



IN068 - Az informatikai kultúra biztonsági szabályozása

Készítette:

Szekér-Németh Nikoletta

FOEBKV

Keszthely, 2025. május 11.

Információbiztonság – kidolgozandó feladat – Copilot-támogatással

1. Általam feltett kérdés

Mi a legfőbb célja a *többfaktoros hitelesítésnek* (MFA) egy informatikai rendszerben?

A) Az, hogy a felhasználók több jelszót használjanak, így nehezebb legyen feltörni a fiókjukat.

B) Az, hogy ha az egyik azonosítási módszer (pl. jelszó) kompromittálódik, akkor a másik független azonosító (pl. SMS-kód vagy biometria) megakadályozza az illetéktelen hozzáférést.

C) Az, hogy a felhasználók kényelmesebben tudjanak belépni rendszerekbe, mivel nem elég csak jelszót használni.

D) Az, hogy egyetlen azonosítási forma (például arcfelismerés) kiváltsa a hagyományos jelszavas belépést, és ezzel csökkenjen az adminisztrációs teher.

Helyes válasz:

B) Az, hogy ha az egyik azonosítási módszer (pl. jelszó) kompromittálódik, akkor a másik független azonosító (pl. SMS-kód vagy biometria) megakadályozza az illetéktelen hozzáférést.

Rövid magyarázat a többi opcióra:

A) Gyakori tévhit, hogy MFA csupán több jelszót jelent – valójában különböző *típusú* azonosító tényezőkről van szó (pl. tudás, birtoklás, biometria).

C) Bár a biztonság növekszik, az MFA gyakran *csökkenti* a kényelmet, nem pedig növeli.

D) Az egyfaktoros biometrikus azonosítás nem MFA – az MFA pont abban különbözik, hogy legalább két, egymástól független faktort használ.

2. CHAT GPT – a kérdés

A többfaktoros hitelesítés (MFA) legfőbb célja az információbiztonság növelése, vagyis annak megakadályozása, hogy illetéktelen személyek hozzáférjenek egy informatikai rendszerhez, még akkor is, ha megszerezték a felhasználó jelszavát.

Az MFA lényege, hogy a felhasználónak legalább két különböző típusú azonosítási tényezőt kell megadnia a bejelentkezéshez. Ezek az alábbi kategóriákból származhatnak:

1. *Tudás alapú tényező (valami, amit tud) – például jelszó vagy PIN-kód.*
2. *Birtoklás alapú tényező (valami, amit birtokol) – például mobiltelefon, biztonsági token.*
3. *Biometrikus tényező (valami, ami ő maga) – például ujjlenyomat, arcfelismerés.*

Egy kérdés: Szeretné, ha konkrét példát is mutatnék egy MFA-rendszer működésére a gyakorlatban?

3. CHAT GPT – kiválasztós variáció

A helyes válasz: B) Az, hogy ha az egyik azonosítási módszer (pl. jelszó) kompromittálódik, akkor a másik független azonosító (pl. SMS-kód vagy biometria) megakadályozza az illetéktelen hozzáférést.

Indoklás:

A többfaktoros hitelesítés célja az, hogy megerősítse a felhasználók azonosítását oly módon, hogy több, egymástól független azonosítási tényezőt kelljen megadni. Ezáltal ha az egyik tényező (például jelszó) veszélybe kerül, a másik tényező (például SMS-ben kapott kód vagy biometrikus azonosító) további védelmet nyújt és megakadályozza az illetéktelen hozzáférést.

A többi válaszlehetőség félrevezető vagy nem a legfőbb célt tükrözi:

- *A) téves, mert nem több jelszót használunk, hanem különböző típusú azonosítókat.*
 - *C) az MFA általában kevésbé kényelmes, de biztonságosabb.*
 - *D) az arcfelismerés önmagában nem MFA, hanem egy egyetlen faktor; az MFA lényege pont a többféle azonosítási módszer együttes használata.*
- Szeretnél további példákat látni MFA alkalmazására a gyakorlatban?*

4. A helytelen válaszopciók mely kérdésekre lennének a helyes válaszok?

A) "Az, hogy a felhasználók több jelszót használjanak, így nehezebb legyen feltörni a fiókjukat."

Ez akkor lenne helyes válasz, ha a kérdés így hangzana:

„Mi a jelszómenedzsment egyik célja?” vagy „Miért érdemes minden fiókhoz külön jelszót használni?”

Indoklás: A több, erős és különböző jelszó használata csökkenti annak kockázatát, hogy egy feltört jelszóval más fiókokhoz is hozzáférjenek.

"Az, hogy a felhasználók kényelmesebben tudjanak belépni rendszerekbe, mivel nem elég csak jelszót használni."

Ez akkor lenne helyes válasz, ha a kérdés így hangzana:

„Mi lehet az egyik oka annak, hogy egyes felhasználók ellenzik az MFA használatát?” vagy „Milyen kompromisszumokkal járhat a többfaktoros hitelesítés?”

Indoklás: Az MFA kevésbé kényelmes, ezért nem növeli a kényelmet, hanem inkább csökkenti, még ha biztonságot növel is.

D) "Az, hogy egyetlen azonosítási forma (például arcfelismerés) kiváltsa a hagyományos jelszavas belépést, és ezzel csökkenjen az adminisztrációs teher."

Ez akkor lenne helyes válasz, ha a kérdés így hangzana:

„Mi az egyik előnye a biometrikus azonosítás használatának a jelszavakkal szemben?” vagy „Mi a célja a jelszómentes (passwordless) bejelentkezési rendszereknek?”

Indoklás: Az arcfelismerés vagy ujjlenyomat használata valóban csökkentheti az adminisztrációs terheket, de ez nem MFA, hanem jelszómentes azonosítás.