IAM-MEGOLDÁSOK COVID-JÁRVÁNY IDEJÉN

A „zero trust” jelenti a digitális bizalmat

A home office terjedése az Identity and Access Management (IAM), vagyis az identitás- és jogosultságkezelés területét is megváltoztatta: a „zero trust” megközelítés népszerűsége megnövekedett, a multifaktoros autentikáció szükségszerűvé vált, és a különböző információk korrelációja is nagyobb szerephez jutott.

FORRÁS: 123RF.COM

Alapból sem egyszerű feladat egy nagyobb szervezetben, ahol az emberek már nem ismerik személyesen egymást, számon tartani, hogy ki kicsoda a vállalatban, milyen eszközök és információk hozzáféréséhez jogosult az adott kolléga. A feladatot tovább bonyolította a hibrid iroda megjelenése, amikor az emberek gyengébb biztonságú környezetből, változó időben és változó helyekről jelentkeznek be.

Az is tény, hogy a cégek sorra vettek igénybe új felhős megoldásokat és szolgáltatásokat, amelyek ugyancsak a felhasználók azonosítását, a hozzáférési körök meghatározását igényelték. Emellett változnak a felhasználók igényei is, hiszen biztonságban akarnak dolgozni, de nem akarják minden egyes kattin-

táskor bizonyítani, hogy nyomták meg a bal gombot. A digitális szervezet a digitális bizalmon alapszik, melyet az IAM-rendszerek tudnak megteremteni – paradox módon éppen a nulla bizalom megközelítés segítségével.

Kihasználják a meglevő funkciókat

„A hibrid munkavégzés sok szervezet számára jelentett új kihívást biztonság szempontjából", mondja *Lengyel Zoltán,* a Balasys IAM-csapatának vezetője. Plusz biztonsági kontrollokat igényelt az a tény, hogy a felhasználók többsége a vállalati hálózaton kívülről kezdte el használni a céges infrastruktúrát. Ezért több, korábban elhanyagolt funkciót is elkezdtek bekapcsolni a szervezetek. Ide tartozik például a multifaktoros autentikáció az érzékeny üzleti rendszerek esetében, amellyel csökkenthető az illetéktelen hozzáférések kockázata.

A home office hatására megnövekedett az IT-helpdesk terhelése is. Ennek mérséklését segíthetik elő a végfelhasználók számára kialakított önkiszolgáló funkciók, mint például a jelszavak kezelését, helyreállítását segítő webes felületek. Az IT terheltsége tovább csökkenthető az adott rendszerekhez való hozzáférés vagy eszközök igénylésével kapcsolatos feladatok kiszervezésével önkiszolgáló felületre, ami egy fejlett IAM-megoldás sajátossága.

Új kihívást jelentett a vállalatok infrastruktúrájában egyre nagyobb teret kapó felhőmegoldások adminisztrációja is a hozzáférés és azonosítás kezelése szempontjából. Szerencsére a népszerű szolgáltatások viszonylag egyszerűen illeszthetők az IAM-megoldásokhoz.

„A home office a zero trust biztonsági megközelítés elterjesztésében is segített", mondja a szakember. Ez azt jelenti, hogy már nem a vállalati hálózat határait kell védeni, hanem a felhasználókra és az elérhető adatokra, erőforrásokra kerül át a fókusz. Az alapbizalom már nem jár senkinek, még a vállalati hálózaton belül sem. A teljes infrastruktúrát monitorozni kell. Az információk elemzése alapján dinamikusan lehet szabályozni az adott session idejére szóló jogosultságokat. „Alapbizalom hiányában folyamatosan ellenőrizni kell, hogy a felhasználó az-e, akinek mondja magát, és valóban hozzáférhet ahhoz, amit kér vagy használ. Ehhez az IAM-rendszerek mellett egy megfelelő hálózati biztonsági infrastruktúra kialakítása is szükséges", fejezte be Lengyel Zoltán.

Zavaros folyamatainkat nem teszi rendbe az IAM

„Az identitások ellenőrzése, a jogosultságok kezelése már a járvány előtt nagy kihívást jelentett a vállalatok számára, a pandémia miatt bekövetkezett változások azonban még inkább fókuszba helyezték a területet", mondja *Urzica Olivér*, a Prianto regionális vezetője. Mindenki érezte, hogy a felhős megoldások terjedésével szükség van egy olyan identitáskezelő rendszerre, mely védi a felhasználókat, a vállalati rendszereket, szinkronban a lokális eszközökkel.

„Azonban az IAM-megoldások csak úgy működnek jól, ha vállalaton belül a folyamatok átgondoltak, tervezettek, eldöntött, hogy kinek milyen jogosultsága van, ki, mihez és mikor férhet hozzá, a standard és a kiemelt felhasználók esetében egyaránt", hangsúlyozta.

A vállalatok a járvány miatt több új, felhő alapú rendszert vezettek be, amelyek támogatják a távoli munkavégzést, például Office 365-öt, Hibrid Active Directory-t, kollaborációs alkalmazásokat, TeamViewert stb. Az alkalmazotti életutat, a kollégát a toborzás pillanatától egészen a vállalattól való kilépésig végigkísérő IAM-megoldások kulcsfontosságúak a fenti rendszerek védelmében. Komoly biztonsági kockázatot jelent, ha a felhasználó jogosultsága gyakran még fél évvel a szervezettől történő távozása után is él.

Kiemelt figyelmet kapott ebben az időben a különböző törvényi és iparági megfelelőségekhez kapcsolódó, személyre szabott riportok készítésének lehetősége, az auditálási folyamatok hatékonyságának és naprakészségének támogatása. A funkcionalitás főleg a pénzügyi vagy állami szektorban dolgozó szervezeteknek jelent nagy segítséget, ahol sok hasonló jellegű ellenőrzés történik.

Urzica Olivér megerősítette, hogy a járvány hatására az IAM-területen megerősödött az automatizáció jelentősége, egyre több vállalatnál terjed a zero trust megközelítés. Meglátása szerint fontossá vált a különböző információk korrelációja is mint funkcionalitás. „A távoli munkavégzés világában kritikus, hogy a szervezet tisztán lássa, ki, mihez fér hozzá, milyen jogosultságokkal, milyen módosításokat végzett az adott felhasználó, az pedig milyen hatással van a szervezetre", zárta javaslatait.

Vass Enikő

Csökkennek a kockázatok

Az IAM rendszer legnagyobb előnye az Identity Management Institute 2022-es tanulmánya szerint a megerősített adatvédelem és kiberbiztonság. Az adatszivárgások 80 százaléka a gyenge vagy ellopott jelszavak miatt történik, a GoTo (volt LogMeIn) adatai szerint. Amikor a cég bevezet egy IAM-rendszert, akkor a multifaktoros autentikáció és az előírt erős jelszavak a veszélyeknek legalább egy részét kiszűrik.

Az Identity Management Institute adatai szerint a biztonsági incidensek 65-70 százaléka a szervezeten belülről indul el, belsős alkalmazott vagy partner szándékos vagy véletlen hibája miatt. Egy IAM-rendszer azzal csökkenti a kockázatokat, hogy szerepkör szerint biztosítja a hozzáférést a vállalati erőforrásokhoz.

LENGYEL ZOLTÁN, BALASYS

FORRÁS: ITB

URZICA OLIVÉR, PRIANTO

FORRÁS: PRIANTO