

Jogosultságkezelés vizsgálata biztonsági auditoknál

Biztonsági audit során tulajdonképpen kockázatelemzést végeznek; felmérést arról, hogy a vállalat megtesz-e minden elvárható lépést annak érdekében, hogy a szervezet számára potenciálisan nagy kárt okozó kockázati tényezőket kivédje. Ennek érdekében a biztonsági audit során a vállalat infrastruktúráját, informatikai rendszereit és szabályzatait számos szempont alapján vizsgálják.

Az átvilágításra kerülő területek egyike – a kritikusság szempontjából kiemelkedőnek számító – felhasználói jogosultságok kezelése. A szabályozottság, dokumentáltság, nyomon követhetőség és a valós állapot tükrözésének képessége itt is elvárás. Annak érdekében, hogy megfelelő kontrollal rendelkezünk ezen az igen kényes területen, szabályoznunk kell azon folyamatokat, amelyeket egy új felhasználó belépésekor, munkakör betöltésekor, munkakör módosításakor, helyettesítésakor, illetve kilépésekor végre kell hajtani – ebbe beleértve az adminisztratív és dokumentációs feladatokat is. Abban az esetben, ha minden eljárásrendet kialakítottunk, az audit során bizonyítanunk kell, hogy ettől nem történt eltérés, tehát a folyamatot megkerülve más jogosultságok nem lettek kiosztva, nem maradt ki semmi visszavonás esetén.

A feladat nagyságából és összetettségéből adódóan mindezt csupán szabályozással, eljárásrendekkel, illetve manuális legyűjtésekkel megvalósítani rendkívül nehézkes, időigényes feladat és az eredménye is megkérdőjelezhető.

Gyakorlati tapasztalatok alapján azonban elmondhatjuk, hogy azoknál a vállalatoknál, ahol egységesített jogosultságkezelő rendszert (IdM) vezettek be, a feladatok elvégzése leegyszerűsödött, illetve a rendszerből kapott kép valósághoz viszonyított állapota is megfelelő volt.

Az IdM-rendszer képes a belső szabályozások mentén automatizálni a jogosultságok kiosztását, módosítását és visszavonását egyaránt. Egy megfelelően kiválasztott és kialakított rendszer képes az egyedi elvárásoknak is eleget tenni; a delegálási és helyettesítési folyamatokat egyidejűleg kezelni, valamint több audit szempont szerinti elemzést elvégezni –

elkerülve a manuális munka erőforrásigényét. Ilyen lekérdezés lehet például az egyes végponti rendszerekben meglévő felhasználók és jogosultságaik valós idejű lekérdezése, illetve az egymást kizáró jogosultságok vizsgálata, ami kialakítástól függően megvalósulhat akár üzleti, akár informatikai szerepkörök alapján.

Az IdM-megoldások az elmúlt időszakban kulcsszerepet kaptak minden olyan szervezetben, ahol a jogosultságok kezelésében előforduló hibalehetőség jelentős üzleti károkat okozhat. A pénzügyi szektor szereplői emelték be elsőként a technológiát IT-biztonsági alkalmazásaik közé, azonban

ennek hasznosságát és jelentőségét már egyre több nagyvállalat ismeri fel. Ennek oka, hogy nem szektorfüggő a jogosultságkezelés biztonsági kockázata, hiszen az informatikai rendszereket használó alkalmazottak számára arányosan nő az azonosság- és jogosultságkezelésben való hibalehetőség.

Amíg korábban elsődlegesen a kívülről érkező támadások elleni védekezés volt a fókuszban, az elmúlt években már nagyobb figyelmet kapnak a belső védelmi megoldások is – az információvédelem szükségessége miatt. Így a biztonsági auditok alkalmával mindkét szempont vizsgálatára számítani kell.



Kádár Sándor

üzletág-igazgató
Synergon
Rendszerintegrátor

Auditálja hálózata védettségét!

Válassza a Malware Radart a Panda Security audit szolgáltatását.

Ne foglalkozzon a logok bogarászásával.
Ne kutasson biztonsági rések után.

Bízva profikra!
Kérje ingyenes demo szolgáltatásunkat.

www.malwareradar.com

24 órán belül:

- Vezetői és
- Technikai riport a teljes hálózatról.

PANDA SECURITY | One step ahead.

Fenyegetések a radaron

A folyamatosan megújuló, egyre trükkösebb terjedési módszereket alkalmazó kártékony programok elleni küzdelem sokszor nehéz feladat elé állítja az IT-rendszerek üzemeltetőit. A Panda Security felmérése szerint a közepes és a nagyvállalatok 72 százalékának hálózatában található aktívan működő rosszindulatú programok, amelyek gyakran észrevétlenül, rootkit-összetevők felhasználásával tevékenykednek, és okoznak kárt.

A vállalati hálózatokban esetlegesen megbújó számítógépes kártevők, valamint sebezhetőségek feltérképezésének egyik leghatékonyabb eszköze a Panda Malware Radar online audit szolgáltatás, amely egyszerűen kezelhető megoldások révén akár már meglévő, más gyártóktól származó védelmi eszközök mellett is képes fellépni a különféle veszélyforrások ellen, és jelentésekkel segíteni a rendszerek auditálását.

A Malware Radar használatához nincs szükség rezidens szoftverek telepítésére, mindössze néhány komponens rendszerekre való eljuttatásáról kell gondoskodni. Ez elvégezhető többek között Tivoli, SMS vagy Active Directory révén, illetve a Malware Radar saját disztribúciós eszközének segítségével. Ezt követően a szolgáltatás elkezd az auditálást, amely az aktív kártevők felismerésére kifejlesztett, gyors keresési funkció segítségével néhány perc alatt lefut.

Természetesen teljes körű ellenőrzésre is van mód, amely a rejtőzködő károkozók, valamint a sebezhetőségek mélyreható feltárását teszi lehetővé, többek között fejlett heurisztikus eljárásokkal és Kollektív Intelligencia bevetésével. Mindezek mellett a biztonsági eszköz górcső alá veszi a számítógépeken futó védelmi szoftverek állapotát és azok naprakészségét. A Malware Radar a vizsgálatok befejeztével kétféle jelentést generál. Az egyik technikai információkat tartalmaz a felfedezett problémákról, míg a másik egy vezetői kimutatás. Az online szolgáltatás természetesen arra is lehetőséget ad a rendszergazdáknak, hogy a fertőzött számítógépekről – központosított eljárások révén – eltávolítsák a kártékony programokat.

A Panda Malware Radar szolgáltatás a www.malwareradar.com weboldalon keresztül érhető el.