Offline: Világgazdaság, 2017. április 24. - 15. oldal

BIZTONSÁG | Jövőre már nyilvánosságra kell hozni az adatszivárgást

Kiküszöbölhető emberi hibák

A felhasználók gyakran kezelik túl lazán munkahelyi jelszavaikat

FOTÓ: SHUTTERSTOCK

DÉNES ZOLTÁN | Jövő év májusától a vállalatoknak már hazánkban is nyilvánosságra kell hozniuk, amennyiben adatok szivárogtak ki tőlük, és az érintetteket is tájékoztatni kell erről. Ezért még fontosabb lesz, hogy a cégek elkerüljék az ilyen eseteket.

Nem véletlen, hogy a vállalatok egyre nagyobb számban igyekeznek ellenőrzés alatt tartani az informatikai (IT) rendszerüket és az azt használó dolgozókat. Felmérések szerint ugyanis az IT-rendszerek hibáinak 73 százaléka vélhetően emberi mulasztásra vezethető vissza – nyilatkozta a Világgazdaság megkeresésére Hargitai Zsolt, a NetIQ Novell SUSE Magyarországi Képviselet üzletfejlesztési igazgatója. A társaság rendelkezésére álló adatok azt mutatják, hogy világszinten az adatszivárgási esetek 63 százalékánál közrejátszott a jelszavak nem megfelelő kezelése, többek között a gyenge vagy ellopott jelszó. A NetIQ tudomása szerint kifejezetten erre a területre irányuló, hazai kutatási adatok nem elérhetők. A jelenség azonban értelemszerűen érint minden olyan céget, ahol az alkalmazottak bizalmas adatokkal dolgoznak, ez Magyarországra ugyanúgy igaz, ahogyan a világ többi pontjára. Az IDC elemzőcég 2019-ig évi 7 százalékos növekedést jósol a személyazonosság- és hozzáférés-kezelési (Identity and Access Management, IDM) szoftverek esetében, ami nem véletlen, hiszen ezek többek között az ilyen jellegű felhasználói hibák kiküszöbölésében is fontos szerepet játszanak.

Magyarországon nem hoztak nyilvánosságra olyan esetet, ahol a felhasználó hibájából szivárogtak ki adatok. Ugyanakkor a NetIQ szakértői kiemelték, hogy hazánkban egyelőre nem kötelezi előírás a vállalatokat arra, hogy közzétegyék az ilyen jellegű eseteket és a körülményekre, felelősökre vonatkozó információkat. Ez változni fog 2018. május 25. után, amikor már minden vállalatra kötelező érvényű lesz az új európai adatvédelmi rendelet, a GDPR. Ez előírja, hogy a cégek minden adatvédelmi incidensről kötelesek tájékoztatni a hatóságokat és az érintetteket, akiknek az adatai kiszivárogtak.

Az IDM-megoldások elsősorban a jogok menedzselésére alkalmasak, ezek viszont napjainkban már nem elegendők a biztonság fenntartásához – mutatott rá Hargitai Zsolt. Szükség van mellettük olyan Identity Governance- (IG) termékekre, amelyekkel azt is lehet ellenőrizni, hogy kinek mihez van hozzáférése, s ha változtatásokra lenne szükség, képesek átadni az ehhez szükséges információkat az IDM-szoftvernek. A NetIQ szakértői szerint úgy valósítható meg a felhasználói hibákat a legnagyobb mértékben kivédő stratégia, ha az IDM-termékek funkcióit az IG-eszközök képességeivel egészítik ki. Az ilyen átalakítások esetében a tipikus projektek mérete 5 és 50 millió forint közé esik.

Ehhez első lépésként a személyazonosságokat és az igényelhető jogosultságokat kell felmérni és katalogizálni, majd a pontos kapcsolatokat a felhasználók, az alkalmazások, a fiókok, a szerepek és a kiosztott engedélyek között. Azaz össze kell gyűjteni, hogy milyen felhasználók milyen elérésekkel rendelkeznek a vállalaton belül. Következő lépésként egy olyan rendszert érdemes kialakítani, amelyben folyamatosan ellenőrizhető, hogy ezek a hozzáférések még mindig megfelelők-e, vagy esetleg már elavultak. Ehhez személyazonosság-alapú házirendeket kell létrehozni, és rendszeresen értékelni a kockázatokat. Segíti a folyamatokat, ha automatizáltan működő eszközöket használnak a jogosultságok beállításához, valamint a kihágások és kivételek észleléséhez. Mivel az üzleti vezetők fontos szerepet játszanak a folyamatban, harmadik lépésként célszerű olyan felületet bevezetni, amelyet ők is egyszerűen és kényelmesen használhatnak, és lehetővé teszi számukra, hogy könnyen átlássák és jóváhagyják, illetve ellenőrizzék a hozzáféréseket.