HADMÉRNÖK

IX. Évfolyam 3. szám - 2014. szeptember

**Györkös Roland István - Nagyné Takács Veronika**
kh.ifuf@nav.gov.hu

# JAVASLAT AZ ELEKTRONIKUS INFORMÁCIÓS RENDSZEREK 77/2013. (XII. 19.) NFM RENDELET ALAPJÁN ELVÉGZENDŐ BIZTONSÁGI OSZTÁLYBA SOROLÁSA VONATKOZÁSÁBAN

***Absztrakt***

*A közigazgatási szervek számára jelentős feladatokat határoz meg a 2013-ban hatályba lépett új, informatikai biztonsági tárgyú jogi szabályozás, Az állami és önkormányzati szervek elektronikus információbiztonságáról szóló 2013. évi L. törvény és annak végrehajtási illetve technikai rendeletei. A jogalkotói szándék az informatikai rendszereket használó szervezetek tudatos – tervezett és ellenőrzött – információvédelmi tevékenységének előmozdítása, részben értékelési, tervezési és tényleges információvédelmi feladatok előírásával, részben a feladatok ellátását ellenőrző, koordináló szervezetrendszer létrehozásával. A jogszabályoknak való megfelelés első lépése az alkalmazott informatikai rendszerekkel kapcsolatos helyzetfelmérés, ezt követheti a felmérés eredményei alapján szükséges intézkedések meghatározása és végrehajtása. A jogalkotói elvárás egyértelmű, a végrehajtás módját az érintett szervezeteknek kell egyedileg meghatározniuk. A szerzők a feladatot a Nemzeti Adó- és Vámhivatal szempontjából tekintik át és tesznek javaslatot az első szakaszban meghatározott elvárások teljesítésére.*

*The new information security Law was issued in the beginning of 2013. This Law and its implementing technical regulations define major tasks for the State or local government agencies in the field of security of electronic information. The main aims of the new law were to enhance the information security activities and provide assessment, planning and effective information management tasks, partially exercising control due the establishment of a coordinating body system. The first step is a survey of regulatory compliance status of the used IT systems, and may be followed by the definition and implementation of the necessary measures based on the results of the survey. The legislative requirements are absolutely clear: the measures have to be determined by the individual organizations. The authors of this study focuse on the tasks and the fulfillments of the National Tax and Customs Administration in the first phase.*

***Kulcsszavak:*** *információbiztonság, kockázatelemzés, közfeladatot ellátó szervek adatai ~ information security, security risk management, public sector information*

## ELMÉLETI ALAPVETÉS

Az informatikai biztonságra vonatkozó jogi szabályozás 2012 óta zajló megújításának célja - *Az állami és önkormányzati szervek elektronikus információbiztonságáról szóló* 2013. évi L. törvény (a továbbiakban: Ibtv.) indokolása szerint - egy „preventív szabályozási környezet" létrehozása, amely „ténylegesen a megelőzést helyezi előtérbe és ezen keresztül a biztonsági problémák kialakulásának mérséklését és az előforduló biztonsági események számának csökkentését, illetve tudatos kezelését célozza". [1]

A *megelőzés* és a *tudatos kezelés* alapja minden esetben egy teljes körű és korrekt helyzetfelmérés kell, hogy legyen, amely első lépésként a tevékenységgel érintett *vagyontárgyak* számbavételére, második lépésként a *végrehajtandó intézkedések* meghatározására irányul.

Az Ibtv. szerint két kiindulópont van: az *elektronikus információs rendszerek biztonsági osztályba sorolása*, illetve az *elektronikus információs rendszerrel rendelkező szervezetek biztonsági szintjének meghatározása*. Az előbbi a vagyonleltár felvételét és a vagyontárgyak minősítését, az utóbbi a szervezet biztonsági feladatokra való felkészültségének meghatározott szempontok szerinti mérését és az esetleges hiányosságok (a továbbiakban: megteendő intézkedések) azonosítását jelenti az irányadónak tekintett szabványok alapján (lásd később).

*Az állami és önkormányzati szervek elektronikus információbiztonságáról szóló 2013. évi L. törvényben meghatározott technológiai biztonsági, valamint biztonságos információs eszközökre, termékekre vonatkozó, valamint a biztonsági osztályba és biztonsági szintbe sorolási követelményeiről szóló* 77/2013. (XII. 19.) NFM rendelet (a továbbiakban: technológiai rendelet) 1. sz. mellékletének 1.2. pontja szerint *az elektronikus információs rendszerek biztonsági osztályba sorolását kockázatelemzés alapján kell elvégezni, amit az érintett szervezet vezetője hagy jóvá. A kockázatelemzés során ajánlott a nemzetközi vagy hazai szabványok, ajánlások, legjobb gyakorlatok figyelembevétele.* [2]

Az említett helyzetfelmérés végrehajtásához a jogalkotói elvárás alapján négy, az érintett szervezet jellemzői alapján további egy elméleti kiindulópontot rögzítettünk.

1. A jogszabály alapján a biztonsági osztály „az elektronikus információs rendszer védelmének elvárt erőssége", aminek alapja „az elektronikus információs rendszerben kezelt adatok és információk bizalmassága, sértetlensége és rendelkezésre állása"[1], továbbá magának „az elektronikus információs rendszernek a sértetlensége és rendelkezésre állása" biztosításának követelménye. Az *adat/információ* és a *rendszer* tehát „együtt mozog"; ebből következően *a rendszer biztonsági osztályba sorolása az adatok/információk osztályba sorolásán alapulhat*.
2. Az Ibtv. szerint a biztonsági osztályba sorolást kockázatelemzés alapján kell elvégezni. A besorolás – értékelés – módszere tehát adott, ajánlott szempontjai és számítási módja nem ismertek. Az Ibtv. indokolása néhány irányelvi jellegű utalást tartalmaz (a védelemnek költséghatékonynak kell lennie; a kár meghatározása során a nagyságrend megállapítása elégséges, a pontos értéket nehéz és költséges meghatározni; a besorolásnál mindhárom védelmi szempontot – CIA-elv – figyelembe kell venni), továbbá utal a Közigazgatási Informatikai Bizottság 25. számú Ajánlására. Konkrét eligazítást azonban a biztonsági besorolás, illetve a kockázatelemzés vonatkozásában e dokumentum sem tartalmaz. [3]
3. Az Ibtv. és a technológiai rendelet is ajánlja a nemzetközi vagy hazai szabványok, ajánlások, legjobb gyakorlatok figyelembevételét. Erre figyelemmel a biztonsági

[1] Az eredeti angol kifejezések - confidentiality, integrity, availability - kezdőbetűi alapján a közkeletű rövidítés: CIA-elv.

osztályba soroláskor *az MSZ ISO/IEC 27001:2006 szabvány* (a továbbiakban: 01 szabvány) *ajánlásait vettük figyelembe*. [4]

4. A kockázatelemzés egy lehetséges módszertanával részletesen foglalkozó *MSZ ISO/IEC 27005 szabvány* (a továbbiakban: 05 szabvány) kétszintű kockázatelemzést javasol. Eszerint először egy *magas szintű biztonsági kockázatelemzés* elvégzése indokolt. Részben azért, mert így általános, a legfontosabb szempontokra koncentráló áttekintést lehet nyerni a szervezet vonatkozásában felmerülő kockázati elemekről. Részben pedig azért, mert egy túlzottan részletes kockázatelemzés jelentős energiákat köthet le, ugyanakkor – amennyiben nem állnak rendelkezésre megfelelő (jellemzően pénzügyi) erőforrások az elemzés alapján végrehajtandó intézkedésekre – idő előtti lehet. A szabvány szerint egy-két éves időtávban megvalósítható intézkedések esetén a részletes elemzés korai. Az értékelés második szintjeként valósulhat meg a *részletes biztonsági kockázatelemzés*, amelynek során *minőségi jellemzők* értékelésére kerülhet sor egy 3-5 fokozatú skála mentén. Egy későbbi, matematikai műveletekkel végrehajtandó elemzéshez azonban még ez is kevés lehet. [5]
5. Esetünkben a Nemzeti Adó- és Vámhivatal (a továbbiakban: NAV) elektronikus információs rendszerei biztonsági besorolása és biztonsági szintjének meghatározása a feladat. 2013. évi adatok szerint a NAV-nak 4 központi, 18 közép- és 49 alsó fokú területi szerve, valamint 7 alsó fokú vámszerv kirendeltsége van, engedélyezett létszáma 22.482 fő (ennyi potenciális felhasználó van a Hivatalon belül, ezen túl milliós ügyfélkörrel rendelkezik), hatásköri jegyzéke több mint 1040 elemet tartalmaz, éves szinten mintegy 66 millió dokumentumot kezel, egy évben a levelező rendszereiben mintegy 129 millió dokumentum keletkezik. A NAV tevékenységét támogató informatikai infrastruktúra legtöbb adata nem nyilvános, azonban a nyilvános források megemlítik, hogy a NAV közel 20.500 db PC-t és 3.500 db laptopot üzemeltet és az idézett forrás 26 rendszert/alkalmazást nevesít. [6] A magyar közigazgatás egyik legnagyobb szervezete esetében olyan elemzés és besorolás szükséges, amely a részletek túlzott hangsúlyozása helyett stratégiai szintű áttekintést biztosít, ezzel egyidejűleg az informatikai szempontból jelentős szempontokra helyezi a hangsúlyt.

A technológiai rendelet rendelkezéseinek és a szabványok ajánlásainak való együttes megfelelés vonatkozásában, a NAV szervezeti sajátosságait és informatikai infrastruktúráját alapul véve, az alábbi javaslatot fogalmazzuk meg.

## BIZTONSÁGI OSZTÁLYBA SOROLÁS

A 01 szabvány az informatikai osztályozás elveit az alábbiak szerint határozza meg: *Az információkat értékük, a jogi előírások, a szervezet szempontjából képviselt érzékenységük és kritikusságuk szempontjából kell osztályozni.*

Tekintettel a fent már kifejtettekre, a 01 szabvány előírásain alapuló osztályozást az adatokra vonatkoztatva végezzük. Álláspontunk szerint – figyelemmel arra, hogy az informatikai rendszereket nagymértékben meghatározza a bennük kezelt adat – ugyanezen kategóriák mérvadóak az informatikai rendszerek besorolásánál is.

A technológiai rendelet 1. sz. mellékletének 1.1. pontja szerint *az érintett szervezet az elektronikus információs rendszere biztonsági osztályba sorolásakor a bizalmasság, sértetlenség és rendelkezésre állás követelményét a rendszer funkciójára tekintettel, ahhoz igazodó súllyal érvényesíti.*

## A szabvány kategóriáinak való megfelelés

Az *érték* az adatot kezelő informatikai rendszert használó szervezet működését, megítélését befolyásoló tényező, ami alapvetően az adatok hiánya, elérhetetlensége, kitudódása vagy sérülése folytán bekövetkező kár nagyságrendjén keresztül fogható meg.

Ezért javaslatunkban a kár mind a bizalmasság, mind a sértetlenség, mind pedig a rendelkezésre állás vonatkozásában értékelésre kerül, figyelemmel a technológiai rendelet 1. sz. mellékletének 1.2.1.1. pontjára is, amely szerint *az adatok és az adott információs rendszer jellegéből kiindulva a kockázatelemezés alapját* egyrészt *az adatok bizalmasságának, sértetlenségének és rendelkezésre állásának*, másrészt *az elektronikus információs rendszerelemek sértetlenségének és rendelkezésre állásának sérüléséből, elvesztéséből bekövetkező kár, vagy káros hatás, terjedelme, nagysága képezi*.

A technológiai rendelet 1. sz. melléklete 1.4. pontjának alpontjai a fenyegető vagy bekövetkező *károk* fajtáit határozzák meg. Eszerint figyelembe kell venni a

*1.4.1. társadalmi-politikai káros hatásokat, károkat vagy a jogsértésből, kötelezettség elmulasztásából fakadó káros hatásokat, károkat (így pl. alaptevékenységek akadályozása, különösen a létfontosságú információs rendszerelemek működési zavarai, a nemzeti adatvagyon sérülései, jogszabályok és egyéb szabályozások megsértése, jogszabály által védett adatokkal történő visszaélés vagy azok sérülése, a közérdekűség követelményének sérülése, személyiséghez fűződő jogok megsértése, bizalomvesztés hatóságokkal, felügyeleti szervekkel szemben, az ország jogrendjének sérülése, vagy ennek lehetővé tétele);*

*1.4.2. személyeket, csoportokat érintő károk, káros hatások (pl. különleges személyes adatok, banktitkok, üzleti titkok megsértése, szervezet, személyek vagy csoportok jó hírének károsodása, személyi sérülések, vagy haláleset bekövetkeztének - ideértve az elektronikus információs rendszer működésének zavara, vagy információhiány miatt kialakult veszélyhelyzetet - veszélye);*

*1.4.3. közvetlen anyagi károk (az infrastruktúrát, az elektronikus információs rendszert ért károk, és ezek rendelkezésre állásának elvesztése miatti pénzügyi veszteség, adatok sértetlenségének, rendelkezésre állásának elvesztése miatti költségek, dologi kár);*

*1.4.4. közvetett anyagi károk (pl. helyreállítási költségek, elmaradt haszonnal arányos költségek, a környezet biztonságának veszélyeztetése, perköltségek).*

Természetesen kijelenthető, hogy nem minden szervezet esetében jöhet szóba mindegyik kártípus; az adott szervnél értelmezhető, szóba jöhető és a tapasztalatok alapján releváns károkat kell figyelembe venni. Ezt a rugalmasságot írja elő a technológiai rendelet 1. sz. mellékletének 1.4. pontja is, amely szerint *az érintett szervezetnél szóba jöhető - közvetett, vagy közvetlen kárt okozó hatásokat, veszélyeket és károkat kell - az érintett szervezet jellemzőire tekintettel - figyelembe venni.*

A besorolási táblázatban az egyes környezetek vonatkozásában értelmezhető és szóba jöhető károk összességükben értékelendőek, azok közül nem emelhető ki egyik sem.

A technológiai rendelet 1. sz. mellékletének 2. pontja ajánlást tartalmaz az egyes biztonsági osztályok jellemzői vonatkozásában. E körben megjegyezzük, hogy e jellemzők nem teljesen illeszkednek a technológiai rendelet 1. sz. mellékletének 1. pontja alatt szereplő általános elvekhez. A 2. pont a biztonsági osztályok fő jellemzőjévé a bekövetkező vagy fenyegető kár jelentőségét teszi. Ezzel szemben az 1. pont 1.3. pontja szerint *a biztonsági osztályba sorolásnál nem a lehetséges legnagyobb kárértéket, hanem a releváns, bekövetkezési valószínűséggel korrigált fenyegetések által okozható kárt, káros hatást kell figyelembe venni.* Tehát nem önmagában a kár nagysága a mérvadó, hanem figyelembe kell venni a káresemény bekövetkezési valószínűségét is.

A kockázatok számba vételénél – megelőzendő a kialakított rendszer szétesését, egyben elősegítve az áttekinthetőséget – mellőztük a bonyolult matematikai képletek és számítások alkalmazását. A NAV informatikai rendszereit fenyegető kockázatok vonatkozásában, az

eddigi tapasztalatok fényében – figyelemmel a kialakult jó gyakorlatra is –, kiemeltük az egyes biztonsági célok megvalósulását fenyegető tényezők közül a legjellemzőbbeket és ezek fennálltához, illetve hiányához (vagy egy háromfokozatú skálán való elhelyezkedésük alapján) rendeltünk besorolási pontszámot.

Meg kívánjuk jegyezni, a NAV esetében – ahogyan az a legtöbb központi közigazgatási szervre jellemző – az objektumvédelemre és a tűzvédelemre vonatkozó szabályozás markánsan elkülönül az informatikai biztonság szabályozásától. Erre figyelemmel az e körben felmerülő kockázatok – mint az informatikai területen túli kockázatok – a biztonsági besorolás tekintetében figyelmen kívül maradtak.

Az előbbiekhez hasonlóan ugyancsak nem kerültek tekintetbe vételre a személyi állomány (felhasználók) személyében rejlő, az informatikai vetülethez közvetlenül nem kapcsolódó biztonsági kockázatok, mivel azok alapvetően a kiválasztási kritériumrendszer működtetésének, valamint a személyügyi biztonsági szabályozás körébe tartoznak. Azonban a személyi biztonság informatikailag közvetlenül leképezhető kockázatai (felhasználók informatikai alapú azonosítása az informatikai rendszerek használata előtt és alatt – autentikáció és autorizáció, naplózás, manuális beavatkozás lehetősége) értékelésre kerültek.

A megoldás a 05 szabvány magas szintű kockázatelemzési eljárására tekintettel az informatikai szempontból releváns elemeket tartalmazza, azonban az egyszerű számbavétel helyett („van-nincs”) a részletes kockázatelemzésnél elvárt – súlyozást is tartalmazó – értékelést valósít meg.

A technológiai rendelet rendszerében a biztonsági osztályok jellemzése során hangsúlyt kap az adatok mennyisége, valamint a különleges személyes adatok érintettsége. E körülmények a NAV tekintetében azonban nem tekinthetőek relevánsnak. A NAV informatikai rendszerei szinte kizárólag hatalmas adattömeget kezelnek, különösen amennyiben a rendszerkapcsolatok létét és számát is figyelembe vesszük, így az adatok mennyisége – a NAV esetében – nem alkalmas szempont az egyes rendszerek jelentőségének megkülönböztetésére.

Ezen túlmenően a különleges személyes adatok kezelése sem tekinthető relevánsnak, mivel a NAV esetében ilyen adatok kezelése nem tekinthető tipikusnak és általánosnak. E jellemzők alapvetően a NAV-ra vonatkoznak, így más szerv esetén ezek a kategóriák alkalmazása természetesen nem kizárt, sőt adott esetben kiemelt fontossággal bírhat.

A *jogi előírások* kategóriáján az informatikai rendszerekben tárolt adatok jogi minősítését értjük. A hatályos jogszabályok több mint 10 adatfajtát nevesítenek, ennek alapján a kezelt adatok körét három kategóriába sorolva célszerű meghatározni: nyilvános adat, törvény által védett adat és minősített adat. A törvény által védett adat fogalmába tartoznak különösen a személyes adat, adótitok, vámtitok, banktitok, értékpapírtitok stb. A rendszerben kezelt adatok fajtája a bizalmasság kategóriájának a részét képezi. Nyilvános adat esetén a bizalmasság kérdése irrelevánsnak tekinthető, figyelemmel arra, hogy azokat bárki megismerheti, míg törvény által védett adat vagy minősített adat kezelése esetén e tény döntő befolyást gyakorol az informatikai rendszer jelentőségére.

Az *érzékenység* szempontja a bizalmasság és a sértetlenség kategóriáin, mint biztonsági célokon keresztül érvényesül, így ez a szempont bővebben e kategóriáknál kerül kifejtésre.

A *kritikusság* szempontja pedig a rendelkezésre állás biztonsági céljának felel meg, így kifejtését lásd ott.

### A technológiai rendeletnek való megfelelés

Amint azt fent már említettük, a technológiai rendelet, valamint a 01 szabvány alapján az értéket, és az azt kifejező kárt mind a bizalmasság, mind a sértetlenség, mind pedig a rendelkezésre állás tekintetében értékeljük. A technológiai rendelet 1. sz. mellékletének 1.2.1.2. pontja szerint azonban nem elegendő a kár mértékének a figyelembe vétele, hanem a

kockázatelemzés alapját képezi *a kár bekövetkezésének, vagy a kárral, káros hatással fenyegető veszély mértéke, becsült valószínűsége* is.

A technológiai rendelet 1. sz. mellékletének 1.3. pontja alapján kijelenthető, hogy *a biztonsági osztályba sorolásnál nem a lehetséges legnagyobb kárértéket, hanem a releváns, bekövetkezési valószínűséggel korrigált fenyegetések által okozható kárt, káros hatást kell figyelembe venni.* A kár bekövetkezési valószínűsége vonatkozásában pedig a technológiai rendelet 1. sz. mellékletének 1.5. pontja szerint pedig *a veszélyeztetettségnek a bekövetkezés valószínűségének megfelelő kárérték szinteknek megfelelő biztonsági osztályba sorolásakor a bizalmasság, sértetlenség és rendelkezésre állás követelménye külön-külön értékelendő.*

A fentiekre figyelemmel, a technológiai rendelet követelményeinek való megfelelés érdekében mind a bizalmasság, mind a sértetlenség, mind pedig a rendelkezésre állás biztonsági céljai vonatkozásában egyszerre kerülnek értékelésre a biztonsági célok teljesülését veszélyeztető fenyegetések mértéke, valamint a bekövetkező vagy fenyegető kár is.

A *bizalmasság* fogalma alapvetően az adathoz való jogosulatlan hozzáférést jelenti, sérülése az ebből következő, a szervezet működését és megítélését befolyásoló negatív hatás.

A bizalmasság egyik elemének tekinthető a rendszerben kezelt adatok *jogi minősítése,* amely alapján az adat lehet nyilvános adat, törvény által védett adat vagy minősített adat. A törvény által védett, illetve minősített adatot kezelő rendszereknél a bizalmasság alapvető fontosságúnak tekinthető, mivel törvény ezen adatok vonatkozásában korlátozza a megismerésre jogosultak körét. Ezzel szemben a nyilvános adatok esetén a bizalmasság fogalma irreleváns, mivel ebben az esetben az adatokat bárki megismerheti. Meglátásunk szerint a bizalmasság sérüléséből fakadó kár is objektíven a jogi minősítésen keresztül ragadható meg. Egy törvény által védett vagy minősített adat esetében a bizalmasság sérülése okozhatja a szervezetnek a legnagyobb kárt, különös figyelemmel arra, hogy ebben az esetben esetlegesen mind anyagi kár (pl. személyiségi jogok sérelme miatti sérelemdíj, kártérítés), mind presztízsveszteség (pl. negatív sajtóvisszhang, közbizalom megrendülése) nyomatékosan felmerülhet, illetve esetlegesen a szerv alaptevékenységének sikeres ellátása is veszélybe kerülhet (pl. a NAV esetében a kockázatkezelési tevékenységhez kapcsolódó szakmai ismeretek, informatikai programok, algoritmusok stb. kitudódása).

A bizalmasság kérdésköre kapcsán azonban a technológiai rendelet fentebb említett rendelkezése alapján figyelemmel kell lenni a veszélyeztetettség mértékére is. E körben a NAV informatikai struktúrájából fakadó, a gyakorlat alapján felmerülő kockázatokat vettük alapul. Természetesen más informatikai jellemzőkkel bíró szervezet esetében e kritériumok változhatnak.

A bizalmasság körében kockázatként a külső hálózatokhoz (pl. internet) való csatlakozást, továbbá az autentikáció és autorizáció formáját, biztonságosságát határoztuk meg. A külső kapcsolat megléte önmagában kockázatot jelent, ugyanis az fizikailag lehetővé teszi a külső, illetéktelen behatolást az informatikai rendszerbe. Az autentikáció és autorizáció módja is meghatározza a rendszerbe történő illetéktelen belépés kockázatát. E körben jelenleg a tudás alapú azonosítás (jelszavas védelem) jelenti a legkisebb védelmet, így a legnagyobb kockázatot. Amennyiben az azonosító- és jelszóhasználat birtoklás alapú védelemmel egészül ki (pl. hardvereszköz, token), úgy a kockázat csökken. E körben – a jelenlegi elterjedt védelmi megoldások közül – a legnagyobb biztonságot a tulajdonság alapú (biometrikus) azonosítás garantálhatja, e módszerrel gyakorlatilag kizárható az illetéktelen belépés lehetősége.

Az említett tényezők együttes figyelembe vételével valósul meg a technológiai rendelet azon követelménye, miszerint *a releváns, bekövetkezési valószínűséggel korrigált fenyegetések által okozható kárt, káros hatást kell figyelembe venni.*

A *sértetlenség* biztonsági célja az adat megváltozásának, megsemmisülésének, valamint jogosulatlan megváltoztatásának, megsemmisítésének a szervezet működését és megítélését befolyásoló hatását jelenti.

E körben a fentiek alapján értékelendő, hogy az adatok esetleges megváltozása milyen kárt jelent a szervezet szempontjából. Utalva a korábban már kifejtettekre, a szóba jöhető károkat összességükben kell értékelni, anélkül, hogy azok közül bármelyiket is kiemelnénk.

A kockázatok körében értékelendő, hogy az adat helytelensége belső eljárás vagy informatikai megoldás következtében a szervezet belső működése során, az ügyintézés szempontjából releváns időn belül ki derülhet-e. Amennyiben ugyanis az adat helytelensége az adott informatikai rendszeren kívüli módon kiderülhet, ez a körülmény csökkenti a sértetlenség biztonsági célja sérülésének kockázatát. Ugyancsak a kockázatok körében értékelendő, hogy az adott rendszer lehetővé teszi-e a felhasználók és az üzemeltetésben részt vevő informatikusok részéről a (nem indokolt) manuális beavatkozás lehetőségét. Amennyiben ilyen lehetőség nem adott, az nyilvánvalóan csökkenti az informatikai rendszert fenyegető veszélyt. E körben értékelendő még az adott rendszer naplózottsága is az adatok megváltozása vonatkozásában, ez ugyanis szinte biztossá teszi az illetéktelen adatmódosítás felderítését, és az ehhez kapcsolódó felelősségre vonást, ami a felhasználók számára komoly visszatartó erővel bírhat.

E körben is a kár és a kockázati tényezők egyes elemeinek az együttes értékelése adja ki a sértetlenség besorolási pontszámát.

A *rendelkezésre állás* az informatikai rendszer (és így az adat) jogosultak általi elérésének, felhasználásának előre nem tervezett korlátozottságát vagy hiányát jelenti.

E körben alapvető fontossággal bír, hogy milyen mértékben befolyásolja (veszélyezteti, akadályozza, lehetetlenné teszi) a szervezet működését, illetve, hogy a szervezet mennyi ideig tudja nélkülözni az adott adatot, informatikai rendszert bármilyen kár felmerülése nélkül.

A rendelkezésre állás biztonsági céljának a kategóriájában is értékelésre kerül a tűréshatáron túli kieséssel okozott kár.

Ezen túlmenően a veszélyeztetettség két elemből áll össze.

Egyrészt definiálni kell, hogy az adott rendszer kiesése (az adat elérhetetlensége) mennyi idő után okoz a szerv számára bármilyen kárt. Ez sávokban adható meg. Egyrészt vannak olyan rendszerek, amelyek esetében szinte a szünet nélküli működés az elvárás. E rendszerek esetében a helyreállítás elvárt határideje legfeljebb 4 óra. Másrészt vannak olyan rendszerek is, amelyek 4 órán túli hiánya nem gyakorol alapvető befolyást a szerv napi tevékenységi körébe tartozó feladatok elvégzésére. A 4 óra helyreállítási idő, mint határ, a NAV belső munkafolyamatainak és az informatikai rendszereinek jellemzői alapján, a felhasználó szakmai területek igényeinek a figyelembe vételével, valamint az általános helyreállítási idő körében szerzett tapasztalatok alapján került meghatározásra. Természetesen más jellemzőkkel bíró szervezet esetében más időkorlát lehet megfelelő.

Másrészt a veszélyeztetettség körében javasoljuk értékelni azt, hogy az empirikus tapasztalatok alapján az adott rendszer üzemidejéhez képest átlagosan hány százalékot tesz ki az előre nem tervezett leállás, elérhetetlenség. Ennek meghatározásához javasoljuk az utolsó három év adatainak az átlagát venni. Ez a rendelkezésre állás biztonsági céljának sérülése vonatkozásában az utóbbi idők tapasztalatai alapján jelöli meg a valós kockázatot. E dinamikus, minden évben változó értékű kategória kialakítása során mindenképpen középtávú átlagot javaslunk figyelembe venni, ami korrigálhatja az időszakos kilengéseket, illetve tekintetbe tudja venni az egyes fejlesztésekkel járó minőségi javulást is. E körben a skála egyes értékei (kicsi, közepes, magas) kapcsán a százalékos határokat (pl. átlagban 99% feletti rendelkezésre állás – kicsi; átlagban 98-99%-os rendelkezésre állás – közepes; átlagban 98% alatti rendelkezésre állás – magas) minden esetben az adott szerv munkafolyamatai és elvárásai alapján javasoljuk meghatározni.

## ÖSSZEGZÉS

Az ismertetett besorolási javaslat megfogalmazásakor a szerzők elsődleges célja egy elvi szempontok szerint *alkalmazható* és a jelenlegi adottságokat figyelembe véve *végrehajtható* értékelési rendszer kidolgozása volt, amely:

- az elvi kereteket tekintve a jogszabályok és a meghatározó szabványok közötti összhang megteremtésével konzisztens alapokat nyújt;
- figyelemmel van a közigazgatási szervek azon sajátosságára, miszerint a különböző információvédelmi aspektusok jellemzően más-más (személyügyi, objektumvédelmi, informatikai) szakterület, szervezeti egység kompetenciájába tartoznak, így a felméréseket, az intézkedések tervezését és végrehajtását egy-egy szakterület önállóan végzi saját feladatkörén belül, és az intézkedések összehangolása már az egyes szervezetek közötti/feletti koordinációval valósulhat meg;
- mivel a jogszabályok hatályba lépésével keletkező, több évre szóló kötelezettségek, feladatok teljesítésére többlet-erőforrás nem lett tervezve, az érintett közigazgatási szerv meglevő erőforrásai teljesítőképességéhez és konkrét adottságaihoz igazodó, a már rendelkezésre álló tudást hasznosító értékelési szempontrendszert biztosít;
- tekintettel arra, hogy kész, azonnal használatba vehető értékelési módszertanok nincsenek, a rendelkezésre álló – a szakirodalom szerint rövid – határidőn belül alkalmazható módszertant bocsát az informatikai szakterület rendelkezésére.

A biztonsági osztályba soroláshoz szükséges értékelési adatokat a mellékelt táblázat tartalmazza.

A közigazgatási szerv biztonsági szintbe sorolásával kapcsolatos elméleti és gyakorlati kérdések egy másik tanulmány tárgya lehetnek.

### Felhasznált irodalom


[1] Az állami és önkormányzati szervek elektronikus információbiztonságáról szóló 2013. évi L. törvény (Ibtv.)

[2] Az állami és önkormányzati szervek elektronikus információbiztonságáról szóló 2013. évi L. törvényben meghatározott technológiai biztonsági, valamint biztonságos információs eszközökre, termékekre vonatkozó, valamint a biztonsági osztályba és biztonsági szintbe sorolási követelményeiről szóló 77/2013. (XII. 19.) NFM rendelet

[3] Közigazgatási Informatikai Bizottság 25. számú Ajánlása. 2008. június

[4] MSZ ISO/IEC 27001:2006 szabvány. Informatika. biztonságtechnika. Az információbiztonság irányítási rendszerei. Követelmények

[5] MSZ ISO/IEC 27005 szabvány. Information technology – Security techniques – Information security risk management

[6] Nemzeti Adó- és Vámhivatal Évkönyve. Budapest, 2013.

| **Bizalmasság** | | **pont** | **Sértetlenség** | | **pont** | **Rendelkezésre állás** | | **pont** | **összes pont-szám** |
|---|---|---|---|---|---|---|---|---|---|
| Kezelt adatfajta | nyilvános adat | 0 | Megváltozás esetén a kár mértéke | kicsi | 0 | A rendszer kiesésének tűrési ideje | 4 órán belül | 1 | |
| | törvény által védett adat | 1 | | közepes | 1 | | | | |
| | minősített adat | 2 | | nagy | 2 | | 4 órán túl | 0 | |
| Azonosítás formája | jelszavas | 2 | Van-e naplózás az adat megváltozására? | van | 0 | A tűrési időn túli kiesés által okozott kár | kicsi | 0 | |
| | jelszavas + token | 1 | | nincs | 1 | | közepes | 1 | |
| | biometrikus | 0 | Biztosított-e a manuális beavatkozás lehetősége? | igen | 1 | | magas | 2 | |
| Van-e a rendszernek külső kapcsolata? | igen | 1 | | nem | 0 | Átlagos veszélyeztetettség az utolsó három év adatai alapján | kicsi | 0 | |
| | | | | | | | közepes | 1 | |
| | nem | 0 | Egyéb módon kiderül-e az adat helytelensége? | igen | 0 | | magas | 2 | |
| | | | | nem | 1 | | | | |
| Összes pont: | | | | | | | | | |

Biztonsági osztályba sorolás:

1. biztonsági osztály 0-3 pont
2. biztonsági osztály 4-6 pont
3. biztonsági osztály 7-9 pont
4. biztonsági osztály 10-12 pont
5. biztonsági osztály 13-15 pont