Saját tulajdonú eszköz munkahelyi használatának (BYOD) biztonsági követelményei

VFP2 KiberVéd - NIS2 Audit felkészítés jogi állásfoglalás 2026/19

VERZIÓKÖVETÉS

Verziószám	Dátum	Módosította	Módosítások leírása
1.0	2026.02.20	Kálmán és Társai Ügyvédi Iroda	Első kiadott verzió

1. ÖSSZEFOGLALÁS

Jelen dokumentum a magántulajdonú eszközök szervezeten belüli használatát (BYOD) vizsgálja kiberbiztonsági szempontból. BYOD alatt azt szervezeti IT politikát értjük, amely lehetővé teszi/meghatározza, hogy a munkavállalók, esetleg külső szerződéses partnerek vagy más felhatalmazott végfelhasználók használhassák a saját tulajdonú hordozható elektronikus eszközeiket (laptop, okostelefon vagy egyéb személyes eszközeiket) a szervezet hálózatán a munkavégzéssel kapcsolatos feladataik ellátása érdekében.

Nem értjük a BYOD fogalmába az alábbi eseteket:

- a felhasználó, vállalati internetes erőforrásokat (pl levelezés, céges felhő szolgáltatások) éri el a saját eszközéről, pl böngészőn keresztül és nem tárol adatot az eszközön;
- magánhasználatú eszközöknek a szervezet azon vezeték nélküli hálózatához történő csatlakozásával kapcsolatos kérdéseket, amely hálózatot kifejezetten a „vendégeknek” tartják fenn, és amelyen keresztül a szervezet belső rendszereit nem lehet elérni.

A legfontosabb megállapítások:

- A szervezeti adatokért való végső felelősség minden esetben a szervezetet terheli, függetlenül az eszköz tulajdonjogától.
- Ugyanakkor a BYOD modell alkalmazása jelentős informatikai és jogi kockázatokat hordoz, mivel a szervezet elveszíti a közvetlen fizikai kontrollt az adatokat feldolgozó eszközök felett, az elégtelen felügyelet pedig adatvédelmi incidenshez vezethet.
- A BYOD engedélyezése számos információbiztonsági és adatvédelmi többletkockázatot okoz, lehetőleg érdemes kerülni.
- Amennyiben a munkáltató engedélyezi a saját eszközök használatát, az csak szigorú, komplex technikai (MAM/MDM, konténerizáció) és szabályozási keretek között lehetséges.

2. PROBLÉMAFELVETÉS

A modern munkavégzési kultúrában a BYOD (Bring Your Own Device) modell egyre elterjedtebb a hibrid munkavégzés és a munkavállalói rugalmasság iránti igények miatt. Ezzel párhuzamosan azonban számos jogi és kiberbiztonsági probléma merül fel annak kapcsán, hogy a szervezeti adatok, köztük érzékeny üzleti és személyes adatok kikerülnek a szervezet biztonságos informatikai környezetéből olyan eszközökre, illetve a szervezet informatikai rendszeréhez olyan eszközök csatlakozhatnak, amelyek felett a vállalatnak csak korlátozott ellenőrzése van, illetve ez az ellenőrzés (vagy éppen a biztonsági intézkedések végrehajtása) a munkavállalók magánszféráját jelentősen érintheti. A BYOD engedélyezésével kapcsolatos döntés csak a lehetséges előnyök/hasznok és kockázatok, a szervezet rendelkezésére álló infrastruktúra technikai és biztonsági állapota, valamint a felhasználói igények alapos felmérése

után hozható. A döntés meghozatalában a kiberbiztonsági és az adatvédelmi szempontokat egyenlő súllyal kell mérni: bármelyik elégtelen volta a BYOD alkalmazását kizárja.

Megjegyzésre érdemes, hogy a BYOD kérdése relevánsabb volt akkor, amikor a szervezetek asztali számítógépet biztosítottak a munkahelyi munkavégzéshez. Amikor az a jellemző, hogy laptopot biztosítanak, azokat a munkavállaló bárhol használhatja és nem elsődlegesen az eszköz biztonsága a kérdés, hanem a kapcsolat biztonságos volta.

3. INDOKOLÁS

3.1 Általános kérdések

A munkaviszonyra vonatkozó szabályok szerint a munkavégzéshez szükséges feltételeket – eltérő megállapodás hiányában – a munkáltató köteles biztosítani. A BYOD ilyen „eltérő megállapodás”-on alapuló szituáció. A „megállapodás” mögött egy jól kidolgozott szabályzatnak kell állnia, ami a BYOD-val kapcsolatos kérdéseket rendezi, különösen:

- a BYOD-eszköznek a szervezet hálózatához és alkalmazásaihoz való hozzáférés megadásához szükséges követelményrendszer, alapelvek,
- a BYOD-ként hálózatába lépésre jogosult eszközök leltárának naprakészen tartását biztosító szabályok,
- az eszközön a felhasználó és a szervezet által végezhető műveletek szabályrendszere,
- az eszköznek a szervezet hálózatához és alkalmazásaihoz való hozzáférés visszavonásának, és az eszközön elérhető adatok törlésének (távoli) eljárásrendje,
- a BYOD-eszközök tekintetében a hiba, incidens-bejelentés eljárásrendje.

Ezen szabályzattal szemben is alapkövetelmény a szabályzat naprakészen tartása, elérhetősége és folyamatos ellenőrzése.

A magántulajdonú eszközök szervezeti célra történő használata dokumentált kockázatelemzés után hozható meg. A folyamat végén elfogadandó belső szabályzat ezen kockázatokra válaszul adott kiberbiztonsági és jogi válaszok lenyomata.

A szabályzaton túl, a szervezet infrastruktúráját is fel kell készíteni a BYOD eszközök kezelésére, pl. eszközmenedzsment megoldások alkalmazása, a vezeték nélküli hálózati rendszer kialakítása, hálózati zónák kialakítása a távoli elérést biztosító infrastruktúra biztosítása stb. révén.

3.2 A BYOD-val kapcsolatos kockázatok

A BYOD-val kapcsolatos legfontosabb kockázatok a következők:

a) az eszközök feletti rendelkezési jog hiányából, illetve az „árnyék infrastruktúrából” eredő kockázatok;

b) a nem ellenőrzött hálózati kapcsolatokból és elégtelen eszközvédelmi intézkedésekből eredő kockázatok;

c) az infrastruktúra eltérő minőségéből és széttöredezettségéből adódó kockázatok;

d) a felhasználói hibákból, gondatlanságból eredő kockázatok;

e) a munkaviszony megszűnése esetén követett eljárások hiányosságaiból eredő kockázatok;

f) az adatvédelmi kockázatok.

Mindezen kockázatok ellen a szervezet védekezni köteles a kiberbiztonsági szabályok szerint.

a) A BYOD esetén a szervezet, a szükséges védelmi intézkedések hiányában gyakorlatilag semmilyen rendelkezési joggal nem rendelkezik azon készülékek felett, amikkel az szervezet adataihoz és alkalmazásaihoz hozzáférhetnek, vagy ahol azokat tárolhatják. Ez nem csak szűken vett adatvédelmi probléma, hanem az üzleti információk/titkok védelmének (általános) problémája is. Az eszközfelügyelet hiánya miatt nagyobb az esélye rosszindulatú vagy sérülékeny alkalmazások telepítésének is. A kontroll hiánya nagymértékben megnöveli az adatok ellopásának veszélyét, a rosszindulati behatolásokat, a szervezet rendszereinek sérülékenységét, és rejtve maradhatnak az eszköz használatával kapcsolatos anomáliák (szokatlan időben történő aktivitások, vagy ismételt bejelentkezési hibák).

Az „árnyék-infrastruktúra” („Shadow-IT”) akkor keletkezik, amikor az alkalmazottak nem jóváhagyott eszközöket vagy szolgáltatásokat használnak (csatlakoztatnak). A különböző forrásokból letöltött alkalmazások, a gyakran bármilyen biztonsági ellenőrzés nélküli, akár harmadik országba megfelelő garanciák nélküli adattovábbítást, szinkronizálást végző felhőalapú tárolási szolgáltatások (pl. fájlmegosztó platformok vagy személyes üzenetküldő alkalmazások) használata biztonsági problémákat okoz a BYOD-val kapcsolatban, és rejtett sebezhetőségeket teremt. Mindemellett a szervezeti adatoknak a magántulajdonú eszközre letöltése/átmásolása, azoknak ezt követően kontrollálhatatlan terjesztése adatvédelmi incidenst is jelenthet.

Ezek a problémák kiküszöbölhetők, vagy legalábbis csökkenthetők olyan eszközkezelő-, monitorozó alkalmazásokkal, amelyek figyelik az anomáliákat. A naplók ellenőrzése a szokatlan időben történő aktivitások, vagy ismételt bejelentkezési hibák kiszűrését segítheti.

b) Jelentős problémák forrása lehet, ha a BYOD eszközök nem a szervezet hálózatához csatlakoznak, hanem egyéb, nem ismert, nem kontrollált, így láthatatlan veszélyeket és fenyegetéseket jelentő hálózat részei lehetnek. A nem biztonságosnak minősíthető otthoni, magán vagy nyilvános WiFi hálózatokhoz, veszélyes hotspotokhoz való csatlakozás a felhasználó aktív magatartása nélkül is lehetséges (automatikus csatlakozás beállítását követően), ami révén az adott infrastruktúrákhoz kapcsolódó egyéb eszközök is kockázatot jelenthetnek az szervezet számára.

A mobileszköz-menedzsment alkalmazásokkal ezek a problémák is kezelhetők (blokkolható az alkalmazásoknak, károsnak minősített hálózatoknak a használhatósága, biztosítható a végpontvédelem naprakészen tartása). Fontos szerepe van a képzésnek, annak tudatosításának, hogy ismeretlen vagy nyitott Wi-Fi-hez megfelelő védelem nélkül (VPN) ne csatlakozzanak (vagy a VPN használatának alapból történő kikényszerítése). Megkövetelhető adott feltételeknek megfelelő végpontvédelmi alkalmazás telepítése és fenntartása.

A magántulajdonú eszközök védelmi intézkedéseinek hiányosságai (pl. gyenge jelszavak, vagy szokásos képernyőnyitási minták használata) szintén növeli a készülék sebezhetőségét, ami ellen erős jelszó megkövetelésével, kétfaktoros hitelesítés előírásával lehet védekezni.

Amikor minden eszköz ugyanahhoz az alhálózathoz csatlakozik, a BYOD sebezhetőségei megnőnek. Egyetlen feltört eszköz veszélyeztetheti a szervezet teljes adatállományát. Az ilyen beállítás megnehezítheti a BYOD biztonsági fenyegetések megfékezését. Ezt a kockázatot a hálózatoknak szerepkör és eszköztípus alapján történő szegmentálásával lehet mérsékelni.

c) Magántulajdonú eszközök használata eleve azzal jár, hogy különböző típusú, operációs rendszerű (ezen belül különböző verziójú operációs rendszerű), különböző korú („avultságú") eszközöket kell menedzselni; lehetnek olyan mobil eszközök is ezek között, amire már a gyártó nem biztosít frissítést, és amiket az üzemeltető egyébként már selejtezne vagy kivenne az eszközállományból. Az eszközt tulajdonló munkavállaló számára az üzemeltetési (és esetleg kiberbiztonsági) szempontból lényegtelen tényezők (mint például a külcsín vagy alacsony ár) fontosabbak lehetnek.

Minél vegyesebb egy infrastruktúra, annál több humánerőforrás és anyagi ráfordítás szükséges a biztonsági javítások, az új konfigurációk és szolgáltatások, egyedi fejlesztésű alkalmazások illesztéséhez, teszteléséhez, karbantartásához, informatikai támogatásához, eszközkövetéshez, kompatibilitási problémák kezeléséhez.

A felsorolt problémákat a központi eszközmenedzsment, vagy a szeparált hálózati hozzáférési stratégia alkalmazása részben orvosolhatja, de a szervezet előírhatja azt is, hogy csak meghatározott paraméterekkel (pl. típus, operációs rendszer és annak minimális verziója) rendelkező eszközök esetén engedélyezi a BYOD-t és az említett paraméterek rendszeres felülvizsgálata esetén megvonhatja az elavult készülékkel rendelkező munkatársaktól a BYOD lehetőségét. Kötelezheti a felhasználót a frissítések telepítésére (automatikus telepítés beállítására),

d) Közhely, hogy kiberbiztonsági szempontból egy rendszer leggyengébb láncszeme a felhasználó. A már említetteken (árnyékinfrastruktúra, elégtelen jelszavak, elavult eszközök használata) túl olyan veszélyekkel is kell számolni, mint a social engineering technikák alkalmazása a munkavállalóval szemben, ami a felhasználó hozzáférési adatai kompromittálódása révén lehetővé teszik illetéktelen személyek számára a védett tartalmakhoz való hozzáférést, kártékony kódok telepítése és futtatása révén megkerülhetik a végpontvédelmi megoldásokat.

A szervezet által felügyelt rendszerekhez képest a személyes eszközök általában kevésbé fejlett víruskeresővel és e-mail-szűréssel rendelkeznek. Ezért könnyű célpontjai az adathalász támadásoknak, amelyek során egyetlen kattintás egy rosszindulatú linkre veszélyeztetheti a vállalat hitelesítő adatait, és további támadásokat tehet lehetővé. A személyes eszközökön található kártevőket használó fertőzések gyorsan terjedhetnek, kiterjedtebb hálózati behatolásokká válhatnak, különösen, ha felhőalapú szinkronizált adatokat vagy védelem nélküli VPN-kapcsolatokat használnak.

A többfaktoros azonosítás alkalmazása, vagy a VPN kapcsolat felépítésének meghatározott IP címekről történő engedélyezése, a felhasználói tevékenység naplózása, a naplók elemzésének automatizált kidolgozása, a naprakész végpontvédelem biztosítása lehetséges védelmi intézkedés.

További nagy veszély, hogy az eszközök a szervezet tudomása nélkül is tulajdonost, vagy birtokost válthatnak, beleértve azt is, hogy a munkavállaló elveszti az eszközöket vagy eltulajdonítják tőle. Ennek eredményeként az eszközök, és az eszközökön lévő adatok, hozzáférések, illetéktelenekhez kerülhetnek, ami önmagában adatvédelmi és biztonsági incidens megvalósulását eredményezi. Ennek kivédésére olyan szervezési intézkedések szolgálhatnak, mint pl. a távoli törlési funkció aktiválása, az erős jelszavas zárak alkalmazása, illetve annak kötelezővé tétele, hogy az eszközök elvesztését/eltulajdonítását azonnal jelentsék a munkáltatónak.

e) A munkavállalók kiléptetése során a BYOD eszközökön keresztüli hozzáférési jogosultságok megszüntetésére, valamint a BYOD eszközökön tárolt szervezeti információk törlésére is figyelmet kell fordítani.

f) Az adatvédelmi kockázatok a fentiekből következnek. A GDPR 32. cikke értelmében az adatkezelő a tudomány és technológia állásának, a megvalósítás költségeinek, illetve az adatkezelés kockázatainak megfelelő adatbiztonsági intézkedéseket köteles meghozni és végrehajtani. A szükséges védelmi szintet, illetve az adatkezelő teendőit további jogszabályok, mint pl. a Magyarország kiberbiztonságáról szóló 2024. évi LXIX. törvény (Kiberbiztonsági tv.), illetve a biztonsági osztályba sorolás követelményeiről, valamint az egyes biztonsági osztályok esetében alkalmazandó konkrét védelmi intézkedésekről szóló 7/2024. (VI. 24.) MK rendelet (a továbbiakban: Rendelet) határozzák meg, illetve részletezik. Az egyes technikai védelmi intézkedések paramétereit, az azokkal szembeni elvárásokat további, nem jogi természetű dokumentumok (pl. ajánlások, szabványok) tartalmazzák.

Az adott szervezetnek a BYOD eszközökkel együttesen kell az elvárt kiberbiztonsági szintet biztosítania, azaz a BYOD-ra bármelyik követelmény vonatkozhat, ami az szervezet elektronikus információs rendszerére egyébként alkalmazandó. A BYOD környezetben alkalmazott védelmi intézkedéseknek kompenzálniuk kell az eszköz feletti fizikai kontroll elvesztését. A legkisebb jogosultság elvét és az adatszeparációt (konténerizáció) érvényesítve a magáneszközön a szervezeti adatok csak egy szigorúan felügyelt, logikailag elkülönített környezetben lehetnek elérhetők. A technikai kontrollok nélkül a BYOD használata nem felel meg a biztonsági követelményeknek.

A BYOD tehát csak megfelelő kiberbiztonsági szint mellett lehetséges, mert a fentebb bemutatott kockázatok mindegyike egyben adatvédelmi incidens kockázatát is hordozza. A BYOD-ra vonatkozó biztonsági követelmények helytelen meghatározása kiberbiztonsági vagy adatvédelmi incidens magas kockázatát hordozza magában.

A BYOD alkalmazása azonban más szempontból is adatvédelmi aggályokat vethet fel. Mivel a szervezetnek felügyelnie kell a saját adatait egy magántulajdonú eszközön, ez könnyen a munkavállaló magánszférájának aránytalan sérelméhez vezethet: az eszközön végzett aktivitás

monitorozása a munkavállaló szabadidejében történő tevékenységéről adhat információt, az alkalmazások letiltása, adott védelmi intézkedés megkövetelése pedig kényelmetlenséget, esetleg költséget okozhat. A BYOD modellben a munkáltató könnyen "túlmonitorozhatja" a munkavállalót. A GDPR alapelvei szerint az adatkezelésnek célhoz kötöttnek és arányosnak kell lennie: a munkáltatónak garantálnia kell, hogy a felügyeleti eszközök (MAM) nem gyűjtenek szükségtelen információkat (pl. magáncélú alkalmazásleltár, folyamatos GPS követés munkaidőn kívül) a munkavállalóról, ami adott esetben ellentétbe kerülhet a fentebb bemutatott kockázatok miatt szükséges intézkedésekkel.

A szervezetnek átláthatóan tájékoztatnia kell a munkavállalót arról, hogy mit monitoroz, és garantálnia kell, hogy a technikai felügyelet (pl. távoli törlés) csak a szervezeti konténert érintse, a munkavállaló magánadatait ne.

3.3 A BYOD szempontjából releváns védelmi intézkedések és hatásaik

A 7/2024 (VI.24) MK rendelet számos olyan követelményt támasztanak, amelyek a magáneszközök használhatóságát a vállalati célú felhasználás érdekében korlátozzák.

A Rendelet 2. melléklete kifejezetten nevesíti a nem a szervezet tulajdonát képező eszközök használatának szabályozását. Bár ez a katalógusban opcionális intézkedésként jelenik meg, a BYOD bevezetésekor a kockázatelemzés alapján javasolt a megvalósítása:

> *2.118. A szervezet a meghatározott feltételek szerint korlátozza a nem szervezeti tulajdonban lévő rendszerek és rendszerelemek használatát a szervezeti információk feldolgozására, tárolására vagy továbbítására. [7/2024. (VI. 24.) MK rendelet 2. melléklet 2.118. pont] (O)*

Figyelembe kell venni, továbbá, hogy a saját tulajdonú eszközök használata jelentős biztonsági kockázatokat hordoz, ezért a jogszabály a „nem szervezeti tulajdonban lévő rendszerek”, a „külső rendszerek”, a „mobil eszközök”, valamint a „viselkedési szabályok” fogalomkörei alatt támaszt szigorú követelményeket. A BYOD modell bevezetése során a szervezetnek több, egymásra épülő kontrollt kell bevezetnie, amelyek lefedik, a nem szervezeti tulajdonban lévő eszközök használatának korlátozását, a mobil eszközök hozzáférés-ellenőrzését és titkosítását, a külső rendszerek használatának feltételrendszerét, a hálózati határvédelmet és a felhasználói viselkedési szabályok rögzítését.

3.3.1 Mobileszköz-kezelő és alkalmazáskezelő rendszerek bevezetése

Amennyiben a felhasználó a szervezet adatvagyonát saját tulajdonú eszközein kezeli, a Rendelet megköveteli a mobil eszközök kapcsolódásának engedélykötelessé tételét és a megfelelő titkosítás alkalmazását. Nem tartozik ide az az eset, ha vállalati internetes erőforrásokat (pl levelezés, céges felhő szolgáltatások) éri el a saját eszközéről, pl böngészőn keresztül és nem tárol adatot az eszközön. A BYOD környezetben a teljes eszköztitkosítás alkalmazása (amikor a szervezet az egész telefont menedzseli) jogi és adatvédelmi szempontból túlzó lehet, ezért a leginkább célravezető technológiai megoldás a MAM (Mobile Application Management) szoftverek, vagyis a konténerizációs technológiák alkalmazása.

2.113. A szervezet: 2.113.1. Kialakítja a konfigurációs követelményeket, kapcsolódási követelményeket és alkalmazási útmutatót az általa ellenőrzött mobil eszköz számára, beleértve azokat az eseteket is, amikor ezek az eszközök a szervezet által ellenőrzött területen kívül helyezkednek el. 2.113.2. Engedélykötelessé teszi a szervezet rendszereihez mobil eszközökkel történő kapcsolódást. (A,J,M)
2.114. A szervezet teljes eszköztitkosítást vagy tárolóalapú titkosítást alkalmaz a meghatározott mobil eszközökön tárolt információk bizalmasságának és sértetlenségének védelme érdekében. [7/2024. (VI. 24.) MK rendelet 2. melléklet 2.113. és 2.114. pont] (A, J, M)

A konténerizációs megoldások bevezetése során a szervezet a következő biztonsági funkciókat tudja érvényesíteni:

- Vállalati adatterület létrehozása, amely egy titkosított, jelszóval vagy biometrikus azonosítással védett, elkülönített virtuális tároló a privát eszközön belül;
- Szelektív törlés képessége, amely lehetővé teszi, hogy az eszköz elvesztése vagy a munkaviszony megszűnése esetén a szervezet csak a céges adatokat törölje távolról, a magánadatok (például személyes fotók, üzenetek) érintése nélkül;
- Adatmásolás megakadályozása, amely technológiailag blokkolja a céges konténerből, például a vállalati levelezőből a magán alkalmazásokba történő másolási és beillesztési műveleteket.

3.3.2 Hálózati határvédelem és hozzáférés-szabályozás

A magántulajdonú eszközök hálózati hozzáférését szigorúan ellenőrizni kell, hiszen ezek az eszközök külső hálózatról csatlakoznak, és a felhasználók függetlenül konfigurálják őket. A modern kiberbiztonsági gyakorlatban, a Rendelet elvárásaival összhangban a hálózati hozzáférés-szabályozó (NAC) rendszerek és a Zero Trust (zéró bizalom) architektúra kiépítése a javasolt irány. BYOD esetén ajánlott alkalmazni az ilyen kliensek közötti közvetlen kommunikáció hálózati szintű tiltására vonatkozó opcionális követelményt.

17.33. Az EIR blokkolja a bejövő és a kimenő kommunikációs forgalmat azok között a kliensek között, amelyeket a végfelhasználók és a külső szolgáltatók a szervezettől függetlenül konfigurálnak. [7/2024. (VI. 24.) MK rendelet 2. melléklet 17.33. pont] (O)

A hálózati hozzáférés-szabályozás során az alábbi ellenőrzési lépéseket érdemes technológiailag kikényszeríteni:

- Az eszközmegfelelőség vizsgálata a csatlakozás pillanatában, amely során a rendszer ellenőrzi a frissített operációs rendszer, az aktív vírusirtó és a bekapcsolt képernyőzár meglétét;
- Hálózati szegmentáció alkalmazása, amely biztosítja, hogy a csatlakozó BYOD eszköz csak az általa feltétlenül szükséges vállalati szervereket érje el, és ne tudjon más, a hálózaton lévő kliensekkel kommunikálni;

- Többfaktoros hitelesítés (MFA) kikényszerítése minden céges erőforrás elérésekor, függetlenül attól, hogy az eszköz fizikai értelemben hol tartózkodik.

3.3.3 Szabályozás és felhasználói nyilatkozattétel

A technológiai beállítások önmagukban nem garantálják a megfelelést. A felhasználói tudatosság és a jogi keretek tisztázása érdekében kötelező belső szabályozást alkotni. A BYOD programba történő belépés feltétele egy belső szabályzat kiadása és a felhasználói nyilatkozat aláíratása.

> *2.115. A szervezet: 2.115.1. Meghatározza a felhasználási feltételeket, és megállapítja, hogy az elvárt követelmények megvalósultak-e a külső rendszerekben, összhangban a külső rendszereket birtokló, üzemeltető, illetve karbantartó más szervezetekkel létrehozott bizalmi kapcsolatokkal, amelyek lehetővé teszik az arra jogosult személyek számára, hogy: 2.115.1.1. hozzáférjenek a rendszerhez külső rendszerekből; és 2.115.1.2. feldolgozzák, tárolják vagy továbbítsák a szervezet által ellenőrzött információkat külső rendszerek használatával; vagy 2.115.2. megtiltja a meghatározott típusú külső rendszerek használatát. (A, J, M)*
> *13.3.2. A szervezet az EIR-hez való hozzáférés engedélyezése előtt dokumentált nyilatkozattételre kötelezi a hozzáférési jogosultságot igénylő személyt, felhasználót, aki nyilatkozatával igazolja, hogy az EIR használatához kapcsolódó, rá vonatkozó biztonsági szabályokat és kötelezettségeket megismerte, saját felelősségére betartja. [7/2024. (VI. 24.) MK rendelet 2. melléklet 13.3.2. pont] (A, J, M)*

A jogkövető magatartás biztosítása érdekében a BYOD szabályzatnak az alábbi elemeket kell tartalmaznia:

- Az engedélyezett eszközök, gyártók és operációs rendszerek pontos köre, amely rögzíti, hogy milyen feltételekkel vonható be egy eszköz a céges munkavégzésbe;
- A szervezet informatikai ellenőrzési jogosultságainak határai, amely egyértelműsíti a munkavállaló számára, hogy az informatikai osztály kizárólag a céges konténerhez fér hozzá, a privát adatforgalmat nem monitorozza;
- A biztonsági incidensek esetén követendő eljárásrend, amely kötelezi a munkavállalót, hogy az eszköz elvesztése, ellopása vagy gyanús informatikai tevékenység észlelése esetén azonnal értesítse az incidenskezelő csapatot.
- Engedélyezett eszközök és platformok listájának (whitelist) összeállítása, amely rögzíti, hogy kizárólag a gyártói támogatással rendelkező, frissített operációs rendszerrel (például minimum iOS 16 vagy Android 13) rendelkező eszközök vonhatók be a munkavégzésbe;
- Bizonyos eszköztípusok vagy állapotok kifejezett tiltása (blacklist) a 2.115.2. alpont alapján, például a szoftveresen feltört (rootolt vagy jailbreakelt) eszközök kizárása a vállalati hálózatból, mivel ezek alapvető biztonsági funkciói sérültek;
- B2B (szervezet és szervezet közötti) BYOD modell esetén, például amikor egy külső alvállalkozó a saját eszközét használja a megfelelőséget egy adatfeldolgozói vagy

titoktartási megállapodás (NDA) biztonsági mellékletében kell jogilag kikényszeríthetővé tenni.

3.3.4 Biztonsági követelmények technológiai ellenőrzése és kikényszerítése

A jogszabály nem elégszik meg a feltételek papíralapú rögzítésével; kötelezővé teszi a védelmi intézkedések meglétének tényleges, technikai ellenőrzését az információkhoz való hozzáférés megadása előtt.

> *2.108. A szervezet: 2.108.1. A vezeték nélküli hozzáférés minden egyes típusára vonatkozóan konfigurációs követelményeket, kapcsolódási követelményeket és alkalmazási útmutatást alakít ki. 2.108.2. Engedélyezési eljárást folytat le a rendszerhez való vezeték nélküli hozzáférés minden egyes típusára, az ilyen kapcsolatok lehetővé tételét megelőzően (A,J,M)*
> *2.109. pont: A szervezet titkosítással és a felhasználók vagy eszközök hitelesítésével védi a vezeték nélküli hozzáférést. (J,M)*
> *2.116. A szervezet csak akkor engedélyezi a jogosult személyek számára a külső rendszer használatát, a rendszerhez való hozzáférést, illetve a szervezet által ellenőrzött információk feldolgozását, tárolását vagy továbbítását, ha: 2.116.1. ellenőrzésre került a külső rendszeren alkalmazott védelmi intézkedések végrehajtása, amelyeket a szervezet biztonsági szabályzatai és tervei határoznak meg; vagy 2.116.2. betartja és betartatja a jóváhagyott rendszerkapcsolati vagy feldolgozási megállapodásokat a külső rendszert üzemeltető szervezettel. [7/2024. (VI. 24.) MK rendelet 2. melléklet 2.116. pont] (A, J, M)*

Ezt a technológiai ellenőrzést a modern IT környezetben az alábbi folyamatokkal és rendszerekkel lehet hatékonyan megvalósítani:

- Feltételes hozzáférés és eszközmegfelelőségi házirendek bevezetése, amelyek a bejelentkezés pillanatában, automatikusan megvizsgálják az eszköz biztonsági állapotát, például a bekapcsolt képernyőzárat vagy az aktív titkosítást;
- Mobileszköz-kezelő (MDM), mobilalkalmazás-kezelő (MAM) vagy UEM (Unified Endpoint Management) szoftverek alkalmazása, amelyek folyamatos és automatizált „postura ellenőrzést” végeznek a BYOD eszközön, és hiányosság esetén (például notebookon kikapcsolt vírusirtó) automatikusan megvonják a hozzáférést a vállalati adatoktól;
- Mobil végpontvédelmi megoldások (Mobile Threat Defense - MTD) integrálása, amelyek valós időben detektálják az eszközön lévő kártékony kódokat vagy a hálózati anomáliákat, ezzel biztosítva a 2.116.1. alpont szerinti folyamatos védelmi ellenőrzést.

Ezek a technológiai és adminisztratív lépések együttesen biztosítják, hogy a szervezet a hatályos jogszabályoknak, különösen a Rendelet követelményeinek megfelelően engedélyezhesse a saját tulajdonú eszközök biztonságos használatát.

4. FORRÁSOK

Jogszabályok és rendeletek:

- Az Európai Parlament és a Tanács (EU) 2016/679 rendelete (GDPR)
- 2024. évi LXIX. törvény Magyarország kiberbiztonságáról (Kiberbiztonsági tv.)
- 7/2024. (VI. 24.) MK rendelet a biztonsági osztályba sorolás követelményeiről

Ajánlások és szabványok:

- NIST SP 1800-22: Mobile Device Security: Bring Your Own Device (BYOD)
- ENISA NIS2 Technikai Implementációs Útmutató