Offline: Műszaki Magazin

2020. szeptember 15.

Digitális átállás

ADATBIZTONSÁG Napjainkban a digitális átalakulás természetes evolúciós folyamatnak számít a vállalatok körében. A cégeknek meg kell tanulniuk kihasználni a technológiai fejlesztések lehetőségeit hiszen csak így tudnak megfelelni a gyorsan változó fogyasztói elvárásoknak.

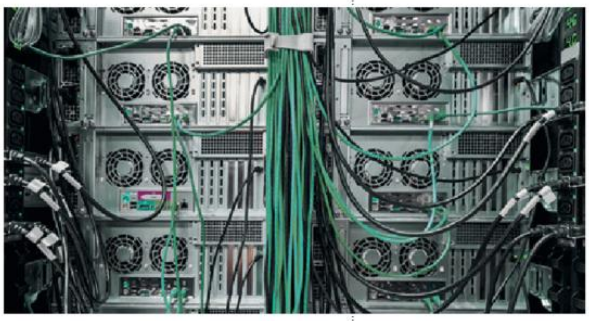
A Micro Focus szakértői szerint az átállás során nem hagyhatjuk figyelmen kívül a biztonsági aspektusokat sem, ennek érdekében pedig célszerű a leghatékonyabb megoldásokat igénybe venni a kockázatok minimalizálásához, beleértve az egyszerű adattitkosítást vagy a biztonságot automatizáló szoftvereket.

A digitális átalakulás stratégiai előnyöket kínál a vállalatok számára, ugyanakkor rendkívül összetett folyamat, és alapjaiban változtatja meg a szervezetek működését, így biztonsági kockázatokkal is jár. Digitalizált működéssel a vállalatok óriási mennyiségű adatot termelnek, amit megfelelően elemezve jobb döntéseket hozhatnak, és javíthatják szolgáltatásaikat. Ezen információk egy része azonban érzékeny adat, aminek a védelméről nehéz gondoskodni, ha a tárolás és az analizálás több helyszínen történik, ami globális működés esetén különösen szerteágazó lehet.

A digitális működés során keletkező adatmennyiség eseté biztonsági szempontból kulcsfontosságú, hogy a cégek átlássák, pontosan hol találhatók az érzékeny adataik, és rendszeresen felülvizsgálják, hogy továbbra is megfelelően erős-e a védelmük. Ehhez olyan különféle hasznos eszközök érhetők el, mint például a Data Discovery, amely segít feltérképezni és osztályozni az adatokat, és szükség esetén a megóvásukról is gondoskodik. Miután rendszerezték és besorolták ezeket az adatokat, a vállalatoknak azt is érdemes fontolóra venniük, melyeket érdemes közülük titkosítani, hogy csökkentsék az adatszivárgás kockázatát. Az lenne a biztos, ha minden információt titkosítanának, így azonban nem lehetne azokat felhasználni a különféle üzleti elemzésekhez. Jó kompromisszumot jelenthet azonban a formátummegőrző titkosítás.

Száz százalékos védelem természetesen nem létezik, de jelentősen csökkenti a kockázatokat, ha a vállalat a nulla bizalom elvét követi. A megközelítés garantálja, hogy a felhasználók csak azután férhetnek hozzá az érzékeny információkhoz, miután ellenőrizték a személyazonosságukat és az érvényes engedélyeket. Ehhez az szükséges, hogy a cégnél erős személyazonosság- és hozzáféréskezelő rendszereket használjanak, amelyek egyszerűen képesek a felhasználónév és jelszó kombinációján túlmutató, fejlett hitelesítési módszereket, például biometrikus azonosítókat és tokeneket is kezelni. Ezek a megoldások a kockázati szinteknek megfelelően követelik meg az autentikációt a felhasználóktól. Például kockázatosnak számít, ha egy üzleti kiküldetésben lévő alkalmazott külföldről, egy hotel wifijéről szeretne bejelentkezni a céges hálózatba a munkaidőn kívül, ezért indokolt, hogy egy SMS-ben küldött kóddal is erősítse meg a személyazonosságát. Ugyanakkor a vállalat székhelyéről, munkaidőben bejelentkező felhasználó tevékenysége nem számít kockázatosnak, ezért az ő idejét nem szükséges plusz azonosítási körökkel rabolni.

A digitalizálásnak köszönhetően a gépek ma már képesek ellátni olyan feladatokat, amelyekről korábban emberek gondoskodtak. Napjainkban egyre több helyen automatizálják például az üzleti és pénzügyi folyamatokat, a teljesítménytesztek futtatását vagy éppen a szoftverek kódjainak ellenőrzését. Az automatizálás jobban skálázhatóvá és biztonságosabbá teszi a műveleteket, hiszen kiküszöböli az emberi hibák lehetőségét. Ugyanakkor ezeket a folyamatokat is meg lehet úgy hackelni, hogy rosszindulatú tevékenységeket vigyenek véghez, például egy banki átutalást egy módosított számlaszámra irányítsanak. MM



„Ha helyesen végzik a digitális átalakítást, az olyan, mint amikor a hernyó átalakul pillangóvá. Ha viszont rosszul csinálják, akkor a végeredmény mindössze egy nagyon gyors hernyó.“

GEORGE WESTERMAN,
AZ MIT CENTER FOR DIGITAL BUSINESS KUTATÓJA