Termékismertető

Jelszókezelés

Egy átlagos hálózati felhasználó egy átlagos napon megérkezik a munkahelyére és azon aggódik, hogy vajon a számítógépe bejelentkező képernyőjén megjelenik-e az értesítés, hogy hány napja maradt… egy új jelszó kitalálására. Amint kiderül, hogy már csak kettő, felfordítja az egéralátétet, leszedi róla az éppen aktuális jelszót és kétségbeesetten próbál kitalálni valami olyat, amit eddig még nem használt. Ahogy beírta kedvenc háziállata nevét, a rendszer közli, hogy a jelszónak még meg kell felelnie bizonyos biztonsági előírásoknak, szerepelnie kell benne speciális karakternek, nagybetűnek, számnak, és persze nem lehet túl rövid sem. Szomorúan néz körbe az íróasztalon, hátha eszébe jut valamiről a megfelelő jelszó, de semmi… Ugye, ismerős a dilemma?

Vállalati vs. felhasználói érdekek

Egy átlagos hálózati felhasználó gyakran találkozik a fent vázolt problémával, de egy dologban biztosak lehetünk: nem fog mindenféle, a hálózat biztonságát maximalizáló, matematikai alapú jelszósémát kitalálni, sem használni, ő bizony a lehető legegyszerűbb módszert fogja választani. A felhasználók és a vállalatok a biztonságos számítógép használathoz ezért olyan megoldást keresnek, amely egyszerre szolgálja ki a biztonsággal és a hozzáféréssel kapcsolatos igényeket, de a vállalatnál a használt platformok sokszínűsége ellenére is költséghatékonyan vezethető be.

Minden vállalati eszköz valamilyen módon az IT-hálózatra kapcsolódik. Az alkalmazottak, a partnerek és az ügyfelek elvárják az egyszerű hozzáférést bármikor és bárhonnan, a versenytársakat és a bűnözőket viszont agresszív módon távol kell tartani. A biztonság mellett ugyanakkor azt is szem előtt kellett tartani, hogy a megoldást bármely alkalmazott a tartózkodási helyétől, illetve az operációs rendszertől és platformtól függetlenül, problémamentesen tudja használni. A megoldásnak mindezek mellett lehetővé kell tenni, hogy a vállalat egyszerű, átlátható módon feleljen meg a szigorú törvényi előírásoknak anélkül, hogy a rendszergazdák értékes idejét rabolná.

A jelszókezelési problémák megoldásának megközelítései

A jelszavakkal kapcsolatos kihívások-szinte általános érvényűek, de a vállalatok által a megoldásukra alkalmazott módszerek és technikák nem azok. Ha a különböző jelszókezelési összetevők és technológiák mind felhasználhatják a személyazonosság-kezelő rendszert, akkor együtt tudnak működni, és még egyszerűbben oldják meg a jelszavakkal kapcsolatos kihívásokat. Számos különböző tényezőtől – például az IT infrastruktúrától, az adott megfelelőségi követelményektől és a felhasználói elvárásoktól – függően számos különböző megközelítés és technológia közül választhatunk:

- Kiszolgálói jelszó-szinkronizálás: a módszer a jelszókezelést egy nagyobb személyazonosság életciklus-kezelő és felhasználói hozzáférés-kiosztási megoldás részévé teszi. Ennek keretében a felhasználók egyetlen jelszót kapnak, amelyet a rendszer a környezet összes kapcsolódó rendszerén szinkronizál.

- Webes hozzáférés-felügyelet: a módszer a webes alkalmazások hitelesítésére és engedélyezésére szolgál egy biztonságos webes portálon keresztül. A webes hozzáférés-felügyeleti rendszerek egy felhasználói hozzáférés-kiosztási eszközzel együttműködve szabályozzák, hogy ki milyen erőforrásokhoz férhet hozzá a portálon keresztül.

NetIQ megoldások

- Személyazonosság-kezelés és biztonság

Termékek

- Identity Manager
- Access Manager
- SecureLogin

NetIQ®

www.netiq.hu

- Vállalati egyszeri bejelentkezés: a módszer alkalmazása esetén a felhasználók egy hitelesítő adatkészlet megadásával jelentkeznek be a hálózatba. A rendszer előhívja a megfelelő felhasználóneveket és jelszavakat, és a felhasználó nevében automatikusan átadja őket, az egyszeri bejelentkezést engedélyező alkalmazásoknak pedig hitelesítő adatokat hív le a könyvtárból, és szinte minden alkalmazásnak vagy erőforrásnak továbbítja azt a felhasználó helyett.

A NetIQ jelszókezelési megoldásai

A NetIQ kiszolgálói szinkronizációs megoldása: NetIQ Identity Manager

A NetIQ Identity Manager nagymértékben leegyszerűsíti a személyazonosságkezelés folyamatát, miközben garantálja a kritikus fontosságú adatok védelmét. A NetIQ megoldása automatizálja a felhasználó-létrehozás és jelszókezelés felügyeletét a felhasználó teljes életciklusára vonatkozóan – azonnali hozzáférést biztosít az új felhasználóknak, szükség szerint módosítja vagy megszünteti a hozzáférést az összes rendszeren, és egységesíti a jelszókezelést. Az Identity Manager szinkronizálja a felhasználó összes jelszavát, és egyetlen jelszavas elérést nyújt az összes rendszerhez. Szabályokkal garantálható, hogy a használt jelszavak biztonságosak: erős, az egész rendszerre kiterjedő jelszóirányelvek alakíthatók ki, amelyek védenek a szótár alapú támadások ellen. A NetIQ termékével megszüntethető a felhasználói hozzáférési igények költséges és időigényes kézi adminisztrálása is.

A NetIQ webes hozzáférés-felügyeleti megoldása: NetIQ Access Manager

A NetIQ Access Manager segítségével az alkalmazottak, partnerek és vásárlók egyszerűen és biztonságosan érhetik el a szükséges információkat, ugyanakkor a rendszer hatékonyan megakadályozza, hogy bárki más hozzáférjen az értékes adatokhoz. Funkciói közé tartozik, hogy a felhasználó részére SMS-ben is küldhető vele egy egyszer használatos bejelentkezési kód. Pontosan meghatározható, hogy kik jogosultak az erőforrások elérésére, ők pedig mindent, amihez jogosultságuk van, egyetlen jelszóval érhetnek el. NetIQ Access Managerrel szabályozható mind a webes, mind a hagyományos üzleti alkalmazások hozzáférése.

A NetIQ Access Manager támogatja a webszolgáltatás-összevonást (WS-Federation), egy olyan egypontos bejelentkezési módszert, amelynek köszönhetően a NetIQ Access Manager az iparág legteljesebb webes hozzáférés-kezelési szolgáltatását kínálja.

A NetIQ vállalati egyszeri bejelentkezés megoldása: NetIQ SecureLogin

A NetIQ SecureLogin lehetővé teszi, hogy az alkalmazottak egyetlen, biztonságos bejelentkezéssel hitelesítsék magukat a vállalati erőforrásokon, amelylyel kiválthatók a különböző felhasználónevek és jelszavak kezelésével járó feladatok. A NetIQ SecureLogin zökkenőmentesen működik együtt a Windows rendszerekkel, valamint a webes, Java-alapú és egyéb vállalati alkalmazásokkal, és segítségével ezek az alkalmazások kiegészíthetők erős hitelesítésen alapuló felhasználó azonosítással. A SecureLogin varázslója számos alkalmazást automatikusan integrál, így az ügyfelek és a partnerek más gyártók termékeihez képest sokkal gyorsabban realizálhatják az egypontos bejelentkezés nyújtotta előnyöket. A NetIQ SecureLogin jól működik más NetIQ jelszó és személyazonosságélettartam-kezelő termékekkel is, például a NetIQ Identity Manager és a NetIQ Access Manager programokkal.

A legjobb válasz megtalálása: mi a megoldás a jelszókezelés problémáira?

Figyelembe véve az összes előnyt és hátrányt, a három jelszókezelési módszer közül vajon melyik nyújtja a legjobb, legteljesebb és legköltséghatékonyabb jelszókezelési megoldást a vállalatok számára? A legjobb válasz erre a kérdésre az egyes megoldásoknak az igények szerinti kombinálása. Használhat például kiszolgálói szinkronizálást a jelszókezelés egyszerűsítéséhez néhány központi rendszeren, alkalmazhat egy webes hozzáférés-felügyeleti terméket az egységes portálkörnyezet biztosításához a felhasználók számára, majd egy vállalati egyszeri bejelentkezési rendszer használatával kiterjesztheti a jelszókezelési funkciókat. Ha a különböző jelszókezelési összetevők és technológiák mind felhasználhatják a személyazonosság- kezelő rendszert, akkor együtt tudnak működni, és megoldják a jelszavakkal kapcsolatos kihívásokat.

Keresse meg helyi megoldásszállítóját, vagy vegye fel a kapcsolatot a NetIQ magyarországi képviseleti irodájával az alábbi elérhetőségek valamelyikén:

MOM Park, SAS torony
1124 Budapest, Csörsz u. 45.
Tel: +36 (1) 489-4600
Fax: +36 (1) 489-4601
info@netiq.hu
www.netiq.hu