KI VAGY ÉS MIT CSINÁLSZ?

Szigorúan ellenőrzött felhasználók

FORRÁS: SPIRIT.COM.AU

Az IT-biztonságban mindig is fontos volt, hogy a számítógépes rendszerekben kinek milyen jogosultságai vannak és hogyan azonosítja magát. Hatványozottabban jelentkezik a probléma, amikor hirtelen nagyon sokan akarnak, illetve kénytelenek távmunkában dolgozni.

Nemcsak a gyártók hangoztatják, hogy az identitás, a kiemelt felhasználók és a jelszavak kezelése kiemelt fontosságú –, mondta a márciusi ITBUSINESS Clubon *Csinos Tamás,* az IT-biztonsági megoldások disztribúciójával foglalkozó Clico ügyvezető igazgatója. Az elmúlt hónapokban két, a kiberbiztonsággal kapcsolatos, fontos anyag is megjelent. Az egyik a Kibervédelmi Intézet „Fehér Könyve", amely a közigazgatás szereplőinek határoz meg minimumkövetelményeket; a másik a Magyar Nemzeti Bank ajánlása a pénzügyi szervezetek részére. „Mindkettőben hangsúlyos elem a fenti három problémakör, leginkább azért, a jelszavak, a felhasználók, az identitások kezelése mindig kényes egyensúlyozást jelent a kényelem és a biztonság között. A többség általában úgy gondolkodik, hogy a biztonság ne menjen a kényelem, a felhasználói élmény, és ezáltal a termelékenység rovására. És mindaddig így is marad, amíg be nem üt a baj", mondta Csinos Tamás.
Ugyanakkor az erős biztonságnak nem kell feltétlenül együtt járnia a kényelmetlenséggel. A megfelelő rendszerek nem csak módot adnak átfogó biztonsági szabályrendszerek létrehozására és betartására, hanem teszik mindezt úgy, hogy közben a felhasználó bizonytalansága is megszűnik: ők is mindig tudják, hogy mihez, milyen körülmények között és miért van jogosultsága. Csinos Tamás három ilyen rendszert mutatott be, egyet-egyet az azonosításra, az identitáskezelésre és a privilegizált felhasználók menedzsmentjére. A három rendszer funkcionalitása némiképp átfedésben van, de ez nem gond, mert mindegyik több modulból álló platform, amely könnyen együtt tud működni más megoldásokkal.

Állj! Ki vagy?

Az egész kérdéskör első lépése annak igazolása, hogy a rendszerbe belépni szándékozó felhasználó tényleg az, akinek mondja magát – vagyis azonosítanunk kell őt. Erre szolgál a Thales többfaktoros azonosítást és az egységes bejelentkezést (single sign-on-t, SSO-t) is lehetővé tévő megoldása.
Az előbbi mindenki számára ismerős lehet, aki internetbankot használ: nem elég a felhasználónév-jelszó párost megadni, be kell írni az egyszer használatos, a mobilra kapott kódot is. A mögöttes koncepció az, hogy van valami, amit tudunk és van egy másik azonosítási mód, ami csak nekünk van meg. Ez utóbbi lehet az SMS, a token, az egyszer használatos jelszó, a biometrikus azonosító, és így tovább; a Thales mindezeket kezelni tudja.
Az SSO a jelszókezelés miatt fontos. Azt már mindenki tudja (legalábbis elvben), hogy minden egyes elérni kívánt rendszerhez, szolgáltatáshoz más-más jelszót kell használni, a jelszavaknak pedig megfelelően erősnek kell lennie (legyen hosszú, tartalmazzon többféle karaktert, és lehetőleg ne legyen az illetőhöz köthető). De ha az embernek már több száz jelszava van, akkor mindenképpen valamire szüksége van a jelszavak kezeléséhez. Ezt a segítséget adják meg az SSO/j jelszókezelő megoldások. A felhasználónak csak egyszer kell belépnie, onnan az SSO intézi a többi rendszerrel kapcsolatos autentikációt. „Ily módon elkerülhető a jelszókezelés egyik nagy problémája, a jelszavak többszöri felhasználása. Ez ugyanis legalább annyira kompromittálja a biztonságot, mint a gyenge jelszavak", figyelmeztetett Csinos Tamás.

Identitások másképpen

Az informatikai rendszerekben minden olyan identitást kezelni kell, amely hozzáférhet adatokhoz, erőforrásokhoz. Ez alapesetben az emberi felhasználókat jelenti – de ott sem csak a dolgozókat, hiszen ügyfelek, partnerek szintén elérhetnek bizonyos adatokat, rendszereket. Ezen túlmenően viszont egyre több a gép-gép jellegű kapcsolat: alkalmazások érhetnek el adatbázisokat, tudni kell kezelni a robotizált (RPA) folyamatokat, és nem utolsósorban az IoT-eszközök hozzáféréseit is.

A gyakornok egy év alatt bejárja a vállalat különböző osztályait, minden részlegen megkapja az ottani munkához szükséges hozzáféréseket, jogosultságokat. Az év végére több jogosultsága lesz, mint a vezérigazgatónak – ha a felügyelet nem vigyáz

Felhasználók és kockázatok

A következő nagy terület az identitás- és hozzáférés-kezelés, amelyre a Clico a SailPoint platformját ajánlja. Az alapproblémát itt az jelenti, hogy a felhasználók nagyon sokfélék lehetnek, és a sokféleségük időben is változik, a digitális identitásuk sosem statikus, márpedig hozzáférési jogosultságaikat ennek figyelembevételével kell(ene) kiadni.
Egy felhasználó identitása nemcsak a szervezetben és a hierarchiában elfoglalt helyétől függ. Az egyszerű, szerep alapú besorolás helyett (vagy mellett) az általuk jelentett kockázat alapján is osztályozni kell a felhasználókat. Alacsony kockázatot jelent az a dolgozó, aki régi, megbízható munkaerő, többnyire alacsony szintű hozzáférésekkel rendelkezik, nem ér el direkt módon kritikus adatokat. Magasabb lehet a kockázata annak, akivel például valamilyen kellemetlen változás történt (új munkakörbe került, kirúgták a kollégáját, nem emelték a fizetését).
A legnagyobb veszélyt pedig azok a kollégák jelentik, akik rendszeresen és aktívan megsértik a házirendet (többször próbálnak olyan erőforrásokhoz hozzáférni, amelyekhez nincs jogosultságuk), vagy sok érzékeny adathoz kell, hogy hozzáférjenek, de ide tartoznak a már távozott kollégák is, ha jogosultságaikat nem vonták vissza. Az is

IT-biztonság járvány idején

A járvány kapcsán bevezetett hatósági korlátozások arra ösztönzik a bűnözőket, hogy tevékenységük egy részét-egészét az online térbe helyezzék át. A klubunk óta (március 10.) exponenciálisan megugrott a magyar vállalkozások elleni támadások száma, mint ahogy. megnőtt a távmunka feltételeinek megteremtésére törekvő cégek száma is. Ebben a helyzetben különösen fontos, hogy ahol nem volt kialakult szabályozás, bejáratott, biztonságos rendszer, ott a home office miatt megnövekvő támadási felületet megfelelő védelmi rendszerekkel, intézkedésekkel ellensúlyozzuk.
A Clico szakértői ingyenes online konzultációval járulnak hozzá a vészhelyzet kezeléséhez. Keressék őket a support@clico.hu címen időpont-egyeztetés céljából.

lényeges, hogy ezek a kockázat alapú besorolások nem statikusak, hanem időről-időre változnak – új hozzáféréseket kap az illető, változik a munkaköre, a motivációja. Ezért van szükség egy olyan irányító (governance) rendszerre, amely az identitások alakulását folyamatosan követni tudja. (Arról nem is beszélve, hogy identitása nemcsak a dolgozóknak lehet, lásd az „Identitások másképpen” című keretet.)

Prediktív identitás

Az identitás- és hozzáférés-kezelő rendszerek három kérdésre igyekeznek választ adni: kinek van hozzáférése az erőforrásokhoz; kinek kellene hozzáféréssel rendelkeznie; és hogyan férnek hozzá az erőforrásokhoz a felhasználók.
A hozzáférések kiosztása a legtöbb helyen manuális folyamatban zajlik. A felhasználó az alkalmazásgazdától kér hozzáférést, aki általában meg is adja neki. „De tényleg tisztában van azzal az alkalmazásgazda, hogy kinek adott hozzáférést? Biztos abban, hogy az illető megkapta a szükséges oktatást, rendelkezik kellő biztonságtudatossággal ahhoz, hogy használja az adott rendszert?”, tette föl a kérdéseket Csinos Tamás. Érdemes ezért egyfajta ellenőrzési mechanizmust is beépíteni a termékbe,

FORRÁS: APTRONICS.CO.ZA

amely alapján eldönthető, hogy az illető megkaphatja-e a kérdéses jogosultságot.
A SailPoint egyik különlegessége, hogy gépi tanulás segítségével ezt az ellenőrzést prediktívvé tudja tenni. Összekapcsolható például a megoldás a HR-rendszerrel, ahonnan beszerezhetők a kockázati besoroláshoz használható információk. Ezeket, és a korábbi tapasztalatokat felhasználva a rendszer ajánlásokat tesz az egyes identitásokhoz tartozó jogosultságokra – nem túl kockázatos-e magasabb szintű jogosultságokat adni egy bizonyos felhasználónak, vagy éppen nem járna-e további hozzáférés egy másiknak.
Fontos eleme az identitáskezelésnek az életciklus menedzselése. Ide tartozik, hogy a belépő dolgozó megkapja a jogosultságait, a kilépőtől viszont automatikusan vegyék el. Gyakori jelenség az „identity creep", a lopakodó identitás is, hívta fel a figyelmet egy további veszélyforrásra Csinos Tamás. Képzeljünk el egy gyakornokot, aki egy év alatt bejárja a vállalat különböző osztályait. Minden részlegen megkapja az ottani munkához szükséges hozzáféréseket, jogosultságokat, de amikor átmegy a következőbe, az előzőeket nem vonják vissza tőle. Az év végére akár több jogosultsága lesz, mint a vezérigazgatónak, ami óriási kockázatot jelent a vállalatra nézve, különösen, ha ott is marad dolgozni. „Tipikus jelenség az is, hogy egy vállalatban 300 dolgozóra 6 ezer felhasználói fiók jut, ami megint csak a kockázatot növeli", tette hozzá a Clico ügyvezetője.

Veszélytelen hatalom

Végül a harmadik lényeges terület a kiemelt (privilegizált) felhasználók kezelése. Nem lehet mindenkitől minden hozzáférést megtagadni, mert valakinek azért üzemeltetni kell a rendszereket – viszont a legnagyobb kockázatot éppen a legmagasabb szintű jogosultsággal rendelkező felhasználók jelentik. Nem is feltétlenül azért, mert rosszra használják privilegizált helyzetüket, hanem mert egy támadó a hozzáféréseket kihasználva tud egyre magasabb jogosultságokat szerezni magának, hogy hozzáférhessen érzékeny adatokhoz. „Ha nem kezeljük jól a privilégiumokat, biztosak lehetünk abban, hogy előbb-utóbb megszereznek valamilyen adatot tőlünk", emlékeztetett Csinos Tamás.
Itt jön képbe a Cyberark rendszere. A megoldás megakadályozza, hogy a rendszereinkbe már bejutott támadó magasabb szintre tudja emelni a behatolásnál megszerzett privilégiumait. A megoldás alapja egy digitális széf, amelyben a privilegizált felhasználó (például egy rendszeradminisztátor) jogosultságait, jelszavait gyűjtik össze. Az adminisztrátor a saját jelszavával lép be ebbe a széfbe, de az abban található jogosultságokat a felettese helyezte ott el – ő adja ki, vonja vissza azokat, ahogy éppen szükséges. Ennek révén egyetlen felhasználó sem jut túlhatalomhoz: az adminisztrátor nem oszthat magának jogosultságokat, csak felhasználhatja azokat; felettese pedig csak kiadja, de nem használhatja azokat.
Ha pedig ez nem lenne elég, a Cyberark folyamatosan monitorozza a kiemelt felhasználók tevékenységét, mintegy „videofelvételt" készít róluk. A biztonsági szempontból kulcsmomentumnak mondható tevékenységeket külön is megjelöli, így egy későbbi ellenőrzésnél nem kell végignézni a teljes felvételt, hanem egyből a kritikus pontokhoz lehet ugrani.

Schopp Attila

CSINOS TAMÁS, CLICO

FORRÁS: ITB