Gradus Vol 11, No 1 (2024)
ISSN 2064-8014

AZ ELEKTRONIKUS INFORMÁCIÓS RENDSZEREKBŐL KINYERHETŐ JOGOSULTSÁG PILLANATKÉPEK FELHASZNÁLÁSAINAK LEHETŐSÉGEI

POSSIBLE USES OF AUTHORISATION SNAPSHOTS EXTRACTED FROM ELECTRONIC INFORMATION SYSTEMS

Kiss Gábor Zsolt [ORCID 0009-0004-4314-903X*], *László Gábor* [ORCID 0000-0002-1348-8960]

[1] Közigazgatás-tudományi Doktori Iskola, Államtudományi és Nemzetközi Tanulmányok Kar, Nemzeti Közszolgálati Egyetem, Magyarország
[2] Közszervezési és Infotechnológiai Tanszék, Államtudományi és Nemzetközi Tanulmányok Kar, Nemzeti Közszolgálati Egyetem, Magyarország
https://doi.org/10.47833/2024.1.CSC.010

Kulcsszavak:
Jogosultságkezelés
Elektronikus Információs Rendszerek
Szabályozás

Keywords:
Access control
Electronic Information Systems (EIS)
Regulations

Cikktörténet:
Beérkezett 2023. november 23.
Átdolgozva 2024. január 24.
Elfogadva 2024. január 30.

Összefoglalás

A cikk célja, hogy bemutassa az Elektronikus Információs Rendszerekből (EIR) kinyerhető jogosultság pillanatképek felhasználási lehetőségeit, legyen az egy, vagy több EIR-ből kinyert jogosultság pillanatkép. Bemutatásra kerül a jogosultság pillanatképek elemzésével előálló riportok elkészítése, amelyek támogathatják a vonatkozó főbb általános szabályozási elvárásokat és hozzájárulhatnak a napi informatikai működés biztonságosabbá tételéhez.

Abstract

The purpose of this paper is to show possible uses of users' authorization snapshots that can be extracted from Electronic Information Systems (EIS), whether the snapshot is extracted from one or more systems. The preparation of reports generated by the analysis of authorization snapshots is presented, which can support the relevant general regulatory requirements and contribute to making daily IT operation more secure.

1. Bevezetés

Napjaink stratégiai hívószavai közé tartozik a digitális transzformáció. Az Európai Unió Digitális évtized 2030 szakpolitikai program általános célkitűzései között is megjelenik a kiberbiztonság, mint „a kibertámadásokkal szembeni reziliencia javítása, hozzájárulás a kockázatokkal kapcsolatos tudatosság növeléséhez és a kiberbiztonsági folyamatokkal kapcsolatos ismeretek bővítéséhez, valamint az állami és magánszervezetek arra irányuló erőfeszítéseinek fokozása, hogy a kiberbiztonság legalább alapvető szintjét elérjék.” [4]

Magyarországon 2013-ban elfogadásra került az állami és önkormányzati szervek elektronikus információbiztonságáról szóló törvény. [1]

* Kapcsolattartó szerző.
E-mail cím: kiss.gabor.zsolt@stud.uni-nke.hu

Möller bemutatja a digitális transzformáció jelenségét, kitérve az olyan diszruptív, feltörekvő technológiákra is, mint a mesterséges intelligencia, a Big Data és analitika, a blokklánc, a felhőalapú számítástechnika és szolgáltatások, IoT, stb. Felhívja a figyelmet a technológiák gyors fejlődése következtében kialakuló kiberbiztonsági kockázatokra és fenyegetésekre, amelyek kedvezőtlen hatást gyakorolhatnak a szervezetekre. Fontos, hogy ezeket a kiberbiztonsági kockázatokat hatékonyan kezeljék, ezért a kiberbiztonsági kockázatok értékelése és kezelése a szervezetek mindennapjainak szerves részévé kell, hogy váljon. [10]

Az információbiztonság alappilléreinek tekintett – az angol kifejezéseinek kezdőbetűinek összeolvasásából képződött CIA triád – bizalmasság (Confidentiality), sértetlenség (Integrity), rendelkezésre állás (Availability) pontos eredete nem ismert a szakirodalomban. [10] A technológia fejlődésével a kiberbiztonság hatóköre kibővült, így az eredeti koncepció is kibővült. Baars és Spruit 2013-as munkájukban a felhő technológiával kapcsolatosan bővítették a modellt CI3A néven. Az elszámoltathatóság (Accountability) azt jelenti, hogy egyetlen felhasználó se hajthasson végre cselekményeket a rendszereken belül, anélkül, hogy a tevékenysége naplózásra kerüljön. [5] Ez a szempont már Wheeler 2011-es munkájában is megjelent. [12] Az auditálhatóság (Auditability), azaz a környezet auditálhatóságának fogalma közvetlenül kapcsolódik az irányításhoz és a megfelelőséghez. [5]

Cherdantseva és szerzőtársai könyvfejezetükben hosszasan tárgyalják és megpróbálják tisztázni az információbiztonság jelentését, hatókörét és céljait. [7]

Bhaskar és Kapoor az információbiztonsággal kapcsolatos szabványokat meghatározó főbb szervezeteket mutatja be. [6] Godishala és szerzőtársainak célja az Átfogó útmutató az információbiztonság irányításához és ellenőrzéséhez művükben, hogy átfogó képet mutassanak be az információbiztonságról, a 27001-es információbiztonsági szabványnak megfelelő irányítási rendszerről, az audit tervezéséről és előkészítéséről, az auditálási technikákról. [8]

A biztonság leggyengébb láncszeme a felhasználó, amint erre a Thales 2023-as adatfenyegetési jelentése is rámutat, amely az adatvédelmi incidensek elsődleges okaként az emberi hibát emeli ki. [11] A szerzők célja a fent vázolt széles információbiztonsági spektrum területéről – a magyarországi szabályozási környezeten keresztül – az információs rendszerekből kinyerhető jogosultsági pillanatképek elemzéséből adódó gyakorlati felhasználási lehetőségeinek bemutatása.

2. Szabályozási környezet

Az informatikai és információbiztonsági szektorban számos, hasonló elvárásokat megfogalmazó jogszabály, ajánlás támaszt követelményeket a jogosultságokkal és jogosultságkezeléssel kapcsolatosan, melyeknek alappillére a felülvizsgálat. Erre vonatkozóan gyakran találhatóak szervezeti szintű szabályozások is, amik a jogosultságoknak és azok kezelésének megvalósítását, leképezését helyezik szem elé.

2.1. Az Ibtv. vhr előírásai a jogosultságokra vonatkozóan

Az állami és önkormányzati szervek elektronikus információbiztonságáról szóló 2013. évi L. törvényben [1] meghatározott technológiai biztonsági, valamint a biztonságos információs eszközökre, termékekre, továbbá a biztonsági osztályba és biztonsági szintbe sorolásra vonatkozó követelményekről szóló 41/2015. (VII. 15.) BM rendelet (BM rendelet) [2] 3-as biztonsági osztályba vagy a fölé sorolt Elektronikus Információs Rendszerek (EIR-ek) esetén számos előírást támaszt.

A BM rendelet előírja, hogy az érintett szervezetnek meg kell határoznia

- a felhasználói fiókjait és azok típusait;
- ki kell jelölni a felhasználói fiókok fiókkezelőit és ki kell alakítani a csoport- és szerepkör tagsági feltételeket.

A rendelet alapján elvárás, hogy a fiókkezelők értesítve legyenek, amennyiben a felhasználói fiókra már nincs szükség, valamint, ha a felhasználók kiléptek vagy áthelyezésre kerültek. Azaz elvárás a szervezeti szintű fluktuáció naprakész nyilvántartása, és azok EIR-ekben történő jogosultság szintű kezelése.

További elvárás az

- ideiglenes fiókok eltávolítása,

- az inaktív fiókok letiltása,
- a felhasználói fiókok életciklusában történő események naplózása,
- valamint a kockázatot jelentő felhasználó fiókjának azonnali tiltása.

A BM rendelet előírja, hogy a felhasználói fiókok és a fiókkezelési követelményekkel való összhang felülvizsgálata periodikusan megtörténjen. Szintén elvárásként fogalmazódik meg a legkisebb jogosultság elvének betartása, továbbá az is, hogy a biztonsági funkciókhoz külön hozzáférés biztosítása legyen szükséges. Így megkülönböztetésre kerül szerepkör alapon a nem privilegizált és privilegizált felhasználó. Utóbbival szemben elvárás a privilegizált funkciók használatának naplózása és a szakszerű funkcionális elhatárolás.

2.2. A Magyar Nemzeti Bank 8/2020. (VI.22.) számú ajánlása az informatikai rendszer védelméről a jogosultságokra vonatkozóan

Az Magyar Nemzeti Bank 8/2020. (VI.22.) számú ajánlásában [3] megtalálható a hozzáférési rend szabályozása, amely kimondja, hogy a legkevesebb jogosultság elve alapján kell meghatározni és dokumentálni az üzleti és informatikai szerepkörökhöz tartozó hozzáférési szabályokat, ideértve az összeférhetetlen szerepköröket.

Az MNB ajánlás szerint elvárt az informatikai rendszerekhez történő hozzáférés szabályozása, melyet az intézmény az informatikai rendszerében technológiai megoldásokkal kikényszeríti, beleértve az összeférhetetlen szerepkörök egyidejű alkalmazásának kizárását.

Ennek metodikája, hogy az intézmény azonosítja azokat a jogosultsági objektumokat és erőforrásokat, amelyekhez az informatikai rendszerben definiált felhasználók hozzáférhetnek, és amely felhasználókat folyamatok, vagy személyek megszemélyesítenek, melynek keretében elvárt, hogy az intézmény a jogosultsági objektum és erőforrás, a felhasználó és a megszemélyesítő összerendeléseket mindenkor nyilvántartsa.

A hozzáférések kezelése során a tervezett és megvalósult összerendeléseket és az ezeken keresztül megvalósított hozzáféréseket folyamatosan nyomon kell követni, és gondoskodni kell azok összhangjának rendszeres ellenőrzéséről.

Felhasználói adminisztráció tekintetében a szervezettel szembeni elvárás, hogy az informatikai rendszeréhez való hozzáférést egyedi, természetes személyekkel egyértelműen összerendelhető felhasználói fiókok használatához köti és a használatot az informatikai biztonsági szabályozási rendszerében szabályozza, és megvalósítja, hogy az informatikai rendszerekben csak az aktuálisan engedélyezett felhasználók rendelkezzenek jogosultsággal, és a jogosultság ellenőrzése azonnal elvégezhető legyen.

2.3. ISO/IEC 27001:2022 és MSZ ISO/IEC 27001:2023

A magyar nemzeti MSZ ISO/IEC 27001:2023 szabvány teljesen megegyezik az ISO/IEC 27001:2022 nemzetközi szabvánnyal, melynek témája az Információbiztonság, kiberbiztonság és a magánélet védelme. Információbiztonság-irányítási rendszerek. [9] A magyar nyelvű változatot a Magyar Szabványügyi Testület készítette. Célja, hogy követelményeket határozzon meg egy információbiztonság-irányítási rendszer kialakítására, bevezetésére, fenntartására és folyamatos fejlesztésére.

A szabvány A1. táblázatában megfogalmazódnak a hozzáférési jogosultságokkal és a kiemelt hozzáférési jogosultságokkal szembeni elvárások.

Az „5.18. Hozzáférési jogosultságok” része szerint elvárásként fogalmazódik meg, hogy az információkhoz és egyéb kapcsolódó vagyonelemekhez való hozzáférési jogosultságokat a szervezet témaspecifikus politikáinak és hozzáférés-felügyeleti szabályainak megfelelően kell biztosítani, átvizsgálni, módosítani és visszavonni.

A „8.2. Kiemelt hozzáférési jogosultságok” pont elvárása szerint korlátozni és menedzselni kell a kiemelt hozzáférési jogosultságok kiosztását és felhasználását.

2.4. Jogosultsági szintek

A BM rendelet kétféle fiókhoz tartozó jogosultság típust különböztet meg, mint nem privilegizált fiókhoz és privilegizált fiókhoz tartozó jogosultság. 3-as vagy a fölötti biztonsági osztályba sorolás esetén előírás, hogy a szervezet által használt EIR-ek meghatározott biztonsági funkciókhoz vagy biztonságkritikus információkhoz privilegizált fiókkal, míg a nem biztonsági funkciók használatához nem a különleges jogosultsághoz kötött fiókjukat vagy szerepkörüket használják. A kiváltságos jogokkal elérhető funkciókat tiltani kell a nem privilegizált felhasználói fiókkal rendelkező hozzáférések esetén.

A jogosultság felülvizsgálat során minden hozzáférési típust és a jogszabály szerint elvárt EIR nyilvántartásban szereplő minden EIR-t vizsgálni kell. EIR-ek esetén az alkalmazás szintű hozzáférésen kívül a vizsgálat körébe kell tartoznia a rendszer (operációs rendszeri hozzáférés, a telepítési jogok, a bejelentkezési jogok és az adatbázis hozzáférés), az adatbázis (az adatbázis-szerverekhez való hozzáférést és a felhasználók jogosultságait), a fájl- és mappaszintű és a hálózati (fájlmegosztókhoz, nyomtatókhoz és egyéb hálózati eszközökhöz) hozzáférésnek is.

3. Védelmi intézkedések

Egy adott információbiztonsági kockázat bekövetkezési gyakoriságnak vagy hatásának csökkentésére kockázatarányosan védelmi intézkedéseket és kontrollokat kell alkalmazni. A védelmi intézkedések körében kiemelten fontos a hozzáférés menedzsment, melynek eleme a jogosultságok rendszeres felülvizsgálata, a külső félnek kiadott jogosultságok kezelése és a kiváltságos jogokkal emelt felhasználók kezelése.

4. Hozzáférési jogosultságok felülvizsgálata, és annak esedékessége

A jogosultság felülvizsgálat egy olyan folyamat, amelynek során az adott rendszer vagy szervezet belső jogosultságkezelési gyakorlatának ellenőrzése történik annak biztosítása érdekében, hogy a felhasználók csak azokhoz az erőforrásokhoz férjenek hozzá, amelyekre jogosultak.

A jogosultság audit fontos része az Elektronikus Információs Rendszerekhez hozzáférő felhasználók és azok jogosultságainak felülvizsgálata. A jogosultság felülvizsgálatot – a jogosultság nyilvántartás automatizáltságától függetlenül – bármilyen nyilvántartási megoldás esetén szükséges elvégezni, Elektronikus Információs Rendszerenként.

A BM rendelet nem ír elő konkrét időpontot és nem támaszt konkrét elvárást a jogosultságok ellenőrzésével és annak periodicitásával kapcsolatban, de megköveteli, hogy meghatározott gyakorisággal felül kell vizsgálni a felhasználói fiókokat és a hozzájuk tartozó jogosultságokat, és természetesen a fiókkezelési követelményekkel való összhangot;

Az MNB ajánlás elvárásként fogalmazza meg, hogy az intézmény az informatikai biztonsági szabályozási rendszerben meghatározott eljárásrend szerint, az abban meghatározott időközönként, de legkésőbb évente a felhasználói azonosítók és a hozzájuk kapcsolódó jogosultságok dokumentált ellenőrzésével meggyőződjön a hozzáférési és felhasználói adminisztrációs szabályok betartásáról.

Azonban, összhangban az ajánlásokkal, a jogosultság felülvizsgálatot érdemes periodikusan évente végrehajtani. Amennyiben van rá erőforrás, a periódus időtartama csökkenthető, növelve ezzel a biztonságot, és a jogosultság nyilvántartás rendszer – legyen az manuális vagy automatizált – naprakészségét.

A jogosultságok felülvizsgálatának igénye és esedékessége független a jogosultság nyilvántartás megvalósításának módjától, bár a jogosultság nyilvántartás műszaki megvalósításának módja támogathatja azt.

Amennyiben megoldható, a fluktuáló kollégák hozzáféréseinek ellenőrzése minden hónapban javasolt. Ennek segítségével megakadályozható, hogy a kilépett munkavállalók hozzáférései beragadjanak, vagy a szervezeti egység váltó kollégák jogosultságainak aktualizálásában hiba maradjon. A teljes felülvizsgálatnak minden EIR esetén periodikusan minimum évente vagy félévente, míg a fluktuáló munkavállalók jogosultságainak felülvizsgálatának havonta meg kellene történnie.

5. Jogosultsági pillanatképek fogadása a forrásrendszerekből

A forrásrendszerekből érkező jogosultság exportok feldolgozásához ajánlott kiszolgáló fogadó infrastruktúrája minimális erőforrás igényű, mindösszesen 2 db virtuális CPU, 4 GB RAM és 100 GB diszk erőforrás szolgálhatja ki, mely egy darab virtuális gépet alkot a hypervisor rétegen felül. Az operációs rendszer és a futtató környezet ingyenes, az adattranszformációt és feldolgozást támogató megoldás is. Mindösszesen 2 db portnak szükséges nyitva lennie a fogadó oldalon, szolgáltatás szerint az egyik a biztonságos file fogadásra, a másik az adminisztráció ellátására szükséges.

Az arra alkalmas forrásrendszerek – EIR-ek – periodikusan pillanatképet készíthetnek a saját felhasználói adatbázisuk alapján az aktuális jogosultságokról, majd CSV file-ként letárolhatják azt.

Az exportok a jelszavakat és azok lenyomatát sem tartalmazzák, hiszen a jogosultság felülvizsgálathoz nincs is rá szükség.

A pillanatképek a forrásrendszerekből egy biztonságos hálózati átviteli csatornán, SMB-n kerülhetnek el a feldolgozást végző rendszerhez, a fogadás céljára létrehozott, EIR-enként elkülönített mappába, melyek jogosultság szinten is el vannak különítve. A jogosultsági pillanatkép file neve minden esetben tartalmazza a szervezet EIR nyilvántartása szerinti EIR azonosítót, a dátumot és az időt.

A beérkezést követően a jogosultsági pillanatkép mozgatva átkerülhet egy processing mappába, úgy, hogy a fogadó mappa üresen marad. Ezt követően egy script segítségével megtörténhet a feldolgozás. A feldolgozást követően a célfile, amely az elvárt struktúrát és tartalmat tartalmazza a riporting mappában kerül elhelyezésre, immár táblázatkezelő és felhasználó által értelmezhető formátumban.

A forrásrendszerek által szolgáltatott jogosultság pillanatképeinek CSV header-jei bár eltérhetnek, mégis van közös részük, amelyet az 1. táblázat szemléltet.

1. Táblázat. Forrásrendszerek által szolgáltatott jogosultsági pillanatképeinek közös elemei

Név
Felhasználónév
Felhasználóhoz rendelt jogosultságok
Felhasználó státusza (aktív/inaktív)

Amennyiben a forrásrendszerből kinyerhetőek még, javasolt a 2. táblázat szerinti adatok lekérése..

2. Táblázat. Forrásrendszerek által szolgáltatott jogosultsági pillanatképeinek további elemei

Inaktiválás dátuma
Utolsó belépés dátuma
HostAddress
Felhasználói licensz státusz

6. Pillanatképek elemzéséből adódó lehetőségek Elektronikus Információs Rendszerenként

Amennyiben csak egy EIR-ből áll rendelkezésre a forrás oldali export, vagy EIR-enkénti felhasználást nézünk, úgy több felhasználási lehetőségünk van az elemzések elvégzésére.

- Meghatározhatóak az EIR-ben ténylegesen beállított jogosultsági szintek listája, a felhasználók jogosultságainak listája a felhasználók státuszával együtt.
- Szintén meghatározhatóak
  - egy időpontnál régebben bejelentkező felhasználók listája,
  - a jogosultságokban történt változások, és akár
  - a felhasználói licenszek szükségessége is.

6.1. Rendszerek és a rendszerekben található, rendszerekhez tartozó jogosultsági szintek

A forrásoldalról fogadott adatokból disztinktáltan kinyerhető, hogy az adott EIR-ben milyen jogosultsági szintek vannak beállítva, azaz kinyerhető a jogosultsági szintek listája. A kapott információ összevethető az adott EIR Rendszerbiztonsági Tervében (RBT) szereplő vagy egyéb releváns dokumentumokban nyilvántartott jogosultsági szintekkel, és a szervezeti jogosultság nyilvántartásban szereplő jogosultsági szintekkel. Eltérés esetén megtörténhet a jogosultsági szintek listájának korrekciója, mely alappillére a jogosultság felülvizsgálatnak.

Amennyiben például a felhasználók bejelentkezéséhez megkövetelik a többtényezős hitelesítést (MFA – Multi-Factor Authentication), és az EIR-ben ez jogosultsági szintként van menedzselve, kinyerhető, hogy mely felhasználók, mely típusú fiókok vagy további jogosultsági szintek mellé van beállítva az MFA, így akár ez is felülvizsgálható a riport segítségével.

6.2. Rendszerenként a felhasználók, a felhasználó státusza (aktív/inaktív) és a hozzájuk tartozó jogosultsági szintek

Előállítható az adott EIR-re vonatkozó felhasználók listája és a felhasználókhoz tartozó jogosultságainak listája, az aktív/inaktív státuszaikkal együtt. Az így előállított riportból a hibásan beállított aktív státusz mellett a jogosultsági szintek is felülvizsgáltathatóak.

6.3. Felhasználók listája, aki egy megadott időnél régebben jelentkeztek be

Az EIR-ekben előfordulnak olyan felhasználók, melyeknek a hozzáférési státusza aktív, azonban régóta nem jelentkeztek be az adott EIR-be. Amennyiben a forrásoldali export tartalmazza az utolsó bejelentkezés dátumát, lekérdezéssel előállhat egy olyan lista, ami egy, paraméterként megadott időértéknél régebben bejelentkezett felhasználókat tartalmazza az adott EIR-re vonatkozóan. A listára lehet folyamatokat építeni, amivel ellenőrzés alatt tartjuk a régóta be nem jelentkezett felhasználók inaktiválásának folyamatát.

6.4. Jogosultságokban történő változások

Mivel a felhasználók és azok jogosultságainak listája a forrás EIR-től akár naponta megérkezhet, így az előző naphoz képest kimutathatóak a változások. Így kinyerhető az az információ, hogy egy adott időszakban adott felhasználóra vonatkozóan, vagy a rendszer összességére vonatkozóan milyen jogosultságok változtak, és hogyan. Valamint, ennek segítségével riportálható, hogy a kiemelt jogosultságok hogyan változtak egy adott időszakban.

6.5. Felhasználói licenszek

Bizonyos EIR-ekben a felhasználó inaktívvá tétele többféleképpen is történhet. Vagy a felhasználó státuszát inaktiválják, vagy elveszik az EIR-ben a felhasználóhoz tartozó használatra jogosító licensz-et. Bár mindkettő módszer ugyanazt eredményezheti: a felhasználó nem fér hozzá az EIR-hez, azonban az utóbbinak költségvonzata is lehet. Amennyiben a forrásoldali exportba sikerül beletenni a felhasználói licensz státuszra vonatkozó információt vagy flag-et, úgy a kapott riportot felül lehet vizsgáltatni a szervezet EIR nyilvántartás szerinti alkalmazásgazdájával. Az alkalmazásgazda láthatja majd az inaktivált felhasználók melletti licenszinformációt is, és el tudja távolítani az inaktív felhasználókhoz tartozó licenszt, amely az EIR üzemeltetésében költség megtakarítást okozhat.

6.6. Felhasználók, a felhasználó státusza (aktív/inaktív) és a hozzájuk tartozó jogosultsági szintek, több EIR összefüggésében

Amennyiben több EIR esetén is beérkezik forrás oldalról az adatszolgáltatás, úgy elkészíthető egy olyan riport, ami egy adott felhasználó összes, forrás oldalról beállított EIR-hez történő hozzáférését adja meg, jogosultságokkal és aktív/inaktív státuszokkal együtt. A riport amiatt is fontos lehet, mert egy esetleges felhasználó hozzáférésének kompromittálódása esetén információt kaphatunk, hogy a forrásrendszeri exportok alapján mely más rendszereinkhez fér még hozzá az adott felhasználó. Természetesen ez az információ lekérhető a jogosultság nyilvántartásból vagy a

jogosultságkezelő rendszerből, azonban nem biztos, hogy egy jogosultságkezelő rendszer minden felhasználó típust menedzsel.

7. Folyamatba építés, PreDeCo és PDCA

A jogosultsági pillanatkép elemzésből készült riportok tovább alakíthatóak. Az táblázatkezelő által értelmezhető formátumra hozott riportok oszlopai és fejlécei úgy alakíthatóak feldolgozás során, hogy azok értelmezhetőek legyenek úgy az adatgazdának, mint az alkalmazásgazdának, az elektronikus információs rendszerek biztonságáért felelős személynek (IBF-nek) vagy a szervezeti egység vezetőjének.

Az adott riportok a PreDeCo elv (megelőző – preventív kontroll, felismerő – detektív kontroll, és elhárító – korrektív kontroll) szerint mindhárom részhez hozzájárulhatnak, hiszen értelmezhető megelőzőként (preventív), mellyel egy esemény bekövetkeztét akadályozzuk meg, például egy vissza nem vont, vagy rosszul visszavont, esetlegesen tévesen beállított jogosultság által bizalmas adatokhoz való hozzáférés. Értelmezhetjük felismerő, észlelőként (detektív), hogy a korai felismeréssel és meghozott intézkedéssel csökkentsük a kompromittálódás bekövetkezésének esélyét. Természetesen értelmezhetjük elhárítóként (korrektív) is, ahol a károk mérséklése a cél, hiszen több forrásrendszer adatszolgáltatása esetén megvalósulhat vele egy korreláló adathalmaz előállta, amely azonnal megmutatja, hogy az adott felhasználónak milyen rendszerekhez van vagy volt még hozzáférése.

Érdemes a folyamatos fejlesztés, PDCA alapmodell (plan – tervezés, do – cselekvés, check – ellenőrzés, act – beavatkozás) szerint is beépíteni a jogosultság felülvizsgálat folyamatába, ahol az ellenőrzés (check) folyamat szegmensben jól használható.

8. Konklúzió

Az EIR jogosultsági pillanatképeket automatikusan elemző megoldás megvalósítható, azonban természetesen informatikai szaktudás szükséges a kialakításához és fenntartásához. A riportok automatizálhatóak, és ha az adott EIR jogosultságkezelésének megvalósításában nincs változás, úgy a megoldás a változtatásig biztosan működhet.

Míg a jogosultság nyilvántartás - legyen az offline, manuális vagy egy erre bevezetett nyilvántartó vagy esetlegesen interfészelt vagy vezérlő rendszer – a nyilvántartási oldalról közelíti meg a jogosultság felülvizsgálati folyamatot, addig a jogosultsági pillanatkép elemzés megoldása gyakorlati oldalról, azaz az EIR-ben valósan megtalálható és nyilvántartott felhasználók és azok jogosultságainak oldaláról közelíti azt meg. Jól látható, hogy bármelyik jogosultság-nyilvántartási megoldást használja egy szervezet, a vonatkozó jogszabályok, az MNB ajánlás, valamint az MSZ ISO/IEC 27001:2023 szabvány is elvárja a periodikus jogosultság felülvizsgálatot, ami a legprecízebb eredményt adó módon az EIR jogosultság pillanatképének elemzésével és az elemzés jogosultság-nyilvántartással való összevetésével valósítható meg. Ez elvárható akkor is, ha a szervezeten belüli központi jogosultság- és felhasználó kezelő (IDM) rendszer zárt, és interfészen keresztül vezérel, hiszen a vonatkozó jogszabály és ajánlás értelmezés szerint jogosultság felülvizsgálat tekintetében nem tesz különbséget a „táblázatban vezetett” nyilvántartás és az IDM rendszerrel történő nyilvántartás között, valamint azért is, mert az IDM rendszer nem minden esetben akadályozza meg, hogy a rendszergazdák az integrált rendszerekben esetlegesen szabadon módosíthassák a jogosultságokat.

A riportokból adódó lehetőségek folyamatba építése esetén az IBF, az IBIR vezető vagy a jogosultság felülvizsgálatáért felelős személy utasítást adhat a jogosultságok felülvizsgálatára, melyeket a jogosultság-pillanatképekből kinyerhető riportok teljes mértékben támogathatnak. Amennyiben a szervezet nem használ IDM rendszert, a forrás oldali jogosultság felülvizsgálat a megfelelő jogosultsági koncepció kialakítása mellett az egyik alapfeladata lehet a felmérési vagy tervezési szakaszban egy IDM rendszer bevezetésének, mely rendszer támogathatja a hiteles, hibamentes felhasználói jogosultságok kezelését.

Irodalomjegyzék

[1] 2013. Évi L. törvény az állami és önkormányzati szervek elektronikus információbiztonságáról — Hatályos Jogszabályok Gyűjteménye. Forrás: https://net.jogtar.hu/jogszabaly?docid=a1300050.tv
[2] 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 — Hatályos Jogszabályok Gyűjteménye. Forrás: https://net.jogtar.hu/jogszabaly?docid=a1500041.bm
[3] A Magyar Nemzeti Bank 8/2020. (VI.22.) számú ajánlása az informatikai rendszer védelméről https://www.mnb.hu/letoltes/8-2020-informatikai-rendsz-vedelmerol.pdf
[4] Az Európai Parlament és a Tanács (EU) 2022/2481 határozata (2022. december 14.) a Digitális évtized 2030 szakpolitikai program létrehozásáról https://eur-lex.europa.eu/legal-content/HU/TXT/HTML/?uri=CELEX:32022D2481
[5] Baars, T., & Spruit, M. (2013). The SeCA Model. In Security Engineering for Cloud Computing: Approaches and Tools (o. 19–35). IGI Global. https://doi.org/10.4018/978-1-4666-2125-1.ch002
[6] Bhaskar, R., & Kapoor, B. (2014). Chapter 3—Information Technology Security Management. In J. R. Vacca (Szerk.), Managing Information Security (Second Edition) (o. 57–74). Syngress. https://doi.org/10.1016/B978-0-12-416688-2.00003-9
[7] Cherdantseva, Y., Hilton, J., Cherdantseva, Y., & Hilton, J. (2014). Information Security and Information Assurance: Discussion about the Meaning, Scope, and Goals In: In: Organizational, Legal, and Technological Dimensions of Information System Administrator. Almeida F., Portela, I. (eds.). IGI Global Publishing. Ch010; IGI Global. https://doi.org/10.4018/978-1-4666-4526-4.ch010
[8] Godishala, R. B., Gugulothu Narsimha, Aruna Kranthi. (2022). A Comprehensive Guide to Information Security Management and Audit. CRC Press. https://doi.org/10.1201/9781003322191
[9] ISO. (2023, február 2). ISO/IEC 27001:2022. ISO. https://www.iso.org/standard/27001
[10] Möller, D.P.F. (2023). Cybersecurity in Digital Transformation. In: Guide to Cybersecurity in Digital Transformation. Advances in Information Security, vol 103 . Springer, Cham. https://doi.org/10.1007/978-3-031-26845-8_1
[11] Thales, 2023 Data Threat Report: Global Edition
[12] Wheeler, E. (2011). Security Risk Management: Building an Information Security Risk Management Program from the Ground Up, Elsevier