BalaBit IT Security

WHITEPAPER

Naplózás ÜZLETI SZEMSZÖGBŐL

Tartalom

Bevezetés

Hosszú éveken át a naplózás kizárólag az informatikusok kiváltsága volt, de mindez mára gyökeresen megváltozott, hiszen napjainkban épp olyan fontos szerepet képes betölteni a biztonság fenntartásában, mint az üzleti élet egyes területeinek támogatásában. A szervezet több szintjére kiterjedő használata sok esetben jól mérhető üzleti előnyökkel párosul, amelyeket sem gazdasági, sem technológiai oldalról nem célszerű figyelmen kívül hagyni.

E dokumentum keretében bemutatjuk, hogy a naplózás milyen előnyökkel szolgál a döntéshozók számára, hogyan képes a befektetések megtérülését elősegíteni, és miként járul hozzá a szervezetek működésének olcsóbbá, hatékonyabbá tételéhez. Arra is fény derül, hogy azon vállalatoknál, intézményeknél, amelyeknél a megfelelőségi követelmények miatt kötelező a naplózás, milyen módon lehet elérni, hogy ne egy szükséges rosszként kelljen e fontos és valóban sok segítséget nyújtó informatikai területre tekinteni.

A múltból a jelenbe

Ahhoz, hogy a naplózás vagy más néven logolás jelentős fejlődése átérezhető legyen, egy pillanatra három évtizednyit vissza kell ugranunk a múltba. Az 1980-as években Eric Allman amerikai programozó a levelezőrendszerek megfigyelhetőségének céljából kifejlesztette a mai naplózó rendszerek ősét, a Syslogot, amelyről hamar bebizonyosodott, hogy sokkal univerzálisabban használható, mint azt eredetileg bárki is gondolta. Ahogy az informatikai eszközök, alkalmazások elkezdtek szaporodni, úgy vált a naplózás mind általánosabbá, igaz sokáig elsősorban csak diagnosztikai, karbantartási és fejlesztési célokat szolgált. Ekkor még a vezetők, felhasználók leginkább csak annyit vehettek észre a naplózás létezéséből, hogy a rendszergazdák egy monitor előtt egész nap adatok tömegét bogarásszák, és néha felsóhajtanak, hogy de jó lenne egy kis szerverbővítés. Később aztán egyre inkább középpontba került a biztonság, ami már sok esetben közvetlenül is hatással volt a cégek megítélésére, hírnevére, ezért a naplózás szerepe elkezdett felértékelődni.

Napjainkra pedig elérkeztünk oda, hogy a naplózás – ideális esetben – egy szervezet életének meghatározó szereplőjévé vált, és nemcsak az informatikusok, biztonsági szakemberek munkáját segíti, hanem a menedzsment hatékony eszköze is lett. A naplózó rendszerek által szolgáltatott jelentések, információk az üzleti döntések alapjául szolgálhatnak, és hozzájárulhatnak a stratégiai célok eléréséhez.

A naplózás előnyei az üzlet számára

Mint azt az előbbiekben említettük, a naplózás az évek során egyre tágabbra nyitotta a kapuit, és mind több rendszer felügyeletében kapott szerepet. Ez egyben azt is eredményezte, hogy a naplózó rendszerekből rengeteg információ vált elérhetővé. Üzleti szempontból különösen az alkalmazások központi naplózásba való bevonása révén vált lehetővé, hogy ne csak IT és biztonsági célú elemzések készülhessenek, hanem olyan jelentések is, amelyek a menedzsmentet segítik a döntés-hozatalban, illetve a vállalati folyamatok átlátásában. Ennek köszönhetően napjainkra a naplóüzenetek felhasználhatók akár az üzleti stratégia finomítására és a vállalat irányításának támogatására is.

A naplózás segítségével mind a szervezeten belüli tevékenységek, mind az azon kívüli környezet megfigyelhető, ami végül hozzájárulhat például az alkalmazottak hatékonyságának méréséhez, a pénzügyi előrejelzések megalapozásához, vagy az ügyfélszokások feltérképezéséhez és ezáltal a marketing, illetve az értékesítés sikeresebbé tételéhez. Különösen igaz mindez az elektronikus kereskedelemre, hiszen a webáruházak, illetve online szolgáltatások monitorozásával, majd a naplók megfelelő kiértékelésével értékes információkat lehet kapni.

A naplózás előnyei azonban nem merülnek ki ennyiben. A következőkben néhány olyan területet emelünk ki, melyek alapvetően befolyásolhatják a szervezetek életét, és amelyek megfelelő ellenőrzésével pénzügyi veszteségek előzhetők meg, vagy hatékonyságnövelő intézkedések hozhatók.

A biztonság, mint üzleti felelősség

A vállalatok, intézmények menedzsmentje nem egyszer igyekszik minden biztonsággal kapcsolatos felelősséget áthárítani a biztonsági vagy informatikai vezetőre, pedig a valóságban a védelem megteremtése többszereplős folyamat, amelynek a felső vezetéstől az informatikusokon át a felhasználókig mindenkire ki kell terjednie. A vezetői elkötelezettség nélkülözhetetlen ahhoz, hogy a szervezetek minden szintjén megfelelően lehessen kezelni a kockázatokat, és a biztonsági incidensek nagy valószínűséggel megelőzhetők legyenek. Ha ugyanis egy nemkívánatos adatbiztonsági esemény bekövetkezik, aminek közvetlen és közvetett pénzügyi hatása lesz a cégre, akkor a tulajdonosok és a részvényesek sem fogják jó szemmel nézni a történteket. Nem beszélve az ügyfelekről, akik ilyen esetben hamar elfordulnak egy-egy cégtől. Az elsősorban adatvédelmi és információbiztonsági kutatásokkal foglalkozó független szervezet, a Ponemon Institute egyik bankbiztonsági felmérése során beigazolódott, hogy a megkérdezett ügyfelek – akik a kis- és középvállalati szektorból kerültek ki – 10 százaléka már váltott bankot biztonsági problémák miatt.

Érezhető, hogy a menedzsmentnek tisztában kell lennie mind a külső, mind a belső fenyegetettségekkel, és pontos képet kell kapnia a védelmi intézkedések hatékonyságáról. Ez pedig csak akkor tehető meg, ha a naplózó rendszerek megfelelő szintű bevezetésével és gondos üzemeltetésével a biztonság szintje minden időpillanatban ellenőrizhetővé válik, és lehetőség nyílik a támadásokra való gyors reagálásra. Ezzel ugyanis komoly pénzügyi veszteségek előzhetők meg, miközben az IT és biztonsági infrastruktúra kapcsán megtett múltbeli és jövőbeli beruházások hatékonysága is jelentősen fokozható.

Fontos megjegyezni, hogy nemcsak a külső támadások okoznak károkat, sőt! Manapság a belső incidensek járulnak hozzá a legkomolyabb veszteségekhez. Gondoljunk csak bele abba, hogy mi történik akkor, amikor egy személy (például a gazdasági igazgató) úgy jelentkezik be egy pénzügyi rendszerbe, hogy a fizikai beléptető rendszerben nincs nyoma a jelenlétének. Ilyenkor egy több szinten megvalósított naplózó rendszer segítségével felismerhetővé válhat ez az anomália, ellentmondás, és gyors intézkedések révén meg lehet arról győződni, hogy valóban a gazdasági igazgató jelentkezett-e be a rendszerbe, vagy esetleg egy illetéktelen személy próbál információkhoz hozzáférni a vezető nevében. A kockázatokat tovább fokozza például a közösségépítő szolgáltatások egyre népszerűbbé válása, ami az adatszivárgás valószínűségét jelentősen fokozza. Ezek mellett napjaink bizonytalan gazdasági helyzete is növeli a bizalmas adatok kiszolgáltatottságát az egzisztenciájukat féltő alkalmazottak által.

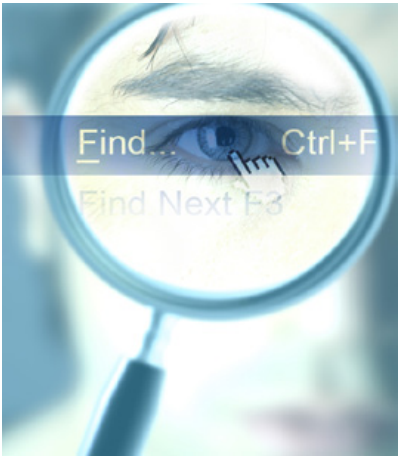
Gartner: log menedzsment nélkül nem megy

"Azoknak a szervezeteknek, melyek a biztonsági auditokhoz és a megfelelőségi problémák kezeléséhez SIEM (Security Information and Event Management) technológiákat kívánnak bevezetni, mindenképpen olyan termékek közül érdemes választaniuk, amik erős log-menedzsment képességekkel is rendelkeznek. Ezek az eszközök támogatják ugyanis a költséghatékony adattárolást, az archiválást, a nagy mennyiségű adaton való elemzést, és a különböző forrásokból származó naplóüzenetek feldolgozását, visszakereshetőségét, valamint az azokra épülő jelentéskészítést.

A log-menedzsment megoldások hatékony szolgáltatásokkal segítik mind a megfelelőségi követelmények kielégítését, mind a naplóadatok gyűjtését, megőrzését és feldolgozását. Ezek a szolgáltatások pedig egyre fontosabbá válnak a szervezetek számára."

Szemügyre vett tevékenységek

A rendszergazdák és a kiemelt jogosultsággal rendelkező felhasználók munkavégzése kapcsán az elmúlt évek során egyre fokozottabb bizalmatlanság alakult ki a szervezeteken belül. Nyilvánvalóan ehhez az is hozzájárult, hogy számos olyan esemény került napvilágra, amelyek belső támadások miatt bekövetkezett biztonsági incidensekkel voltak összefüggésben. Sajnos e problémák gyakran úgy kerülnek említésre, hogy a rendszergazdák alapvetően rafináltak, és ezért kell őket megfigyelni. Erről azonban szó sincs. Sőt azt is látni kell, hogy egy valóban hatékony monitoring rendszer bevezetése a rendszeradminisztrátorok védelmét is szolgálja, hiszen, ha egy incidens során alaptalanul gyanúba keverednek, akkor hitelt érdemlően tudják bizonyítani az ártatlanságukat.



Az egyre gyakrabban emlegetett tevékenység-felügyeleti rendszereknek nemcsak a rendszergazdák, kiemelt felhasználók auditálása miatt fokozódik a szerepe, hanem az outsourcing által is. Az informatikai kiszervezések során ugyanis egy szervezet sok minden felett elvesztheti a kontrollt. Mind az IT-szolgáltatók, mind a szolgáltatást igénybe vevők hosszú távú érdeke, hogy átlátható, ellenőrizhető környezetet teremtsenek. Ezzel ugyanis az ügyfelek felé bizalmat lehet közvetíteni, miközben a menedzsment is nyugodtabb lehet, hiszen jelentős biztonsági kockázatokat küszöböl ki.

Megfigyelhető, hogy a tevékenység-felügyelet egyre inkább az emberi erőforrások kezelésének részévé válik. A naplózó rendszerekből kinyerhető adatok ugyanis nemcsak a belső fenyegetettségekre világíthatnak rá, hanem a hatékonyságelemzést is elősegíthetik, megalapozhatják. Az alkalmazásnaplók központi gyűjtésével felhasználókra bontott kimutatások válhatnak elérhetővé, melyek hozzájárulhatnak a vállalati folyamatok fejlesztéséhez vagy az alkalmazottak hatékonyabb munkavégzéséhez. Például, ha a munkavállalók egy csoportja az átlagosnál több vírusriasztást generál, akkor fontolóra kell venni biztonságtudatosságot növelő képzések megszervezését. Ha pedig a beléptető-rendszerben sok rendellenességre utaló naplóüzenet gyűlik össze, akkor a munkafolyamatok szabályozására lehet szükség.

Hogy ne maradjon hoppon a bíróságon

Az informatika mindennapi életünkbe való beköltözésével, a számítógépes rendszerekkel, bizalmas adatokkal, elektronikus dokumentumokkal, stb. kapcsolatos vitás esetek száma megszaporodott. Mindez természetesen oda vezetett, hogy a bíróságok egyre több olyan ügyet tárgyalnak, amelyek közvetlenül vagy közvetve informatikai rendszerekhez, számítógépes bűncselekményekhez kapcsolódnak. Ilyenkor a naplózásra különösen fontos szerep hárul, hiszen az események rekonstruálásában, bizonyításában kulcsszerepet tölthetnek be. Legyen szó külső vagy belső károkozásról, csalási kísérletekről vagy egyéb jogosulatlan tevékenységek végrehajtásáról a naplóüzenetek sok mindenre fényt deríthetnek. Nyilván olyan ügyekben is, amelyek a szervezetek pénzügyeit, megítélését, hírnevét alapvetően befolyásolhatják.

Sajnos azonban az sokszor elkerüli a cégvezetők figyelmét, hogy nem minden naplóadat használható fel bizonyítékként. A bíróságok ugyanis csak akkor fogadnak el naplózásból származó információkat hitelesnek, ha korábban azok manipulálása senkinek sem állt módjában. Vagyis hiába található meg egy vállalatirányítási rendszerben az adatok utolsó módosításának dátuma, és a módosítást végző felhasználó neve, ha ezeket a bejegyzéseket valaki módosíthatja az adatbázisban. Mindebből az is következik, hogy a naplóüzenetek sértetlenségét, hitelességét és bizalmasságát megfelelő technikai eszközökkel biztosítani kell annak érdekében, hogy a jogi eljárások során megalapozott módon lehessen azokat felhasználni.

Megfelelőség minden téren

Amikor egy szervezetre olyan törvényi és iparági előírások vonatkoznak, amelyek megkövetelik a naplózást, akkor elkerülhetetlen, hogy egy hatékony naplózó infrastruktúra kerüljön kiépítésre. Ugyanez a helyzet akkor, amikor üzleti, biztonsági megfontolások miatt kíván megfelelni egy cég egy-egy szabványnak. Azonban a legfontosabb, hogy a megfelelőség kapcsán kiépített naplózásra ne egy szükséges rosszként tekintsük, hiszen az előbbiekben felsorolt előnyök megfelelően kiválasztott, bevezetett és üzemeltetett naplózó rendszer révén sokszoros megtérülést eredményezhetnek. Ezáltal nemcsak az auditok alkalmával mutatkozhat meg az előnyük, hanem a mindennapokban is kézzelfogható, mérhető eredményeket lehet a segítségükkel elérni.

Így látja a naplózást az IDC

"Az előírásoknak való megfelelőségre való törekvés jelentős hajtóerőt jelent a biztonsági szoftverek piacán. A vállalatok üzleti partnereikkel történő együttműködésük során ma már a nemzetközi szabványok által megfogalmazott követelményeket, legjobb gyakorlatokat is figyelembe veszik. A megfelelőségi elvárások mellett azonban a biztonsági rendszerek komplexitásának növekedésével is számolni kell, amelyek napjainkban már csak központosított módon felügyelhetők. Mindez a log-menedzsment eszközök piacának fejlődését eredményezi. A naplókezelés és a megfelelőség-menedzsment mindegyike olyan eszközöket foglal magában, melyek fontos értékekkel gyarapíthatják a vállalati biztonsági infrastruktúrákat."

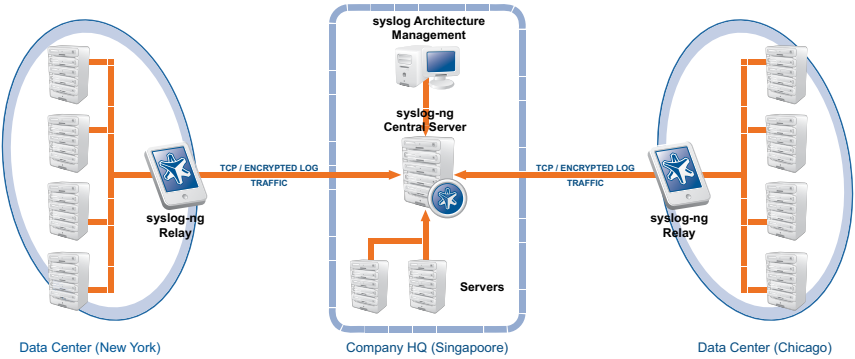
Mit hoz a jövő?

Mint láttuk, a naplózás nagyon komoly fejlődésen ment keresztül. Napjainkban a korszerű eszközöknek köszönhetően nagy mennyiségű adat begyűjtése, tárolása nem okoz problémát még az olyan környezetekben sem, amelyek számtalan különféle operációs rendszert, alkalmazást, informatikai és kommunikációs eszközt foglalnak magukban. Napjainkban a legnagyobb kihívást az adatok kiértékelése, a releváns információk kinyerése jelenti. Ennek kapcsán nagyszabású kutatások, fejlesztések folynak, melyek célja, hogy az emberi erőforrásigényt tovább csökkentsék, és minél hatékonyabb elemzéseket tegyenek lehetővé, például az üzleti intelligencia vívmányainak felhasználásával.

Mit nyújt a BalaBit syslog-ng?

Ebben a dokumentumban sok olyan üzleti előnyt vázoltunk fel, amelyek a naplózásra építkezve eredményesebbé tehetik a vezetők munkáját. Ezek eléréséhez azonban olyan technológiára van szükség, melyet a BalaBit syslog-ng naplózó infrastruktúra egymagában megtestesít. A syslog-ng a vállalati naplózási igények teljes körű kielégítésében, konszolidálásában nyújt segítséget. Megbízható, elemzési célú naplóüzeneteket biztosít, miközben nagy teljesítményű napló-infrastruktúra kialakítására ad módot. Hatékonyabbá teszi a hibakeresést, valamint a forensics vizsgálatokat, és csökkenti az üzemeltetési kockázatokat, költségeket.

A BalaBit a syslog-ng fejlesztése során szem előtt tartja a jellemző nagyvállalati igényeket, a megbízhatóságot, a skálázhatóságot és a komplex környezetekhez való illeszthetőséget. A syslog-ng fontos jellemzője, hogy megfelel azon kívánalmaknak, amelyek révén a naplók a jogi eljárásokban is felhasználhatóvá válhatnak, sőt kielégíti a leggyakrabban alkalmazott nemzetközi előírásokban – SOX, PCI-DSS, HIPAA, ISO 27000, COBIT, stb. – megfogalmazott követelményeket.



A syslog-ng legfontosabb üzleti jellemzői:

- Vállalati naplózási igények központosítása
- Teljes értékű, egységes naplózó infrastruktúra kiépítése
- Törvényi és iparági megfelelés
- Meglévő SIEM-rendszer költség-optimalizálása
- Könnyebb hibaelhárítás és forensics
- Alacsonyabb üzemeltetési költségek és kockázatok

Tudjon meg többet!

A BalaBit IT Security 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, próbaverziót szeretne igényelni, vagy ha szeretne vásárolni, látogasson el a következő oldalakra:

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