Kádár Sándor, üzletágvezető

2007. április 22.

SYNERGON

Többfaktoros azonosítás

A többfaktoros azonosítás létjogosultsága

- Az azonosítás célja az erőforrásokhoz történő hozzáférés esetén biztosítani a hozzáférő személyek egyértelmű azonosítását.
- Az azonosítást követően történhet meg a személyekhez rendelt jogosultsági szint meghatározása.
- Különböző rendszereken belül kell biztosítani az azonosítási funkciókat.

A többfaktoros azonosítás létjogosultsága

- Napjainkban a legelterjedtebb azonosítási forma a felhasználónév – jelszó páros alkalmazása.
- Számos hátránnyal rendelkezik ez a megoldás:
  - Egy faktorra épül – valamit tudni
  - Könnyen „másolható” szándékos tudásátadással
  - Könnyen elleshető, egyszerű technikai eszközökkel megszerezhető
  - Rendszeresen változtatni kell – változtatás gyakoriságának meg kell felelnie humán tényezőknek

A többfaktoros azonosítás létjogosultsága

SYNERGON

- Számos hátránnyal rendelkezik ez a megoldás:
  - Különböző rendszerekben különböző jelszó – felhasználók hajlamosak rögzíteni azokat
  - Gyakran könnyen kitalálható jelszavakat alkalmaznak a felhasználók
  - Számos esetben előfordul, hogy több felhasználó megoszt egy felhasználónév-jelszó párost – nem azonosítható egyértelműen
  - Visszaélés esetén nem megfelelő biztonsággal bizonyítható a felhasználó személye

Megoldás a hátrányokra

- Több faktor alkalmazása
- Azonosító eszköz személyhez kötése
- Nem másolható azonosítás alkalmazása
- Humán kockázati tényező csökkentése

Valamit tudni

Valamit birtokolni

Valakinek lenni

A többfaktoros azonosítás fajtái

SYNERGON

- Egyszer használatos jelszavak

- Smart kártyás rendszerek

- USB kulcsos rendszerek

- Biometrikus rendszerek

Egyszer használatos jelszavak

- Az egyszer használatos jelszavak biztosítják a kétfaktoros azonosítás követelményeit.
- A jelszó a hardveres azonosítón megjelenő számsorból és egy személyes azonosítóból (PIN) áll össze.
- A hardveres azonosítón percenként, vagy gombnyomásra változik a kód.
- Egy kód egyszer használható fel.

Smart kártyás rendszerek

- A Smart kártyás rendszerek biztosítják a kétfaktoros azonosítás követelményeit.
- Az azonosító a Smart kártyán tárolt információból és egy személyes azonosítóból (PIN) áll össze.
- A Smart kártyán tárolt információ lehet privát kulcs, amely PKI (Nyilvános Kulcsú Infrastruktúra) alapú működést tesz lehetővé
- A megoldás előnye, hogy összeköthető más PKI alapú alkalmazások használatával, illetve beléptető rendszerekkel.

USB kulcsos rendszerek

- Az USB kulcsos rendszerek biztosítják a kétfaktoros azonosítás követelményeit.
- Az azonosító az USB kulcson tárolt információból és egy személyes azonosítóból (PIN) áll össze.
- Az USB kulcson tárolt információ lehet privát kulcs, amely PKI (Nyilvános Kulcsú Infrastruktúra) alapú működést tesz lehetővé
- A megoldás előnye, hogy összeköthető más PKI alapú alkalmazások használatával, illetve nem szükséges hozzá speciális olvasó a számítógéphez illesztve.

Biometrikus rendszerek

- A Biometrikus rendszerek biztosítják a kétfaktoros azonosítás követelményeit.
- Az azonosító a felhasználó ujjlenyomatával védett, Smart kártyán tárolt információ.
- Az USB kulcson tárolt információ lehet privát kulcs, amely PKI (Nyilvános Kulcsú Infrastruktúra) alapú működést tesz lehetővé
- A megoldás előnye, hogy összeköthető más PKI alapú alkalmazások használatával, illetve beléptető rendszerekkel.

Kádár Sándor, üzletágvezető

2007. április 22.

SYNERGON

Köszönöm figyelmüket!

SYNERGON GROUP

SPAN SAO infinity FibeX SYNERGON