BalaBit IT Security

WHITEPAPER

ISO 27001

Teljesítsük a Lehetetlent!

Üzemeltetés Ellenőrzés és Audit

Írta: Dellei László, CISA, CGEIT, CRISC, ITIL-F, ISO 27001 LA

Tartalomjegyzék

Vezetői összefoglaló

Az élesedő piaci verseny mellett egyre több cég számára jelent kihívást, hogy megfeleljen az ISO, a PCI DSS, a SOX, a HIPAA, a Basel II, vagy egyéb törvényi előírások követelményeinek. Az informatikai rendszerek biztonságát érintő előírások nagyon szigorúak, a biztonságirányítási rendszer kézenfekvő megvalósítása lehet azonban az ISO/IEC 27001:2005-ös (továbbiakban ISO 27001) szabvány implementálása. A dokumentum bemutatja, hogy a menedzsmentnek milyen feltételeknek célszerű megfelelni az ISO 27001-es tanúsítvány megszerzéséhez, és ez milyen üzleti előnyökkel jár a szervezetnek. Megvizsgáljuk, milyen legjobb és legrosszabb gyakorlatok léteznek az ISO 27001 bevezetése és működtetése kapcsán, és ajánlásokat fogalmazunk meg a közép és felső-vezetés számára.

Az adatlopások, informatikai visszaélések száma mára példátlan méreteket öltött, s az adatok nem megfelelő védelme súlyos anyagi károkat és presztízsveszteséget okozhat minden szervezet számára. Mindezek megelőzése csak a kontroll rendszer teljessé tételével oldható meg. A világ vezető kutatócégei, a Gartner és a Forrester is egyet értenek abban, hogy a megelőzés költségei sokkal kisebbek, mint egy sikeres támadás, adatlopás utáni helyreállítás költségei.

Az ISO 27001 alapú információbiztonság irányítási rendszer bevezetése jelentős erőforrásokat követel meg a szervezettől, de ha jól végzik, jelentős üzleti előnyt is hozhat. Az „ISO 27001 certified" minősítés megnöveli az ügyfelek és partnerek bizalmát, elősegíti és biztonságosabbá teszi az elektronikus adat és információcserét. A vezetőség elkötelezettsége nélkül azonban nem valósítható meg egy ilyen szigorú rendszer, a menedzsmentnek anyagilag és erkölcsileg (szabályzatok betartatása) is támogatnia kell a biztonságot, egyértelművé kell tenni, hogy a biztonság megteremtése nem kizárólag az IT feladata és felelőssége.

Az ISO 27001 szabvány előírásait azonban csak specializált IT eszközökkel lehet maradéktalanul teljesíteni, melyekben a BalaBit által szállított biztonsági megoldások segítséget nyújthatnak.

A BalaBit syslog-ng naplózó rendszere lehetővé teszi, hogy folyamatos és hiteles adatokat lehessen gyűjteni a rendszereink kritikus folyamatairól, amivel kielégíthető az előírás „monitoring" eljárást és eszközt előíró pontja. Manapság szinte minden fórumon elhangzik, hogy a legnagyobb biztonsági kockázatot az ember jelenti, s közülük is leginkább a kiemelt felhasználók ellenőrzése valósítható meg nehezen – erre nyújthat megnyugtató megoldást a BalaBit Shell Control Box nevű terméke, ami az adminisztrátori tevékenységről, illetve a titkosított csatornák forgalmáról is rögzít minden információt.

Mission: Impossible

Jelen esetben a „lehetetlen küldetés” nem informatikai szakkifejezés, hanem egy sikeres akciófilm címe. Hogy kerül ez ide? Az IT vezető van ma hasonló helyzetben, mint egy akciófilm főhőse: a helyzet percről percre változik, mindig máshonnan jön valamilyen váratlan esemény, külső támadások, mesterkémek, belső ellenség. A támadóknál ott a csúcstechnika. Sokan vannak. Az adatainkra vadásznak. S az IT vezetőnek mindig harcra készen, folyamatosan résen kell lenni, ismerni az ellenség minden lépését, azonnal akcióba lépni. De neki be kell tartania a szabályokat. Azok az álmatlan éjszakák…

Tényleg ez lenne a sorsa a ma informatikai menedzserének?

A helyzet ennél bonyolultabb, de már sok fenyegetettségre van jó megoldás. Mindamellett, hogy az informatikai rendszereket védeni kell, szervezettől, iparágtól függően különböző elvárásoknak, törvényi előírásoknak is eleget kell tenni, elsősorban a pénzintézetek és tőzsdei cégek esetén. Sok cég számára jelent kihívást, hogy megfeleljen az ISO, a PCI DSS, a SOX, a HIPAA, a Basel II, vagy egyéb előírások követelményeinek. Az üzleti világban a megbízhatóság, átláthatóság, a jó hírnév megőrzése kézzelfogható, versenyelőnyként megnyilvánuló érték, ezért is törekszik a legtöbb vállalkozás arra, hogy a prudens, szabványokon alapuló, kiszámítható működését deklarálja, s megszerezze a különböző ISO szabványok szerinti tanúsításokat. Elsőként az ISO 9001-es minőségirányítási (minőségbiztosítási) rendszer tanúsítványát szokták beszerezni a vállalkozások, de a vezető vállalatok számára a megbízható informatikai működés is kulcskérdés. Biztosítani kell a folyamatos működést, védeni kell az üzleti információt, az ügyféladatokat.

2011 tavaszának legnagyobb informatikai botránya a Sony-nál bekövetkezett adatlopás, ahol feltételezések szerint összesen mintegy 100 millió felhasználó bizalmas adatai kerültek illetéktelenekhez. Az adatok neveket, lakcímeket, e-mail címeket, születési dátumokat és bankkártya információkat is tartalmazhattak – e cikk megírásának idején még nem tisztázódott minden részlet, de egy bizonyos, a tőzsdén azonnal 4%-ot estek a Sony amúgy is megtépázott részvényárfolyamai, s jelen pillanatban nem látni, hogy milyen hosszabb távú veszteség következhet be – egy biztos, a Sony nem ilyen reklámot szeretett volna.

A megoldást egy szabványos, ellenőrzött és minden elemében jól működő információbiztonsági irányítási rendszer, az angol rövidítéssel ISMS (Information Security Management System) bevezetése jelentheti. Ennek legfontosabb követelményeit fogalmazza meg a Nemzetközi Szabványügyi Testület (ISO) által kibocsátott ISO/IEC 27001-es szabvány: „Informatika. Biztonságtechnika. Az információbiztonság irányítási rendszerei. Követelmények”

Hogyan lehet megteremteni a biztonságos működés feltételeit, s milyen feltételeket kel teljesíteni a 27001-es tanúsítvány megszerzéséhez? A legtöbb előírásra vannak bevált megoldások, megteremthető a fizikai biztonság, lehet tartalék rendszereket biztosítani, de vannak olyan problémák, melyek egyszerű kezelése eddig nem volt megoldott, sok emberi ráfordítást igényel. A szabvány implementálása során ugyanis az egyik legnagyobb kockázatot a kiemelt felhasználók, rendszer-adminisztrátorok munkájának ellenőrzése jelenti.

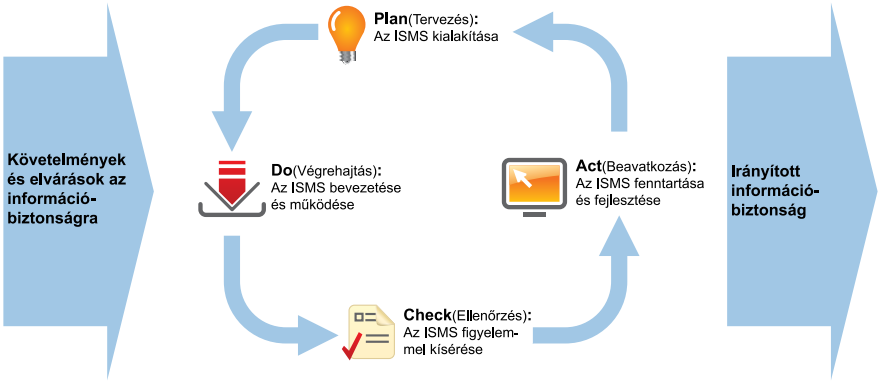
- Hogyan lehet kontrollálni egy olyan felhasználó tevékenységét, akinek mindenhez joga van?
- Hogyan követhető a kiszervezett rendszerek adminisztrációs tevékenysége?
- Hogyan lehet az erős titkosítású protokollok (SSH, VPN, SSL/TLS stb.) alatt végzett fájlműveleteket ellenőrizni?
- Hogyan lehet megbízhatóan dokumentálni a rendszer eseményeit?
- Hogyan lehet bizonyítékokat gyűjteni egy audithoz, hogyan lehet észlelni, és megelőzni a rendellenes tevékenységeket?
- Hogyan lehet egy esetleges csalást, visszaélést bizonyítani, hiteles bizonyítékokat gyűjteni, és biztonságosan tárolni?
- Hogyan lehet egy incidens okát utólag, a leggyorsabban feltárni, és a normál működést mielőbb helyreállítani?

Mindezeket az ellenőrzéseket a szabvány előírja, s ma már megvalósításuk is egyszerűen lehetséges. A BalaBit által fejlesztett syslog-ng naplózó termékcsalád lehetővé teszi valamennyi fontos rendszer napló állományának gyűjtését és a keletkezési helytől független, hiteles, időpecséttel ellátott tárolását. A kiemelt jogosultságú felhasználók tevékenységét a BalaBit másik megoldása, a Shell Conrol Box (SCB) felügyeli és auditálja. A távoli hozzáférések titkosított protokolljaiba „lát bele", így ellenőrizhetővé, követhetővé és auditálhatóvá válik a rendszer-adminisztrátorok valamennyi tevékenysége és az adatok mozgatása.

Megfelelőségi elvárások az ISO 27001 szabványban

Az informatikai biztonsági irányítási rendszer nemzetközi szabványai egy követendő működési modellt határoznak meg.

Az információbiztonság irányítási rendszer középpontjában a követelményeket meghatározó 27001-es szabvány áll. A rendszer bevezetése során létre kell hozni egy folyamat szemléletű biztonsági modellt, amely magában foglalja a rendszer állandó karbantartását, felülvizsgálatát, ami a napra készen tartott, működő rendszer záloga. Az általánosan használt PDCA (Plan, Do, Check, Act) modellt kell megvalósítani.



A lérehozás, karbantartás és fejlesztés ciklusa

A vezetőség elkötelezettsége nélkül nem valósítható meg egy ilyen szigorú rendszer, a menedzsmentnek anyagilag és erkölcsileg (szabályzatok betartatása) is támogatnia kell a biztonságot, egyértelművé kell tenni, hogy a biztonság megteremtése nem kizárólag az IT feladata és felelőssége. Az információbiztonsági előírásoknak integrálódniuk kell a szervezet szabályzati rendszerébe.

A 27001-es szabvány előírásait belső szabályozásokban kell megkövetelni, s a bevezetési folyamatot is dokumentálni kell. A dokumentálás célja, hogy követhető legyen a szabályozások és a kockázatértékelések és kockázatjavítási eljárások közötti összefüggés.

Az általános biztonságpolitikai szabályozáson túl létre kell hozni az üzemeltetéssel és ellenőrzéssel összefüggő specifikus szabályokat, leírásokat is, s azt a folyamatot, amely biztosítja a szabályozások napra készen tartását és azt, hogy valamennyi érintett munkatárs megismerje és elfogadja a rá vonatkozó szabályokat.

A szervezet létrehozása, illetve átalakítása során gondoskodni kell arról, hogy minden munkatárs csak a munkája ellátásához minimálisan szükséges jogosultságokat kapja meg, s az információbiztonsági folyamatok kialakításánál szét kell választani a végrehajtói és ellenőri szerepköröket (Segregation of Duties). A védendő adatok körének és az adatok veszélyeztetettségi besorolásának meghatározása az üzleti oldal felelőseinek, az adatgazdáknak a feladata.

A vezetőség ellenőrzési feladatait egy jól kialakított belső audit rendszernek kell támogatni. A jól működő biztonságirányítási rendszernek kulcseleme a javító és megelőző intézkedések (corrective and preventive controls) rendszerének felállítása. A megfelelően kialakított folyamat során az eltérések és azok okainak azonosítása megtörténik, a szükséges intézkedések meghozatala és azok végrehajtásának ellenőrzése biztosított.

Az ISO 27001 alapú információbiztonság irányítási rendszer kialakítása során kockázati megközelítést kell alkalmazni. Olyan kockázat-felmérési módszertant kell választani, ami illeszkedik a szervezet céljaihoz, követelményeihez és biztosítja azt, hogy az egymást követő kockázatértékelések során összehasonlítható és megismételhető eredmények álljanak elő. Azonosítani kell azokat a hatásokat, amelyek a szervezet információs vagyonát veszélyeztetik, megsértik azok bizalmasságát, sértetlenségét és rendelkezésre állását – ezek az úgynevezett CIA elvek, a követelmények angol megfelelőjének kezdőbetűi alapján: Confidentality, Integrity, Availability.

A rendszer implementálása során kialakítandó kontrollok rendelkeznek egyebek mellett az információbiztonsági szervezet kialakításáról, az információk osztályozásáról, a munkatársak és külső partnerek menedzseléséről, a berendezések biztonságáról és a fizikai védelemről is. Ezek a könnyebben megvalósítható elemei a biztonságirányítási rendszernek, hiszen kézzel fogható, látható dolgokról van szó: szabályzatokat kell létrehozni, annak megfelelően működtetni a szervezetet, a fizikai biztonsági architektúrát az elvárások szerint kell kialakítani, vírus- és behatolás-védelmi rendszert kell telepíteni.

Sokkal nehezebben megfogható azonban az A10-es szabályozási cél, illetve ennek egyes elemei, amelyek a kommunikáció és üzemeltetés irányítását írják elő. Az „üzemeltetési eljárások és felelősségi körök szétválasztása” során a visszaélések lehetőségét csökkenteni kell. A 10.2 pont rendelkezik arról, hogy „a harmadik felek által nyújtott szolgáltatásokat, jelentéseket és feljegyzéseket rendszeresen figyelemmel kell kísérni és át kell vizsgálni, valamint rendszeres auditjukat is el kell végezni. Ez egy outsource-olt, távolról végzett rendszermenedzsment esetén eddig nehezen volt megvalósítható, az esetek többségében az ellenőrzés jó esetben is csak évente egy auditban nyilvánult meg, de az auditor akkor sem tudta a tényleges tevékenységeket kontrollálni, legfeljebb arról tudott meggyőződni, hogy rendszeresen történik valamilyen tevékenység. Megfelelő eszköz támogatása nélkül a feladat a rendszerek eszközeivel nem

kivitelezhető, szükség van egy olyan audit és felügyelő eszközre, amellyel a feladat megvalósítható. Ebben segít a BalaBit Shell Control Box megoldása, amivel a távoli rendszermenedzsmenthez szükséges hozzáférések pontosan kontrollálhatóak és auditálhatóak, akár egyedileg engedélyezhetőek. A rendszergazdák tevékenysége filmszerűen visszanézhető, vagy akár valós időben is követhető és ellenőrizhető.

Sok fejfájást okoz az informatikai vezetőknek a szabvány A10.10 pontja is, amely a figyelemmel követést (monitoring) írja elő. Naplózni kell a felhasználói és a rendszer-adminisztrátori tevékenységeket is, s gondoskodni kell arról, hogy naplóban rögzített információk védettek legyenek a szakszerűtlen kezeléstől (értsd: módosítástól és törléstől) és az illetéktelen hozzáféréstől. A rendszer-adminisztrátorok tevékenységét rögzítik az egyes rendszernaplók, de az adminisztrátorok hozzáférnek ezekhez az állományokhoz, s akár módosítani vagy törölni is tudják ezeket úgy, hogy később azt nem lehet kideríteni. A megoldást a naplófájlok platformtól független, hitelesített gyűjtése és tárolása jelenti, amelyre olyan speciális eszközt célszerű használni, mint például a syslog-ng naplózó rendszer. A syslog-ng platformok és operációs rendszerek széles skáláját támogatja, és képes a naplóüzenetek megbízható, titkosított továbbítására és tárolására is.

A szabvány A11-es pontja, amely a hozzáférés ellenőrzésről rendelkezik, szintén csak részben tartható be a hagyományos rendszereszközökkel, ugyanis az „előjogokkal" rendelkező, privilegizált felhasználók, adminisztrátorok tevékenysége nem követhető megbízhatóan, ugyanis ezek a felhasználók az adott rendszeren az őket felügyelni hivatott eszközökhöz is hozzáférhetnek (A11.2.2.). A hálózati szintű hozzáférés ellenőrzése, különösen a szervezet határain túlnyúló csatlakozások esetén szintén problémás, pedig jellemzően távoli eléréssel dolgozik sok kiszervezett szolgáltató, és a szervezet saját munkatársai is kezelhetnek érzékeny adatokat titkosított csatornákon keresztül. Az ellenőrzés a szokásos rendszer eszközökkel nehezen valósítható meg, de a Shell Control Box itt is segítséget nyújthat, mivel a felügyelt rendszerektől független és transzparensen működő eszközként az ellenőrzött felhasználók nem férhetnek hozzá, és a titkosított csatornák ellenőrzésére és auditálására is képes.

A 27001-es szabvány rendelkezik az információbiztonsági incidensek kezeléséről is. Ahhoz, hogy akár polgári, akár büntetőjogi felelősségre vonást lehessen alkalmazni egy visszaélés esetén, megfelelő, hiteles bizonyítékokat kell gyűjteni az eseményekről, melyeknek a megőrzését, védelmét is biztosítani kell. Az általános rendszer eseményekről a naplózó rendszer megbízhatóan gyűjtött, titkosítottan és autentikáltan továbbított, időpecséttel ellátott, utólagos megváltoztatástól védetten tárolt adatai szolgáltathatnak bizonyítékot. Az adminisztrátori tevékenységekről és a titkosított csatornák forgalmáról pedig az SCB gyűjt hiteles információt, visszanézhetővé, kereshetővé, és számon kérhetővé változtatva az adminisztrátorok munkáját.

Ha a szervezet sikeresen kialakította és működteti a szabvány szerinti szabályzati és kontroll rendszerét, a kialakított ISO 27001 alapú információbiztonság irányítási rendszert időközönként ellenőrizni kell. A belső auditok tervezett időközönként történnek annak meghatározására, hogy a szervezet intézkedései, folyamatai megfelelnek-e a szabvány követelményeinek, a vonatkozó jogszabályoknak és a belső szabályozásnak. Az „ISO 27001 certified" minősítés elnyeréséhez egy külső, erre felhatalmazott szervezet által végzett minősítő audit szükséges, melyet évente meg kell ismételni.

Kapcsolatok más szabványokkal, iparági gyakorlatokkal

Annak ellenére, hogy az ISO 27001 az információbiztonság nemzetközi szabványa, s alapvetően meghatározza az információbiztonsági irányítási rendszer feltétlenül szükséges alapjait, nem élvez kizárólagosságot, mellette sok egyéb, az információbiztonságot támogató keretrendszer, legjobb gyakorlat és egyéb szabvány terjedt el. Az ISO 27001-nek nagy előnye, hogy a megfelelés hivatalosan tanúsíttatható.

Az egyes szakmai területeken más-más biztonsági követelményrendszerek alakultak ki, melyek esetleg az egyes részleteket pontosabban előírják, de szemléletileg nem különböznek a 27001-től.

A pénzügyi területekre vonatkozik talán a legtöbb információbiztonsági előírás, a visszaélések megakadályozása érdekében. Legfontosabbak ezek közül a PCI DSS, a SOX, a HIPAA, a SAS70, és a GLBA. A felsoroltak közül van olyan is, amelyik részletekbe menően határozza meg a technikai követelményeket, mint a bankkártyaadatok és tranzakciók biztonságára vonatkozó PCI DSS, és olyan is, mint a SOX, amely az amerikai tőzsdei cégekre ír elő részletes megfelelési követelményeket, de pontos informatikai előírásokat nem fogalmaz meg. A legtöbb elvárásban közös, hogy az ellenőrizhetőséget, átláthatóságot, dokumentálást, naplózást, és a kritikus tevékenységek kontrollját szigorúan megkövetelik.

A technológiai fejlődés, a rendszerek bonyolultsága olyan szintre emelte a nagyvállalati informatikai környezeteket, hogy egyszerű eszközökkel, specializált szaktudás nélkül nem átláthatók. A fenyegetettségek közül egyre inkább nő a belső fenyegetettség, fokozódik az igény a kritikus információkkal rendelkező munkatársak ellenőrzésére, hiszen növekvő számban kerülnek ki bizalmas adatok a szervezetektől a belső munkatársak rosszindulatú tevékenysége révén. Égető szükség van egyszerűen integrálható, folyamatos megfigyelést biztosító hiteles, független audit megoldásokra. Nagyobb rendszerek esetén naponta több millió rendszerüzenetből kell kiválasztani az üzemeltetést is támogató, minőségileg értékelt információkat.

Az elvárások ilyen szintjén csak automatizált, könnyen integrálható rendszerek jelenthetnek megoldást.

A BalaBbit syslog-ng naplózó rendszere könnyű integrálhatóságával biztosítja, hogy a meglévő komplex infrastruktúrához is illeszteni lehessen. A titkosított, aláírt, időpecséttel ellátott naplóadat-gyűjtés értékes adatokat nyújt az üzemeltetetés támogatásához, de alkalmas belső auditok, felügyeleti, hatósági vizsgálatok esetén, és az előírásszerű naplózási követelmények kielégítésére.

A Shell Control Box a naplózáson túlmenően, a kritikus adminisztrátori tevékenységek felügyeletéhez nyújt közvetlen segítséget, lehetővé teszi a távoli felügyeletet ellátó support tevékenység direkt ellenőrzését, kontrollt nyújt a rosszindulatú hozzáférések ellen, folyamatos auditot biztosítva a kritikus tevékenységek felett.

Praktikák – a 7 legrosszabb és a 7 legjobb gyakorlat

Az ISO 27001 bevezetés és auditálás, a 133 követelmény útvesztője sok problémát vet fel, melyeknek a megoldása könnyebb, ha már a mások által kitaposott utat követjük, s nem esünk bele a leggyakoribb csapdákba. Egyes pontok jól átláthatók, például a szabályozások, folyamatok kialakítása, vagy a fizikai biztonság megteremtése könnyen követhető folyamat. Igazi nehézséget a rendszerfelügyelet és naplózás, a hozzáférések és tevékenységek ellenőrzése, a harmadik felek szolgáltatásnyújtásának menedzselése s az audit bizonyítékok hiteles gyűjtése jelent.

Számos audit során tapasztaltuk, hogy a szervezet IT biztonságért felelős munkatársai is úgy gondolták, hogy egy célalkalmazás bevezetésével eleget tettek a korábban említett felügyeleti elvárásoknak, anélkül, hogy a rendszerben rejlő lehetőségeket kihasználták volna. A szabványoknak, követelményeknek csak akkor felel meg egy kontroll rendszer, ha az a követelményeknek megfelelően be is van állítva, például egy naplózó rendszernél nem elegendő hetente ránézni az sztenderd listákra, napi gyakorisággal kell elemezni a rendellenességeket, s a problémák – legyenek azok üzemeletetési hibák vagy visszaélések – korai észleléséhez megfelelő riasztásokat kell definiálni.

Az is gyakori tévhit, hogy egy biztonságot támogató rendszer, alkalmazás bevezetése után megpihenhetnek a szakemberek. A biztonság magas szintje csak a módszerek, eljárások folyamatos követésével, karbantartásával biztosítható.

Az ISO 27001-es rendszer, illetve a monitoring eszközök bevezetésekor egyes esetekben a cégek pénzügyi vezetői számon kérik az IT vezetőtől a megtakarításokat, az azonnali költségcsökkentést. Ilyen esetben valószínűleg rosszul volt kommunikálva a projekt és várható eredményei, ugyanis legtöbbször az addig ellátatlan funkciókat pótolták egy biztonsági rendszerrel, viszont nem kellett például három szakértőt felvenni ahhoz, hogy a követelményeknek úgy-ahogy eleget tegyenek.

Az alábbiakban kiemeltünk néhány szempontot a biztonságirányítási és kontroll rendszerek bevezetési tapasztalataiból, melyek talán a legfontosabb tevékenységek.

Adatbiztonsági szempontból a 7 legjobb gyakorlat

1. **Biztonsági kockázatok azonosítása,és értékelése.**
2. **A információbiztonság irányítási rendszer (ISMS) kiterjedésének meghatározása** –szereplők, eszközök pontos azonosítása.
3. **Üzletmenet folytonossági- és helyreállítási tervek kidolgozása** és rendszeres tesztelése
4. **Központi monitoring (naplókezelő) rendszer** bevezetése.
5. **Rendszeres audit és automatikus log-elemzés;** riasztások kritikus események fellépésekor.
6. **Funkcionális szerepkörök kidolgozása, az összeférhetetlenségek megállapítása** (Segregation of Duties, SOD).
7. **Adatszivárgási (adatvesztési, adatlopási) kockázatok elemzése,** rendszer-adminisztrációs tevékenységek szoros felügyelet alá vonása.

Elrettentésképpen álljon itt a 7 legrosszabb gyakorlat

1. **Mi megbízunk az adminisztrátorainkban, becsületes emberek!** Ez valószínűleg igaz, de az ellenőrzés nem nélkülözhető! A távoli eléréssel dolgozó külsős partnerek felügyeletét a szabványok előírják.

2. **Nem kell bevezetési támogatás a naplóelemző rendszernél, mert úgyis egyszerű a felület!** Nem javasoljuk, mert a monitoring és audit rendszerek finomhangolása szakértelmet és tapasztalatot igényel.

3. **A rendszereim szállítója megmondja, hogy milyen információ szükséges, úgyis jobban ért hozzá!** Nem igaz! Mindenképpen kell a belső szakértők közreműködése és a jogi terület bevonása is.

4. **Kevesen vagyunk, mindenkinek megvan a jogosultsága mindenhez, hátha szüksége lesz rá!** Nagyon veszélyes! A kontroll funkciók még akkor is szükségesek, ha nem merül fel visszaélés lehetősége, mert a tévedések ellen is védenünk kell a rendszereket.

5. **Közös jelszavakat használunk, hiszen mindenki ugyanazt csinálja!** A megosztott adminisztrátori jelszavak, csoportos felhasználói azonosítók használata esetén nem deríthetők fel a visszaélések elkövetői.

6. **A 27001-es projektre csak IT-s embereket allokáltunk, úgyis ők értenek hozzá!** Hangsúlyt kell helyezni arra, hogy az informatikai biztonság nem csak IT projekt, üzleti részvétel és vezetői elkötelezettség nélkül nem működik.

7. **Megvan az ISO 27001 tanúsítvány, most egy évig nincs semmi teendőnk az információbiztonsággal!** Nem igaz! Folyamatos tevékenységet igényel a megfelelőségi állapot, a védettség fenntartása.

Üzleti előnyök

A hírekben napi gyakorisággal szerepel, hogy adatlopások következtek be tőzsdén is jegyzett nagyvállalatoknál.

Egy rövid felsorolás az utóbbi évek legnagyobb ismert visszaéléseiből, adatvesztéseiből és adatlopásaiból:

Év	Cég	Érintett adatok mennyisége	Következmények
2011. május	Sony	100 millió ügyféladat	Részvény árfolyam csökkenés, várhatóan 2 milliárd dollár kiesés és egyéb költség
2011. január	Fehér Ház, USA	250 ezer személyes adat	Presztízsveszteség, anyagi károk
2009	Heartland Payments Systems	100 millió bankkártya adat	Tőzsdei árfolyamesés, majd a cég megszűnése
2008-2009	RBS Worldpay	1,5 millió kártya adat	Tőzsdei árfolyamesés, nagy anyagi veszteség
2007	Deutsche Telekom	17 millió ügyféladat	Reputáció romlása
2005	Cardsystem Solutions	40 millió ügyféladat	Cég megszűnése

Ismereteink szerint hazánkban is történnek – történtek visszaélések az adatokkal, de ezek eddig viszonylag kevés ügyfelet érintettek s a felelős cégek igyekeztek eltitkolni az eseményeket.

Néhány érdekes statisztikai adat a visszaélésekről, tények százalékokban:

17% A jelentős adatlopások, támadások mintegy 17 %-át belső munkatársak követték el. (Data Breach Investigations Report 2011, Verizon)

72% Az alkalmazottak közel háromnegyede tulajdonított már el adatot a munkahelyéről. (Index.hu)

86% A biztonsági visszaélések 86 %-át nem veszi észre az érintett cég, hanem harmadik fél figyelmezteti rá.

96% Az esetek 96 százalékában megfelelő kontrollok alkalmazásával egyszerűen megelőzhető lett volna a visszaélés. (Data Breach Investigations Report 2011, Verizon)

Elgondolkoztató számok! Nem csak az Internet felé kell figyelni, hanem az alkalmazottakra is, hiszen a „nagy" visszaélések egyötödét belső alkalmazottak követték el, azok a rendszergazdák, bizalmi IT-s munkatársak, akiknek feladatuk lett volna őrködni az adatok biztonsága felett. Az érintett cégek nem tudták a kellő rendszerességgel és alapossággal ellenőrizni munkatársaikat. Mi a kellő rendszeresség és alaposság? Egyszerű: ellenőrizzünk mindig, folyamatosan, és minden kritikus folyamatot.

A megdöbbentő, hogy az adatlopást az érintett cégek legtöbbször maguk nem is vették észre, mert nem volt rá megfelelő eszközük.

A bizalmas adatok nyilvánosságra kerülése részben közvetlen kárt okoz, hiszen finanszírozni kell a vizsgálatokat, leáll a normál üzletmenet, a károkat meg kell téríteni, büntetéseket kell fizetni. A közvetett károk ugyanakkor sok esetben sokkal súlyosabbak lehetnek, mert egy ilyen visszaélés nyilvánosságra kerülése hosszú távon hathat az üzletmenetre, a cég elveszti jó hírnevét, a tőzsdei árfolyama csökken, de volt olyanra is példa, hogy a vállalat egy ilyen adat-kompromittálódás után tönkrement.

A Gartner elemzése szerint, az adatokat érintő biztonsági események utáni elhárító és kompenzáló intézkedések legalább ötször annyiba kerülnek, mint a megelőzésükhöz szükséges informatikai eszközök, melynek eleme például a naplózó rendszer, IDS/IPS rendszer, vagy a folyamatos auditot támogató eszköz. A megállapítás szerint, egy szervezet, amely tízezer ügyfélszámlával rendelkezik, számlánként közel 16 dollárt költ a megfelelő biztonsági architektúra kialakítására. Az adat kompromittálódás után felmerülő költségek a számítások szerint legalább 90 dollárba kerülnek egy számlára vetítve.

Ez a megállapítás pontosan egybecseng a Forrester elemző cég költségszámításával, melyet 28 cég biztonsági eseményeinek helyreállításából állapított meg, miszerint az okozott kár 90 és 305 dollár között van, ügyfélszámlánként számítva.

Az elmondottak alapján egyértelmű, hogy a leghatékonyabb, legkisebb költségű a megelőzés, a megfelelő információbiztonsági rendszer kiépítése és fenntartása – az adatlopásokban érintett cégek 87%-ánál nem voltak megfelelőek a kontrollok.

Az ISO 27001 alapú információbiztonság irányítási rendszer bevezetése jelentős erőforrásokat követel meg a szervezettől a bevezetés időszakában, de ha jól végzik, jelentős üzleti előnyt is hozhat. Maga az „ISO 27001 certified" minősítés megnöveli az ügyfelek és partnerek bizalmát, elősegíti és biztonságosabbá teszi az elektronikus adat és információcserét.

A szervezet számára számos egyéb előnnyel is jár, egyebek mellett felmérésre és értékelésre kerül a teljes informatikai infrastruktúra, beleértve az informatikai eszközöket, berendezéseket, kábelezést, adatátvitelt, riasztókat, tűzvédelmet, klímát stb.

Összefoglalás

Összefoglalásképp az ISO 27001-es rendszert bevezetni és azt a BalaBit technológiáival megtámogatni kívánó vezetők számára a következő üzleti előnyök adódnak:

- A kockázatok értékelése és minimalizálása megtörténik (például hozzáférés-szabályozás, szerepkörök szétválasztása).
- A meglévő folyamatok és szabályozások ellenőrzésre és javításra kerülnek, a hiányzók elkészülnek.
- Javul az üzletkritikus folyamatok biztonsága, tartalék eszközök és megoldások bevezetésével. A kockázatelemzés alapján meghatározott kritikus folyamatok mögé megerősített erőforrások kerülnek, például tartalék vonal vagy hibatűrő kiszolgáló (szerver).

- Egyes információtechnológiai költségek csökkennek, például az automatikus naplózó rendszer (syslog-ng) bevezetésével a naplóállományok felülvizsgálása felgyorsul, s kevesebb képzett munkatárs idejét kell erre fordítani. Az ellenőrzési funkciók automatizálhatók (SCB, négy szem elv).

- Egyértelműen csökken az adatvesztés, adatlopás kockázata, a bevezetett ellenőrzési eszközök technikai és pszichológiai kontrollt is jelentenek a rosszindulatú hozzáférések ellen.

- Csökkennek az audit költségei és időszükséglete, mivel például egy naplózó rendszerből egyszerűen visszakereshető bármely korábbi időpontra vonatkozóan a rendszerek valamennyi releváns rögzített információja. Az SCB eszköz ezen túlmenően, már kész audit információkat nyújt, miszerint a rendszer és adatbázis adminisztrátori tevékenységek teljes dokumentálását elvégzi.

- Az incidensek okainak felderítése gyorsabb lesz, rövidülnek a nem tervezett leállások. Az SCB segítségével a szolgáltatási szintek ellenőrzése könnyebbé válik, üzemzavar esetén többlet információt kapható.

A szerzőről

Dellei László képesített CISA, CGEIT, CRISC, ITIL-F, és ISO 27001 LA szakértő. Jelenleg egy meghatározó hazai rendszerintegrátor cégnél vezető IT biztonsági tanácsadóként tevékenykedik. Az elmúlt években elsősorban az informatikai biztonság, az IT-irányítás és az informatikai audit volt a szakterülete, melynek kapcsán számos megbízást kapott állami intézményektől és a versenyszférából egyaránt. Különböző biztonsági tanácsadási projekt vezetője és szakmai irányítója a mai napig.

Számtalan IT biztonsági témájú cikk és előadás fűződik a nevéhez. Érdeklődésének fókuszában különböző egyedi biztonsági megoldásokkal (pl. IT-biztonsági intelligencia) kapcsolatos új módszerek és technikák kidolgozása áll.

További információ

Tudjon meg többet termékeinkről: http://www.balabit.com/hu/network-security

Kérjen további információt kollégáinktól: http://www.balabit.com/request/callback

Töltse le a syslog-ng próbaverzióját: http://www.balabit.com/downloads/evaluation

Töltse le a Shell Control Box próbaverzióját: http://www.balabit.com/downloads/evaluation