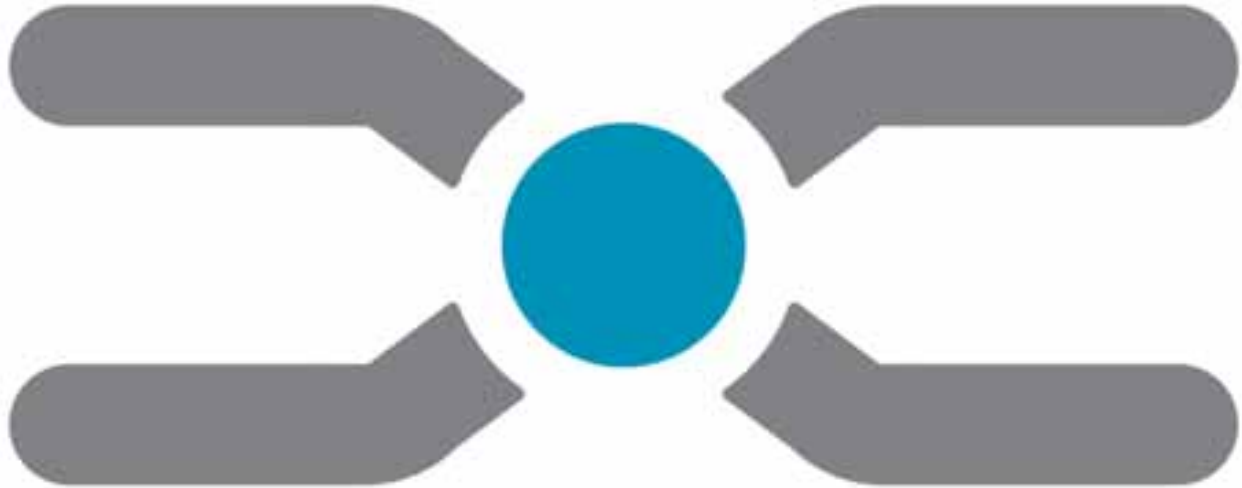

XS MATRIX

A legkisebb jogosultság („need-to-know” / „least privilege”) elv betartásának támogatása, elsősorban üzleti alkalmazásoknál

Mihály Tamás CISA, CISM

mtamas@xsmatrix.com,
www.xsmatrix.com

Agenda

1. Az előadóról
2. Mit jelent a need-to-know elv, és hol kell, hogy megjelenjen az informatikai környezetben?
3. Ki(k)nek kell betartatnia? Milyen területeket érint?
4. Milyen kockázatok jelennek meg a fel nem ismert többletjogosultságok miatt?
5. Hogyan történt eddig ezek kezelése az üzleti alkalmazások szintjén? Milyen problémákkal lehetett szembesülni?
6. Milyen eszközzel tehetjük a kockázatokat mérhetővé és könnyebben kezelhetővé?
7. Hogyan lehet automatizált folyamatot kialakítani a jogosultságok rendszeres felülvizsgálatára?

Az előadóról

- 20 éve az IT biztonsági szakmában
- IT security tanácsadó, IT belső ellenőr, IT biztonsági felelős, IT biztonsági vezető
- 10+ év CISO-ként jelentős hazai kereskedelmi bankokban

- Főbb tapasztalatok:
- Törvényi megfelelőség, nemzetközi szabványok
- Biztonság szervezés, kontroll folyamatok
- Kockázatfelmérés
- Csalásfelderítés / csalásmegelőzés
- Adatszivárgás gátlás
- Jogosultság felülvizsgálat

Mit jelent a need-to-know elv, és hol kell, hogy megjelenjen az informatikai környezetben? – Alapelvek, fogalmak

„Need-to-know”, vagy „Least privilege” elve:

Csak annyi adatot érhessen el és olyan funkciókat végezhessen a munkavállaló, ami a munkavégzéshez, a kijelölt belső folyamatok és tevékenységek ellátásához feltétlenül szükséges.

Nem a számítástechnika térnyerése hozta létre ezt az elvet – már a tisztán papíralapú világban is létezett (ki hová léphet be, mivel mit csinálhat, mihez kap kulcsot, stb.)!

Mit jelent a need-to-know elv, és hol kell, hogy megjelenjen az informatikai környezetben? – Szabályozási háttér

Lényegében az összes ismert, IT biztonsággal foglalkozó, új, vagy hosszú múltra visszatekintő nemzetközi szabvány, vagy törvény tartalmazza.

Például:

ISO 27002 (9.2), COBIT (DS 5.3, 5.4), PCI DSS (7.1, 7.2), NIST 800-53 (AC6), GDPR, SOX, HIPAA

Emiatt a megfelelésben a gazdálkodó szervezetek nagy része érintett!

Mit jelent a need-to-know elv, és hol kell, hogy megjelenjen az informatikai környezetben? – Gyakorlati megjelenése

Az informatikai rendszerekben a felhasználók számára engedélyezett rendszerfunkciók, adatelérések **jellemzően többszintűen: szerepkörökként, azon belül különböző (elemi) jogosultságokként** (többféle paraméterrel meghatározható jogosultsági objektumokként) jelennek meg.

Ettől eltérő, jóval komplexebb jogosultsági struktúrák is létezhetnek, de előfordul egyszintű, csak elemi jogosultsági objektumok kiosztási modellje is!

Ki(k)nek kell betartatnia? Milyen területeket érint?

Elsődlegesen érintett területek:

- **Adatgazdák** (Üzleti vagy szakmai területek vezetői, mint jóváhagyók)
- Jogosultságkezelési folyamat végrehajtói (pl. **IT adminisztrátorok**, **IT biztonsági adminisztrátorok**)
- Jogosultságkezelési folyamatot rendszeresen, operatívan ellenőrző területek (pl. **IT biztonsági csoport**)

További érintett területek:

- Rendszer- és **folyamatszervezők** (a belső folyamatok módosulásának mindig lehet jogosultsági vonatkozása)
- **Belső ellenőrzés** (az éves tervezett üzleti/szakterületi vizsgálatai során, vagy IT biztonság vizsgálatakor)
- Egyéb **biztonsági területek** (pl. fizikai biztonság vagy bankbiztonság)
- Esetlegesen **jogi vagy compliance** területek (összeférhetetlenségek meghatározása, változó törvényi követelmények feltárása, stb.)

Milyen kockázatok jelennek meg a fel nem ismert többletjogosultságok miatt?

Az alábbi típusú **belső incidensek** esélye növekszik jelentősen:

- Egy felhasználó általi **illetéktelen adathozzáférése** – munkacélhoz nem kapcsolható lekérdezések, legyűjtések, rátekintések (majd ebből adatszivárgás…)
- Egy felhasználó általi **jogosulatlan funkcióhasználata**
  - Szándékos – kontrollok kijátszása, **belső visszaélések**
  - Véletlen – hibás, nem szándékolt, ismeretlen funkciók használata
- Rendszerműködést befolyásoló események – főleg kiemelt, **adminisztratív jogokhoz köthető funkciók illetéktelen használata**, pl. konfigurációs változtatások, üzleti paraméteradatok változtatása, feladatütemezések módosítása, stb.
- **Több felhasználó belső összejátszása** – összeférhetetlen funkciók halmozódása esetén, többlépcsős folyamatok lerövidítése, ebből visszaélések

Milyen kockázatok jelennek meg a fel nem ismert többletjogosultságok miatt?

Azonosságlopáson alapuló külső támadások esetén:

- **Nem kell jól védett privilegizált usereket támadni,** az átlagos felhasználók körében könnyebb azonosítókat, jelszavak szerezni, szélesebb kör támadható pl. spear phishinggel.
- A széles jogkörök miatt
  - nagyobb lehet az **illetéktelenül elérhető adatok köre** és/vagy
  - Értékesebb, **magasabb szintű** jogosultságok szerezhetők meg.
- Az összeférhetetlen jogok miatt **kevesebb belső felhasználói hitelesítő adat**ot is elég megszerezni.

Külsős-belsős összejátszások (önmagában is nehezen felderíthető és bizonyítható) esetén:

- Összeférhetetlen funkciók halmozódása esetén **kevesebb belső felhasználó bevonására van szükség**
- Kiemelt jogokkal több a lehetőség a **belső nyomok eltüntetésé**re, véletlenként vagy hibajelenségnek feltüntethető tevékenység, amit a beavatott külsős kihasznál

Hogyan történt eddig ezek kezelése az üzleti alkalmazások szintjén? Milyen problémákkal lehetett szembesülni?

Tipikus megoldások a **jogosultság kezelési folyamatra:**

1. IDM (Identity Management) rendszer
   - Kifejezetten a jogosultsági workflow-t és dokumentálást támogatja
   - Akár automatizáltan be is állít jogokat
2. Helpdesk ticketing rendszer
   - Nem céleszköz, de az igénylések, jóváhagyások dokumentálását akár workflow-szerűen meg tudja oldani, visszakereshetőség is megoldott
   - A jogok beállítására, illetve lekérdezésére biztosan nem képes
3. Excel tábla, Word űrlap + levelező rendszer
   - Nem workflow jellegű működés, csak igénylések, jóváhagyások dokumentálására jó, visszakereshetőség nehéz
   - A jogok beállítására, illetve lekérdezésére ez se képes
4. Papír alapon
   - Kérelmezés, jóváhagyás, dokumentálás megoldott, visszakereshetőség nehéz
   - Mára már talán teljesen kikopott ez a megoldás

Hogyan történt eddig ezek kezelése az üzleti alkalmazások szintjén? Milyen problémákkal lehetett szembesülni?

Tipikus problémák a jogosultság kezelési folyamatban (ezek mind a többlet jogok bővüléséhez vezetnek):

- Meglévő felhasználót (munkakört) tipizálnak (legyen olyan joga, mint XY-é!)
- Nem megfelelő szerepeket (jogosultságot) igényelnek
- Nem teljes körű az igényelhető szerepek köre
- Nem ismert a szerepek tartalma
- A szerepkörök elnevezésből nem látszik különbség
- Többszintű szerepkörök esetén nem a megfelelő szintet igénylik meg (hanem sokkal többet)
- A szerepkör tartalom már elavult
- A szerepkör tartalom már a kialakítása során sem volt megfelelő
- Az igényelt szerepkörök nem fedik le az adott munkakörben szükségeseket
- Munkakörre csoportosított (többszintű) szerepkörök is felesleges jogokat tartalmaztak
- Az új szerepkör nem is volt jóváhagyva
- A szerepkör jóváhagyás nélkül módosult (pl. a szerepkör módosítás nem is eleme a workflow-nak)

Hogyan történt eddig ezek kezelése az üzleti alkalmazások szintjén? Milyen problémákkal lehetett szembesülni?

Tipikus problémák a jogosultság kezelési folyamatban (ezek mind a többlet jogok bővüléséhez vezetnek):

- A módosuló folyamatok miatt nem dolgozzák át a szerepkör tartalmat, csak bővítik azokat (régi tartalmat nem veszik ki), esetleg más meglévővel összevonják
- A szerepkörök struktúráját nem akarják változtatni, hogy átlátható és könnyen kezelhető maradjon
- Az új szerepkörök nem lettek letesztelve, határidők szorításában gyorsan és jelentősen bővítik azokat („ … majd a projekt után kitisztítjuk… ”)
- A jóváhagyások hanyag/tudatlan módon zajlanak (időhiány, nem megfelelő ismeret a rendszerről, folyamatokról) – lényegében minden igény elfogadásra kerül
- A jóváhagyónak nem jelzi senki és semmi, ha érzékeny jogok vannak az igénylésben
- A jóváhagyók változása nincs időben lekezelve
- Nem a jóváhagyott jogokat állítják be (pl. emberi tévedés miatt)

Hogyan történt eddig ezek kezelése az üzleti alkalmazások szintjén? Milyen problémákkal lehetett szembesülni?

Tipikus problémák a jogosultság kezelési folyamatban (ezek mind a többlet jogok bővüléséhez vezetnek):

- A belső áthelyezéskor nem kerülnek visszavonásra a régi jogok, csak újakat kap a dolgozó
- A távozó dolgozónak nem vonják vissza a jogait, nem törlik a rendszerből
- Nincs rendszeres felülvizsgálat a jogosultság kezelési folyamaton
- Nincs rendszeres felülvizsgálat a szerepkör tartalmakon (egészen a legalacsonyabb jogosultsági objektumok mélységéig), azok változását nem figyelik
- Ha van IDM rendszer, és van felülvizsgálat, akkor csak az általa gyűjtött adatokon alapszik a felülvizsgálat (holott a vizsgált rendszerben még lehet, hogy sokkal több felhasználó és jogosultság is van!)
- Ha van az IDM-ben összeférhetetlenségi / kiemelt jogi vizsgálat, akkor az csak munkakör, esetleg szerep mélységig vizsgál, esetleg a beírt szabályok is elavultak már
- Stb.

Hogyan történt eddig ezek kezelése az üzleti alkalmazások szintjén? Milyen problémákkal lehetett szembesülni?

Ha ennyi probléma van vele, akkor **miért nem ez van a fókuszban**? Miért nem kezelik ezeket jobban?

- A **felelősség megosztott**: elsődleges felelősség ugyan a szakmai jóváhagyón, de ő tovább tudja tolni az IT-ra, IT security-ra, egyéb ellenőrző funkciókra – arra hivatkozik, hogy a jogosultságok, szerepkörök túl technikaiak, nem elvárható, hogy mélységében ismerje a rendszert, nem kap támogatást a kockázatokról, stb.
- **Komplex ismeretet igényel** kell a rendszerről, üzleti/szakmai folyamatokról, kockázatokról, és a változásokat is követni kell
- A probléma magja nem is szerepkörökben, hanem mélyebben, **az elemi jogosultsági objektumokban** van, ez valóban technikai szint!
- **Nincs erőforrás** rendszeres felülvizsgálatra a szerepkör tartalmakra (egészen a legalacsonyabb jogosultsági objektumok mélységéig), azok változását nem figyelik
- **Nincs megfelelő eszköz**, amellyel natív módon kiemelhetők a rendszerekből a jogosultságok (hogy ezzel az IDM működése is kontrollálható legyen)
- Stb.

Milyen eszközzel tehetjük a kockázatokat mérhetővé és könnyebben kezelhetővé?

Gyakorlati tapasztalatom alapján az alábbi elvárások teljesítése kell ahhoz, hogy a túlzott jogokat (a vizsgálati területeken pl. IT security) a probléma gyökerénél lehessen kezelni:

- Natív, közvetlen módon ki kell tudni emelni a felhasználók jogosultsági adatait az elemi jogosultságok szintjéig a vizsgálandó rendszerekből
- Az elemi jogosultsági adatok elemzésére van szükség, amely során kiválogathatók a kiemelt, összeférhetetlen, vagy egyéb túlzott jogosultságok!
- Ezeket a jogosultságokat szabályokkal leírhatóvá kell tenni (egyedi, fejlesztett funkciókhoz tartozó jogosultságokhoz is!)
- A szabályokhoz kockázatokat kell rendelni
- A kockázatokat skálázhatóvá és felhasználókra, szerepkörökre összesíthetővé kell tenni
- Az elemzést, kockázatok kimutatása rendszeres workflow-vá alakítható legyen, hogy folyamatosan nyomon követhetőek legyenek a felesleges jogok
- IDM workflow-ba is integrálható legyen

Hogyan lehet automatizált folyamatot kialakítani a jogosultságok rendszeres felülvizsgálatára?

A megfelelő eszköz birtokában az alábbiakat kell elvégezni ehhez:

- Meg kell határozni a vizsgált rendszerek körét!
- Be kell állítani a kapcsolatot a jogosultság felülvizsgáló eszköz és a vizsgálandó rendszer között!
- Meg kell határozni, hogy milyen rendszerességgel gyűjtenénk és vizsgálnánk az egyes jogosultságokat! (pl. napi, heti, havi, negyedéves szinten?)
- Meg kell győződni arról, hogy vannak-e megfelelő szabályaink, amikkel a jogokat vizsgáljuk (egyedi rendszereknél ezt mindig egyedileg kell megtenni), és be kell állítani, hogy milyen szabályrendszer szerint vizsgálunk!
- Meg kell határozni, hogy mely területek, milyen rendszeres riportokat kapjanak a rendszertől (és ki, mit csináljon vele)!

KÉRDÉSEK?

További információért keress bátran! ☺

Mihály Tamás CISA, CISM

mtamas@xsmatrix.com,
www.xsmatrix.com