Tisztelt Üzemi Tanács, Tisztelt Érdekképviseletek!

A MÁV-csoportnál számos alkalommal fordult elő, hogy olyan valós, vagy részben valós adatok kerültek nyilvánosságra, amelyek hátrányosan érinthették valamely Társaság érdekeit.

A munka törvénykönyve 8. § (4) meghatározza, hogy a munkavállaló köteles a munkája során tudomására jutott üzleti titkot megőrizni, továbbá nem közölhet illetéktelen személlyel olyan adatot, amely munkaköre betöltésével összefüggésben jutott a tudomására, és amelynek közlése a munkáltatóra vagy más személyre hátrányos következménnyel járhat. Az Informatikai Biztonsági Szabályzatok előírják a társaságok tulajdonában, kezelésében álló adatok bizalmasságának, sértetlenségének, rendelkezésre állásának biztosítását, valamint az ehhez tartozó munkáltatói és munkavállalói feladatok, kötelességek, felelősségek meghatározását.

Az információs önrendelkezési jogról és az információszabadságról szóló törvény (Infotv.), továbbá a védendő információk körében tartózó ismertek (így különösen a minősített adat, üzleti titok, személyes adat, know-how, döntés megalapozását szolgáló adat) megóvásáról rendelkező törvényi szintű előírásoknak történő megfelelés érdekében a közeljövőben a MÁV-csoport három társaságánál, a MÁV Zrt.-nél, a MÁV-START Zrt.-nél, valamint a MÁV SZK Zrt.-nél adatszivárgás megelőző (DLP) rendszer korlátozott próbaüzembe állítását tervezzük. A bevezetés indoka a megfelelő körültekintés hiányában, vagy a jól értesültség látszata érdekében tudatlanságból, esetleg rosszindulatból, illetve szándékos előnyszerzés érdekében a védett vállalti információk jogosulatlan használatának, továbbításának, az ún. adatszivárgásnak megakadályozása, ami mind anyagi, mind erkölcsi értelemben egyaránt felbecsülhetetlen károkat okozhat az adott szervezetnek.

Az Infotv. előírása szerint a MÁV-csoport mint adatkezelő köteles gondoskodni a személyes adatok biztonságáról, köteles továbbá megtenni azokat a technikai és szervezési intézkedéseket és kialakítani azokat az eljárási szabályokat, amelyek e törvény, valamint az egyéb adat- és titokvédelmi szabályok érvényre juttatásához szükségesek.

A DLP rendszer korlátozott próbaüzeme – amelyről a munkavállalók külön tájékoztatást kapnak – 2016. szeptember 12-én kezdődik, amelynek tapasztalatai alapján a rendszer éles üzemű alkalmazására várhatóan 2017. januárjától kerül sor. A rendszer alkalmazásával megvalósuló technikai ellenőrzés jogalapját a Munka törvénykönyve 11. §-a biztosítja. E szakasz (2) bekezdésének értelmében a munkáltató előzetesen tájékoztatja a munkavállalót azoknak a technikai eszközöknek az alkalmazásáról, amelyek a munkavállaló ellenőrzésére szolgálnak.

A DLP rendszer alkalmazása során kiemelt feladatnak tartjuk a munkavállalói jogok határozott és kifejezett érvényesítését. A keletkező információk felhasználása ezért kizárólag a rendszer korlátozott próbaüzemével összefüggő feladatok teljesítéséhez elengedhetetlenül szükséges mértékben és ideig valósul meg, és a dokumentumvédelmi, ezen belül az adat- és információvédelmi feladatok ellátása semmilyen módon nem irányul a munkavállalók magánéletének ellenőrzésére. A DLP korlátozott próbaüzeme során az adatok kezelésének kizárólagos célja a MÁV-csoport érintett társaságai által kezelt védendő információknak kontrollált továbbítása érdekében beszerzett rendszer beüzemelése, az üzleti területek által meghatározott adatköröknek a rendszer számára történő értelmezése, beállítása és finomhangolása, a rendszer használatának betanulása, a kapcsolódó munkafolyamatok

kialakítása, végül a jog- és szabályszerű működtetés megfelelősége érdekében szükséges vezérigazgatói szabályozás előkészítése. A DLP rendszert a korlátozott próbaüzem szakaszában olyan módon kívánjuk alkalmazni, hogy abból a munkavállalókra nézve hátrányos jogkövetkezmény ne származzon.

A DLP megoldás a munkáltató által a munkavállaló részére munkavégzés céljából rendelkezésre bocsátott hivatalos levelező rendszeréből kiküldött levelekre vonatkozva vizsgálja a szabályrendszerbe történő ütközést, amelyet kizárólag az érintett társaság által kijelölt biztonsági szakértő láthat, más társaság ezekhez az adatokhoz nem férhet hozzá.

A rendszer teljes kiépítésében a következő védelmi lehetőségeket biztosítja:

- azonosítja, a továbbításra kerülő védendő, azaz DLP rendszer szabályrendszerében beállított információkat,
- információt tárol arról, hogy mi történik ezekkel az adatokkal, dokumentumokkal,
- szükség esetén megvédi a védendő információt a rendszerből való kikerüléstől.

A rendszer mindezen funkciókat a következő módon valósítja meg:

Ha egy érintett MÁV-csoporttag munkavállalója elektronikus levelet küld ki a MÁV-csoport hivatalos levelező rendszeréből, akkor a DLP rendszer a szabályrendszernek megfelelően automatikusan átvizsgálja a levél, valamint a csatolmány tartalmát. Amennyiben a DLP szabályrendszerben beállított egyezést talál, akkor erről a minősítési szintnek megfelelő naplóbejegyzés keletkezik. A naplóbejegyzésre adott reakció lehet előre definiált módon történő jelzés, de indokolt esetben akár a levél kiküldésének felfüggesztése (karanténba helyezés) is. Ez utóbbi esetben a levél csak megfelelő felülvizsgálatot követően kerülhet továbbításra. Mindezekből látható, hogy a hálózati szoftver csak a kellő körültekintéssel megfogalmazott szabályok alapján ellenőriz és ad visszajelzést. Alkalmazásával nem a számítógép felhasználó munkatársak ellenőrzése a cél, hanem azon dokumentumok, adatok kiszivárgásának a megelőzése, megakadályozása, amelyek a DLP rendszer által védendő tartalmat hordoznak.

A főtevékenységi körök vezetői az általuk kijelölt DLP felelős útján jelenthetik be tartalomvédelmi igényüket, amelyre csak jogszabály, az MSZSZ vagy egyéb belső utasítás alapján feladatkörükbe utalt tevékenység ellátásához közvetlenül kapcsolódóan, kellően azonosított esetekben tehetnek javaslatot. A szabályrendszer beállítását és a működés során keletkezett naplóbejegyzések elsődleges kezelését a kijelölt biztonsági szakértők hajtják végre.

A rendszer a szabályok megfogalmazását és beállítását követően teljesen automatizált módon, különböző, előre beépített detektálási technológiák alkalmazásával működik. A szabálytípusok lehetnek: kulcsszavak, reguláris kifejezések, fájl attribútumok, strukturált formátumú adatok, személyes adatokat leíró algoritmusok (pl. személyi igazolvány szám, TAJ, adószám), e-mail címek, előterjesztések, tervek, beszámolók, beszerzésekkel kapcsolatos információk, költségekkel kapcsolatos információk, műszaki tervek, ábrák stb.

A szabályok megadásának ellenőrzése logikai kapcsolódásokkal is pontosíthatók. Lehetőség van kivételek kezelésére, pl. bizonyos e-mail címek, vagy domain nevek esetében a küldésre kerülő anyagok nem kerülnek ellenőrzésre. Ilyen lehet a gov.hu, vagy a police.hu, amelyekre továbbított küldemények nyilvánvalóan nem tekinthetők adatszivárgásnak. A szabályok folyamatos karbantartása biztosítja az elévült, megváltozott igények átvezetését.

A beállított szabályok a DLP rendszerben naplózásra kerülnek, amelynek rendszeres ellenőrzésére – garanciális elemként – társaságonként külön auditori feladatkör került létrehozásra.

Hangsúlyozzuk, hogy a rendszer korlátozott próbaüzemének kifejezetten nem célja az egyes munkavállalók tevékenységének, magánéletének megfigyelése, kizárólag a rendszer számára beállított, védendő információt tartalmazó dokumentumok elküldésének kontrollja, szükség szerint a fokozott körültekintésre vonatkozó figyelemfelhívás küldése, vagy a továbbítás döntéstől függővé tétele, esetleg megakadályozása. Amennyiben a kellően tájékozott munkavállaló biztonságtudatos körültekintéssel használja a rábízott adatokat és rendszereket, a DLP rendszerben tevékenysége nem kerül naplózásra, ezzel szemben a rendszertámogatást nyújt számára a véletlen kiszivárogtatás elkerülésére.

Budapest, 2016. augusztus 22.

DLP Projektmenedzsment