BalaBit IT Security

WHITEPAPER

Naplózás mint a megfelelőség alappillére

Tartalomjegyzék

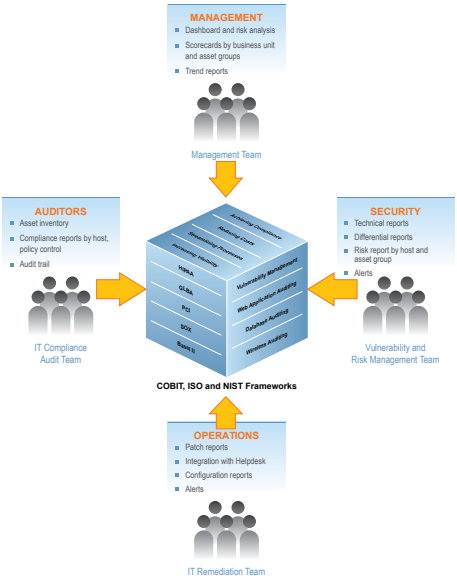
Bevezető

A vállalatok és intézmények körében gyakran megfigyelhető, hogy a különféle biztonsági előírásoknak és az egyre szaporodó nemzetközi szabványoknak való megfelelés épp úgy komoly terhet ró az informatikusokra és a biztonsági szakemberekre, mint a szervezetek menedzsmentjére. Különösen akkor fokozódnak az izgalmak, aggodalmak, amikor egy audit közeleg, és az üzlet folytonosságának fenntartása érdekében nem lehet hibát elkövetni: a megfelelőséget biztosítani kell. Ez azonban korántsem egyszerű feladat, hiszen a különböző előírások nagyon szerteágazó területeken fogalmaznak meg biztonsági elvárásokat, és az auditorok szúrós tekintete a legkisebb hiányosságra is kiterjed.

Érthető módon sokszor merül fel a kérdés, hogy miként lehet az egyre szigorúbb követelményeknek egyszerűen, emberi erőforrás-kímélő módon, a lehető legkisebb ráfordítással megfelelni. Erre a kérdésre nem létezik egyszerű válasz, azonban e dokumentum keretében mégis arra vállalkozunk, hogy a szervezetek menedzsmentje számára olyan lehetőségeket vázoljunk fel, melyek segítségével a megfelelőség megsértése elkerülhető, illetve a vállalati, informatikai és biztonsági folyamatok, események átláthatóvá és nem utolsó sorban folyamatossá válhatnak. A középpontba a naplózást helyezzük, amelyről hamarosan kiderül, hogy megfelelő megvalósítása nélkül napjainkban már nem beszélhetünk megfelelőségről.

Megkerülhetetlen megfelelőség

A kritikus infrastruktúrákat üzemeltető szolgáltatók, az állami, a pénzügyi és az egészségügyi intézmények, valamint a telekommunikációs és nagyvállalati szektorok manapság már nem engedhetik meg maguknak, hogy ne teljesítsék az iparágaikra vonatkozó biztonsági szabályokat és a különböző törvényi előírásokat. Azonban hiba lenne azt gondolni, hogy például a kis- és közepes méretű cégek teljesen figyelmen kívül hagyhatják az előírásokat, hiszen az elmúlt évek trendjei rávilágítottak arra, hogy a megfelelőség minden informatikai infrastruktúrát, rendszert üzemeltető és adatokat kezelő szervezet életében előbb-utóbb fontos szerepet fog betölteni. Azon cégek körében, amelyeknél a szigorú szabványok szerinti működés még nem kötelező jellegű, érdemes áttanulmányozni a következőkben említésre kerülő előírásokat, hiszen a védelem kialakításában, illetve fenntartásában hasznos iránymutatást adhatnak, ami végül a biztonsági incidensek megelőzését segítheti elő. Ez pedig nemcsak a szervezetek, hanem azok ügyfeleinek érdekeit is szolgálja.



A megfelelőség és biztonság integrált nézete

Ahhoz, hogy az adatok valamint az infrastruktúrák megfelelő szintű védelme és ezáltal a megfelelőség biztosítható legyen, pontosan tisztában kell lenni az informatikai rendszerek védelmi képességeivel, az eseteleges hiányosságokkal, biztonsági résekkel, illetve a nemkívánatos eseményekkel. Legyen szó külső vagy belső támadásokról, illetve a rendelkezésre-állás sérüléséről a problémák felderítése és kezelése létfontosságú. Ehhez pedig folyamatos éberségre van szükség.

Nem túlzás kijelenteni, hogy napjainkban a megfelelőség egyik alappillérét a naplózás jelenti, amely nélkül nemcsak azért lenne elképzelhetetlen

a megfelelőség (compliance) biztosítása, mert arra szinte minden szabvány alapkövetelményként tekint, hanem azért is, mert naplózás nélkül rengeteg olyan előírásnak való megfelelés sem lenne megvalósítható vagy igazolható, amelyek első ránézésre semmilyen kapcsolatot nem mutatnak egy naplómenedzsment rendszerrel. Ugyancsak nem lehet figyelmen kívül hagyni a nem megfelelő naplózásból eredő kockázatokat, melyek akár a rendszerek hitelességét aláásó naplóüzenet-vesztésekhez is vezethetnek.

Nyitott szemmel járó vezetés

Mielőtt rátérnénk az egyes szabványok naplózás szempontjából legkritikusabb fejezeteinek ismertetésére fontosnak tartjuk felvázolni azt, hogy a szervezet menedzsmentjének, döntéshozatalban résztvevő vezetőinek, miért is kell foglalkozniuk a megfelelőségi kérdésekkel, és miért nem lehet azt kizárólag a biztonsági szakemberekre, külső tanácsadó cégekre bízni. Ennek egyik legfontosabb oka, hogy a sokszor valóban nem kevés ráfordítást igénylő auditok sikeres teljesítéséhez a vezetői elkötelezettség, azaz a szervezet minden szintjére kiterjedő védelem szükségessége melletti felső vezetői kiállás nélkül a biztonsági projektek könnyen elbukhatnak. Ha pedig a megfelelőség sérül, akkor nemcsak az üzleti tevékenységben, folyamatokban lehetnek fennakadások, hanem a piaci helyzet is erodálódhat, és a biztonságra többet adó versenytársak könnyedén előnybe kerülhetnek. Nyilvánvalóan emiatt a vezetés felelőssége megkérdőjelezhetetlen. Mindeközben pedig arról sem célszerű megfeledkezni, hogy a biztonsági szabványok sok esetben az üzleti folyamatokat is érintik, ami szintén fontossá teszi a menedzsment közreműködését.

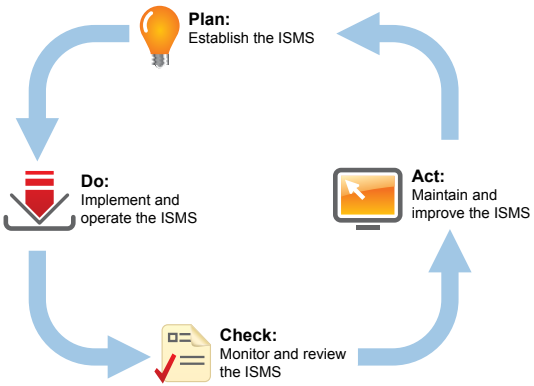
Szerencsére napjainkban már adottak azok a technológiák, amelyek – elsősorban a megfelelően rendezett, szűrt és prezentált információknak köszönhetően – a menedzsmentet is támogatják abban, hogy a compliance kapcsán indított projektek felügyelhetővé váljanak, és a döntéshozatalt megalapozottá lehessen tenni. Mindebben a korszerű naplózó rendszerek nagyon sokat segítenek, hiszen többek között képesek olyan vezetői jelentések készítésére, amelyek kifejezetten a döntéshozók számára tartalmaznak releváns információkat.

A naplózás nem kizárólag átláthatóságot, auditálhatóságot biztosít, hanem folyamatosságot is. Azaz nemcsak az auditok előtti néhány hétben teszi kézzelfoghatóvá a rendellenességeket, amelyeket aztán kapkodva kell megoldani, hanem rendszeres beszámolási lehetőséget biztosít a védelem állapotáról, és akár előrejelzésekkel is megelőzhetővé teheti a problémák kialakulását. Ha mégis bekövetkezik egy nemkívánatos esemény, akkor a felső vezetés épp olyan gyorsan értesülhet a problémákról, mint az informatikusok vagy a biztonságért felelős személyek. Ha pedig mindez tevékenység-felügyelettel is párosul, akkor az alkalmazottak tevékenysége, köztük a rendszergazdák és a kiemelt jogosultságokkal rendelkező felhasználók által végrehajtott műveletek is ellenőrizhetővé válhatnak.

A következőkben azokat a leggyakrabban szóba kerülő szabványokat, előírásokat fogjuk megvizsgálni, amelyek esetében a korszerű technológiákra épülő naplózás nemcsak elengedhetetlen eszköznek bizonyul, hanem jelentős segítséget is nyújt az auditok sikeres teljesítése érdekében.

ISO 27001

A különféle biztonsági szabványok, előírások log menedzsment-központú vizsgálatát az ISO 27001-gyel kezdjük, amely az egyik leggyorsabban és legszélesebb körben terjedő követelményrendszer. Ez nagyon sokszor fogalmazódik meg elvárásként a vállalati szférában is, különösen akkor, amikor egy cég beszállítóként kíván szerepet vállalni a logisztikai láncban. A szabvány 10.10-es fejezetében olvashatók azok az intézkedések, amelyek megtétele nélkülözhetetlen a megfelelőség biztosításához, mely nem más, mint az információ-feldolgozó tevékenységek észlelésének biztosítása. Az ISO 27001 alapvető követelménynek tekinti a felhasználók tevékenységének, az információ-feldolgozó eszközök használatának valamint a rendszer-adminisztrátori, illetve rendszerkezelői tevékenységek naplózását. Kimondja, hogy a naplóadatokat meghatározott ideig meg kell őrizni, és a rendszerhasználattal kapcsolatos naplóbejegyzéseket rendszeresen át kell vizsgálni. A szabvány szerint tehát gondoskodni kell a hibák naplózásáról, és a megfelelő beavatkozások megtételéről.



ISO 27001 PDCA (Plan, Do, Check, Act) stratégia

Amennyiben egy szervezet menedzsmentje korábban úgy határozott, hogy az ISO biztonsági szabványa mellett elkötelezi magát, akkor gondoskodnia kell korszerű naplózó rendszer felállításáról. Nemcsak azért, mert az ISO 27001 ehhez makacsul ragaszkodik, hanem azért is, mert csak így válhatnak ellenőrizhetővé, illetve igazolhatóvá az informatikai infrastruktúrában, és ezen keresztül az üzleti folyamatokban bekövetkező változások.

PCI DSS

Mivel napjainkban a bankkártya-adatok rendkívül népszerűek a kiberbűnözők körében, anyagi haszonszerzést célzó kártékony programok vagy az adathalászat révén megvalósuló biztonsági incidensek is egyre gyakrabban következnek be. Természetesen a kártyatársaságok is felismerték, hogy valamit tenni kell, hiszen nekik sem kedvez, ha a kártyahasználók adatait folyamatosan kompromittálják. Ezért még 2004-ben a legnagyobb kártyatársaságok (élükön a Visa és a MasterCard) összefogtak, és egy olyan szabványt dolgoztak ki, amelynek célja, hogy a bankkártyákkal való visszaéléseket csökkentse a kereskedelmi cégeknél, a bankkártyákat elfogadó webáruházaknál, a szolgáltatóknál és az egyéb kártyaelfogadóknál. Ebből kifolyólag az előírások tulajdonképpen minden olyan szervezetre vonatkoznak, mely bankkártya-adatokat fogad, kezel, továbbít vagy tárol.

A PCI DSS (Payment Card Industry Data Security Standard) kialakítása során a legfontosabb cél a kockázatok csökkentése valamint egy olyan egységes szabályozás kidolgozása volt, ami nem a földtől elrugaszkodott, azaz figyelembe veszi a realitásokat. Ezért tulajdonképpen célokat fogalmaz meg az egyes követelményekkel kapcsolatban. Több konkrétumot tartalmaz, mint például az ISO 27001,

ugyanakkor ad némi szabad kezet az alkalmazók számára, hogy a saját szervezetüknél fontosnak tartott védelmi preferenciákat mérlegeljék, és annak megfelelően alakítsák ki a teljes biztonsági rendszerüket.

A PCI DSS az előírásokat az alábbi fő területekre osztja:

- hálózat
- adatvédelem
- sebezhetőségek kezelése
- hozzáférés-védelem
- biztonsági monitorozás
- biztonsági szabályozás.

A felsorolásból jól látható, hogy csupa olyan területről van szó, amelyek teljes körű megvalósítása naplózás nélkül nem lehetséges. Nélkülözhetetlen a hálózatokat érő események naplózása, az adatvédelmi incidensek felderíthetőségének biztosítása, a sebezhetőségek által hordozott kockázatok kiszűrése, a hozzáférések nyomon követése, a biztonság több szinten történő figyelése, valamint a biztonsági szabályzat által meghatározott követelmények érvényesítésével kapcsolatos események rögzítése, illetve kiértékelése.

Felmerülhet a kérdés, hogy például felső vezetői szinten a PCI DSS által lefedett biztonsági területek miért is fontosak. Elsősorban azért, mert a menedzsment feladata, hogy számon kérje a szervezeten belüli védelmi intézkedéseket, és meggyőződjön azok tényleges, az üzleti tevékenységre gyakorolt hatásairól.

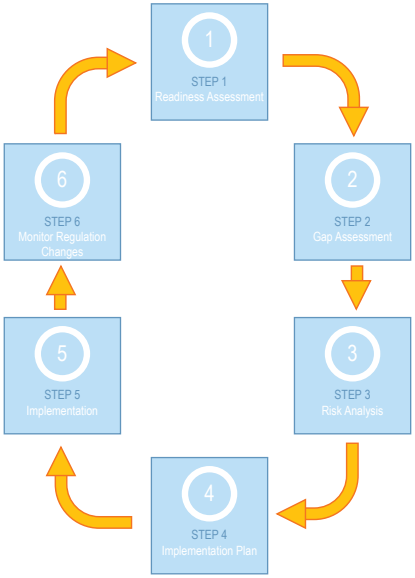
Sarbanes–Oxley (SOX) törvény

A SOX-törvény egyike azon előírásoknak, amelyek a vezetés, az informatika és a biztonság tekintetében is szigorú elvárásokat fogalmaznak meg. Ezek nem teljesítése esetén a menedzsment, de akár az igazgatótanács is a saját bőrén tapasztalhatja meg a megfelelőség csorbulását. A SOX nemcsak a kontrolling, a pénzügy és az ezekkel összefüggő ellenőrzések fontosságát hangsúlyozza, hanem a kellő mértékű információbiztonsági intézkedések szükségességét is. Az ellenőrzések kulcsfontosságú szerepet kapnak a törvényben, amelyeket olyan adatokra lehet alapozni, amik garantáltan megbízható, sértetlen és hiteles forrásból származnak. Emiatt az USA tőzsdéin jelen lévő vállalatokra nézve kötelező érvényű SOX a naplózó rendszerekre is komoly feladatot ró. A naplózásnak ugyanis képesnek kell lennie arra, hogy a csalásokat felderíthetővé, jelezhetővé és lehetőleg megakadályozhatóvá tegye, legyen szó akár külső, akár belső támadók által elkövettet cselekményekről. A naplómenedzsmentnek át kell fognia a teljes informatikai infrastruktúrát, és szem előtt kell tartania az alkalmazások hatékony naplózását is. A SOX esetében az esetleges megfelelőségi hiányosságokért felelősség terheli a vállalat vezetőit – beleértve az első számú valamint a pénzügyi vezetőt is –, akik súlyosabb jogsértés esetén börtönbüntetésre is számíthatnak.

HIPAA

Az egészségügy egyik legfontosabb biztonsági előírása, a HIPAA (Health Insurance Portability and Accountability Act) viszonylag konkrét szabályokat fogalmaz meg a naplózással kapcsolatban, és megköveteli a számítógépen tárolt valamint a hálózaton továbbított érzékeny információk védelmét. Mivel a naplóüzenetek is tartalmazhatnak érzékeny információkat, a naplózó infrastruktúrának is meg kell felelnie ezeknek a követelményeknek, miközben az esetleges incidensek vizsgálatában, bizonyításában is kulcsfontosságú szerepet kell vállalnia.

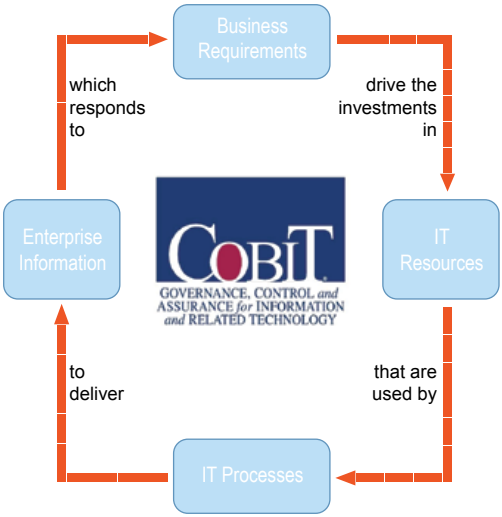
Az előírás többek között foglalkozik az adatok sértetlenségével, bizalmasságával, illetve külön kitér a titkosítás fontosságára. Mindez vonatkozik a naplóadatokra is, ezért csak olyan naplózó rendszerek bevezetésére, illetve üzemeltetésére van lehetőség, amelyek az információbiztonságot a működésük során szigorúan szem előtt tartják.



HIPAA megfelelőségi ciklus

COBIT

Habár a hatóságok viszonylag ritkábban követelik meg, hogy egy naplózó infrastruktúra a COBIT előírásainak is megfeleljen, az mégis fontos, ugyanis egyes előírások (mint például a Sarbanes-Oxley Act vagy a Basel II egyezmény) nem határoznak meg pontos technikai követelményeket, és ezért az ilyen szabályozásoknak való megfeleléshez bevett módszer egy jól bevált keretrendszer – például a COBIT – bevezetése. A COBIT módszertant az ISACA, az informatikai auditorok nemzetközi szervezete dolgozta ki azzal a céllal, hogy az üzleti vezetők felismerhessék, és elfogadható szintre csökkenthessék a kockázatokat.

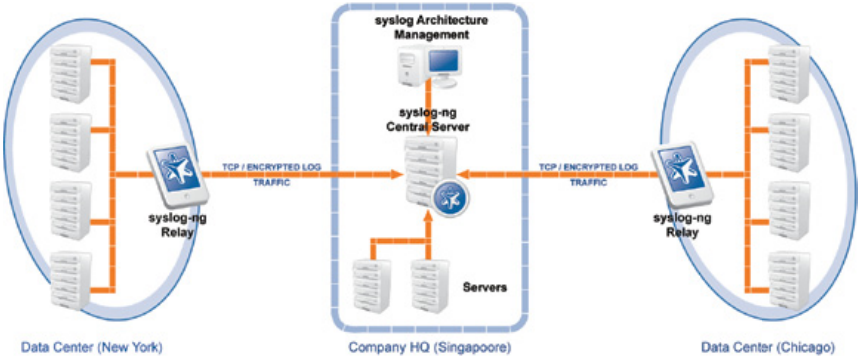


A COBIT naplózással összefüggő fejezeteiből természetesen nem hiányoznak az egyéb előírások kapcsán korábban már említett adatbiztonsági és monitorozási elvárások. Azonban a COBIT esetében fontos kiemelni, hogy olyan követelményeket is tárgyal, mint például a változások kezelése és az informatikai eszközök, szoftverek – és ezekkel együtt természetesen a naplózó rendszerek –konfigurációkezelése. Ez utóbbiak nemcsak a biztonságra, hanem a rendelkezésre-állásra, és ezáltal a termelékenységre, illetve a vállalati teljesítményre is komoly hatással lehetnek.

Hogyan segít a BalaBit syslog-ng a költséghatékony megfelelésben?

Az előbbiekben néhány előírást, szabványt mutattunk be a naplózás szemszögéből. Felvázoltuk, hogy korszerű log-menedzsment nélkül a cégvezetés épp úgy nem képes hatékonyan elvégezni a compliance kapcsán felmerülő feladatait, mint az informatikai vagy a biztonsági csoport. Ezért a syslog-ng naplózó család fejlesztésekor nemcsak technológiai szempontok érvényesülnek, hanem azok az elvárások is, amelyeket a vállalatok menedzsmentje támaszt a napló-kezeléssel szemben.

A syslog-ng a naplózókliensek, naplótovábbító eszközök és naplózószerverek funkcióit egy megbízható naplózóinfrastruktúrába egyesíti. Összegyűjti az operációs rendszerek és alkalmazások naplóüzeneteit, majd egy titkosított, megbízható csatornán keresztül egy nagy teljesítményű naplózószerverre továbbítja, ahol az üzenetek további feldolgozása, osztályozása és biztonságos, titkosított fájlokban vagy adatbázisban való tárolása történik. A syslog-ng nyílt forráskódú változatban is elérhető, azonban a kereskedelmi változat számos, a megfelelőséget és a megbízható, veszteségmentes üzenet-továbbítást elősegítő extra funkcióval rendelkezik.



A syslog-ng nem kizárólag azokat az előírásokat támogatja, amelyekről e dokumentum keretében szót ejtettünk, hiszen ennél bővebb megfelelőségi listával rendelkezik. Minden esetben képes teljesíteni azokat a követelményeket, amelyek a naplóadatok bizalmasságával, hitelességével, sértetlenségével és rendelkezésre állásával összefüggésben merülnek fel. Emellett segíti a compliance-el kapcsolatos költségek lefaragását, az auditok sikerességét, valamint a folyamatok átláthatóságát, felügyelhetőségét és ellenőrizhetőségét a szervezetek minden szintjén.

A syslog-ng, mint a világ egyik legelterjedtebb, univerzális naplómenedzsment eszköze hatékonyan képes helyt állni azon vállalatoknál, intézményeknél, amelyek a legszigorúbb biztonsági követelményekkel néznek szembe nap, mint nap. Ugyanakkor azon cégeknél is hatékony segítőtárs, melyek esetében e dokumentumban említett szabványok inkább csak ajánlásként, kiindulópontként fogalmazódnak meg.

Tudjon meg többet

A BalaBit a világ egyik vezető IT-biztonsági szoftverfejlesztő vállalata a magas jogosultságú felhasználók monitorozása, a loggyűjtés és -tárolás valamint a proxy technológián alapuló tűzfal megoldások területén. Innovatív technológiai megoldásaival a külső és belső fenyegetések megelőzésében, valamint az IT-biztonsági és megfelelőségi előírások betartásában támogatja ügyfeleit. A nyílt forráskódú közösség elkötelezett tagjaként a vállalat megoldásai minden főbb platformot támogatnak az összetett és heterogén IT rendszerekben, fizikai, virtuális és felhő alapú környezetekben egyaránt.

A BalaBit legnépszerűbb terméke a nyílt forráskódú "syslog-ng" nagy teljesítményű naplózó megoldás, amelyet ma már több mint 650.000 ügyfél használ világszerte, ezáltal az iparág de-facto szabványává vált.

A teljes mértékben magyar tulajdonú BalaBit 2009-ben felkerült az EMEA régió leggyorsabban növekvő vállalatait tartalmazó Deloitte Technology Fast 500 listára. A vállalat képviselettel rendelkezik Franciaországban, Németországban, Olaszországban, Oroszországban és az Egyesült Államokban, ügyfelei és partnerei világszerte valamennyi lakott kontinensen megtalálhatók.

Ha bővebb információra van szüksége a syslog-ng alkalmazásról, szeretne próbaverziót igényelni, vagy vásárolni, látogasson el a következő oldalakra:

- A syslog-ng termékek honlapja
- Próbaverzió igénylése
- Visszahívás kérése

BalaBit
IT Security