KPMG
cutting through complexity

Információbiztonsági megfelelés felhőszolgáltatók számára

Hozzáférés-kezelés és naplózás

kpmg.hu

Tartalom

Vezetői összefoglaló

A kiszervezett informatikai szolgáltatásokat nyújtó szervezetekre egyre szigorúbb megfelelési kényszer nehezedik, melynek legfőbb célja a szolgáltató által kezelt adatok védelme. A hírnév és az ügyfelek bizalma törékeny értékek a szolgáltatók számára, melyek megszerzéséhez és fenntartásához nélkülözhetetlen az iparági standardoknak és jogi előírásoknak való megfelelés. A felhőszolgáltatók (Cloud Service Provider – CSP) számára a megfelelőség tehát olyan „bűvszó", amely egyrészt kritikus tényező az üzleti sikerhez, másrészt folyamatos áldozatokat követel.

A megfelelés speciális szelete az információbiztonsági megfelelés, amely törvényi előírásokon és nemzetközi szabványokon alapul. A felhőszolgáltatások nyújtása során azonban a földrajzi határok elmosódnak, így ezt az iparágat lehetetlen kizárólag helyi hatósági előírásokkal szabályozni. Előtérbe kerülnek tehát az olyan nemzetközi információbiztonsági szabványok, mint amilyen a PCI-DSS, az ISO:27001 vagy az SSAE 16/ISAE 3402 (korábban SAS 70). A legnagyobb felhőszolgáltatók, mint az Amazon Web Services vagy a Microsoft Windows Azure is többek között a fenti szabványok szerinti minősítések megszerzésével erősítik ügyfeleik bizalmát.

A szabványok sokrétű követelményeket fogalmaznak meg, ami átfogó megközelítést igényel. A szolgáltatóknak minden esetben meg kell érteniük, és magukra nézve értelmezniük kell az előírásokat, majd egy tudatos felkészülési programot kell végrehajtaniuk. Ennek része, hogy egyes követelmények teljesülését speciális támogató szoftverekkel biztosítják. Tipikusan ilyen terület a privilegizált hozzáférések kezelése és a központi naplókezelés, amely esetén az szoftveres támogatás jelentős ráfordítás-megtakarításhoz vezethet, miközben magasabb biztonsági szint is elérhető általuk.

Az alábbiakban összefoglaljuk a kiszervezett informatikai szolgáltatásokat nyújtó szervezetek számára ajánlott nemzetközi információbiztonsági szabványok hozzáférés-kezelésre és naplózásra vonatkozó előírásait, majd pedig bemutatjuk a legjobb gyakorlatokat, melyeket érdemes szem előtt tartani a kapcsolódó projektek során.

© 2014 KPMG Tanácsadó Kft, a magyar jog alapján bejegyzett korlátolt felelősségű társaság, és egyben a független tagtársaságokból álló KPMG-hálózat magyar tagja, amely hálózat a KPMG International Cooperative-hez ("KPMG International"), a Svájci Államszövetség joga alapján bejegyzett jogi személyhez kapcsolódik. Minden jog fenntartva.

Bevezetés

Globalizálódó világunkban nehéz követni az informatikában bekövetkező változásokat. Ma már természetes, hogy szervezetek szolgáltatókat vegyenek igénybe egyes informatikai feladatok elvégzésére. Ugyanakkor teljesen jogosan felmerül a kérdés, honnan tudja a megbízó, hogy biztonságosan látja el feladatát a megbízott. Szintén fontos, hogy hogyan tudja egy szolgáltató meggyőzni a meglévő és a potenciális ügyfeleit az általa nyújtott szolgáltatások biztonsági megfelelőségéről. Kérdés szintén, hogy miből tudja bárki megállapítani, hogy a vele kapcsolatban álló szervezetek (hivatalok, pénzügyi, közmű-, egészségügyi szolgáltatók, oktatási szervezetek, civil szféra, stb.) információvédelmi szempontból biztonságosan végzik a feladataikat.

Az nem hatékony, hogy minden egyes szerződés esetén a szolgáltató és az ügyfele egyedileg definiálja az információbiztonsági követelményeket, és mérje azok teljesülését. Sokkal hatékonyabb nemzetközileg ismert és elfogadott standardokra hivatkozni, hiszen azokat mindkét fél ismeri, és remélhetőleg egyformán értelmezi.

Bármilyen minősítés megszerzése és fenntartása lehet egyedi döntés, szerződéses kapcsolatból fakadó kötelezettség, de akár törvényi előírás is. Azonban a döntés hátterétől függetlenül komplex információbiztonsági kontrollrendszer kialakítása szükséges a megfeleléshez.

Súlyos következmények meg nem felelés esetén

Nemcsak egy minősítés megszerzése, hanem annak hiánya, illetve elvesztése is jelentőséggel bír,. Legenyhébb következmény a versenyhátrány a többi versenytárssal szemben (például tenderekből való kizárás), de PCI-DSS meg nem felelés esetén súlyos pénzbüntetések is kiszabhatók. A PCI-DSS szabványnak való meg nem felelés esetén akár 500.000 amerikai dollárig is terjedhet a kiszabható büntetés. Emellett az egyes biztonsági incidensek után is jelentős büntetést kell fizetni, melynek mértéke részben függ az érintett kártyák számától is. Jelenleg is bíróságon harcol a VISA és a Genesco (lábbeliket forgalmazó amerikai üzletlánc) egymás ellen a 2010-es biztonsági incidenshez kapcsolódó 13 millió amerikai dolláros PCI-DSS bírság miatt.

Komoly következményekkel járhat egy SSAE 16/ISAE 3402 auditon való meg nem felelés a szolgáltatást igénybe vevő pénzügyi beszámolójának elfogadására, ez pedig befolyásolja a vállalat értékét. Előfordulhat, hogy egy ISO27001:2005 vagy CSA-STAR minősítés elvesztése miatt a szolgáltató megszegi az ügyfeleivel kötött szerződést, így azok akár kötbért is követelhetnek tőle.

A következőkben nem célunk az ISO27001:2013, PCI-DSS v3.0, PCI Cloud Computing Guidelines, CSA-STAR vagy a nem információbiztonság-specifikus SSAE 16/ISAE 3402 szabványok minden aspektusának bemutatása, hanem speciálisan a hozzáférés-menedzsment, illetve naplózás témakörét járjuk körül. Természetesen ez a két témakör kapcsolódik a többi itt nem említett kontrollelemhez (például szabályozás, rendszerfejlesztés), így minden esetben ügyelni kell arra, hogy a kialakítandó megoldás szervesen illeszkedjen a tervezett kontrollkörnyezet egészébe.

© 2014 KPMG Tanácsadó Kft, a magyar jog alapján bejegyzett korlátolt felelősségű társaság, és egyben a független tagtársaságokból álló KPMG-hálózat magyar tagja, amely hálózat a KPMG International Cooperative-hez ("KPMG International"), a Svájci Államszövetség joga alapján bejegyzett jogi személyhez kapcsolódik. Minden jog fenntartva.

„Megfelelőség az IT-szolgáltatói szektorban” – Piackutatás

A KPMG és a BalaBit IT Security közösen nemzetközi piacfelmérést végzett „Megfelelőség az IT-szolgáltatói szektorban” címmel. A felmérést 120 informatikai-, illetve felhőszolgáltatást nyújtó vállalat IT-vezetőjének megkérdezésével végeztük 2014 februárjában. A felmérés a következőket derítette ki.

Eredmények

A szolgáltatók közel 60 százaléka éves informatikai büdzséjének több mint 10 százalékát IT-biztonsági megfeleléssel kapcsolatos beruházásra költi. Sőt, a megkérdezettek közel ötöde éves büdzséjének több mint 20 százalékát költi a fenti célokra, ami az iparági átlagot tekintve már kifejezetten magasnak mondható.

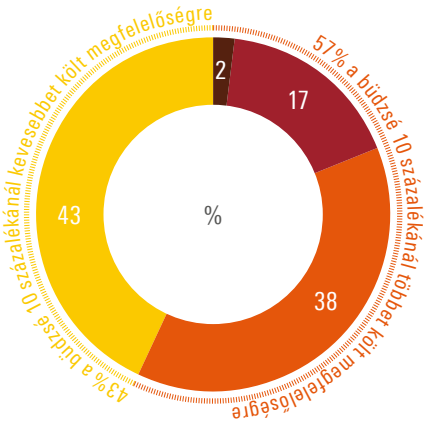
A mintavétel módszeréből adódóan nem ismert azok száma, akikhez elért a meghívó, így természetesen a pontos válaszadási arány sem ismert. Összesen 299-en töltötték ki végig a kérdőívet. A hiányosan kitöltött kérdőíveket nem vettük figyelembe.

A felmérés kiegészítésére öt vállalatvezetői, illetve szakértői interjút is készítettünk. Beszélgető partnereink részére bemutattuk a kérdőíves kutatás eredményeit, majd a beszélgetések alkalmával szerzett véleményekkel és tapasztalatokkal bővítettük saját következtetéseinket.

A megkérdezettek több mint kétharmada elsősorban a biztonságosabb működés miatt törekszik a szabályozóknak való megfelelésre. Ez mindenképpen előremutató fejlemény, hisz azt jelzi, hogy a legtöbb IT-/felhőszolgáltató az iparági előírásokra egyfajta ajánlásként tekint, amely jó keretet ad a cég kockázatkezelési gyakorlatának kialakításához.

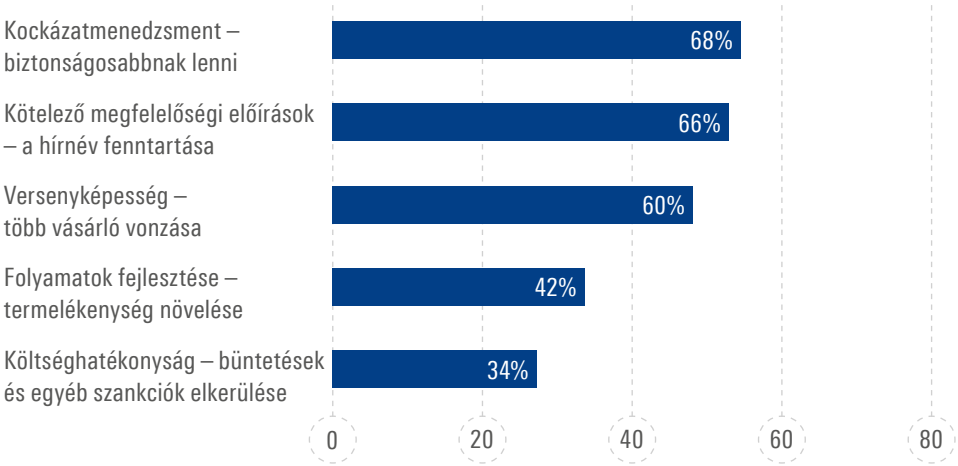
A nagy többség a hírnév fenntartása és további ügyfelek szerzése céljából is törekszik a megfelelésre, mely jól mutatja, hogy a megfelelésre bizalomépítő tényezőként is tekintenek a szolgáltatók.

1. ábra Az éves IT-büdzsé hány százalékát fordítják megfelelőséggel kapcsolatos befektetésekre?



- több, mint 30%
- 21-30%
- 10-20%
- kevesebb, mint 10%

2. ábra A megfelelőségi előírások betartásának indoka



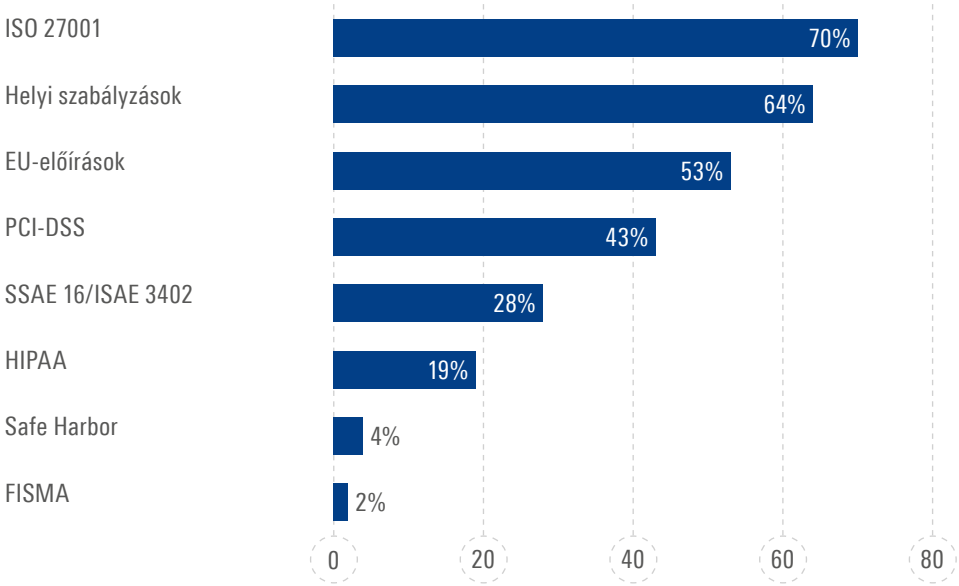
© 2014 KPMG Tanácsadó Kft, a magyar jog alapján bejegyzett korlátolt felelősségű társaság, és egyben a független tagtársaságokból álló KPMG-hálózat magyar tagja, amely hálózat a KPMG International Cooperative-hez (“KPMG International”), a Svájci Államszövetség joga alapján bejegyzett jogi személyhez kapcsolódik. Minden jog fenntartva.

Az alábbi ábrán jól látható, hogy a nemzetközi szabványoknak (például ISO 27001, PCI DSS) való megfelelést a legtöbb IT-szolgáltató fontosnak tartja. Természetesen azon ország(ok) adatvédelmi előírásai is kiemelt fontosságúak, ahol a szolgáltató adatközpontjai megtalálhatók. Itt érdemes megjegyezni, hogy a törvényi szabályozások is legtöbbször valamelyik nemzetközi szabvány alapelveire épülnek.

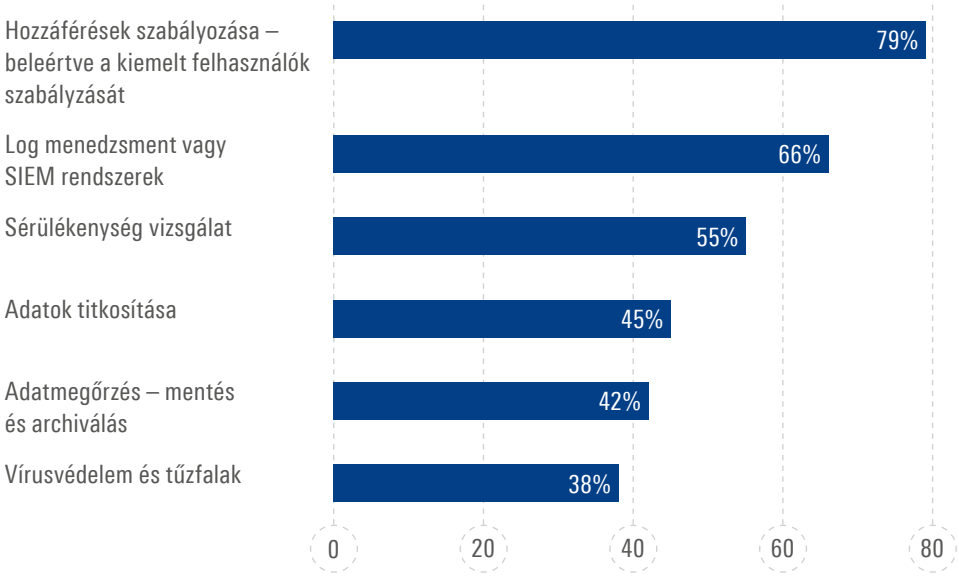
Kiderült, hogy a (kiemelt) felhasználók hozzáférésének ellenőrzése illetve a naplókezelés és -elemzés kulcsfontosságú területek a szolgáltatók megfelelőségi stratégiájában, míg érdekes módon az olyan alaptechnológiák, mint az antivírus- vagy tűzfalrendszerek már kevésbé lényegesek.

A válaszadók többsége (57 százalék) számára a felhőinfrastruktúrához történő bármilyen kiemelt jogú, külső vagy belső hozzáférés felügyelete egyaránt fontos. Ez azzal magyarázható, hogy a hozzáférés-felügyeleti rendszerek erős bizonyítékként szolgálhatnak az ügyfelekkel való felelősségi viták eldöntésében, és az ilyen nézeteltérések gyors és költséghatékony lezárása a szolgáltatók elemi érdeke.

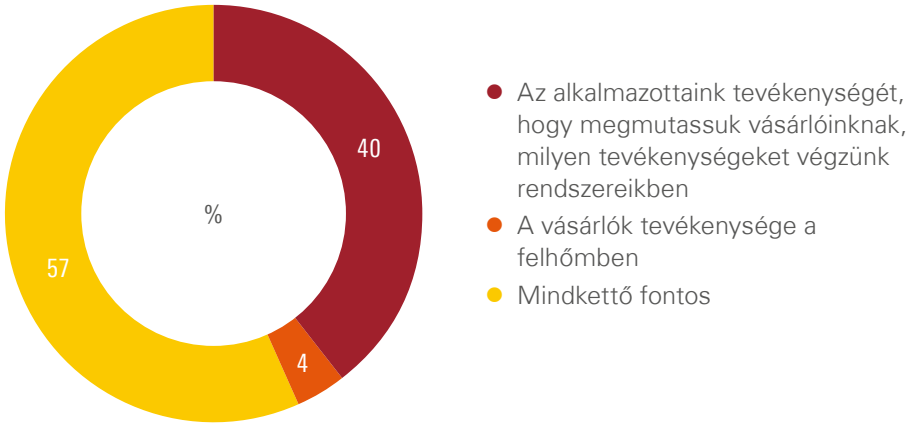
3. ábra A fontosabb előírások/standardok, amelyeknek meg kell felelniük



4. ábra Mely szabályzási terület jut eszébe először, mikor a megfelelőségi stratégia kerül szóba?



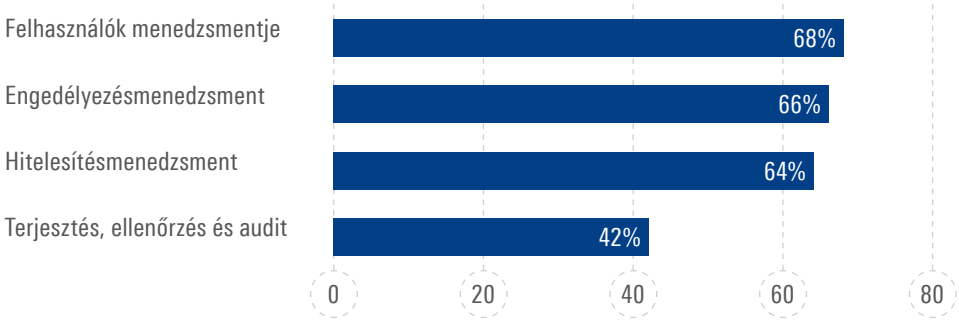
5. ábra Mely kiemelt felhasználók tevékenységét monitorozzák elsődlegesen?



© 2014 KPMG Tanácsadó Kft, a magyar jog alapján bejegyzett korlátolt felelősségű társaság, és egyben a független tagtársaságokból álló KPMG-hálózat magyar tagja, amely hálózat a KPMG International Cooperative-hez ("KPMG International"), a Svájci Államszövetség joga alapján bejegyzett jogi személyhez kapcsolódik. Minden jog fenntartva.

A felmérésünkből jól látható, hogy a felhasználók általános nyilvántartása, valamint különböző szintű engedélyezési és hitelesítési mechanizmusok a legtöbb szolgáltatónál már működnek. A kiemelt felhasználók tevékenységének felügyelete és auditálása azonban még csak a válaszadók 42 százalékánál megoldott. Ez azért probléma, mert megfelelő auditeszköz nélkül nem lehet egyértelműen megválaszolni, hogy ki és pontosan mit csinált egy adott rendszerben, ami felelősségi vitákhoz vezethet, a bizonyítási eljárást pedig rendkívül költségessé teszi.

6. ábra A kiemelt felhasználók menedzsmentjének érettsége a szervezetekben



© 2014 KPMG Tanácsadó Kft, a magyar jog alapján bejegyzett korlátolt felelősségű társaság, és egyben a független tagtársaságokból álló KPMG-hálózat magyar tagja, amely hálózat a KPMG International Cooperative-hez ("KPMG International"), a Svájci Államszövetség joga alapján bejegyzett jogi személyhez kapcsolódik. Minden jog fenntartva.

Hozzáférés-kezelés és naplózás az ISO27001:2013 szabvány tükrében

Az ISO27001:2013 szabvány az információbiztonság-irányítási rendszer (IBIR) (Information security management systems – ISMS) követelményeit határozza meg. A rendszer bevezetése során ki kell alakítani egy folyamatszemléletű biztonsági modellt, amely magában foglalja a rendszer állandó karbantartását és felülvizsgálatát, ami a napra készen tartott, működő rendszer záloga. Ugyanakkor a fenti biztonsági modell implementálása nem lehetséges a hozzáférés-menedzsment és a naplókezelés implementálása nélkül.

Felhőalapú szolgáltatások üzemeltetői számára különösen fontos a hozzáférés-kezelés és a naplózás kérdése, hiszen ugyanazt a fizikai infrastruktúrát több (akár egymással versenyben álló) szervezet is használja. A szolgáltatónak biztosítani kell az adatvédelmi (személyes adatok, üzleti titkok) szempontokat is figyelembe vevő hozzáférés-kezelést, amelynek folyamati és technikai kontrollokra is ki kell terjednie. Emellett a szolgáltatónak és az ügyfeleinek is elemi érdeke, hogy a rendszerben végzett minden tevékenység kellő részletességgel legyen naplózva. Ha egy incidens esetén a szolgáltató egyértelműen bizonyítani tudja „ártatlanságát" (azaz rajta kívül álló okból következett be az incidens), a kártérítési felelőssége is megszűnik. Értelemszerűen a szolgáltatónak nemcsak a saját munkatársai tevékenységét kell rögzítenie, hanem – a visszaélések és nem engedélyezett rendszerhasználat feltárása miatt – érdemes a szolgáltatást igénybe vevők tevékenységét is naplóznia és elemeznie.

Az ISO27001:2013 szabvány **hozzáférés-kezelésre** vonatkozó pontjai az architektúra minden szintjét lefedik. Ezek a következők:

- A.9.2 (Felhasználói hozzáférés-menedzsment \ User access management),
- A.9.4 (Rendszer- és alkalmazás-hozzáférési kontrollok \ System and application access control).

A kontrollkörnyezetek kialakításának mindenféleképpen kockázatelemzésen kell alapulnia. A gyakorlatban érdemes lehet más kontrollkörnyezetet kialakítani a privilegizált jogokkal rendelkező vagy szenzitív adatokhoz hozzáférő felhasználókra, mint a normál felhasználókra. (Ezt a költség-haszon elemzések eredményei is alátámaszthatják.)

Különösképpen biztosítani kell, hogy:

- csak munkakörükből adódó személyek rendelkezzenek privilegizált hozzáféréssel;
- a rendszer/adat csak az előírt autentikációt követően legyen elérhető;
- a rendszerben végzett tevékenység konkrét személyhez legyen köthető;
- a rendszerben végzett tevékenység naplózható, visszakövethető legyen;
- az egyes hozzáférések csak jóváhagyás után legyenek használhatóak.

A szabvány A.12.4 (Naplózás és monitorozás\Logging and monitoring) szabályozási céljában előírja a jogosulatlan információ-feldolgozó tevékenységek észlelését. Az **auditnaplózás** során mindenképpen biztosítani kell, hogy

- a naplóbejegyzések létrejönnek a szükséges adattartalommal;
- azokat biztonságos módon továbbítják a naplóüzenetek forrása és a központi naplógyűjtő között;
- a naplófájlok kereshető formában megőrződnek az elvárt időpontig, utána viszont törlik/ archiválják őket;
- az összegyűjtött naplóbejegyzések védve vannak minden véletlen vagy szándékos módosítás ellen;
- csak olyan személyek férnek hozzá a naplókhoz, akiknek szükséges, hiszen számos szenzitív információ van a fájlokban;
- kereshetőek, elemezhetőek legyenek a naplófájlok (akár azonnal, akár utólagosan is).

Hiába tűnnek triviálisnak a fenti szabályozási célok, közel sem egyszerű mindegyik követelményt megvalósítani heterogén informatikai környezetekben. Ráadásul a naplózásnak nemcsak hardver- és operációsrendszer-szinten kell megtörténnie, hanem magasabb szinteken, például az adatbázis és az alkalmazás szintjén is.

Az ISO27001:2013 szabvány külön fejezetet szentel a külső szolgáltatók kezelésének. Így a felhőszolgáltatóknak is fel kell készülniük, hogy az ISO27001 tanúsított ügyfelek előírják és számon kérik a biztonsági követelmények érvényesítését.

© 2014 KPMG Tanácsadó Kft, a magyar jog alapján bejegyzett korlátolt felelősségű társaság, és egyben a független tagtársaságokból álló KPMG-hálózat magyar tagja, amely hálózat a KPMG International Cooperative-hez ("KPMG International"), a Svájci Államszövetség joga alapján bejegyzett jogi személyhez kapcsolódik. Minden jog fenntartva.

Hozzáférés-kezelés és naplózás a PCI-DSS v3.0 szabvány tükrében

A Payment Card Industry Data Security Standard (PCI-DSS) 3.0 szabvány a bankkártya-adatokkal dolgozó szervezetek körében megkerülhetetlen kötelezettséget jelent. A szabvány természetesen kitér mind a hozzáférés-kezelésre, mind a tevékenységek naplózására, hiszen ezek nélkül nem érhetné el alapvető célját – a kártyabirtokosok adatainak védelmét és az esetlegesen bekövetkező károk minimalizálását.

A PCI Security Standards Council haladva a korral Cloud Computing Guidelines kötetében foglalta össze a felhőalapú szolgáltatásokkal kapcsolatos előírásait. A hozzáférés-kezelést és a naplózást külön területként is kiemeli az irányelv, hiszen felhőalapú szolgáltatások esetén sem lehet eltekinteni az alapcéltól – a kártyabirtokosok adatainak védelmétől. Mindenképpen hangsúlyozandó, hogy az érintett felhőszolgáltató által biztosított szolgáltatásnak meg kell felelnie a PCI-DSS követelménynek a rá értelmezhető módon.

A szabvány egyértelműen kiemeli, hogy a felhőszolgáltatóknak és ügyfeleiknek közösen kell biztosítani a megfelelőséget. Bármilyen is a felhőszolgáltatás modellje (IaaS, PaaS, SaaS), a szolgáltató felelőssége a kontrollok megfelelő kialakítása és üzemeltetése kapcsán megkerülhetetlen.

Nemcsak a Cloud Computing Guidelines kiadásával nyújtott támogatást az új technológiák implementálásához a PCI Security Standards Council, hanem a PCI-DSS új (version 3.0) verziója is nagyobb hangsúlyt helyez egyes új technológiai megoldásokkal szembeni követelményekre.

A szabvány 7. (Üzleti igényen alapuló korlátozott hozzáférés a kártyabirtokosok adataihoz / Restrict access to cardholder data by business need to know) és 8. fejezete (Rendszereszközökhöz való hozzáférés azonosítása és autorizálása / Identify and authenticate access to system components) konkrét követelményeket fogalmaz meg a **hozzáférés-védelem** kapcsán. A hatókörbe tartozó rendszerek esetén megfelelően megtervezett és technikailag is támogatott kontrollokat kell kialakítani és fenntartani. Ennek része, hogy:

- rendszerhozzáférést és kártyaadatokhoz való hozzáférést csak az arra felhatalmazott személyek és csak a szükséges mértékben kaphatnak (7.1*, 7.2*);
- a vezetőknek dokumentált módon kell a hozzáféréseket jóváhagyni (7.1*);
- automatizmusokkal kell biztosítani a hozzáférés-kezelést (7.2*);
- egyedi felhasználói azonosítókat kell használni a beazonosíthatóság érdekében, a megfelelő autentikációs előírások kikényszerítésével egyetemben (8.1*, 8.2*);
- a külső támogatók által használt felhasználókat kontrollálni kell (8.1*)
- megosztott (shared) és generikus (generic) felhasználók használata tilos (8.5*).

Természetesen a hozzáférés-kezelés preventív kontrolljait a szabvány kiegészíti **a naplózás** detektív kontrolljaival (10. fejezet, Minden hálózati erőforráshoz és kártyaadathoz való hozzáférés követése és monitorozása \ Track and monitor all access to network resources and cardholder data).
A szabvány megköveteli, hogy

- minden scope-beli rendszeren be legyen kapcsolva a naplózás és az minden felhasználóra terjedjen ki (10.1*);
- a naplózás terjedjen ki:
  - minden kártyaadathoz való hozzáférésre (10.2*);
  - minden privilegizált felhasználóval végzett tevékenységre (10.2*);
  - a naplófájlokhoz való hozzáférésre (10.2*);
  - a sikertelen bejelentkezési kísérletekre (10.2*);
  - az autentikációs és autorizációs változásokra (10.2*);
  - a naplózás elindítására, leállítására és felfüggesztésére (10.2*)
  - a rendszerobjektumok létrehozására és törlésére (10.2*).

Nemcsak a naplózandó eseményeket taglalja részletesen a szabvány, hanem meghatározza, hogy minimálisan milyen adattartalommal kell az egyes naplóbejegyzéseknek rendelkezniük (10.3*).

Természetesen a szabvány a naplófájlok védelmét sem hagyja figyelmen kívül, így:

- korlátozni kell a naplófájlokhoz való hozzáférést a fájlokban található szenzitív adatok miatt (10.5)*;
- védeni kell a fájlokat a szándékos és véletlen módosulás ellen (10.5*);
- továbbítani kell egy központi szerverre a módosítás elleni védelem részeként (10.5*);
- monitorozni kell a naplófájlok integritását (10.5*);
- biztosítani kell a három hónapnál nem régebbi naplófájlok azonnali hozzáférését (10.7*);
- legalább egy évig minden naplófájlt meg kell őrizni (10.7*).

Persze a naplógyűjtés nem öncélú, hanem az adatok kompromittálódásának feltárása, az incidensek hatásainak minimalizálása a célja. Ez nem valósulhat meg a naplófájlok folyamatos elemzése nélkül (10.6*).

Természetesen naplókezeléshez kapcsolódó szabályozást dokumentálni kell, és az érintett feleknek meg kell ismerniük azt. (10.8*)

© 2014 KPMG Tanácsadó Kft, a magyar jog alapján bejegyzett korlátolt felelősségű társaság, és egyben a független tagtársaságokból álló KPMG-hálózat magyar tagja, amely hálózat a KPMG International Cooperative-hez ("KPMG International"), a Svájci Államszövetség joga alapján bejegyzett jogi személyhez kapcsolódik. Minden jog fenntartva.

Hozzáférés-kezelés és naplózás a CSA-STAR megfelelés tükrében

A felhőalapú szolgáltatások megkerülhetetlenné váltak napjainkban. A 2008-ban alakult Cloud Security Alliance (CSA) küldetésében azt fogalmazta meg, hogy a felhőalapú szolgáltatások biztonsági minősítésének érdekében felhívja a figyelmet a legjobb gyakorlatokra . A szervezet tevékenységét hamar elismerte a közösség, így a Cloud Security Alliance Security Trust & Assurance Registry (CSA-STAR) megfelelés megszerzése rövid idő alatt a felhőszolgáltatók egyik célja lett.

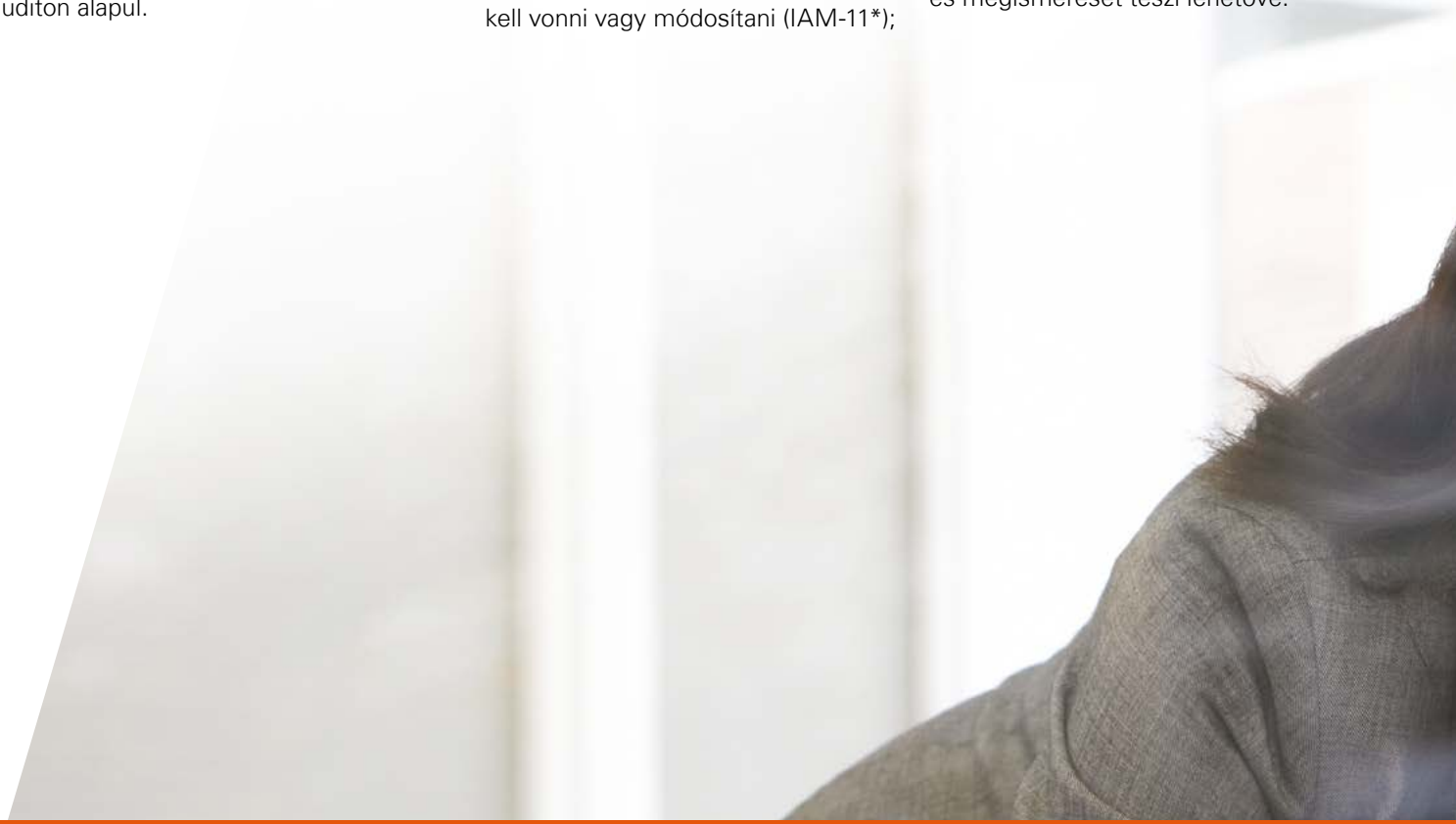
A CSA-STAR Registry fokozat más tanúsításokkal szemben önértékelésen (self assessment), illetve a nyilvánosság erején alapszik, ami azonban nem csökkenti elismertségét és elfogadottságát. Magasabb bizonyító erővel rendelkeznek a STAR Certification/STAR Attestation minősítések, amelyek esetén harmadik fél értékelése bizonyítja a megfelelést. A STAR Continuous fokozat pedig a folyamatos nyomon követésen, auditon alapul.

A szabvány Cloud Control Matrix-a (version 3.0) (CCM) kitér a hozzáférés-kezelés kérdésére, illetve a naplózásra. A **hozzáférés-kezelés** kapcsán előírás, hogy:

- technikailag is biztosítani kell a legkevesebb jogosultság szabályának/„rule of least privilege" érvényesülését és az üzleti igényeknek megfelelő feladatkör-szétválasztási/„Segregation of Duties" szabályok betartását (IAM-02*, IAM-05*, IAM-08*);
- a hozzáféréseknek vezetői engedélyezésen kell alapulnia, és azokat rendszeresen felül kell vizsgálni (IAM-09*, IAM-10*);
- technikailag is korlátozni kell a forráskódokhoz és egyéb szellemi tulajdonokhoz való hozzáférést (IAM-06*);
- a külső felek hozzáférését kockázatarányosan kell kezelni, szükség esetén kompenzáló kontrollt kell alkalmazni (IAM-07*);
- a felhasználók jogait időben vissza kell vonni vagy módosítani (IAM-11*);
- a felhasználók azonosítását a megfelelő technológiákkal kell biztosítani (IAM-12*);
- a speciális rendszereszközökhöz, illetve rendszer-konfigurációs portokoz való hozzáférést korlátozni kell (IAM-03*, IAM-13*).

A **naplózás** kapcsán a CCM előírja, hogy annak teljes életciklusát a jogi és egyéb megfelelőségi követelmények figyelembe vételével kell kialakítani, hogy biztosítva legyen az egyedi személyhez kapcsolható elszámoltathatóság gyanús tevékenységek és biztonsági incidensek feltárása esetén (IVS-01*). Természetesen ezeket a naplófájlokat is meg kell őrizni a kapcsolódó előírások szerint (BCR-12*).

A felhőszolgáltatások sokszínűsége miatt hasznos része a CSA-STAR regisztrációnak a Consensus Assessments Initiative Questionnaire (CAIQ), amely az adott felhőszolgáltatónál meglévő kontrollok dokumentációját és megismerését teszi lehetővé.



© 2014 KPMG Tanácsadó Kft, a magyar jog alapján bejegyzett korlátolt felelősségű társaság, és egyben a független tagtársaságokból álló KPMG-hálózat magyar tagja, amely hálózat a KPMG International Cooperative-hez ("KPMG International"), a Svájci Államszövetség joga alapján bejegyzett jogi személyhez kapcsolódik. Minden jog fenntartva.

SSAE 16/ISAE 3402 auditálási szabványok kapcsolata a hozzáférés-kezeléssel és a naplózással

Az SSAE 16/ISAE 3402 nem információbiztonsági szabványok, hanem minősítési előírások, amelyek alapján egy független auditor véleményt alkot egy szolgáltató szervezet (service organization) kontrollkörnyezetéről. Az auditori vélemény célja, hogy alátámassza a kialakított kontrollok megfelelő tervezését, illetve működési hatékonyságát. Nincsenek konkrét információbiztonsági követelmények ezen előírásokban (hiszen nem ez a célja az előírásoknak), hanem az érintett szervezetre bízza, hogy kialakítsa és működtesse a megfelelő kontrollkörnyezetet. Ugyanakkor a Public Company Accounting Oversight Board (PCAOB) előírásai meghatározzák azon kontrollok körét, amelyeket ki kell alakítani egy megfelelően megtervezett és implementált kontrollkörnyezet esetén.

A kontrollkörnyezet kialakításakor a menedzsment nem tekinthet el a kockázatok előzetes értékelésétől. A tapasztalatok azt mutatják, hogy a kialakított belső kontrollkörnyezetnek része a hatékonyan működő jogosultságkezelés (mint preventív kontroll), illetve a rendszerekben végzett tevékenységek rögzítése és átvizsgálása (mint detektív kontroll), bár ez utóbbi terület kevésbé hangsúlyos.

A **hozzáférés-menedzsment** területére vonatkozó kontrolloknak mindenképpen ki kell térnie:

- a privilegizált felhasználók hozzáféréseinek kezelésére;
- a hozzáféréseket biztosító, dokumentált vezetői jóváhagyásokra;
- a hozzáférések természetes személyekhez való kötésére.

A **naplóbejegyzések** kezelése kapcsán sem tekinthet el a szervezet azok teljes életciklusának védelméről, így:

- a naplózás bekapcsolásától és a megfelelő naplózási szint beállításától;
- azokat a vétlen vagy szándékos módosulás elleni védelmétől a továbbítás, illetve tárolás során;
- annak biztosításától, hogy megőrzésük, archiválásuk és törlésük a belső, más szabványi, illetve törvényi előírásoknak megfelelően történjen;
- annak biztosításától, hogy a napló-jegyezésekhez mind a továbbításuk, mind a tárolásuk során csak az arra feljogosított emberek férjenek hozzá;
- a naplófájlok rendszeres vizsgálatától.

Természetesen a kontrollok köre szervezetről-szervezetre változhat, de ilyen alapvetések implementálása nélkül nem lehet megfelelő kontrollkörnyezet kialakítani.

© 2014 KPMG Tanácsadó Kft, a magyar jog alapján bejegyzett korlátolt felelősségű társaság, és egyben a független tagtársaságokból álló KPMG-hálózat magyar tagja, amely hálózat a KPMG International Cooperative-hez ("KPMG International"), a Svájci Államszövetség joga alapján bejegyzett jogi személyhez kapcsolódik. Minden jog fenntartva.

Legjobb gyakorlatok a naplókezelésben

A következőkben összefoglaljuk azon szempontokat, amelyeket érdemes egy költséghatékony naplókezelési rendszer kialakításakor követni.

Célok megállapítása, az érintettek azonosítása

A legfontosabb lépés a naplókezelés hatókörének helyes megállapítása, hogy a legtöbb eredményt nyerhessük ki a befektetett időből és pénzből. Fontos reálisan meghatározni, hogy mit kívánunk elérni az adatgyűjtéssel. Más szakterületek bevonásával növelhetjük a naplókezelő megoldással kapcsolatos befektetésünk megtérülését, ha e technológiát használva ők is használható információkat nyerhetnek.

A naplóforrások azonosítása

Ha a naplókezelés hatókörét meghatároztuk, azonosítsuk az összegyűjtendő naplóbejegyzések forrásait. Mindenképpen fel kell mérni, hogy egy adott eszköz/szoftver naplóz-e. Sajnos a naplózás alapértelmezetten nincs bekapcsolva számos eszköz/szoftver esetén, vagy ha mégis, nem biztos, hogy a megfogalmazott céljainkhoz illeszkedik annak módja. Azonosítani kell a céljaink szempontjából irreleváns naplókat is, hogy ne gyűjtsük és elemezzük azokat feleslegesen, így pazarolva az erőforrásokat.

A korlátok és szűk keresztmetszetek azonosítása

A megbízható működés biztosítása követelményeket támaszt az adatokat összegyűjtő és továbbító infrastruktúrával szemben. Ezért a tervezés során célszerű azonosítani a korlátokat, úgymint a hálózat sávszélessége és megbízhatósága, tárhelykapacitás, pénzügyi erőforrások vagy az emberi erőforrások. A korlátok ismerete nélkül a célok elérése nem lehetséges.

A naplók formátumának felmérése és normalizálása

A naplókezelés egyik legnagyobb kihívása, hogy kinyerjük a hasznos információt a „zajból", azaz a nagy mennyiségű, különböző formátumú és/vagy gyakran strukturálatlan adathalmazból. A szabványos formátumok elősegítik a naplók gyűjtését és normalizálását.
Ezek közül az alábbiakat emeljük ki:

- A syslog a naplók legszélesebb körben elfogadott szabványos formátuma. A syslog-protokollnak két változata van, az RFC3164 és az újabb RFC5424. Az újabb változat a végrehajtott fejlesztések révén felülmúlja a régebbit.
- A Simple Network Management Protocol (SNMP) egy szintén gyakran használt formátum, melyet általában a hálózati eszközök használnak állapotuk jelentésére, de a felhasználási kör nem korlátozódik csupán erre.
- A Windows az Event Log nevű saját naplóformátumát használja. Ezt használhatják a Windows felett futó alkalmazások is.
- Sok alkalmazás adatbázisok tábláiba naplóz, szabványos vagy kevésbé szabványos adattartalommal.
- Többféle, új naplózási forma is felbukkant mostanában elsősorban a Java-hoz kapcsolódóan (például log4j).

A naplóbejegyzésekben lévő hasznos információt csak úgy lehet hatékonyan összegyűjteni, ha közös formátumra alakítják azokat. A normalizálást már a naplózási projekt felmérési szakaszában érdemes megkezdeni.

A naplóbejegyzések fontosságának és érzékenységének felmérése

Miután meghatároztuk a gyűjteni kívánt naplóbejegyzéseket, lényeges hogy megállapítsuk azok fontosságát és érzékenységét. Értelemszerűen a magas prioritású naplóüzeneteket gyorsabban kell értelmezni, és gyakran azonnal kell reagálni. Néhány naplóüzenet tartalmazhat érzékeny vagy személyes információt, például bankkártyaszámot, társadalombiztosítási azonosítót, vagy egy páciens egészségügyi adatait. Adott esetben szükséges lehet ezen adatok elrejtése vagy törlése a naplókezelés során.

A naplókhoz való hozzáférés és azok elemzése

Az egyik legnagyobb előnye a központosított naplógyűjtésnek, hogy a hozzáférés-szabályozás egyszerűen menedzselhető.
A szabványok és törvényi előírások megszabják, hogy a naplókban lévő adatokhoz való hozzáférést a szükséges személyekre kell korlátozni.
Az érintettek a naplófájlokhoz csak akkor férhetnek hozzá, ha azt a munkakörük feltétlenül megkívánja.

A megfogalmazott naplózási célok jellemzője, hogy azok eléréséhez adatokat nyerünk ki az összegyűjtött adattengerből. A naplófájlok elemzés nélküli gyűjtése és archiválása minimális hozzáadott értéket képvisel csak, ráadásul számos előírás megköveteli azok rendszeres áttekintését. Növeli a befektetések megtérülését, ha nemcsak egy szűk terület igényei szerint elemezzük az adatokat, hanem más területek szempontjait is figyelembe vesszük.

© 2014 KPMG Tanácsadó Kft, a magyar jog alapján bejegyzett korlátolt felelősségű társaság, és egyben a független tagtársaságokból álló KPMG-hálózat magyar tagja, amely hálózat a KPMG International Cooperative-hez ("KPMG International"), a Svájci Államszövetség joga alapján bejegyzett jogi személyhez kapcsolódik. Minden jog fenntartva.

Legjobb gyakorlatok a privilegizált felhasználók kezelésében

A következőkben összefoglaljuk azokat az elveket, amelyeket a privilegizált felhasználók felügyelete kapcsán javaslunk. Természetesen ezek akár az összes felhasználóra alkalmazhatóak, ha a kockázatkezelési szempontok ezt szükségessé teszik.

Megőrzési szabályok kialakítása

A naplók megőrzési idejét több tényező is befolyásolja. A biztonsággal kapcsolatos naplóüzeneteket érdemes hosszabb ideig megőrizni, mint a működési naplókat. Sok törvényi előírás vagy szabvány konkrét követelményeket ír elő naplófájlok megőrzésére. Ezen követelmények megértése révén alakítható ki, hogy mely adatot meddig szükséges tárolni. Gondos tervezés nélkül már tárhely szempontjából is kihívásokkal szembesülhet a szervezet.

A naplózás szabályozása

Mint minden területet, így a naplózást is szabályozni kell, hogy a feladatok, felelősségek tisztázva legyenek. A szervezet jogi és szabványi környezetének változásai, az új rendszerek vagy rendszerfunkciók, a potenciális naplóforrások mind-mind a naplózásra vonatkozó szabályozás folyamatos frissítését igénylik.

Hozzáférés szabályozása

Természetesen a hozzáférés-kezelést is formális szabályozás és folyamatok mentén kell felépíteni. Ezek kialakításakor mindenképpen a vonatkozó törvényi és szabványi előírásokat kell figyelembe venni, és gyakran a privilegizált jogosultsággal rendelkező felhasználókat külön is érdemes szabályozni.

Minimális jogosultság biztosítása

Minden felhasználó, így a kiemelt felhasználók is csak olyan jogosultságokkal rendelkezzenek, amelyek feltétlenül szükségesek a feladataik elvégzéséhez. A rendszeradminisztrátoroknak is csak azon rendszerekhez legyen hozzáférése, amelyek ezt megkövetelik üzleti és üzemeltetési szempontból.

„God" mód használata csak vészhelyzetben

A rendszerek beépített adminisztrátorai (például „root", „administrator", „system") a napi munkavégzéshez alapvetően nem szükségesek. Érdemes az ezekhez való hozzáférést korlátozni, és a használatukat szigorúan kontrollálni.

Nevesített felhasználók használata

A személyes felelősségre vonhatóságot csak a nevesített felhasználók használata teremti meg. Fel kell mérni, hol és kik használnak nem nevesített felhasználókat, és ezen eseteket milyen módon lehet megszüntetni. Ha a megosztott felhasználók technikai okok miatt szükségesek, meg kell vizsgálni, hogy milyen kompenzáló megoldással lehet a kockázatukat csökkenteni.

Központi felhasználó-felügyeleti rendszer bevezetése

A naplókezelő-rendszerek nem minden esetben alkalmasak a privilegizált felhasználókhoz kapcsolódó események, illetve az általuk végzett tevékenységek rögzítésére. Ezt a rést hidalják át a kiemelt tevékenység-felügyeleti rendszerek (Privileged Activity Monitoring – PAM), melyek részletesen és visszakövethető módon rögzítik a privilegizált felhasználókkal végzett tevékenységeket. A fejlettebb megoldások működése transzparens, így bevezetésük a napi munkavégzést nem befolyásolja.

Erős autentikáció a kiemelt felhasználók esetén

Amikor egy privilegizált felhasználó fér hozzá a rendszerhez, a megfelelő erősségű és biztonságú azonosítás különösen fontos, hiszen a felhasználó jelentős hatással lehet a rendszer működésére. Vannak olyan PAM-rendszerek, amelyek alapértelmezetten támogatják a magasabb biztonságot nyújtó autentikációs megoldásokat. Ugyanakkor vannak rendszerek, amelyek ezt nem támogatják. Ez esetben kiegészítő megoldásra van szükség.

Valós idejű védelemi mechanizmusok kialakítása

Érdemes megvizsgálni, hogy a privilegizált felhasználóknak van-e joguk olyan funkciókhoz és/vagy adatokhoz, amelyek csak esetenként szükségesek, de mégis kockázatot jelentenek a szervezet számára. Ha vannak ilyenek, védelmi megoldásokat kell kialakítani. Az utólagos naplóvizsgálatoknál nagyobb hozzáadott értéket képviselnek az olyan felhasználóitevékenység-felügyeleti rendszerek, amelyek akár valós időben riasztanak, vagy megakadályozzák egyes nem kívánt parancsok végrehajtását.

© 2014 KPMG Tanácsadó Kft, a magyar jog alapján bejegyzett korlátolt felelősségű társaság, és egyben a független tagtársaságokból álló KPMG-hálózat magyar tagja, amely hálózat a KPMG International Cooperative-hez ("KPMG International"), a Svájci Államszövetség joga alapján bejegyzett jogi személyhez kapcsolódik. Minden jog fenntartva.

Zárszó

Az informatikai szolgáltató szervezeteknek (beleértve a felhőszolgáltatókat is) számos adatvédelmi előírást és szabványt figyelembe véve kell végezniük a feladataikat. Az ISO27001:2013, a PCI-DSS (Cloud Computing Guidelines), a Cloud Security Alliance Security Trust & Assurance Registry és a SSAE 16/ISAE 3402 szabványok hasonló naplókezelési és hozzáférés-kezelési elvárásokat támasztanak. Elvárás az ügyféladatok biztonságának folyamatos fenntartása, a hatékony és kontrollált felhasználó-kezelés kialakítása, a privilegizált felhasználók fokozott felügyelete és a rendszerekben végezett tevékenységek naplózása. Mindez egy komplex és kiterjedt informatikai rendszerben megköveteli az ezen célokat támogató eszközök/szoftverek bevezetését. Ezen támogató eszközök nemcsak a követelmények teljesülését biztosítják, hanem bizonyítékot is szolgáltatnak a megfelelőségi auditok során, erősítve ezzel a szolgáltatók biztonsági megfelelését és ügyfelek bizalmát.

Melléklet – Szabvány-összerendelés

Követelmény	Vonatkozó ISO27001:2013 szabványpontok	Vonatkozó PCI-DSS v3.0 szabvány	Vonatkozó CCM v3.0 szabványpontok
Privilegizált felhasználók kezelése	A.9.2.3	10.2	IAM-02; IAM-05
Autentikációs követelmények betartása	A.9.2.4; A9.4.2	8.1; 8.2	IAM-12
Hozzáférések rendszeres felülvizsgálata	A.9.2.5	8.5	IAM-08; IAM-10
Hozzáférések korlátozása	A9.4.1	7.1; 7.2	IAM-03; IAM-13
Forráskódokhoz való hozzáférés korlátozása	A9.4.5	7.2	IAM-06
Naplófájlok hozzáférés-védelme	A12.4.2	10.5	IVS-01;
Naplófájlok védelme módosítás, törlés ellen	A12.4.2	10.5	IVS-01;
Naplóbejegyzések központi gyűjtése	A12.4.2	10.5	IVS-01;
Naplófájlok kötelező megőrzése a szükséges ideig	A12.4.2	10.7	IVS-01; BCR-12

© 2014 KPMG Tanácsadó Kft, a magyar jog alapján bejegyzett korlátolt felelősségű társaság, és egyben a független tagtársaságokból álló KPMG-hálózat magyar tagja, amely hálózat a KPMG International Cooperative-hez ("KPMG International"), a Svájci Államszövetség joga alapján bejegyzett jogi személyhez kapcsolódik. Minden jog fenntartva.

Kapcsolat

Sallai György
igazgató
T.: +36 1 887 6620
E.: gyorgy.sallai@kpmg.hu

Biczók Sándor
menedzser
T.: +36 1 887 7293
E.: sandor.biczok@kpmg.hu

kpmg.hu

Az itt megjelölt információk tájékoztató jellegűek, és nem vonatkoznak valamely meghatározott természetes vagy jogi személy, illetve jogi személyiség nélküli szervezet körülményeire. Társaságunk ugyan törekszik pontos és időszerű információkat közölni, ennek ellenére nem vállal felelősséget a közölt információk jelenlegi vagy jövőbeli hatályosságáért. Társaságunk nem vállal felelősséget az olyan tevékenységből eredő károkért, amelyek az itt közölt információk felhasználásából erednek, és nélkülözik társaságunknak az adott esetre vonatkozó teljes körű vizsgálatát és az azon alapuló megfelelő szaktanácsadást.

A KPMG név, a KPMG logó és a „cutting through complexity" a KPMG International lajstromozott védjegye.

© 2014 KPMG Tanácsadó Kft, a magyar jog alapján bejegyzett korlátolt felelősségű társaság, és egyben a független tagtársaságokból álló KPMG-hálózat magyar tagja, amely hálózat a KPMG International Cooperative-hez ("KPMG International"), a Svájci Államszövetség joga alapján bejegyzett jogi személyhez kapcsolódik. Minden jog fenntartva.