Michelberger Pál – Dombora Sándor

A FELHASZNÁLÓI PROFIL SZEREPE AZ INFORMÁCIÓBIZTONSÁGBAN

Az információbiztonság kialakítását jogszabályok írják elő az állami és önkormányzati szervezetek számára, amelyek komplex szabályozási környezet kialakítását és információvédelmi megoldások bevezetését szorgalmazzák. Az előírások nagy hangsúlyt fektetnek a feladatok elvégzéséhez szükséges és elégséges minimális jogosultság elvének megvalósítására, a felhasználókat saját feladataik elvégzésére korlátozó kontrollrendszer kialakítására. Emellett a kulcsfontosságú vagy nagy mennyiségű személyes adatot kezelő szervezetek számára kötelezővé teszi az informatikai rendszerek naplóbejegyzéseinek elemzését. Figyelembe véve, hogy a leggyengébb láncszem az ember, a naplóelemzés egyik legfontosabb eleme a felhasználói tevékenységek elemzése, felhasználói profil kialakítása, ezek alapján a szokatlan tevékenységek azonosítása és elemzése a munkatársakról rendelkezésre álló adatok alapján. A tanulmány a felhasználói profil kialakításának és elemzésének célját, lehetőségét, fontosságát, megvalósítási lehetőségeit és korlátait tárgyalja, a hatékonyság, teljeskörűség, valósidejűség, hamis riasztások és adminisztrációs feladatok minimalizálásának tükrében, a felhasználókról elektronikus formában rendelkezésre álló adatok mentén. Ezt követően egy költséghatékony elméleti modellt mutat be felhasználói tevékenységek automatizált elemzésére és annak alapján felhasználói profil kialakítására.

Kulcsszavak:
felhasználói aktivitás, jogosultság, konfigurációkezelés, SIEM rendszerek, személyazonosság, szerepkör

1. BEVEZETÉS

Számos, tanácsadó cégek által készített nemzetközi felmérés igazolja, hogy a legnagyobb információbiztonsági kockázatot az információs rendszereket alkalmazó és üzemeltető ember,

munkavállaló, ill. vezető jelenti.[1, 2, 3] A humán kockázatot – amely fokozottan jelenik meg a közigazgatásban (személyes adatok, szolgálati és államtikok védelme) – az információtechnológia fejlődése is fokozza. Gondoljunk csak a közösségi oldalakra, a saját mobileszközök munkahelyi alkalmazására.

Fontos kérdésként jelenik meg az állami és önkormányzati intézmények esetében a humán kockázatok csökkentése (az információbiztonság megerősítésének érdekében), az alkalmazható eszközök azonosítása és hatékonyságának vizsgálata. Jelen tanulmány arra keresi a választ, hogy a felhasználóiprofil-elemzés milyen módon és feltételek mellett, milyen hatékonysággal járulhat hozzá az intézmények információbiztonságához.

Az emberi tényező kockázatkezelésének egyik módja lehet a hagyományos személyazonosság-, jogosultság- és szerepkörkezelés szabályozása, valamint új eszközökkel történő kiegészítése. A fájlszervereken rendszeresen lekérdezhetők a bizalmas állami, ill. intézményi dokumentumokhoz és adatokhoz történő hozzáférések (File Audit). Természetesen ennek feltétele az adatok, adatfájlok bizalmasság szerinti osztályozása is.

Felhasználói profil készítésével az információs rendszerek működése, üzemeltetése során folyamatos „megfigyelést" végezhetünk. A megszokottól eltérő viselkedés esetén megvizsgálható a felhasználó motivációja, információbiztonsággal kapcsolatos ismeretei, hozzáállása és tudatossága. Ez egy preventív információvédelmi tevékenységet jelent, ami nem tekinthető az információvédelmi vezető paranoiájának. A rutinszerű és szabályos működést rögzítő adatbázisokból kiszűrhetők azok a naplózási adatok, amelyek a felhasználói viselkedés szokatlanságát mutatják.

A korszerű SIEM (Security Information and Event Management) rendszerek segítségével átfogó képet kaphatunk a szervezet információbiztonsági tevékenységéről.[4] Az ilyen speciális informatikai alkalmazás rögzíti és gyűjti a biztonsággal kapcsolatos eseményeket a végfelhasználó, az adatforgalom, a hálózat és a biztonsági eszközök (pl. tűzfalak, vírusirtók, behatolásjelzők) vonatkozásában. Az események biztonsági vizsgálata a „szokásos" működéshez történő viszonyítást jelenti. A különböző forrásokból származó naplóadatok összefuttatása és elemzése révén könnyen behatárolhatjuk a szándékos vagy a vétlen károkozást.

1 Ernst & Young: *Get ahead of cybercrime EY' Global Information Security Survey,* 2014, 40. Forrás: www.ey.com/Publication/vwLUAssets/EY-global-information-security-survey-2014/$FILE/EY-global-information-security-survey-2014.pdf (2015. 02. 27.)

2 PwC: *Managing cyber risks in an interconnected world. Key findings from The Global State of Information Security®*, 2015, 40. Forrás: www.pwc.com/gx/en/consulting-services/information-security-survey/index.jhtml# (2015. 02. 27.)

3 A Frost & Sullivan Market Study in Partnership with ISC2: *The 2013 (ISC)² Global Information Security Workforce Study,* 2013, 28. Forrás: www.isc2cares.org/uploadedFiles/wwwisc2caresorg/Content/2013-ISC2-Global-Information-Security-Workforce-Study.pdf (2015. 02. 27.)

4 David R. Miller, Shon Harris, Allen Harper, Stephen Vandyke, Chris Blask: *Security Information and Even Management (SIEM) Implementation*, McGraw–Hill, 2014, 464.

2. PARADIGMAVÁLTÁS AZ INFORMÁCIÓ- ÉS IT-BIZTONSÁGI KOCKÁZATOK ELEMZÉSÉBEN

A szervezetek ez idáig a felhasználókat korlátozó, az üzleti folyamatokat kiszolgáló információs rendszereket pedig szigorúan szabályozó, kontroll alapú biztonsági megközelítést alkalmazták. Ez a teljes körű „védekezés" (esemény-ellenőrzés a nap 24 órájában, különböző egymást átfedő biztonsági technológiák kezelése, naplóelemzés, üzemeltetés) amellett, hogy megterheli az informatikai személyzetet, a változó fenyegetések miatt egyre kevésbé tekinthető hatékonynak.

Az informatikai biztonsági szolgáltatások mára már sok tehermentesítő lehetőséget biztosítanak:[5]

- tűzfalmenedzselés,
- automatikus napló- és logelemzés (adathozzáférések monitorozása),
- belső sérülékenység vizsgálata (hálózaton belüli eszközök felderítése, osztályozása, elemzése, kockázatértékelés, sérülékenységek javítása és azok ellenőrzése),
- internetes alkalmazások automatikus biztonsági ellenőrzése,
- wifibiztonság ellenőrzése,
- hálózati hozzáférés ellenőrzése (felhasználói hitelesítés, nem megfelelő felhasználók kezelése, illetéktelen hozzáférési végpontok kizárása),
- behatolásjelzés,
- érzékeny adatok adatosztályozás utáni kiemelt kezelése,
- és végül, de nem utolsósorban az eseménymenedzselés (infrastruktúra, az eszközök és alkalmazások naplóelemzése).

A SIEM rendszerek alkalmazása a felhasználók viselkedésének folyamatos megfigyelését és a szokatlan tevékenységek matematikai módszerekkel (eloszlásvizsgálat, minták keresése, szöveganalízis) történő kiszűrését, valamint célorientált kivizsgálását jelenti. A naplóüzenetek kockázatok szerinti rangsorolása után történik a személyzet riasztása, akik így csak az igazán fontos és kockázatos eseményekre koncentrálhatnak. A biztonsági intézkedések eredményességét növelheti a kockázatelemzés területének észszerű szűkítése.

A naplózás során rögzítésre kerül, hogy mi és mikor változott, ki volt a végrehajtó és milyen hozzáférési pontról indították az aktuális tranzakciót, valamint az is, hogy a változtatás engedélyezett/jóváhagyott volt-e.

Az információs rendszerek biztonságát és ehhez kapcsolódóan a szervezet információbiztonságát több oldalról is vizsgálni szükséges. A SIEM rendszerek hatékonysága megkívánja az illesztést a szervezeti információbiztonsági intézkedésekhez (politikához), IT-eszközökhöz és a szervezeti folyamatokhoz.

5 Póser Valéria, Schubert Tamás, Kozlovszky Miklós, Prém Dániel: *Security on-demand megoldások az informatikai infrastruktúrákban*, Hadmérnök, 8(2013)/3, 211–222.

Az információvédelemben több biztonsági szintet is megkülönböztetünk:[6]
– információtechnológiai infrastruktúra (konfigurációkezelés, hardver-, szoftver- és hálózatvédelem);
– információkezelés (adatfelvétel, -módosítás, -törlés, informálódás, ill. lekérdezés);
– ügyviteli folyamatok (folyamatszabályozás, workflow, termékek és szolgáltatások informatikai támogatása, vevőszolgálati tevékenység);
– szervezet (információbiztonsági stratégia, kockázatkezelés, szervezeti struktúra, vezetési stílus, szervezeti kultúra, vezetői feladatok támogatása).

Erre jó példa a jogosultsági rendszer „holisztikus" kialakítása. Mind a négy szinten vannak ezzel kapcsolatos feladatok:
– IT-szint – felhasználóazonosítás,
– információkezelési szint – csak a munka elvégzéséhez minimálisan szükséges adathozzáférések biztosítása,
– folyamatszint – kritikus folyamatok megosztása, helyhez és személyhez kötött jogosultság,
– szervezeti szint – kockázatkerülés, jogosultsági csoportok kialakítása és a jogosultsági rendszer állandó felügyeletének szabályozása.

Maria Karyda és szerzőtársai[7] olyan általános információs rendszerekre alkalmazható biztonsági működési modellt dolgoztak ki, amelyben a biztonsági szintek mellett szerepet kap:
– a változáskezelés (szervezeti felépítésben, szervezeti magatartásban, folyamatokban és az információtechnológiában) – mint *információtartalom*,
– a külső és belső kapcsolatok, *összefüggések* (gazdasági, jogi, politikai és szociális tényezők, iparági verseny, beszállítói viszonyok, szervezeti kultúra belső elemei),
– valamint az üzleti folyamatok kulturális és hatalmi szempontból történő megközelítése (biztonsági igények megjelenése a szervezeti kultúrában és a hatalmi viszonyok érvényesítése az információbiztonsági politikában).

3. JOGOSULTSÁG-, SZEREPKÖR- ÉS SZEMÉLYAZONOSSÁG-KEZELÉS

A tranzakciófeldolgozó és vezetői információs rendszerek támogatják, modellezik és sok esetben optimalizálják a szervezet értékteremtő és kiszolgáló folyamatainak végrehajtását. A munkatársak (a felhasználók) az információtechnológiai erőforrásokhoz hozzáférve munkakörükből adódó „elemi" feladatokat látnak el. Adatokat rögzítenek, módosítanak, lekérdeznek, esetleg törölnek azért, hogy az információ – mint erőforrás – biztosítva legyen a különböző szintű döntéshozóknak.

Sok felhasználó és több, inhomogén információtechnológiai alapokon nyugvó információs rendszer esetén a felhasználók azonosítása és rendszereléréseik nyomon követése teljesen kaotikussá válhat. Rések és/vagy átfedések keletkezhetnek a hozzáféréseknél. A jogosultsá-

6 Ji-Yeu Park, Rosslin John Robles, Chang-Hwa Hong, Sang-Soo Yeo, Tai-Hoon Kim: *IT Security Strategies for SME's*, International Journal of Software Engineering and its Applications, Vol. 2. No. 3., July 2008, 91–98.

7 Maria Karyda, Evangelos Kiountouzis, Spyros Kokalakis: *Information systems security policies: a contextual perspective,* Computers & Security 25., 2005, 246–260.

got nem mindig a tényleges feladat- vagy munkakör alapján határozzák meg. Inkább informális szokásokat és hagyományokat vesznek figyelembe. Többszörös felhasználókezelés alakulhat ki az egymástól független információs rendszerekben. Változások alkalmával (áthelyezés, kilépés, új folyamatok, kiszervezés stb.) ad hoc módon végzik a jogosultsági kérdések – sok esetben utólagos – adminisztrációját.

A megoldás a folyamatok és szervezet elemzésén alapuló szerepkörök kialakítása lehet, ami azután összekapcsolódhat a szerepekbe bekerülő felhasználók személyazonosságának kezelésével.

A felhasználó a folyamatok végrehajtásából adódó feladatainak elvégzéséhez információtechnológiai eszközöket is alkalmaz. Természetesen nincs szüksége minden IT-erőforrásra és minden tárolt adatra. A *jogosultság* korlátozza a felhasználó közreműködését, optimális esetben csak a munkaköréből adódó tényleges információkezelési feladatok elvégzését teszi lehetővé, de azt viszont teljeskörűen. Meghatározásának alapja a folyamat(ok), azok céljai, a szervezeti felépítés és az informatikai infrastruktúra. Szerepet játszanak benne az információbiztonsági kockázatok is (értékes állami, ill. intézményi információk elvesztése v. illetéktelen kezekbe kerülése). A tényleges jogosultsági rendszer kialakítására hatással van a szervezeti és egyéni tudás, a szervezeti kultúra, valamint a munkakörhöz rendelt felelősség.

A jogosultság formálisan is nyilvántartható és nyilvántartandó (kiadható, beállítható, ellenőrizhető, jóváhagyható, elutasítható, szüneteltethető, elvehető). Fontos a munkahelyi vezető és az adott terület adatbiztonságáért felelős hozzájárulása. A felhasználó egyszerűbb esetben felhasználói nevet (login) és jelszót (password) kap. Ez magasabb biztonsági igények esetén kiegészíthető vagy helyettesíthető biometrikus „azonosítókkal" vagy kiegészítő hardvereszközökkel. Ezeket rendeljük a folyamatoknak és a szervezeti céloknak megfelelően az információs rendszerek, alkalmazások moduljaihoz, menüihez, menüpontjaihoz, képernyőihez és adatmezőihez, valamint adatbázis-lekérdezési lehetőségeihez. A jogosultság a felhasználókon túl köthető alkalmazási helyhez és időszakhoz is.

A felhasználónak munkafeladataiból adódóan esetenként akár több szervezetnél működő információs rendszerhez is hozzá kell férnie. Ez azt jelenti, hogy akár többszörösen is „bizonyítani" kell jogosultságát. Ez történhet a felhasználó birtokában lévő (You have…) azonosításra alkalmas eszközökkel (chip- és mágneskártyák, hardverkulcsok).

A tudásalapú (You know…) azonosítás sok rendszer esetén már nehezen megvalósítható. Hiszen egy magánembernek is mennyi jelszót és/vagy PIN kódot kell fejben tartania. Ráadásul ezeket biztonsági okokból időközönként illik megváltoztatni. Segítséget és egyszerűsítést jelenthet, ha biometrikus elemeket (ujj- és tenyérlenyomat, írisz, véna, DNS) is használunk azonosításra (You are…), de ezek használata személyiségi jogi kérdéseket is felvet. A munkáltató (intézmény, államigazgatási szerv) nem kérheti minden esetben ezek alkalmazását a munkavállalójától. Az azonosítás egyébként is a védelmi tevékenység felhasználót érintő része.

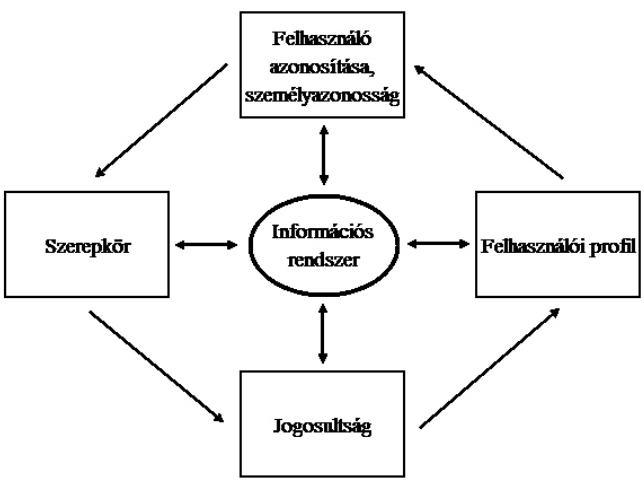
A biztonság a megfelelő *szerepkör* és a hozzá kapcsolódó jogosultsági rendszerek révén válna teljessé. Nagyobb létszámú, több telephelyes „szabványosított" folyamatokat végrehajtó szervezetek esetén megfontolandó szerepkörök kialakítása. Ugyanabban a szerepkörben dolgozó felhasználók azonos jogosultságot kapnak. A szerepkör nem csak egy informatikai alkalmazáshoz kötődhet. Így a jogosultságok beállítása automatizálható és nagy számban

egyszerre változtatható. A felesleges hozzáférések kiszűrhetők, és az egyéni jogosultságok száma csökkenthető. A szerepkörök száma tehát kevesebb lesz, mint a felhasználók száma.

A szerepkörök köthetők folyamatokhoz (folyamatelemekhez) és szervezeti egységekhez. Az előbbi a szervezet tevékenységének funkcionális kiszolgálását teszi lehetővé, az utóbbi pedig a szervezeti működést és a döntéshozatalt támogatja. A szerepkörök „állandóak", az információtechnológia fejlődése vagy új folyamatok változtathatják csak meg. A felhasználói fluktuáció így kevésbé van hatással az intézményi, ill. állami információs rendszerek működésére. A legtöbb IT-kereskedelemben kapható, tranzakciókezelésen alapuló megoldás már használja az ún. szerepkör alapú hozzáférés-ellenőrzést (Role Based Acces Control). A szerepkörök kialakításának kezdetén a tényleges folyamatokon és szervezeten alapuló szerepelvárás általában nem egyezik meg az informatikai megoldások által biztosított információkezelési lehetőségekkel. A szerepkör-kialakítás egyik fontos célja tehát az információtechnológia és szervezeti működés összhangba hozása.[8]

A *személyazonosság-kezelés* révén azonosíthatjuk a munkatársakat és a külső partnereket egy vagy több szervezethez tartozó információs rendszerben. Így szabályozhatjuk hozzáférésüket a különböző információtechnológiai erőforrásokhoz. Összeköti a felhasználói jogosultságokat és tiltásokat a rendszerekben meglévő információkezelési feladatokkal. Ez akkor válik különösen fontossá, amikor a szervezetnek több, egymással kapcsolatban álló, eltérő információtechnológiai infrastruktúrán alapuló információs és kommunikációs rendszere is van. Nem feladata a felhasználói hozzáférés hitelesítése (authentication) és új jogosultság (authorisation) létrehozása. Végigköveti a felhasználói életciklust egyénenként (pl. belépést, munkakör-bővülést, átszervezésből adódó pozícióváltozást, hosszabb fizetés nélküli szabadságot vagy a kilépést) (1. ábra).

1. ábra • *A felhasználóanalízis részterületei (saját szerkesztés)*



8 Heiko Klarl, Korbinian Molitorisz, Christian Emig, Karsten Klinger, Sebastian Abeck: *Extending Role-based Access Controll for Business Usage*, SECURWARE '09, The Third International Conference on Emerging Security Information Systems and Technologies, Athens/Glyfada, Greece, June 18–23., 2009, 136–141.

Az információs rendszereket üzemeltető szervezetek a *felhasználói profil* megalkotásával, folyamatos karbantartásával és a szokatlan viselkedés kiszűrésével a vétlen károkozás lehetőségeire is felhívhatják a munkavállaló figyelmét.

A felhasználói profil kialakítása során felhasználjuk a naplókat, amelyekben rögzítésre kerülnek a felhasználó által kezdeményezett adatmozgások (információkérés, új adat rögzítése, adat módosítása vagy törlése) és tranzakciók.

A felhasználói viselkedés alapján kapott adatok gyors elemzésével és a szokatlan viselkedési formák kiszűrésével kezelhetők a felhasználók információbiztonsági kockázatai. A szokatlanság (unusuality) mindenképpen kockázati tényező.

4. A FELHASZNÁLÓK CSOPORTOSÍTÁSA

A felhasználói viselkedés vizsgálatát érdemes felhasználói csoportok kialakítása után elvégezni. J. M. Stanton és szerzőtársai (2005) a felhasználókat két tényező alapján sorolták be:[9]

– IT és IT-biztonsági szakértelem (expertise) – alacsony vagy magas,
– felhasználói szándék vagy hozzáállás (intentions) – rosszindulatú (malicious), semleges (neutral) vagy támogató (beneficial).

Az alkalmazott lehet elégedetlen (akár tudatos szabotőr is), naiv, vagy külső szervezet által felbérelt is. A vizsgálat szempontjából az indíték meghatározása is fontos lehet.

Ez kiegészíthető generációs különbségekből származó, információbiztonságot is érintő szokásokkal is. A szociológusok szerint a mai munkavállalók születési adataik alapján öt csoportba sorolhatók:[10]

– veteránok (1946 előtt születtek; munkavállalói szempontból már nem érdekesek),
– „baby boom" generáció (születési idő: 1946–1965),
– X generáció (születési idő: 1965–1980),
– Y generáció (1980 és 1995 között születtek),
– Z generáció (1995 után jöttek a világra).

Az öt generáció eltérő biztonságtudatosságot képvisel, mindegyikre más-más információbiztonsági kockázat jellemző.[11]

Csoportosítási szempont lehet a szervezeti hierarchiában betöltött szerep is. Érdemes megkülönböztetni a felhasználókat a közép- és felsővezetőktől, valamint az információs rendszerek üzemeltetéséért felelős szakembereket is.

9 Jeffrey M. Stanton, Kathryn R. Stam, Paul Mastrangelo: *Analysis of end user security behaviors,* Computers & Security, 2005/24, 124–133.

10 Lynne C. Lancaster, David Stilmann, Harvey Mackay: *When generations collide,* New York, First Collins Business Edition, 2005, 355.

11 Michelberger Pál, Beinschróth József, Horváth Gergely Krisztián: *The Employe, An Information Security Risk = Acta Oeconomica Universitatis Selye,* 2(2013)/1, 187–200.

5. BIZTONSÁGTUDATOSSÁG

A felhasználók a védendő információkhoz munkájukból (és jogosultságukból) adódóan hozzáférnek. Rosszindulatú támadás esetén kézenfekvő, hogy a támadó a felhasználó biztonságtudatossági hiányosságait próbálja kihasználni.

A profil elemzése során fény derülhet a szokatlan felhasználói viselkedésre, és meghatározható a gondatlanság, esetleg a szándékos károkozás is. Ez alapján a felhasználót tájékoztathatjuk a tevékenységéből adódó kockázatokról, kérhetjük a biztonsági szabályozás betartását, valamint javíthatunk a nem megfelelő munkakörnyezeten is.

A tudatosságot, ill. az információbiztonságot gyengítheti az új eszközök, szoftverek kellő biztonsági ismeret nélküli szervezeti alkalmazása (pl. fájlmegosztók, hordozható eszközök, közösségi oldalak).

A felhasználók gyakran érzik azt, hogy az információbiztonsági szabályozás nem egyértelmű, nehezen betartható, és nem illeszkedik a szervezeti folyamatokhoz.[12] Nincs összehangolva a szerepkör és a felelősség. Ilyenkor „találják ki", hogy hogyan használják az információs rendszereket. Tudatos felhasználóként nyilatkoznak felméréseken és vizsgákon, de egy-egy egyedi esemény kezelésekor a praktikus és gyors üzleti eredményt tartják fontosabbnak. A helyzettudatosság (situation awareness),[13] ill. annak hiánya nagyban befolyásolja az információbiztonságot. A felhasználóknak fontos lenne megérteni, hogy a kezelt információ mit jelent számukra most, és mit jelenthet majd a jövőben, milyen célok megvalósításához (lesz) szükséges.

Az eseménymenedzsment révén kontrollálható egy ún. „social engineering" audit is. Ennek során egy független külső szakértői csoport megpróbálja feltérképezni a szervezet információbiztonsági szempontból gyenge pontjait (biztonsági réseket) és tesztelni a kialakított védelmi intézkedéseket. Ez behatolást (fizikai is), információ-hozzáférést, eszközeltulajdonítást, kémprogram-telepítést, adathalászatot, fertőzött program/fájl beküldését, ill. ezekre tett kísérletet jelent.

6. A FELHASZNÁLÓ ANALÍZISE

A felhasználó tulajdonságainak, szokásainak és viselkedésmódjának elemzése annak munkavégzése során, ami a felhasználói profiljával elvégzett feladatok végrehajtásának és végrehajtási módjának vizsgálatával történik. A vizsgálat során felhasználhatók a munkáltató felhasználóról nyilvántartott adatai, és munkavégzése során az információs rendszerekben elvégzett feladatainak naplóbejegyzései. Az így előállított adatok alapadatként használhatók fel az információbiztonsági naplóelemzés során, szokatlan események azonosításának és információbiztonsági események kiszűrésének érdekében. A naplóelemzések új információt szolgáltathatnak a felhasználói profilról, amelyek visszacsatolhatók annak pontosításához.

12 Eirik Albrechtsen: *A Qualitative study of users' view on information security*, Computers & Security, 2007/26, 276–289.

13 Jeb Webb, Atif Ahmad, Sean B. Maynard, Greme Shanks: *A situation awareness model for information security risk management,* Computers & Security, 2014/44, 1–15.

7. A FELHASZNÁLÓI AKTIVITÁS ANALÍZISE

A felhasználói aktivitás elemzése az egy felhasználóra jutó információmennyiséget, annak összegyűjtéséhez és elemzéséhez szükséges erőforrásokat figyelembe véve nagyobb szervezetek esetében jelentős feladat, de kisebb szervezetek esetében sem elhanyagolható. A feladatok manuális elvégzése kisebb szervezetek esetében ugyan lehetséges, de a felhasználó személyes és tevékenységére vonatkozó nyers, feldolgozás előtti adatainak hozzáférhetősége visszaélésekre adhat lehetőséget.

A felhasználói profil automatizált elemzéséhez szükség van a felhasználóról rendelkezésre álló adatok leképezésére az elemzést végző SIEM rendszerben. A felhasználókról elérhető információkat rendszerekben tárolható és nem tárolható csoportba sorolhatjuk. A személyes, vagy személyekhez köthető információk tárolása személyiségi jogokat sérthet, és a helyi jogszabályok figyelembevételével kell eljárni a rögzítendő adatok körének meghatározásakor, az adatok rögzítésekor és a felhasználás során is. Ugyanakkor biztosítani kell az adatok biztonságát – bizalmasságát, sértetlenségét és rendelkezésre állását, hogy csak az arra jogosultak férhessenek hozzá, és csak akkor, amikor arra szükség van.

A felhasználói profil összeállításához szükséges ritkán változó, a felhasználó személyes és tulajdonságait leíró adatait tekinthetjük alapadatoknak, amelyek rendelkezésre állnak a szervezet számára:

- a munkaügyi nyilvántartásban, amely tartalmazza:
  - a felhasználó szerepkörét és feladatait;
  - korcsoportját – mely generációhoz tartozik;
  - a szervezetben betöltött pozícióját;
- a beléptető rendszerekben, amelyek szabályozzák, hogy a szervezet telephelyén belül mely területekre van belépési engedélye;
- a munkaidő-nyilvántartó rendszerekben, amelyek szabályozzák, hogy a felhasználó mikor és honnan végezhet munkát,
- az elektronikus címtárban – amely tartalmazza:
  - a felhasználó azonosítóját;
  - az elérhetőségére és a munkavégzés helyére vonatkozó információkat;
  - csoporttagságait, amelyek adott esetben hozzáférési jogosultságokat is takarnak;
- a személyazonosság- (Identity Management – IDM) kezelő rendszerekben vagy annak hiányában jogosultság-nyilvántartásban, amelyek támogatják a felhasználóknak kiosztott jogosultságok nyilvántartását;
- a konfigurációkezelési adatbázisban (Configuration Management Database – CMDB), amely tartalmazza a felhasználók által használt eszközöket.

A felhasználói tevékenységek elemzéséhez további adatokra is szükség van, amelyek folyamatosan változhatnak, nem érhetők el informatikai rendszerekben, de többnyire előállíthatók a felhasználó által elvégzett feladatok naplóbejegyzéseinek elemzése alapján. Ezek lehetnek viselkedési szokások, személyiségi jegyek, segítőkészség, gépelési gyorsaság, felhasználói készség, biztonságtudatosság, szokásos bejelentkezési végpont, bejelentkezési útvonal és

időtartam, informatikai rendszerekben használt parancsok és azok sorrendje. A naplóelemzések során észlelt kisebb eltéréseket érdemes visszacsatolni a rendszerbe a korábban letárolt felhasználói adatok historikus megőrzésével, így az adatok folyamatosan pontosíthatók, a nagyobb eltérések szokatlan eseményeknek minősülhetnek, és további vizsgálat vagy riasztás tárgyát képezhetik.

Információbiztonság szempontjából a felhasználók tevékenységeire vonatkozó adatok képezik a legfontosabb információforrást. Ezt nevezhetjük a felhasználók megfigyelésének is, de valódi célja a szokatlan események azonosítása, kiszűrése és az információbiztonság megerősítésére való felhasználása. Az informatikai rendszerek folyamatosan naplózzák a felhasználók tevékenységeit, hogy bármilyen hiba esetén javítani lehessen az adatokat. Ezek az információk rendszerenként is elemezhetők és értelmezhetők, de információbiztonság szempontjából csak az adott rendszerre vonhatók le következtetések. Mivel az információbiztonság elleni támadások rendszerint több rendszert is érintenek, sokkal hatékonyabban szűrhetők ki, ha az összes rendszerben naplózott tevékenység elemzése összevontan történik. A felhasználók tevékenységeinek elemzésében fontos szerepet játszik a biztonsági eszközök naplóbejegyzéseinek, de adott esetben a hálózati adatforgalom elemzése is. Az elemzések SIEM rendszerekben történnek, amelyek összegyűjtik a különböző rendszerekben keletkező naplóbejegyzéseket, komplex algoritmusokkal azonosítják és összeillesztik a tevékenységek összetartozó adatait.

Annak ellenére, hogy mára már léteznek szabványok az események naplózására, a különböző rendszerek sok esetben mégis más-más formátumban hozzák létre a naplóbejegyzéseket. Az eltérések ellenére a naplóbejegyzések legtöbb esetben tartalmazzák az eseményekre vonatkozó lényeges adatokat, amelyek alapján előállíthatók a következő információk:

– ki az esemény kiváltója;
– mi az esemény tárgya – mi történt;
– mikor történt az esemény;
– hol történt az esemény – melyik eszközön;
– melyik objektumon történt az esemény (fájl, adatbázis stb.);
– az esemény forrása – honnan indult az esemény kiváltása;
– mire irányult az esemény.

Ez lehetővé teszi a különböző naplóbejegyzések egységes formátumra hozását,[14] amit normalizálásnak nevezünk, ami alapját képezi az egységes tárolásnak[15] és feldolgozásnak. Vannak olyan informatikai rendszerek, amelyek egy eseményt rendszeres időközönként addig naplóznak, amíg meg nem szűnik annak oka, így a normalizáláson túl fontos szerepet játszik az eseményhez tartozó duplikátumok kiszűrése. Nagyobb szervezeteknél ez nagy mennyiségű adat valós idejű összegyűjtését, feldolgozását és tárolását jelenti. A naplóállomá-

14 Securosis: *Understandig and Selecting SIEM/Log Management,* August 25., 2010. 40. Forrás: securosis.com/assets/library/reports/Securosis_Understanding_Selecting_SIEM_LM_FINAL.pdf (2015. 06. 07.)

15 Hargitai Zsolt: *A belső védelmi rendszer megerősítése* – Információvédelem menedzselése LXIV. Szakmai fórum, Budapest, 2015. január 21., 12–20. Forrás: letoltes.etrend.hu/Hetpecset/ppt_LXIV_3/Novell_Hetpecset_2015.pdf (2015. 03. 16.)

nyok feldolgozásának következő fázisa az események korrelációja, amelynek során a SIEM rendszer bonyolult matematikai modelleket alkalmazva összefüggéseket keres a különböző rendszerekből származó naplóbejegyzések között. Ez egyre fontosabbá vált az APT (Advanced Persistent Threat) támadások megjelenésével, amelyek során a támadó időben elnyújtva, a pillanatot kivárva hosszú időn keresztül hajtja végre a támadását, miközben információt gyűjt a szervezetről, annak munkatársairól és eszközeiről.

A felhasználói aktivitás elemzésének megvalósítása komplex feladat. SIEM rendszerek keretében való megvalósítása sok esetben hosszú előkészítést igényel. Rendszerint magas költséggel jár, fenntartásuk folyamatos munkavégzést és költséget generál.[16] Az információbiztonsági piacon megtalálható SIEM termékek különböző funkcionalitást, feldolgozási és riport-előállítási sebességet és időegységre eső naplóbejegyzésdarabszám-elemzési korlátot kínálnak.[17] Egyes termékek az események valós idejű feldolgozásának érdekében naplóbejegyzéseket dobnak el feldolgozatlanul, mások pedig a teljeskörűségre teszik a hangsúlyt, és ezáltal elveszítik a valós idejű reagálási képességet. A legtöbb támadás végrehajtásának átfutási ideje kevesebb, mint 1 óra, de sok esetben percek alatt zajlik le, ezért fontos a valós idejű riasztási képesség. Nagy szervezetek esetében fontos szerepet játszik a skálázhatóság, mivel hatalmas mennyiségű információbiztonsági adat áll elő, amelynek valós idejű elemzése jelentős számítási kapacitást igényel, de a naplóállományok tárolására, utólagos elemzésére és időszakos jelentések elkészítésére is szükség van.[18] Ehhez megfelelő tárolási struktúrákra, tárolási kapacitásra és információvédelmi megoldásokra van szükség.

8. A FELHASZNÁLÓI AKTIVITÁS ELEMZÉSÉNEK AUTOMATIZÁLÁSA

Méretüktől és tevékenységi körüktől függően változnak a szervezetek információfeldolgozási, tárolási és biztonsági szükségletei. A kiépített információfeldolgozási és tárolási kapacitás általában megfelel a szükségletnek, mert elengedhetetlen a napi munkavégzéshez. Mivel az információbiztonság – sok esetben annak sérülése is – láthatatlan, a támogató rendszerek kiépítettsége sok esetben elmarad a szükséges mértéktől, pl. megvalósul a naplóállományok gyűjtése, de nem történik meg azok feldolgozása, elemzése, legfeljebb információbiztonsági incidens kivizsgálásához veszik igénybe.

A rendelkezésre álló naplóállományok feldolgozása felhasználóiaktivitás-elemzéshez és felhasználóiprofil-készítéshez szervezetre szabott SIEM rendszerrel valósítható meg.[19] Mint

16 Jerry Shenk: *Sorting Through the Noise,* SANS Institute Infosec Reading Room, May 2012, 17. Forrás: www.sans.org/reading-room/whitepapers/analyst/eighth-annual-2012-log-event-management-survey-results-sorting-noise-35230 (2015. 08. 01.)

17 J. Michael Butler: *Benchmarking Security Infromation Event Management (SIEM),* SANS Institute Infosec Reading Room, February 2009, 16. Forrás: www.sans.org/reading-room/whitepapers/analyst/benchmarking-security-information-event-management-siem-34755 (2015. 07. 05.)

18 Dave Shackleford: *Security Intelligence in Action: SANS Review of McAfee,* Enterprise Security Manager (ESM) 9.2. SANS Analyst Program, May 2013, 18. Forrás: mpa.co.nz/media/34691/security-intelligence-in-action-sans-review.pdf (2015. 07. 14.)

19 Nyikes Zoltán: *A mobileszközök biztonsági kérdései, avagy, hogyan használjuk a nyilvános WIFI2 hálózatokat,* Kommunikáció 2014, Nemzeti Közszolgálati Egyetem, Budapest, 2014. november 12., 26.

láthattuk, a felhasználói tevékenység elemzésének automatizálásához számos törzsadat beállítására van szükség, ezek a szervezet fejlettségétől függően állnak rendelkezésre informatikai rendszerekben, ahonnan a SIEM rendszer automatikusan átveheti. Amennyiben az adatok átvétele nem automatizálható, különös figyelemmel kell eljárni annak érdekében, hogy frissítésük megfelelő időben megtörténjen, főleg a felhasználói fiókok és jogosultsági körök létrehozása, módosítása és törlése esetében.

Az első generációs SIEM rendszerek beállítása és karbantartása nehézkes, erőforrásigényes és költséges a hozzáadott értékükhöz képest. A költségek és feladatok csökkentése részben a beállítások automatizálásával, interfészen keresztüli rendszeres beolvasásával és frissítésével, továbbá a naplóállományok elemzésének felhasználásával valósítható meg. Elindultak kutatások olyan SIEM rendszerek elkészítésére, amelyek minimális konfigurálással és nagy pontossággal szűrik ki a szokatlan eseményeket.

9. A KONFIGURÁCIÓ- ÉS VÁLTOZÁSKEZELÉS SZEREPE A FELHASZNÁLÓI AKTIVITÁS ELEMZÉSÉBEN

A *konfigurációkezelést* értelmezhetjük szűkebb ITIL szerinti értelemben, amely a konfigurációs elemek [informatikai eszközök (hardver, szoftver és hálózat) és felhasználók] és kapcsolataik konfigurációkezelési adatbázisban (CMDB) való nyilvántartásának naprakészen tartásával foglalkozik, „Mi lenne, ha…?" elemzések elvégzésének lehetőségével támogatva a változáskezelést, tágabb értelemben pedig beleértjük a konfigurációs elemek beállításait és azok kezelését is. A konfigurációkezelés szoros kapcsolatban áll az IT-eszközgazdálkodással is, nyilvántartja az eszközök helyét, felelősét, karbantartóit, támogatóit és felhasználóit.

A konfigurációkezelés nagymértékben támaszkodik a *változáskezelésre*, ami fontos szerepet játszik a konfigurációs elemek a CMDB-ben való naprakészen tartásában. A változáskezelés legfontosabb szerepe, hogy nyilvántartsa az IT-változáskérelmeket, nyomon kövesse tervezésüket, kivitelezésüket, megfelelő kontrollt biztosítson a változások biztonságos végrehajtása során és jelezze a konfigurációs elemekben okozott változásokat. A változáskérelmek jóváhagyását és a változások tervezését követően az IT infrastruktúrában okozott módosítások tervezetét érdemes rögzíteni a CMDB-ben, mint az eszközök leendő állapota, a változás végrehajtását követően pedig véglegesíteni azokat.

A konfigurációkezelést támogató megoldásokat is két nagy csoportra oszthatjuk:

– konfigurációs adatbázis automatizált frissítését támogató eszközök, amelyek folyamatosan figyelik az informatikai infrastruktúrát, észlelik a konfigurációs elemekben és beállításaikban történt változásokat, amennyiben azok szerepelnek a változáskezelési nyilvántartásban a tervezett változások között, nyugtázzák, egyébként riasztást küldenek a konfigurációmenedzsernek nem engedélyezett változásról;
– automatizált frissítést nem támogató eszközök, amelyek esetében az adatok frissítése manuálisan történik a tervezett változások kivitelezését követően.

Információbiztonság szempontjából mindkét megoldástípus támogatja a naplóelemzést és ezáltal a felhasználók tevékenységeinek elemzését az eszközök, felhasználók, kapcsolataik és paramétereik változásának átadásával, ill. historikus adatainak SIEM rendszerek általi lekérde-

zésével. A konfigurációs adatok automatizált frissítését támogató konfigurációkezelési megoldások észlelik a konfigurációs elemekben és kapcsolataikban bekövetkezett változásokat, ezeket elemezhetik és a nem engedélyezett változásokat jelezhetik a konfigurációmenedzsernek, miközben naplózzák az eseményt. A naplófájlokat feldolgozó SIEM rendszerek észlelik a nem engedélyezett IT-infrastruktúra-változásokat, és ez alapján információbiztonsági eseményt jelenthetnek az adminisztrátoroknak.

Egy jól felépített és bevezetett IT-üzemeltetési modell és CMDB-re épülő támogató IT-szolgáltatásmenedzsment (Information Technology Service Management – ITSM) rendszer fontos szerepet játszik a felhasználói tevékenységek elemzésében, a szokatlan tevékenységek azonosításában és információbiztonsági események feltárásában.

10. LEHETSÉGES MŰKÖDÉSI MODELL FELHASZNÁLÓI TEVÉKENYSÉGEK AUTOMATIZÁLT ELEMZÉSÉRE

A SIEM rendszerek esetében a szokatlan események valós idejű azonosítása és riasztások küldése mellett – az üzemeltetés megkönnyítése érdekében – az adminisztráció mértékének minimalizálása is kulcsfontosságú feladat. Ez megfelelő működési modell kialakításával és a felhasználói profil kialakításához szükséges alapadatok partnerrendszerekből való automatizált feltöltésével, rendszeres frissítésével és automatikus lekérdezésével érhető el.

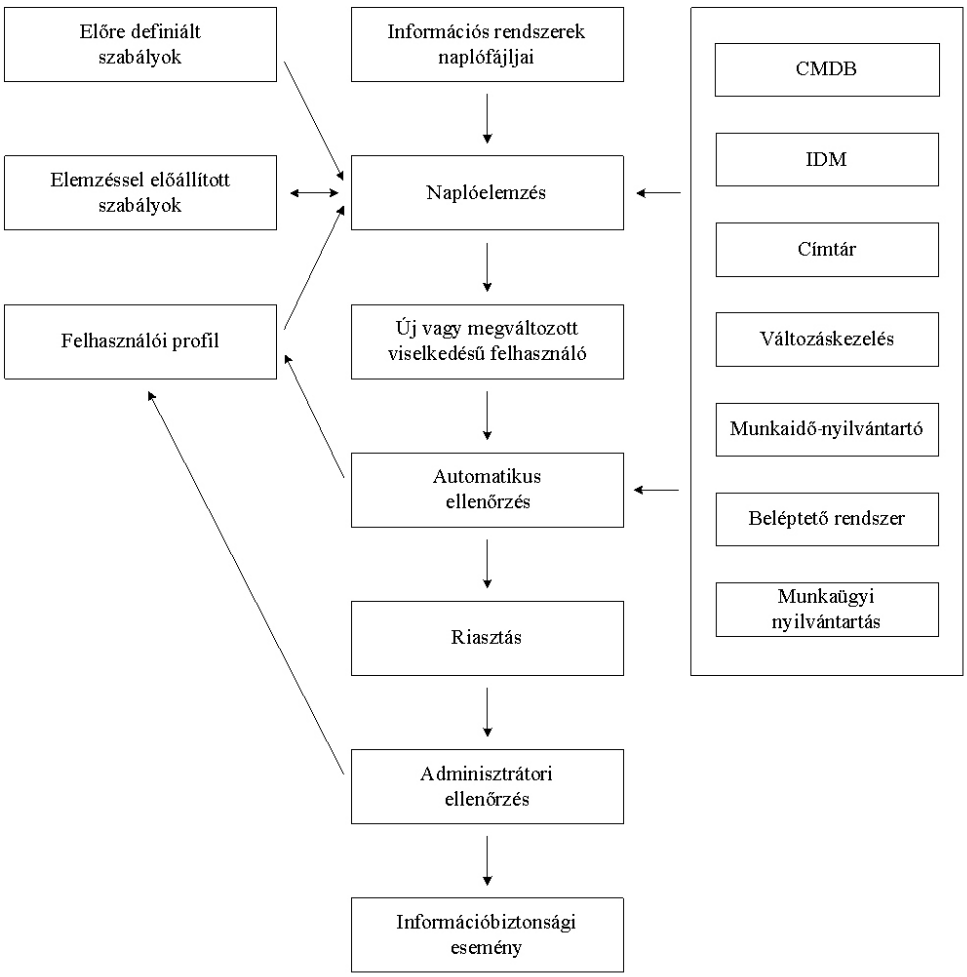
A modern SIEM rendszerekkel szemben követelmény, hogy kapcsolódási lehetőséget biztosítanak rendszerfelügyeleti és információbiztonsági megoldásokhoz,[20] mint pl. címtár, CMDB (Configuration Management Database – Konfigurációkezelési adatbázis), incidenskezelés, változáskezelés, IDS (Intrusion Detection System – Behatolásjelző rendszer), IPS (Intrusion Prevention System – Behatoláselhárító rendszer), vírusirtók, proxyszerverek, amelyek lekérdezésével felgyorsíthatják a naplófájlok feldolgozását, és javíthatják a szokatlan események meghatározásának pontosságát.

Ha megfelelően részletes naplóállományok állnak rendelkezésre, lehetőség nyílik az új és módosult felhasználók, szerepkörök és jogosultságok azonosítására. A rendelkezésre álló alapadatok lekérdezésével és felhasználásával azonosítható a létrehozás vagy módosítás jogossága. Ha nem áll rendelkezésre megfelelő mennyiségű és minőségű alapadat, a felhasználó- és szerepkör-módosításokat a rendszer szokatlan eseményként továbbíthatja az adminisztrátoroknak, akik azt elemezhetik és nyugtázhatják mint új vagy megváltozott felhasználót, vagy azonosíthatják mint információbiztonsági eseményt. A szervezet infrastruktúrájának fejlettsége, a felhasználói tevékenységek elemzéséhez szükséges alapadatok informatikai rendszerekben való rendelkezésre állása jelentősen befolyásolja a beállítás és karbantartás során elvégzendő feladatok mennyiségét és az információbiztonsági események azonosítását. A naplóelemzések elvégzése során új adatok állhatnak elő a felhasználókról, ame-

20 James Tarala: *Implementing the 20 Critical Controls with Security Information and Event Management (SIEM) Systems – SANS Institute Infosec Reading Room*, April 2011, 16. Forrás: www.sans.org/reading-room/whitepapers/analyst/implementing-20-critical-controls-security-information-event-management-siem-systems-34965 (2015. 07. 01.)

lyeket a hatékonyság érdekében a SIEM rendszernek historikusan kell rögzítenie, folyamatosan pontosítva azokat.

2. ábra • *Automatizált felhasználóiprofil-elemzési modell (saját szerkesztés)*



A szervezetek többsége nem rendelkezik a felhasználói tevékenységek elemzéséhez szükséges alapadatok teljes körű elektronikus leképezésével, ezért számukra nem elérhető a felhasználói profil teljes körű elemzése. Kétféle megközelítés létezik ennek áthidalására:

– a hiányzó alapadatokhoz kapcsolható elemzések kihagyása, ami szokatlan események azonosításának elmaradásával és információbiztonsági események észlelésének elmulasztásával járhat;
– a hiányzó alapadatokhoz kapcsolható elemzések elvégzése és a kapcsolódó gyanús naplóbejegyzések esetén adminisztrátori riasztás küldése.

Mindkét megközelítésnek megvan a maga előnye és hátránya: ha nem teljes körű az elemzés, gyorsabban végrehajtható, de információbiztonsági események maradhatnak észrevétlenül, míg a hiányos adatokon futtatott elemzések több időbe telnek, pontatlanabbak és sok lehet a hamis riasztás, amely nagyobb adminisztrációs terhet jelent a szervezet számára. Nemcsak a két véglet létezik, minden szervezetnek meg kell találnia azok között azt a beállítást, amely azonosítja a számára jellemző információbiztonsági eseményeket, de nem jelent túl nagy adminisztrációs terhet a hamis riasztások kiszűrése során (2. ábra). A SIEM rendszerek bevezetésének tervezéséhez és kivitelezéséhez hasznos támogatást nyújt David Swift: Successful SIEM and Log Management Strategies for Audit and Compliance[21] című tanulmánya.

11. FELHASZNÁLÓIPROFIL-ELEMZÉS A KÖZIGAZGATÁSBAN

A közigazgatásban sok intézmény kezel nagy mennyiségű személyes adatot, szolgálati titkot és államtitkot, amelyek hozzáférhetősége, sérülése és elvesztése kritikus lehet. A valós idejű felhasználóiprofil-elemzés nagymértékben hozzájárulhat az adatok védelméhez. Ugyanakkor a felhasználóiprofil-elemzés megvalósíthatóságának szempontjából fontos szerepet játszik a szervezet infrastruktúrájának fejlettsége, a rendelkezésre álló szakemberek tudása, az anyagi erőforrások rendelkezésre állása. Ezek az állami intézmények és szervezetek esetében sajátos képet mutatnak.

Gyakran előfordul, hogy az állami szervezetek költséghatékonyságra vagy pénzhiányra hivatkozva elhalasztják a szoftverek verziófrissítését, lecserélését újabb, modernebb megoldásokra. Az elavult technológiák jelentősen befolyásolhatják a felhasználói viselkedés elemzéséhez szükséges naplóbejegyzések rendelkezésre állását és a szükséges törzsadatok automatizált átemelését.

A bérezési modell miatt a nagyobb tudással rendelkező informatikai szakemberek egy része távozik a közigazgatásból, ezáltal folyamatos kihívás a megfelelő szaktudás biztosítása. Ez megnehezíti a magas szintű üzemeltetés fenntartásának folyamatosságát, és magas kockázatot jelent a kilépő munkatársak felhasználói jogosultságainak megszüntetése.

A költségvetési szervek gazdasági lehetőségei korlátozottak, rendszereik megújítása folyamatos kihívást jelent. Az információbiztonságot jogszabály írja elő, amelynek megvalósítása folyamatosan zajlik. A kritikus rendszereket üzemeltető szervezetek esetében előírás a naplóelemző megoldás bevezetése.

A felsorolt feltételek mentén első generációs SIEM rendszerek megvalósítása magas bevezetési és fenntartási költségek miatt csak kevés szervezet számára volt elérhető.

A modern, automatizált törzsadat-karbantartással bíró és öntanuló felhasználóiprofil-elemzést megvalósító SIEM rendszerek bevezetési és üzemeltetési költségei lehetővé teszik azok alkalmazását az állami szervezetek számára is. Automatizáltságukból adódóan üzemeltetésük kisebb szakmai felkészültség mellett is biztonságos, és a legnagyobb kihívást az elavult rendszerek naplózási hiányosságai jelentik.

21 David Swift: *Successful SIEM and Log Management Strategies for Audit and Compliance,* SANS Institute Infosec Reading Room, November 4, 2010, 40. Forrás: www.sans.org/reading-room/whitepapers/auditing/successful-siem-log-management-strategies-audit-compliance-33528 (2015. 07. 02.)

A naplózási hiányosságok megszűnhetnek az alkalmazásokkal szemben támasztott új vagy módosított ügyviteli igények megvalósítása során és új, korszerűbb rendszerek bevezetésével. A folyamatos fejlődésnek köszönhetően idővel megszűnnek a naplózási hiányosságok, de az időtáv fontos szerepet játszhat.

12. ÖSSZEFOGLALÁS

A tanulmány hangsúlyozza a felhasználóiprofil-elemzés szükségességét és sikeres alkalmazásának feltételeit. Számba veszi a szükséges eszközöket, és a hatékonyság növelésének lehetőségeit a rendelkezésre álló információk felhasználásával. Átfogó képet nyújt a szervezetek számára a sikeres megvalósítás feltételeiről, támogatva a bevezetésre való felkészülést. Javaslatot tesz egy lehetséges öntanuló felhasználóiprofil-elemzés modellre, amely lehetővé teszi a költséghatékony bevezetést és üzemeltetést, ezáltal a lkalmazhatóvá válik a közigazgatásban is. A bemutatott SIEM rendszerekbe integrált automatizált felhasználóiprofil-elemzés modell növeli a biztonsági naplóinformációk feldolgozását.

Az állami intézmények és államigazgatási szervek számára infrastruktúrájuk fejlettségétől függően a felhasználói elemzéssel kiegészített SIEM rendszer működtetése többek között az alábbi előnyöket nyújthatja:

- a felesleges jogosultságok és hozzáférések csökkentése,
- a rendszergazdai, üzemeltetői tevékenység kiemelt ellenőrzése,
- a szokatlan és információbiztonsági események azonosítása,
- munkatársak kényszerhelyzeti cselekvéseinek azonosítása és lojalitásának megfigyelése,
- felhasználói profilok illegális használatának azonosítása,
- lopott felhasználói azonosítókkal való visszaélés felderítése,
- információs rendszerek biztonsági hiányosságainak feltárása,
- információs rendszerek elleni, szervezeten belülről és kívülről érkező támadások felderítése és elhárítása,
- információszivárgás és -sérülés megakadályozása,
- működésfolytonosság növelése,
- biztonságtudatossági hiányosságok feltárása és kiküszöbölése,
- az eseményekben részt vevők egyértelmű azonosítása (az eseménymenedzsment, a felhasználóazonosítás és a konfigurációkezelés integrációja).

A SIEM rendszerek bevezetése és fenntartása akkor mondható sikeresnek, ha megvalósul az információbiztonsági események azonosítása minimális számú hamis riasztás mellett, és kezelhető, ill. még elfogadható terhet ró a biztonsági személyzetre.

SUMMARY IN ENGLISH: The implementation of information security in governmental institutions is regulated by law, which provides a complex regulation framework. The regulations emphasize the principle of least privilege, which means employees should be provided with necessary and sufficient access to do their jobs, while also requiring a

control system which limits their access to the execution of their tasks only. It also requires organizations handling large volume of personal data to carry out security analysis of the information systems' log files. Considering that the weakest link is the user, the most important aspect of log file processing is user activity analysis, building user profiles, identifying unusual events and analyzing them based on the available data. The paper discusses the goal, role, possibility, importance and limitations of building user profiles based on log files analysis, considering efficiency and inclusivity taking into account the need to minimize false alarms and administration workload. By the end of paper a cost-effective model is presented for automated user activity and profile analysis.

Dr. Michelberger Pál (michelberger.pal@kgk.uni-obuda.hu): Jelenleg egyetemi docens az Óbudai Egyetem Keleti Károly Gazdasági Karán, a Szervezési és Vezetési Intézetben. 1988-ban gépészmérnöki, 1997-ben pedig integrált menedzser – gazdasági mérnöki oklevelet szerzett a Budapesti Műszaki Egyetem Gépészmérnöki Karán. Doktori (PhD-) fokozatát a Zrínyi Miklós Nemzetvédelmi Egyetemen kapta katonai műszaki tudományokból 2005-ben. Értekezése honvédelmi célú informatikai rendszerelemek kiválasztásával és bevezetésével foglalkozott. 2015-ben az Óbudai Egyetemen habilitált. Tézisfüzetének címe: Információbiztonság és üzleti bizalom. Több mint 10 év iparvállalati gyakorlat után 2001-ben kezdett el a felsőoktatásban dolgozni. Volt a Gábor Dénes Főiskola, a Pannon Egyetem és a Budapesti Műszaki Főiskola oktatója is. Szakmai érdeklődése főleg az informatikai projektmenedzsmenthez, valamint a szabványos integrált (minőség-, környezet-, információbiztonsági) irányítási rendszerek kialakítási lehetőségeihez kapcsolható.

Dombora Sándor (dombora.sandor@kvk.uni-obuda.hu): Tanársegéd (Óbudai Egyetem Kandó Kálmán Villamosmérnöki Kar, Híradástechnika Intézet). 1996-ban programtervező matematikus oklevelet, 1997-ben pedig integrált informatikai rendszerek szervezése és fejlesztése szakirányú mester fokozatot szerzett a Kolozsvári Babes-Bolyai Tudományegyetem Matematika és Informatika Karán. Pályafutását szoftverfejlesztéssel kezdte, majd adatbázis-szakértőként és üzemeltetési csoportvezetőként folytatta. Ezzel párhuzamosan többdimenziós adatbázisok témakörben kezdett kutatásokat, és adatbázis-kezelési gyakorlatot vezetett az Eötvös Loránd Tudományegyetemen. 2005-től kezdődően ITIL alapú üzemeltetési modellek kidolgozásával, IT-üzemeltetéstámogató rendszerek tervezésével és bevezetésével, valamint az optimális üzemeltetési folyamatok optimalizálásával foglalkozott. 2008-tól kezdődően információbiztonsági irányítási rendszerek kialakításával és bevezetésével kezdett foglalkozni. 2013-ban kezdett információbiztonsági és IT-üzemeltetési témákat oktatni az Óbudai Egyetem Kandó Kálmán Villamosmérnöki Karán. 2015-től az Óbudai Egyetem Biztonságtudományi Doktori Iskola hallgatója, kutatási témája az információbiztonsági irányítási keretrendszerek.