kapcsolatban rendelkezik a magáncélú telekommunikációs eszközökkel kapcsolatosan. „30. § Az országos parancsnok, az országos főigazgató vagy az állományilletékes parancsnok munkabiztonsági okból vagy a szolgálatellátás rendjének fenntartása és ellenőrizhetősége érdekében megtilthatja, hogy a hivatásos állomány tagja a szolgálatban a miniszteri rendeletben meghatározott egyes vagyontárgyakat, magáncélú telekommunikációs eszközöket, valamint meghatározott összeget meghaladó készpénzt vagy – a bankkártya kivételével – a hitelintézetekről és a pénzügyi vállalkozásokról szóló törvény szerinti készpénz-helyettesítő fizetési eszközt magánál tartson, továbbá korlátozhatja a magáncélú telekommunikációs eszközöknek a szolgálatellátás során történő használatát.” [20]

Ez azt jelenti, hogy ha az implicit vagy explicit BYOD, vagy a CYOD modellt alkalmazza egy szervezet, akkor figyelemmel kell lenni az idézett jogszabályhely rendelkezéseire, mert ha a hivatásos állomány saját mobil eszközét használja hivatali célból, akkor ez a helyzet ellentmondásos lehet számukra.

Az országos parancsnoknak, az országos főigazgatónak vagy az állományilletékes parancsnoknak a 30. §-ban foglalt tiltó rendelkezés meghozatala és kihirdetése előtt minden esetben meg kell vizsgálni, hogy milyen modell alapján történik a mobil eszközök hivatali használata, és ha az említett modellek szerint, akkor erre figyelemmel kell a tiltást – az ellentmondást feloldó megfelelő kiegészítésekkel – megfogalmazni és közzétenni.

- A munkatörvénykönyve alapján foglalkoztatottak

A munka törvénykönyvéről szóló 2012. évi I. törvény (a továbbiakban: Mt.) tartalmaz rendelkezéseket a jogszabály alapján foglalkoztatott személyekre vonatkozóan.

[20] Hszt. 30. §

Az 51. § (1) bekezdése szerint a munkáltató köteles a munkavállaló munkavégzéshez szükséges feltételeket biztosítani, tehát szükség esetén mobil eszköz használatát is biztosítani, ha ez a munkavégzéshez szükséges.

Távmunkavégzés során a 196. § (1) bekezdése szerint a munkavállaló a munkáltató telephelyétől elkülönült helyen rendszeresen tevékenységet folytat információtechnológiai vagy számítástechnikai eszközzel, és eredményét elektronikusan továbbítja. Ebben az esetben a munkáltatónak előzetesen tájékoztatni kell a munkavállalót a munkáltató általi ellenőrzésről, a számítástechnikai vagy elektronikus eszköz használata korlátozásának szabályairól.

A 197. § (2) bekezdése szerint a munkáltató előírhatja, hogy az általa biztosított számítástechnikai vagy elektronikus eszközt a munkavállaló kizárólag a munkavégzéshez használhatja. A (3) bekezdés alapján a munkavégzés ellenőrzése során a munkáltató nem tekinthet be a munkavállalónak a munkavégzéshez használt számítástechnikai eszközön tárolt, nem a munkaviszonnyal összefüggő adataiba. A betekintési jogosultság tekintetében a munkaviszonyból származó kötelezettséggel összefüggő adatnak minősül a (2) bekezdés alapján előírt tilalom vagy korlátozás betartásának ellenőrzéséhez szükséges adat.

Bedolgozói munkaviszony esetén a 199. § (2) bekezdése szerint a munkavállaló, eltérő megállapodás hiányában, feladatát a saját eszközeivel végzi, tehát ennek alapján a saját mobil eszközét is használhatja.

7.2. Információbiztonság

Az Ibtv. szerint elektronikus információs rendszernek minősül az adatok, információk kezelésére használt eszközök (környezeti infrastruktúra, hardver, hálózat és adathordozók), eljárások (szabályozás, szoftver és kapcsolódó folyamatok), valamint az ezeket kezelő személyek együttese.[21] Az előző fogalommeghatározásból következik, hogy a mobil eszközök elektronikus információs rendszerelemnek minősülnek, ezért a jogszabály értelmében védelemben kell őket részesíteni. A törvény rendelkezéseit a 2. § (1) bekezdés a) pontja szerint a központi államigazgatási szervekre is alkalmazni kell. A jogszabályban a hivatali mobil eszköz használat konkrétan nem jelenik meg, viszont arról más kapcsolódó jogi szabályozás rendelkezik.

A törvény végrehajtásáról szól a 41/2015. (VII. 15.) BM rendelet az állami és önkormányzati szervek elektronikus információbiztonságáról szóló 2013. évi L. törvényben meghatározott technológiai biztonsági, valamint a biztonságos információs eszközökre, termékekre, továbbá a biztonsági osztályba és biztonsági szintbe sorolásra vonatkozó követelményekről már közvetve és közvetlenül is megfogalmaz elvárásokat a mobil eszközök vonatkozásában. Ezen előírásokat, más egyebekkel együtt, információbiztonsági szabályzatba kell foglalnia a szervezetnek. Az információbiztonsági szabályzat felépítését a tanulmány 3. fejezetében már részletesen ismertettem.

Az említett rendelet 3.3.8. pontjában az Adathordozók védelméről rendelkezik. A mobil eszközök adathordozóknak is tekinthetőek, ezért az előírásokat hivatali alkalmazásuk során be kell tartani és be kell tartatni a használókkal.

A 3.3.8. pont leírja, hogy a szervezet részéről az adathordozók védelmével kapcsolatos eljárásrend megfogalmazása szükséges, melyet meghatározott gyakorisággal felülvizsgálni és frissíteni kell. Rendelkezni kell továbbá az adathordozókhoz történő hozzáférésről, azokat címkézni kell, megfelelő módon tárolni, szállítani, kriptográfiai védelemmel ellátni. Meg kell határozni a

[21] Ibtv. 1. § 14b. pont

helyreállíthatatlanságot biztosító törlési technikákat, eljárásokat, és ezt ellenőrizni, tesztelni kell. Meg kell fogalmazni az adathordozók használatának a rendjét is.

A rendelet 3.3.10. pontja a hozzáférések ellenőrzését írja le, s a 3.3.10.15. pontban konkrétan megjelenik a mobil eszközök hozzáférésének ellenőrzése. A szervezetnek belső szabályozásában felhasználási korlátozásokat, konfigurálásra és kapcsolódásra vonatkozó követelményeket, valamint technikai útmutatót kell kiadnia az általa ellenőrzött mobil eszközökre, továbbá engedélyhez kell kötnie az elektronikus információs rendszereihez mobil eszközökkel megvalósított kapcsolódást. A következő pontban megfogalmazásra kerül az eszközök titkosítása is, a szervezet teljes eszköztitkosítást, tároló alapú titkosítást vagy más technológiai eljárást alkalmaz az általa meghatározott mobil eszközökön tárolt információk bizalmasságának és sértetlenségének a védelmére vagy az információk hozzáférhetetlenné tételére. [22]

A 3.3.10.16.3. pontja szerint a hordozható adattároló eszközökkel kapcsolatban a szervezetnek lehetősége van arra, hogy korlátozza vagy megtiltsa az ellenőrzött hordozható tárolóeszközök használatát a külső elektronikus információs rendszerben is jogosultsággal rendelkező személyek számára.

Bár nem tartozik közvetlenül a mobil eszközökhöz az elektronikus információs rendszeren keresztüli hangátvitel (a továbbiakban: VoIP), de például hordozható számítógépen is lehetőség van olyan szoftver használatára, melyen így is lehet kommunikálni, ezért figyelemmel kell lenni a rendelet 3.3.13. pontjában található Rendszer- és kommunikációvédelmi előírásokra. A 3.3.13.15.1.1. pont alapján a szervezet használati korlátozásokat vezethet be, vagy megvalósítási útmutatót adhat a VoIP technológiákhoz, felmérve a rosszindulatú használat esetén az elektronikus információs rendszerben okozható károkat, illetve a következő pont szerint engedélyezi, felügyeli és ellenőrzi a VoIP használatát az elektronikus információs rendszeren belül.

Ahogy a 2. fejezet végén is megállapítást nyert, de érdemes még egyszer kiemelni, hogy a különböző védelmi intézkedéseket nem általánosságban vagy véletlenszerűen kell, hanem minden esetben meghatározott biztonsági osztályba sorolt elektronikus információs rendszerek védelme érdekében kötelező alkalmazni.

7.3. Adatvédelem

Az adatvédelem területén az Európai Parlament és a Tanács (EU) 2016/679 rendelete a természetes személyeknek a személyes adatok kezelése tekintetében történő védelméről és az ilyen adatok szabad áramlásáról, valamint a 95/46/EK rendelet hatályon kívül helyezéséről (általános adatvédelmi rendelet) (a továbbiakban: GDPR), valamint az információs önrendelkezési jogról és az információszabadságról szóló 2011. évi CXII. törvény (a továbbiakban: Infotv.) az irányadó.

A jogszabályok kiegészítéseként figyelembe kell venni a Nemzeti Adatvédelmi és Információszabadság Hivatal (a továbbiakban: NAIH) ajánlásait és állásfoglalásait is.

Az adatvédelmi részt a hivatali mobil eszköz használat modelljeinek részletezésekor, az 5. és 6. fejezetekben már részben bemutattam.

Az adatvédelem kérdése azért fontos, mert a különböző használati rendszerek alkalmazása esetén a használó munkavállaló személyes adatai az eszköz használatából kifolyólag megjelenhet, illetve az eszközön tárolódhat.

[22] 41/2015. (VII. 15.) BM rendelet 3.3.10.15.1.1., 3.3.10.15.1.2., 3.3.10.15.2. pontok

Ha a szervezet olyan mobil eszköz alkalmazást üzemeltet, melynek során az eszköz a munkavállalóé (BYOD, CYOD), akkor a magánhasználat egyértelmű a felhasználó részéről. Ebben az esetben figyelemmel kell lenni arra, hogy a mobil eszköz integrálása megtörténik-e a szervezet informatikai infrastruktúrájával, és ha igen, akkor milyen mértékben. Tisztázni kell, hogy a munkáltató képes lesz-e a munkavállaló saját tulajdonú eszközét bármilyen formában ellenőrizni, mert ha igen, akkor ennek részleteiről a munkavállalót a jogi szabályozásnak megfelelően tájékoztatni kell, illetve a szükséges szabályozást ki kell hozzá dolgozni.

Ha olyan mobil eszköz használati modellt vezetnek be a szervezetnél, ahol az eszközt a munkáltató biztosítja a munkavállalók részére (COPE, COBO), a használatba adás előtt szabályozni kell a magánhasználat lehetőségét, konkrétan meg kell fogalmazni, hogy engedélyezett-e vagy sem. Ha nem engedélyezett, akkor is előfordulhat, hogy a munkavállaló személyes adata megjelenhet vagy tárolódhat az eszközön. Ebben az esetben is gondoskodni kell arról, hogy a munkavállalók a megfelelő tájékoztatást megkapják, és a szabályozás kidolgozása ugyanúgy szükségessé válik.

Mindegyik esetben szükséges még az ellenőrzési folyamat kialakítása: ki, hogyan, mit és mikor ellenőrizhet a mobil eszközök vonatkozásában. A kialakított szabályokról a mobil eszközöket használó munkavállalókat tájékoztatni szükséges.

7.4. Minősített adatok

Ha a szervezet minősített adatokat is tartalmazó dokumentumokat is tárol, szerkeszt stb. a mobil eszközökön, akkor figyelemmel kell lenni és be kell tartani a minősített adat védelméről szóló 2009. évi CLV. törvény (a továbbiakban: Mavtv.) rendelkezéseit. A jogszabály alapján a minősített adat lehet nemzeti és külföldi is.

Nemzeti minősített adatnak nevezzük a minősítéssel védhető közérdekek körébe tartozó, a minősítési jelölést a törvényben, valamint a törvény felhatalmazása alapján kiadott jogszabályokban meghatározott formai követelményeknek megfelelően tartalmazó olyan adatot, amelyről – megjelenési formájától függetlenül – a minősítő a minősítési eljárás során megállapította, hogy az érvényességi időn belüli nyilvánosságra hozatala, jogosulatlan megszerzése, módosítása vagy felhasználása, illetéktelen személy részére hozzáférhetővé, valamint az arra jogosult részére hozzáférhetetlenné tétele a minősítéssel védhető közérdekek közül bármelyiket közvetlenül sérti vagy veszélyezteti, és tartalmára tekintettel annak nyilvánosságát és megismerhetőségét a minősítés keretében korlátozza. [23]

Külföldi minősített adatnak nevezzük az olyan adatot, amelyet az Európai Unió valamennyi intézménye és szerve, továbbá az Európai Unió képviseletében eljáró tagállam, a külföldi részes fél vagy nemzetközi szervezet által készített és törvényben kihirdetett nemzetközi szerződés vagy megállapodás alapján átad, amelyhez történő hozzáférést az Európai Unió intézményei és szervei, az Európai Unió képviseletében eljáró tagállam, más állam vagy külföldi részes fél, illetve nemzetközi szervezet minősítés keretében korlátozza. [24]

A jogszabály a biztonsági feltételek megteremtéséről rendelkezik a 10. §-ban:

(4) Minden olyan szervnél, ahol minősített adatot kezelnek, meg kell teremteni a minősített adat védelméhez szükséges, az adat minősítési szintjének megfelelő,

> a) az e törvényben és a végrehajtására kiadott rendeletekben meghatározott személyi, fizikai és adminisztratív, valamint

[23] Mavtv. 3. § 1. a) pont
[24] Mavtv. 3. § 1. b) pont

b) ha a szerv a minősített adatot elektronikus információs rendszeren kezeli, az e törvényben és az elektronikus információbiztonságról szóló törvényben és végrehajtásukra kiadott jogszabályokban meghatározott elektronikus biztonsági feltételeket.

(5) Minden olyan helyiséget, épületet, építményt, ahol minősített adatot kezelnek, fizikai biztonsági intézkedésekkel kell védeni az arra nem jogosult személyeknek a minősített adathoz történő hozzáférése ellen.

(6) Az adminisztratív biztonsági intézkedésekkel gondoskodni kell a minősített adat nyomon követhetőségéről, bizalmasságáról, sérthetetlenségéről, rendelkezésre állásáról.

(7) Elektronikus biztonsági intézkedéseket kell tenni az elektronikus rendszeren kezelt minősített adat és az elektronikus rendszer bizalmassága, sérthetetlensége és rendelkezésre állása érdekében.

(8) A biztonsági feltételek tervezése során figyelembe kell venni:

a) a kezelt minősített adat minősítési szintjét,

b) a minősített adat mennyiségét és megjelenési formáját,

c) a helyszín és a szerv, illetve az elektronikus rendszer veszélyeztetettségi szintjét és sebezhetőségét, valamint

d) a nemzetbiztonsági kockázatokat.

A fentiek is, ahogyan más jogszabály is, azt mutatják, hogy többek között a mobil eszközök alkalmazása estén is szükséges a szervezetnek különböző adminisztratív, fizikai és elektronikus biztonsági intézkedéseket megtenni.

Az idézett szabályozást egészítik ki a törvényhez kapcsolódó végrehajtási rendeletek, a 90/2010. (III. 26.) Korm. rendelet a Nemzeti Biztonsági Felügyelet működésének, valamint a minősített adat kezelésének rendjéről és a 161/2010. (V. 6.) Korm. rendelet a minősített adat elektronikus biztonságának, valamint a rejtjeltevékenység engedélyezésének és hatósági felügyeletének részletes szabályairól.

A 90/2010. (III. 26.) Korm. rendelet 59. § (2) és (3) bekezdései a következőket rögzítik:

(2) A minősített adatot kezelő szerv vezetője biztosítja, hogy azok a biztonsági területek, ahol „Titkos!”, vagy ennél magasabb minősítési szintű minősített adatokról rendszeresen tárgyalnak, lehallgatás mentesek legyenek.

(3) A katonai, nemzetbiztonsági és bűnügyi műveletekben a személyi biztonsági tanúsítvánnyal rendelkező személy személyes felügyelete alatt álló minősített adatot tartalmazó technikai eszköz, valamint a művelet végrehajtásához szükséges minősített adat, a minősített adatot kezelő szerv vezetője vagy a biztonsági vezető által meghatározott biztonsági intézkedések betartása mellett biztonsági területen kívül is felhasználható.

A (2) bekezdésben megfogalmazottak biztosításának érdekében célszerű figyelembe venni a mobil eszközök azon negatív lehetőségeit, hogy a rajtuk található kamerák és hangszórók távolról üzembe helyezhetőek, azok jogosulatlanul használhatóak és így akár biztonsági esemény is bekövetkezhet.

A 161/2010. (V. 6.) Korm. rendelet 1. § 9. pontjában, meghatározásra kerül a rejtjel anyag fogalma, és az a) és e) pontja érdekel figyelmet a témát illetően:

1. § 9. rejtjelanyag:

a) a rejtjelezés céljára szolgáló gépek, berendezések, számítástechnikai és egyéb eszközök,

…

e) más rendeltetésű számítástechnikai eszközök, amennyiben rejtjelező programot működtetnek vagy a rejtjelezés folyamatát szolgáló adatokhoz hozzáférhetnek, vagy ilyen adatot tartalmaznak,…

A mobil eszközök számítástechnikai eszköznek is minősülnek, ezért ebben az esetben erre is figyelemmel kell lenni.

A Kormányrendelet **2. §** (1) bekezdése szerint minősített adat kizárólag olyan rendszeren kezelhető, amely rendelkezik a Nemzeti Biztonsági Felügyelet (a továbbiakban: NBF) által kiadott, legalább a kezelni kívánt minősített adat minősítési szintjével megegyező szintű rendszerengedéllyel.[25] Ebből kifolyólag, a mobil eszközökön csak akkor kezelhető minősített adat, amennyiben a szervezet, előzetesen a rendszerengedélyt kérelmezte és megkapta az NBF-től.

[25] 161/2010. (V. 6.) Korm. rendelet 2. § (1) bekezdés

8. Összegzés

A mobil eszközök használata szerves részét képezi mindennapjainknak, illetve munkahelyünkön is megjelentek ezek az eszközök, és egyre több munkáltató látja el velük munkavállalóit, hogy munkájukat hatékonyabban és kényelmesebben tudják végezni. A mobil eszközök használatának lehetnek biztonsági kockázatai, biztonsági események következhetnek be, de ezek a megfelelő adminisztratív, fizikai és logikai védelmi intézkedésekkel kezelhetőek és minimalizálhatóak.

Többféle mobil eszköz, hivatali használati modellt elemeztünk és mutattunk be, az implicit és explicit BYOD-tól kezdve, a CYOD és COPE modellen keresztül, a COBO rendszerrel bezárólag, illetve kifejtettük a különböző modellek bevezetési stratégiáit is.

A bemutatott implicit és explicit BYOD modellek alkalmazása azért nem megfelelő, mert a mobil eszközök a munkavállaló magántulajdonában vannak, és még megfelelő szabályozás mellett is magas kockázatot hordoz magában ez a kettőség, mert keveredhetnek a magán és a hivatali információk az eszközön, ami növeli a biztonsági események bekövetkezésének valószínűségét. Ezen esetekben az ellenőrzés sem lehet magas szintű, ami tovább fokozza az egyébként is magasabb kockázatokat.

A CYOD modell alkalmazásának előnyei és hátrányai nem térnek el nagyban a BYOD modellekétől, de annyi pozitívuma van, hogy a szervezet határozza meg az eszközök körét, így homogénebb informatikai rendszer alakítható ki, melynek működése biztonságosabb lehet. A végső döntés mindig az alkalmazó szervezeté, viszont mindent összevetve, a fenti elemzéseket összehasonlítva, nagyméretű, nagy létszámú, fejlett informatikai infrastruktúrát alkalmazó szervezet esetében véleményem szerint a legelőnyösebb választás a COPE vagy COBO modell alkalmazása lehet.

A COPE modell esetében nagyobb fokú biztonság érhető el, mert az informatikai rendszerek összhangban vannak a mobil eszközökkel, felügyeletük teljeskörűen megvalósul, és ezek az előnyök nagyobbak, mint a megnövekedő adminisztrációból és az eszközök és szoftverek beszerzésének anyagi többletterhéből fakadó hátrányok. A COPE modell választásakor viszont nagy figyelmet kell fordítani az adatvédelmi jogszabályok betartására, hogy a hivatali ellenőrzések során ne sérüljenek a munkavállalók jogai.

A COBO modell, a COPE modell szigorúbb változata, a magánhasználat ebben az esetben nem megengedett, de a modell alkalmazása ugyanakkor magában hordozza azokat az előnyöket, amelyeket a COPE modell. A COBO modell azzal a rugalmas kikötéssel is alkalmazható, hogy ha mégis történik magánhasználat, az bizonyos előre meghatározott keretek között nem szankcionálandó. Mind a COPE, mind a COBO modell alkalmazásakor nagy figyelmet kell fordítani arra, hogy egy mindenre kiterjedő és mindent lefedő szabályozói környezetet kell kialakítani, illetve ehhez rendszeres ellenőrzési rendszert is szükséges társítani. Nem szabad megfeledkezni a munkavállalók tudatosságának fokozásáról sem, mert csak így lehet biztosítani, hogy a nem kívánt biztonsági események száma minimalizálható, csökkenthető legyen.

A jogszabályi háttér vizsgálata eredményeként megállapítást nyert, hogy a mobil eszközök hivatali használata során több terület szabályait kell alkalmazni. A jogi megfelelés érdekében el kell készíteni a szükséges, informatikai biztonsági és adatvédelmi szabályzatokat, illetve ha a minősített adatkezelés is megtörténik az eszközökön, akkor az erre vonatkozó jogszabályoknak is meg kell tudni felelni minden szempontból, rendelkezni kell a szükséges engedélyekkel.

A mobil eszköz hivatali használata elsőre talán bonyolultnak, sok adminisztrációval járó tevékenységnek tűnik, viszont egy előre átgondolt és kidolgozott bevezetési stratégia mentén, megfelelő kommunikációval és oktatással megvalósított bevezetés nemcsak a munkavállalók napi munkavégzését könnyíti meg, ami az alkalmazó szervezet számára is előny, hanem további, talán nem is remélt előnyökkel járhat a szervezet esetében, de ezek csak az alkalmazás közben érezhetőek majd valójában.

Felhasznált jogszabályok

1992. évi XXXIII. törvény a közalkalmazottak jogállásáról

2009. évi CLV. törvény a minősített adat védelméről

90/2010. (III. 26.) Korm. rendelet a Nemzeti Biztonsági Felügyelet működésének, valamint a minősített adat kezelésének rendjéről

161/2010. (V. 6.) Korm. rendelet a minősített adat elektronikus biztonságának, valamint a rejtjeltevékenység engedélyezésének és hatósági felügyeletének részletes szabályairól

2011. évi CXII. törvény az információs önrendelkezési jogról és az információszabadságról

2011. évi CXCIX. törvény a közszolgálati tisztviselőkről

2012. évi I. törvény a munka törvénykönyvéről

2013. évi L. törvény az állami és önkormányzati szervek elektronikus információbiztonságáról

2015. évi XLII. törvény a rendvédelmi feladatokat ellátó szervek hivatásos állományának szolgálati jogviszonyáról

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

Az Európai Parlament és a Tanács (EU) 2016/679 rendelete a természetes személyeknek a személyes adatok kezelése tekintetében történő védelméről és az ilyen adatok szabad áramlásáról, valamint a 95/46/EK rendelet hatályon kívül helyezéséről (általános adatvédelmi rendelet)

Felhasznált irodalom

- A Nemzeti Adatvédelmi és Információszabadság Hatóság tájékoztatója a munkahelyi adatkezelések alapvető követelményeiről. NAIH, 2016. 10. 28. https://www.naih.hu/files/2016_11_15_Tajekoztato_munkahelyi_adatkezelesek.pdf
- https://www.isaca.org/pages/default.aspx
- https://www.asisonline.org/
- https://auth0.com/blog/ten-mobile-security-threats-and-what-you-can-do-to-fight-back/
- Bizarro, Pascal A. PhD – Garcia, Andy PhD – Nix, Jacob: *Using Personal Mobile Devices in a Business Setting.* 2013. https://www.isaca.org/Journal/archives/2013/Volume-1/Pages/Using-Personal-Mobile-Devices-in-a-Business-Setting.aspx
- Ekler Péter – Forstner Bertalan – Kelényi Imre: *Bevezetés a mobilprogramozásba.* 2008.
- http://www.szak.hu/konyvek_htm/sample_chapters/mobilprog/chap1.pdf
- Előházi János: *Mobil eszközök biztonsági problémái.* Robothadviselés 7. Tudományos szakmai konferencia, 2007. november 27. http://hadmernok.hu/kulonszamok/robothadviseles7/elohazi_rw7.html
- Fei Yu: *Mobile Device Security.* 2011. https://www.cse.wustl.edu/~jain/cse571-11/ftp/mobiles/index.html

- *Guidelines for Managing the Security of Mobile Devices in the Enterpris.* NIST Special Publication 800-124, Revision 1, 2013. https://nvlpubs.nist.gov/nistpubs/specialpublications/nist.sp.800-124r1.pdf
- Kassai Károly: *A mobil kommunikációs eszközök használatának és védelmi rendszabályainak szabályozása.* Hadmérnök, V. évfolyam, 3. szám, 2010. szeptember. http://hadmernok.hu/2010_3_kassai.pdf
- Kitteringham, Glen: *Lost Laptops = Lost Data - Measuring Costs, Managing Threats.* 2008. https://www.asisonline.org/globalassets/foundation/documents/crisp-reports/crisp-lost-laptops-lost-data.pdf
- Priyadarshi, Gaurav: *Leveraging and Securing the Bring Your Own Device and Technology Approach.* 2013. https://www.isaca.org/Journal/archives/2013/Volume-4/Pages/Leveraging-and-Securing-the-Bring-Your-Own-Device-and-Technology-Approach.aspx

Táblázatjegyzék

Rövidítésjegyzék

Rövidítés	Idegen nyelvű jelentés	Magyar nyelvű jelentés
BYOD	Bring Your Own Device	Hozd a saját eszközöd
COBO	Corporate Owned, Business Only	Vállalati tulajdonú, csak üzleti célra
COPE	Corporate Owned, Personally Enabled	Vállalati tulajdonú, magánhasználat megengedett
CYOD	Choose Your Own Device	Válassza ki saját készülékét
GDPR		Az Európai Parlament és a Tanács (EU) 2016/679 rendelete a természetes személyeknek a személyes adatok kezelése tekintetében történő védelméről és az ilyen adatok szabad áramlásáról, valamint a 95/46/EK rendelet hatályon kívül helyezéséről (általános adatvédelmi rendelet)
GSM	Global System for Mobile Communications	Globális rendszer a mobil kommunikációért

Hszt.		2015. évi XLII. törvény a rendvédelmi feladatokat ellátó szervek hivatásos állományának szolgálati jogviszonyáról
Ibtv.		2013. évi L. törvény az állami és önkormányzati szervek elektronikus információbiztonságáról
Infotv.		2011. évi CXII. törvény az információs önrendelkezési jogról és az információszabadságról
Kjtv.		1992. évi XXXIII. törvény a közalkalmazottak jogállásáról
Kttv.		2011. évi CXCIX. törvény a közszolgálati tisztviselőkről
MAM	Mobile Application Management	Mobil Applikáció Menedzsment
Mavtv.		2009. évi CLV. törvény a minősített adat védelméről
MCM	Mobile Content Management	Mobil Tartalom Menedzsment
MDM	Mobile Device Management	Mobil Eszköz Menedzsment
NAIH		Nemzeti Adatvédelmi és Információszabadság Hivatal
NBF		Nemzeti Biztonsági felügyelet
VoIP	Voice over IP	Internetprotokoll Feletti Hangátvitel
VPN	Virtual Private Network	Virtuális Magánhálózat