CTI jelentés

A 2FA jelentősége a kiberbiztonságban

NEMZETBIZTONSÁGI SZAKSZOLGÁLAT

NEMZETI KIBERVÉDELMI INTÉZET

Tartalomjegyzék

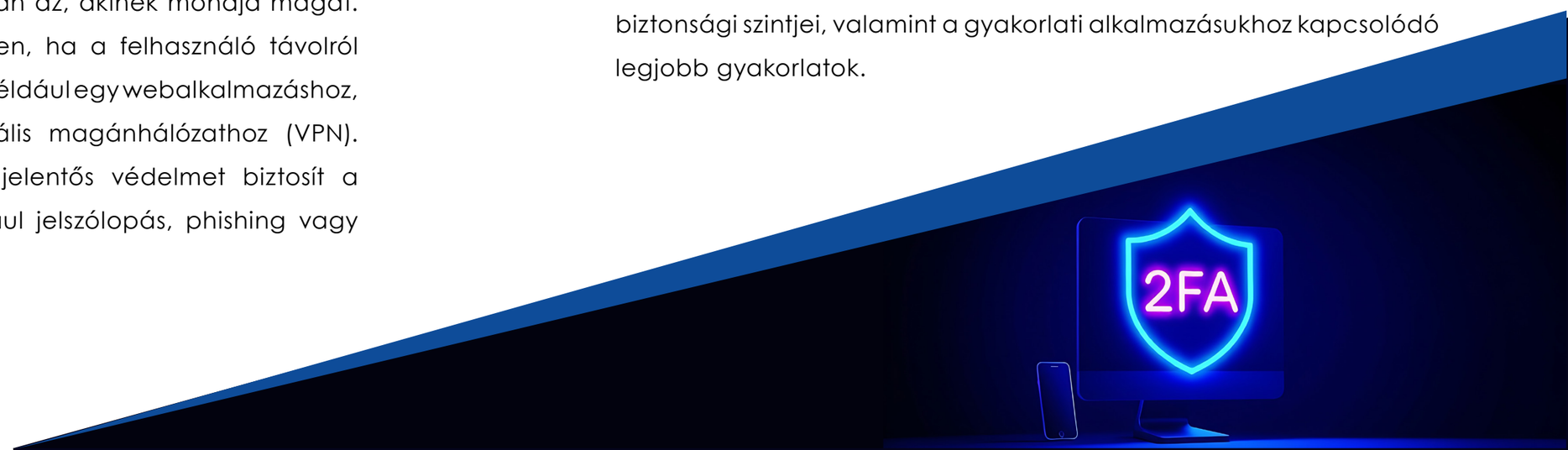
Bevezetés

A digitális információbiztonság korszakában a személyes adatok, üzleti titkok és kritikus rendszerek védelme kiemelt fontosságú. A jogosulatlan hozzáférés elleni védekezés egyik leghatékonyabb eszköze a **többtényezős hitelesítés** (Multi-Factor Authentication, MFA), amely egy olyan biztonsági protokoll, amelyben a felhasználóknak a hozzáférés megszerzéséhez legalább két – de ideálisan több – egymástól független hitelesítési tényezőt kell megadniuk. Az MFA részeként értelmezhető **kétfaktoros hitelesítés** (Two-Factor Authentication, 2FA) az egyik legszélesebb körben alkalmazott gyakorlat, amely a hitelesítési folyamat során két különböző típusú azonosítási tényező kombinációját írja elő – például egy jelszót és egy eszközalapú kódot –, ezzel erőteljesen csökkentve az egyetlen kompromittált hitelesítő adatból fakadó kockázatokat.

A többtényezős hitelesítési eljárások lényege, hogy a hozzáférés engedélyezéséhez nem elegendő csupán egy felhasználóhoz tartozó jelszó. A rendszer egy második – 2FA esetében –, illetve akár harmadik tényezőt is bekér – MFA környezetben – annak megerősítésére, hogy a belépni kívánó személy valóban az, akinek mondja magát. Ez különösen fontos abban az esetben, ha a felhasználó távolról csatlakozik az adott infrastruktúrához, például egy webalkalmazáshoz, üzleti e-mail rendszerhez vagy virtuális magánhálózathoz (VPN). Az ilyen többtényezős megközelítés jelentős védelmet biztosít a kifinomultabb kibertámadások, például jelszólopás, phishing vagy credential stuffing ellen.

A hitelesítési technológiák fejlődése szorosan összefonódik a fenyegetési környezet alakulásával és a vállalati IT-stratégiák változásával. A korai egytényezős hitelesítési modellek – mint amilyet Fernando Corbató vezetett be 1961-ben a világ első digitális jelszavával a Massachusettsi Műszaki Egyetem időmegosztó rendszerében – hamar elavulttá váltak a digitális fenyegetések növekvő komplexitásával szemben. Bár a kétfaktoros hitelesítés elméleti alapjai már az 1990-es években megjelentek, az iparági elterjedése csak évtizedekkel később, a felhőalapú szolgáltatások, a vállalati mobilitás és a saját eszközök használatát (BYOD – Bring Your Own Device) szabályozó trendek térnyerésével indult meg.

Napjainkban az MFA nem csupán egy ajánlott biztonsági intézkedés, hanem számos iparági szabvány és megfelelőségi követelmény része (pl. GDPR, NIS2, PCI-DSS). Az identitásalapú hozzáférés-szabályozás (Identity and Access Management, IAM) rendszereken belül az MFA olyan védelmi réteget képez, amely elengedhetetlen a kritikus információs rendszerek és digitális identitások megbízható védelméhez. A továbbiakban részletesen bemutatásra kerülnek a hitelesítési tényezők típusai, azok technológiai megvalósításai, biztonsági szintjei, valamint a gyakorlati alkalmazásukhoz kapcsolódó legjobb gyakorlatok.



Mi az a kétfaktoros hitelesítés?

A többtényezős hitelesítési rendszerek alapját az eltérő típusú hitelesítési tényezők képezik, amelyek kombinálása révén jelentősen növelhető a hozzáférési biztonság. A tényezőket aszerint csoportosítjuk, hogy a felhasználó mit tud (tudásalapú tényező), mivel rendelkezik (birtokalapú tényező), micsoda ő maga (biometrikus tényező), illetve milyen környezetben és hogyan próbál azonosítani (kontextuális tényezők). A különböző kategóriák egymástól független tulajdonságokon alapulnak, és csak akkor nyújtanak valódi védelmet, ha nem cserélhetők ki vagy helyettesíthetők ugyanazon típusú információval.

A következő szakaszok ezeknek a hitelesítési tényezőknek a működését, alkalmazási területeit és biztonsági sajátosságait mutatják be, technológiai példákkal alátámasztva.

Tudástényező

A többtényezős hitelesítés egyik legalapvetőbb pillére a tudásalapú tényező, amely olyan információkra épít, amelyeket kizárólag a felhasználó ismer. Ez a faktor klasszikusan a jelszavakat, PIN-kódokat és titkos kérdésekre adott válaszokat foglalja magában. Mivel ez az egyik legősibb és legelterjedtebb hitelesítési forma, alkalmazása szinte minden digitális rendszerben megtalálható, ugyanakkor a kizárólagos használata ma már biztonsági szempontból elégtelen.

A jelszavakra alapozott hitelesítés rendkívül sebezhető a brute force, credential stuffing, phishing és keylogger típusú támadásokkal szemben, különösen akkor, ha a felhasználók egyszerű, újrahasznosított vagy gyakran használt jelszavakat alkalmaznak.

A PIN-kódok, mint például egy négy- vagy hatjegyű numerikus kód, hasonló elven működnek, de gyakran egy adott eszközhöz kötöttek – ilyen például a mobiltelefon képernyőzárának feloldása. A biztonsági kérdésekre adott válaszok alkalmazása – például az *„Édesanyád leánykori neve?”* típusú kérdések – manapság egyre inkább visszaszorul, mivel az ilyen információk gyakran könnyen kinyerhetők közösségi médiából vagy nyilvános adatbázisokból.

Mindezek ellenére a tudástényező továbbra is **elengedhetetlen építőeleme** a hitelesítési folyamatoknak, különösen akkor, ha más tényezőkkel kombinálva alkalmazzuk. A jelszavas hitelesítés biztonságossá tehető például jelszószéfek használatával, erős jelszópolitika előírásával, valamint azzal, ha a jelszavakat kizárólag másodlagos tényezőként, például TOTP vagy biometrikus azonosítás mellett alkalmazzuk.

Birtoklási tényező

A többtényezős hitelesítés második alappillére a **birtokláson alapuló tényező**, amely olyan fizikai vagy digitális eszközöket jelent, amelyek kizárólag a jogosult felhasználó birtokában vannak, és amelyeken keresztül a hitelesítés technikailag megvalósítható. Mivel ezek az eszközök elvileg nem ismerhetők meg távolról vagy harmadik fél által egyszerűen, jelentős biztonsági többletet képviselnek a kizárólag tudásalapú megoldásokhoz képest.

Az egyik legelterjedtebb birtokalapú hitelesítési megoldás az egyszer használatos jelszavak (OTP – One-Time Password) használata. Az OTP egy dinamikusan generált numerikus vagy alfanumerikus karakterlánc, amely kizárólag egyetlen belépési vagy tranzakciós művelet során érvényes. Az ilyen kódokat többféle módon lehet kézbesíteni a felhasználóhoz: SMS-ben, e-mailben, mobilalkalmazásokban vagy hardveres eszközökön keresztül.

Az SMS-ben vagy e-mailben küldött OTP-k a legelterjedtebbek, de biztonsági szempontból gyengébb megoldások. Az SMS-alapú OTP különösen sebezhető a SIM-csere (SIM swapping) és az SS7 hálózati támadásokkal szemben, míg az e-mailes kézbesítés biztonsága a felhasználó levelezőrendszerének védelmétől függ, és gyakran hosszabb érvényességi idővel rendelkezik. Mindkét esetben jelentkezhet késleltetés vagy kézbesítési hiba, ami a felhasználói élményre is hatással lehet.

Jóval magasabb biztonsági szintet képviselnek a **TOTP** (Time-Based One-Time Password) algoritmuson alapuló megoldások, amelyeknél az egyszer használatos kódokat a felhasználó eszköze – például egy mobiltelefon – generálja egy szinkronizált időalapú algoritmus szerint. Ezek az alkalmazások – például a Google Authenticator, Microsoft Authenticator, Bitwarden, Aegis Authenticator vagy Raivo OTP – 30 vagy 60 másodperces időablakokban új kódokat állítanak elő, és csak az adott időintervallumon belül érvényesek. Mivel a kód generálása nem igényel hálózati kapcsolatot, és a felhasználónál fut, az ilyen megoldások sokkal ellenállóbbak a lehallgatással és újrafelhasználással szemben.

A TOTP-hez szorosan kapcsolódik a **HOTP** (HMAC-based One-Time Password) algoritmus, amely az idő helyett egy eseményszámláló alapján generál új kódokat. Minden kódgeneráláskor a számláló értéke növekszik, és ez kerül feldolgozásra egy megosztott titkos kulcs mellett. A HOTP kódok nem járnak le automatikusan, hanem érvényesek maradnak egészen addig, amíg a hitelesítési szerver nem fogadja őket. Ez megkönnyíti a használatot olyan környezetekben, ahol nem garantálható a pontos időszinkron, viszont érzékenyebb lehet a számlálók szinkronvesztésére. Az ilyen típusú megoldásokat alkalmazó eszközök közé tartoznak a vállalati környezetben elterjedt hardveres tokenek – például a **Yubico YubiKey OTP**, amely megbízható, offline módon is működő biztonsági réteget biztosít.

A birtokalapú tényezők tehát nemcsak eszközalapú biztonságot kínálnak, hanem képesek adaptálódni a felhasználók mobilitásához, hálózati környezetéhez és biztonsági érettségéhez is. Bár magukban alkalmazva nem nyújtanak teljes védelmet, más tényezőkkel – például jelszóval vagy biometrikus azonosítással – kombinálva a legmegbízhatóbb és leggyakorlatiasabb hitelesítési megoldások egyikét képezik.

Biometrikus tényező

A többtényezős hitelesítés harmadik alappillére az **inherenciaalapú tényező,** ismertebb nevén a **biometrikus azonosítás,** amely a felhasználó egyedi, természetes jellemzőit használja a személyazonosság ellenőrzésére. Ez a megközelítés azon a feltételezésen alapul, hogy az adott jellemző – például ujjlenyomat, arckép vagy hang – kizárólag az adott egyénre jellemző, nem másolható hitelesen, és nem továbbítható másik személy számára.

A biometrikus tényezők a gyakorlatban gyakran szolgálnak második hitelesítési lépcsőként, de bizonyos esetekben – például eszközoldali biztonsági modulokkal kombinálva – akár önálló, elsődleges hitelesítési tényezőként is működhetnek.

A legismertebb fizikai biometrikus azonosító az **ujjlenyomat**, amelynek feldolgozása és összevetése mára már széles körben elérhető a legtöbb okostelefonban, laptopban, valamint FIDO2-kompatibilis biztonsági kulcsban. Az ujjlenyomat-alapú azonosítás pontossága és megbízhatósága különösen magas, ha a minta helyi, titkosított tárhelyen – például TPM vagy Secure Enclave típusú modulban – kerül tárolásra, és nem kerül továbbításra a hálózaton. Az olyan megoldások, mint a Windows Hello, Apple Touch ID vagy a YubiKey Bio például kifejezetten a biztonságos, decentralizált ujjlenyomat-feldolgozásra épülnek.

Az **arcfelismerés** szintén széles körben használt biometrikus technológia, különösen mobilplatformokon. Az arckép alapú azonosítás megbízhatósága nagymértékben függ a használt szenzortechnológiától: míg a 2D kamerák könnyebben megtéveszthetők, a 3D-s mélységérzékelő rendszerek – mint az Apple Face ID – pontosabb azonosítást és fokozott védelmet nyújtanak a visszaélésekkel szemben.

Az **írisz- és retinaalapú azonosítás** rendkívül pontos, de specializált technikai infrastruktúrát igényel. Ezek a módszerek a szem belső mintázatának leképezésével azonosítják a felhasználót, így különösen nagy biztonsági igényű környezetekben – például katonai rendszerekben, államigazgatási hozzáférésvezérlésben vagy kutatólaboratóriumokban – alkalmazzák őket. Használatuk azonban ritkább a kereskedelmi környezetben, mivel az eszközök költségesek és kevésbé elterjedtek.

A **hangazonosítás** az emberi hang egyedi akusztikai jellemzőit – mint a frekvencia, hangszín, intonáció és beszédritmus – használja az azonosítás során. Ez a módszer különösen telefonos ügyfélszolgálatok és call centerek esetében bizonyul hasznosnak, ahol a vizuális hitelesítési formák nem alkalmazhatók. A technológia folyamatosan fejlődik, de érzékeny a háttérzajokra és a felhasználó hangjának pillanatnyi változásaira.

Az újabb generációs biometrikus rendszerek egyre nagyobb figyelmet szentelnek a viselkedésalapú biometrikus jellemzőknek, mint például a **gépelési dinamika**, a **járásminta**, a **képernyőn végzett mozgások** vagy az **egérhasználat sajátosságai**. Ezek a módszerek a felhasználó interakcióinak egyedi mintázatát elemzik, és különösen alkalmasak a folyamatos hitelesítésre, amikor nemcsak a belépés pillanatában, hanem a munkamenet során is aktívan figyelik, hogy valóban a jogosult személy használja-e a rendszert.

A viselkedésalapú tényezők gyakran kockázatalapú döntéstámogatás részeként működnek: ha a felhasználó viselkedése eltér a megszokottól, a rendszer automatikusan magasabb szintű hitelesítést kérhet, például másodlagos MFA-t vagy biometrikus újraazonosítást.

Egy különleges, de rendkívül biztonságos fizikai biometrikus megoldás az **ujj- vagy kézfej vénatérképének használata**, amely infravörös fény segítségével feltérképezi a bőr alatti érhálózat mintázatát. Ez a minta rendkívül egyedi és nem másolható fizikai kontaktus nélkül, így különösen megbízható és magas biztonsági szintet képvisel, elsősorban pénzintézeti, egészségügyi vagy katonai rendszerekben.

Összességében a biometrikus tényezők alkalmazása nemcsak a hitelesítés biztonsági szintjét emeli meg, hanem a felhasználói élményt is javítja azáltal, hogy kényelmes, gyors és – megfelelő implementáció mellett – robusztus védelmet biztosít. Fontos azonban hangsúlyozni, hogy a biometrikus adatok érzékeny személyes adatoknak minősülnek, ezért az ilyen rendszerek tervezésénél és üzemeltetésénél különös figyelmet kell fordítani az adatvédelmi és jogi megfelelőségre is, különösen a GDPR és más nemzetközi szabályozások keretei között.

Egyéb tényezők

A klasszikus háromfaktoros hitelesítési modell – tudás, birtoklás és inherencia – mellett a korszerű azonosítási rendszerek egyre gyakrabban alkalmaznak **kontextuális tényezőket**, köztük a helyalapú és időalapú hitelesítési elemeket, melyek célja a hitelesítési próbálkozás környezetének vizsgálata és kockázatalapú döntések támogatása.

A **helyalapú tényező** (location factor) a felhasználó fizikai vagy hálózati helyzetét veszi figyelembe a hitelesítési döntés során. A rendszer például nyomon követheti, hogy a felhasználó milyen földrajzi régióból próbál bejelentkezni, és ezt összeveti a korábbi aktivitási mintákkal. A helyadatok meghatározása történhet az IP-cím geolokációja alapján, de sok esetben GPS-adatok, mobilhálózati cellainformációk vagy Wi-Fi hálózatok alapján pontosabb lokalizáció is elérhető.

Az **időalapú tényező** azonosítási döntésekhez az adott esemény időpontját vagy időintervallumát veszi alapul. A bejelentkezések időbeli mintázata – például a megszokott munkaidőn belüli vagy kívüli próbálkozások – kockázatértékelési szemponttá válik. Tipikus példa, ha egy rendszer kizárólag munkanapokon és munkaidőben engedi a hozzáférést, vagy ha éjszakai bejelentkezési kísérlet esetén automatikusan erősebb MFA-t kér, vagy akár tiltja is a hozzáférést. Az időalapú szabályok nem csak a **biztonsági protokollokban**, hanem a **dinamikus hozzáférés-vezérlésben** (*adaptive authentication*) is szerepet játszanak.

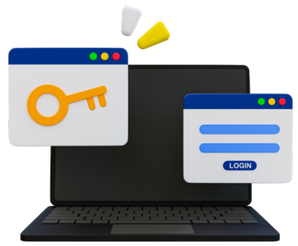
Fontos megjegyezni, hogy az idő tényező nem csupán kontextuális jelleggel bír, hanem technikai alapját képezi bizonyos birtokalapú hitelesítési eljárásoknak is, elsősorban az időalapú egyszer használatos jelszavaknak (TOTP – Time-based One-Time Password). Itt az időablak határozza meg, hogy az adott kód mikor érvényes – jellemzően 30 vagy 60 másodperces intervallumokkal –, így ha a felhasználó nem használja fel időben a kódot, az érvénytelenné válik. Ez a megközelítés különösen hatékony a brute force és replay támadásokkal szemben.

Összességében a hely- és időalapú tényezők nem képeznek önálló hitelesítési faktort a klasszikus MFA-sémában, azonban **kontextuális, kockázatalapú döntéstámogató mechanizmusként** kritikus szerepet játszanak a modern, adaptív biztonsági rendszerekben. Ezek alkalmazása jelentősen javíthatja a felhasználói élményt is azáltal, hogy megszokott környezetben „csendes" módon működnek, de gyanús körülmények esetén automatikusan szigorítják a hitelesítést.

Hogyan működik általánosságban?

A többtényezős hitelesítés működési logikája arra épül, hogy a rendszer nem csupán egyetlen adat, például egy jelszó alapján dönti el, hogy a belépni próbáló felhasználó valóban az, akinek mondja magát. Ehelyett a felhasználót **több, egymástól független hitelesítési tényező** alapján kell azonosítani. A kétfaktoros hitelesítés (2FA) esetén ez általában egy elsődleges, tudásalapú lépéssel kezdődik – például egy felhasználónév és jelszó megadásával –, amelyet egy második lépés követ, amely egy másik típusú hitelesítési tényezőt igényel, például birtokalapú vagy biometrikus elemet.

Tipikus példaként említhető, amikor a felhasználó megadja jelszavát egy webes alkalmazásban, majd ezt követően a rendszer egy hat számjegyű, egyszer használatos kódot kér, amelyet a felhasználó egy mobilalkalmazásból (TOTP), SMS-ből vagy hardveres tokenből tud lekérni. Más esetekben a második tényező lehet egy ujjlenyomat vagy arcfelismeréssel történő azonosítás is, különösen olyan eszközökön, amelyek rendelkeznek beépített biometrikus szenzorral. Amennyiben mindkét lépés érvényes és sikeres, a rendszer hitelesítettként azonosítja a felhasználót, és hozzáférést biztosít a kívánt erőforráshoz.



Kiemelten fontos, hogy az alkalmazott hitelesítési tényezők **ne legyenek egymással technikailag összefüggésben**, és ne származhassanak ugyanabból a forrásból. Ellenkező esetben az MFA biztonsági előnyei részben vagy teljesen elveszhetnek. Például, ha a jelszót és az egyszer használatos jelszót is ugyanazon eszköz tárolja titkosítás nélkül – és ez az eszköz illetéktelen kézbe kerül –, a támadó potenciálisan mindkét faktort kompromittálhatja egyetlen támadási vektoron keresztül. Az MFA lényege éppen az, hogy az azonosítás során **eltérő természetű, fizikailag vagy logikailag elkülönített tényezőket kombinálunk**, így ha az egyik kompromittálódik, az nem elég a másik hiányában a hozzáférés megszerzéséhez.

A gyakorlatban tehát a többtényezős hitelesítés nemcsak technikai akadályt jelent a támadók számára, hanem egy ellenálló, rétegzett védekezési stratégiát, amely jelentősen növeli a rendszer ellenálló képességét a jelszólopáson, adathalászaton vagy brute force támadáson alapuló visszaélésekkel szemben.

Miért fontos ez a kiberbiztonságban?

A többtényezős hitelesítés alkalmazása a kiberbiztonság egyik legalapvetőbb védekezési stratégiájává vált az elmúlt évtizedben. A digitális rendszerek elleni támadások többsége nem technikai sérülékenységeken keresztül történik, hanem a **hitelesítő adatok – elsősorban jelszavak – megszerzésére** irányul. A jelszólopás, adathalászat, adatbázis-szivárgások, illetve különféle brute force és szótár alapú támadások által kompromittált fiókok gyakran szolgálnak belépési pontként a támadók számára vállalati és intézményi rendszerekhez. Mivel **még az erős jelszavak is kikerülhetnek rosszindulatú szereplők kezébe**, önmagukban már nem nyújtanak kielégítő védelmet a mai fenyegetési környezetben.

A **két- vagy többtényezős hitelesítés** egy olyan kiegészítő védelmi réteget biztosít, amely a jelszavak kompromittálódása esetén is megakadályozhatja a jogosulatlan hozzáférést. Tipikus forgatókönyv például, amikor egy támadó sikeresen megszerzi egy felhasználó jelszavát egy adathalász e-mail vagy hamis bejelentkezési oldal segítségével, azonban a belépési kísérlet mégsem jár sikerrel, mert a rendszer egy második, birtokláson vagy biometrikus jellemzőn alapuló tényezőt is megkövetel – például egy időalapú kódot vagy ujjlenyomatot. Ezzel az MFA hatékony védelmet nyújt a social engineering típusú támadások ellen is, amelyek a klasszikus technikai védekezéssel kevéssé szűrhetők ki.

A többtényezős hitelesítés nemcsak technikai előnyökkel jár, hanem egyre inkább megfelelési követelménnyé is válik a különböző iparági szabványok és szabályozások keretében. Számos vállalat, állami szerv és szolgáltató már **alapértelmezésként írja elő a kétfaktoros hitelesítés használatát**, különösen érzékeny adatokat kezelő rendszerek vagy távoli hozzáférést biztosító infrastruktúrák esetén. Az MFA támogatását biztosító technológiák jellemzően **szabványosított hitelesítési protokollokra épülnek**, amelyek lehetővé teszik az interoperabilitást, a biztonságos adattovábbítást és a felhasználói élmény javítását.

Az egyik legelterjedtebb ilyen szabvány a **FIDO** (Fast IDentity Online) protokollcsalád, amely nyilvános kulcsú titkosítást alkalmaz az adathalászat ellen védett hitelesítési folyamatokhoz. A FIDO-megoldások esetén a felhasználó eszközén létrehozott privát kulcs soha nem hagyja el az eszközt, míg a publikus kulcs a szolgáltatóhoz kerül regisztrálásra. A FIDO U2F, FIDO UAF és FIDO2 szabványok lehetővé teszik mind a másodlagos, mind a jelszómentes hitelesítést különböző felhasználási forgatókönyvekben.

Az **OAuth 2.0** egy másik elterjedt szabványosított keretrendszer, amely ugyan nem hitelesítési, hanem engedélyezési protokollként működik, mégis fontos szerepet tölt be abban, hogy külső alkalmazások biztonságosan hozzáférhessenek a felhasználók erőforrásaihoz anélkül, hogy azoknak közvetlenül jelszót kellene megadniuk.

Az **OpenID Connect** (OIDC) erre a keretrendszerre épül, és hitelesítési réteggel egészíti ki az OAuth 2.0-t, lehetővé téve a személyazonosság igazolását webes, mobil- és API-alapú alkalmazásokban.

Szintén kiemelkedő szerepet tölt be a **SAML** (Security Assertion Markup Language) szabvány, amely XML-alapú üzenetváltással biztosítja a felhasználók hitelesítését különböző szolgáltatók között. A SAML a vállalati és oktatási környezetekben gyakori **Single Sign-On** (SSO) megoldások technológiai alapját képezi, lehetővé téve, hogy egyetlen hitelesítéssel több szolgáltatás is elérhető legyen a felhasználó számára.

Összességében a többtényezős hitelesítés alkalmazása nemcsak technikai védelem, hanem szabályozási megfelelőség szempontjából is **kulcsfontosságú**. Megfelelő implementációja jelentősen hozzájárulhat a szervezetek kockázatkezelési stratégiájához, miközben erősíti a digitális identitás integritását és bizalmát az online szolgáltatások igénybevétele során.

Különböző hitelesítési módszerek és működési elvük

A többtényezős hitelesítés megvalósítása során számos különböző technológia és megközelítés áll rendelkezésre, amelyek eltérő biztonsági szintet és felhasználói élményt kínálnak. A kiválasztott módszer hatással van a rendszer biztonságára, az alkalmazás egyszerűségére és az esetleges támadási lehetőségek típusára is. A következőkben részletesen bemutatjuk a legelterjedtebb hitelesítési megoldásokat, azok működési elvét, előnyeit és ismert korlátait.

SMS-alapú hitelesítés

Az **SMS-ben küldött egyszer használatos jelszó (OTP)** az egyik legrégebbi és legszélesebb körben alkalmazott kétfaktoros hitelesítési módszer. A felhasználó az elsődleges azonosító adatainak – például felhasználónév és jelszó – megadását követően egy rövid élettartamú, véletlenszerűen generált kódot kap a regisztrált telefonszámára SMS-ben, amelyet a rendszer a hitelesítés befejezéseként kér be.

Előnye, hogy nem igényel külön alkalmazást vagy speciális hardvert, és szinte minden mobilkészüléken működik. Felhasználóbarát megközelítés, hiszen az SMS használata széles körben ismert és nem igényel technikai előképzettséget.

Ugyanakkor az SMS-alapú hitelesítés biztonsági szempontból ma már elavultnak tekinthető, különösen célzott támadások esetén.

Az alábbi fenyegetések miatt alkalmazása kockázatot jelenthet:

- **SIM-csere** (SIM swap) támadások, melyek során a támadó a mobilszolgáltatónál eléri, hogy az áldozat telefonszáma az ő birtokában lévő SIM-kártyára kerüljön. Ezáltal a támadó megkapja a hitelesítő kódokat, és teljes hozzáférést szerezhet a célzott fiókhoz.
- **Üzenet-elfogás és átirányítás**, például kártékony alkalmazások vagy hálózati kompromittálás révén.
- **A távközlési rendszerek protokollszintű sebezhetőségei**, különösen az SS7 (Signaling System No. 7) rendszer hibái, amelyek lehetővé tehetik a támadók számára az SMS-forgalom megfigyelését és módosítását.

A biztonsági aggályok miatt a National Institute of Standards and Technology (NIST) már **nem javasolja az SMS-alapú 2FA használatát kritikus rendszerek védelmére**. Bár sok szolgáltató továbbra is alkalmazza ezt a módszert, ajánlott olyan korszerűbb alternatívákat előnyben részesíteni, amelyek valódi birtokláson vagy biometrikus azonosításon alapulnak, mint például:

- **TOTP-alapú hitelesítő alkalmazások** (pl. Google Authenticator, Microsoft Authenticator),
- **FIDO2/U2F hardverkulcsok**,
- vagy **push alapú hitelesítési rendszerek**.

A megfelelő alternatíva kiválasztása jelentősen növelheti a digitális fiókok biztonságát, különösen olyan környezetekben, ahol érzékeny adatokhoz vagy rendszerekhez való hozzáférés történik.

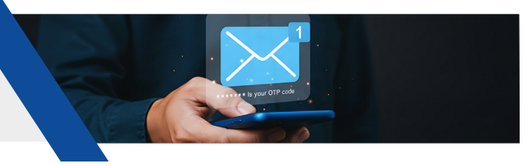
Hangalapú hitelesítés

A **hangalapú hitelesítés** működése hasonló az SMS-alapú megoldáshoz, azonban ebben az esetben a rendszer automatikus hanghíváson keresztül közli az egyszer használatos jelszót (OTP) a felhasználóval. A bejelentkezési folyamat során a rendszer egy előre rögzített telefonszámot hív fel, és szövegfelolvasó algoritmus segítségével bemondja az érvényesítendő kódot, amelyet a felhasználónak a megfelelő mezőbe kell beírnia.

A megoldás fő előnye, hogy nem igényel internetkapcsolatot, és olyan esetekben is használható, amikor SMS fogadására nincs lehetőség – például bizonyos szolgáltatói beállításoknál vagy nemzetközi utazás közben.

A módszer azonban számos **biztonsági korláttal bír**. A hanghívás, akárcsak az SMS, könnyen elfogható, átirányítható vagy manipulálható a megfelelő technikai háttér birtokában. Továbbá szoftveres kártevők és social engineering technikák révén a támadók is megszerezhetik a hangalapú kódokat. Ennek következtében a hangalapú hitelesítés csak korlátozott biztonsági értékkel bír, és nem javasolt önálló másodlagos azonosításként érzékeny rendszerekhez.

E-mail alapú hitelesítés



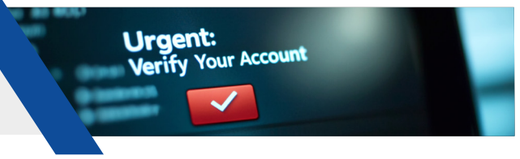
Az **e-mail alapú kétfaktoros hitelesítés** során a rendszer a regisztrált e-mail címre küld egy egyszeri jelszót (OTP) vagy egy hitelesítő linket, amely a második hitelesítési faktorként működik. A felhasználó a bejelentkezést követően az e-mailben kapott információ alapján erősíti meg személyazonosságát, jellemzően egy időkorlátos link megnyitásával vagy egy kód begépelésével.

Az e-mailes megoldás kényelmes, mivel nem igényel okostelefont, külön alkalmazást vagy fizikai eszközt. Elérhető minden olyan eszközről, ahol az e-mail fiók elérhető, ezért gyakran választják azok a felhasználók, akik nincs technikai háttérrel rendelkező, alacsony biztonsági szintű szolgáltatásokat használnak.

Ennek ellenére az e-mail alapú 2FA **számos komoly biztonsági sebezhetőséget rejt**. Az e-mail fiókok nincsenek eszközhöz kötve, így a támadó távoli hozzáféréssel – például egy korábban megszerzett jelszó vagy social engineering technikák révén – megkerülheti a védelmet. Ha az e-mail fiók kompromittálódik, az összes olyan rendszer veszélybe kerül, amely az e-mailre támaszkodik a másodlagos hitelesítés során.

Éppen ezért ez a módszer **nem ajánlott kizárólagos 2FA eszközként**, különösen nem magas biztonsági igényű környezetben. Az e-mail hitelesítés alkalmazása csak akkor tekinthető elfogadhatónak, ha további védelemmel (például hitelesítő alkalmazás vagy hardverkulcs) is kiegészül.

Push értesítések



A **push alapú hitelesítés** egy korszerű és kényelmes kétlépcsős azonosítási megoldás, amely során a felhasználó eszközére – jellemzően egy okostelefonra – érkezik egy valós idejű értesítés, amely tartalmazza a hitelesítési kísérlet részleteit. A felhasználó ezután jóváhagyhatja vagy elutasíthatja a hozzáférési kérelmet egyetlen érintéssel, például egy „Allow" vagy „Deny" gomb megnyomásával.

Ez a típusú hitelesítés azon az elven működik, hogy csak az azonosított eszköz birtoklása igazolja a felhasználó személyazonosságát. A rendszer általában megerősítést kér a hitelesítési kérelem eredetiségéről, így a felhasználó tudatos döntéssel hagyja jóvá vagy utasítja el a belépést. A megoldás tipikus példája a Microsoft Authenticator push értesítése, amely a Microsoft-fiókok bejelentkezésénél használható.

A push értesítések egyik **fő előnye** a felhasználóbarát működés, hiszen nincs szükség kódok begépelésére vagy külön eszközre. Emellett hatékonyan védenek az olyan támadások ellen, mint az adathalászat (phishing), a közbeékelődéses (MITM) támadások vagy a social engineering módszerek.

Biztonsági kockázata abban rejlik, hogy a felhasználó – különösen sietős vagy figyelmetlen helyzetekben – automatikusan jóváhagyhat egy csaló hitelesítési kérelmet. Ez az úgynevezett **push fatigue** jelenség, amikor a felhasználó megszokásból vagy zavartságból engedélyezi az illetéktelen hozzáférést.

A védelem hatékonysága tehát nemcsak a technológián, hanem a **felhasználói tudatosságon** is múlik. A push értesítések alkalmazása olyan környezetben javasolt, ahol az eszköz biztonsága és a felhasználó körültekintése garantált.

Hitelesítő alkalmazások használata

A **hitelesítő alkalmazások** (authenticator apps) az egyik legbiztonságosabb és legszélesebb körben elfogadott 2FA megoldást kínálják. Ezek az alkalmazások – mint a Google Authenticator, Microsoft Authenticator, Twilio Authy vagy Duo Mobile – egy időalapú egyszeri jelszót (TOTP) generálnak, amelyet a felhasználó a bejelentkezés második lépéseként ad meg.

Az alkalmazások jellemzően offline is működnek, azaz nem igényelnek aktív internetkapcsolatot a kód generálásához. Az egyszeri jelszavak 30–60 másodpercenként változnak, így rendkívül nehéz őket visszafejteni vagy másolni, még akkor is, ha egy korábbi kód kompromittálódott.

A hitelesítő alkalmazások használatának legnagyobb előnye, hogy ellenállnak az SMS-alapú megoldásokkal szembeni ismert támadási módszereknek, például a SIM-cserének, lehallgatásnak vagy SS7 sebezhetőségek kihasználásának. Továbbá az alkalmazások **nem kötődnek közvetlenül az e-mail fiókokhoz**, így kevesebb támadási felületet biztosítanak.

Ugyanakkor hátrányt jelenthet, ha a felhasználó elveszíti a készülékét, meghibásodik az eszköz vagy szoftverhiba miatt újra kell telepítenie az alkalmazást. Ezekben az esetekben a kódok is elveszhetnek, ha nem történt **biztonsági mentés vagy másodlagos eszköz beállítás**. A visszaállítás lehetősége alkalmazásonként eltérő, ezért a megfelelő megoldás kiválasztása és beállítása kritikus fontosságú a hosszú távú biztonság fenntartásához.

A hitelesítő alkalmazások tehát **nagyfokú védelmet** nyújtanak, de csak akkor, ha a felhasználók megfelelően kezelik az eszközhasználat, mentés és visszaállítás kérdéseit is.

Melyik hitelesítő alkalmazást válasszuk?

A különböző hitelesítő alkalmazások (pl. Google Authenticator, Microsoft Authenticator, Authy, Duo Mobile) eltérő funkciókkal és képességekkel rendelkeznek, ezért érdemes előzetesen mérlegelni a használat célját és környezetét. A kiválasztásnál több szempont is fontos lehet.

Ha **több eszközön** szeretnénk elérni a hitelesítési kódokat, akkor érdemes olyan megoldást választani, amely támogatja a felhőalapú szinkronizálást. Az **Authy** ilyen funkciót kínál, így a kódokat automatikusan elérhetjük más eszközökön (pl. laptopon vagy tableten) is. Ez ideális olyan felhasználók számára, akik rendszeresen váltanak eszközt vagy több platformot használnak párhuzamosan.

Egyetlen eszközre korlátozódó használathoz megfelelő lehet a **Google Authenticator**, amely egyszerűen használható, offline is működik, azonban nem kínál szinkronizálási vagy biztonsági mentési lehetőséget, így eszközcsere esetén manuális visszaállításra van szükség.

A **Microsoft Authenticator** erőteljes integrációt biztosít a Microsoft ökoszisztémával, de más szolgáltatásokkal is kompatibilis. Felhőalapú biztonsági mentést és push értesítést is támogat, ami gyorsabb és kényelmesebb hitelesítést tesz lehetővé.

Fontos megvizsgálni azt is, hogy az alkalmazás kínál-e biztonsági mentési funkciót, és ha igen, hol tárolja a visszaállításhoz szükséges adatokat (pl. titkosított formában felhőben vagy helyileg).

Visszaállítási kódok

A **visszaállítási kódok** (recovery codes) lehetővé teszik a fiókhoz való hozzáférés visszanyerését akkor is, ha a másodlagos hitelesítési eszköz – például egy okostelefon – elveszik, megrongálódik vagy elérhetetlenné válik. Ezek a kódok egyszer használatosak, és az MFA aktiválása után azonnal létrehozhatók. Javasolt ezeket biztonságos helyen, például jelszókezelő alkalmazásban tárolni, és nem ugyanazon az eszközön, ahol a hitelesítő **alkalmazás** fut.

A legtöbb szolgáltatás lehetőséget biztosít új kódok generálására is, amelyekkel a régi visszaállítási kódokat lecserélhetjük, ha azok kompromittálódtak vagy már nem aktuálisak. A visszaállítási kódok megléte **kulcsfontosságú** az üzletmenet-folytonosság biztosításához, különösen kritikus rendszerek esetében.

Jelszókezelők és hitelesítő alkalmazások integrációja

A **jelszókezelők** és a **hitelesítő alkalmazások** integrációja lehetőséget ad arra, hogy egyetlen felületen belül kezeljük jelszavainkat és MFA-kódjainkat is. Ez a megközelítés nemcsak kényelmi szempontból előnyös, hanem biztonság szempontjából is: csökkenti a hibalehetőségeket (pl. elgépelés, keresgélés), és automatizálhatóvá teszi a hitelesítési folyamatot.

A **Bitwarden**, a **1Password**, a **LastPass** és más vezető jelszókezelők már rendelkeznek beépített TOTP-támogatással, amely lehetővé teszi az egyszeri jelszavak generálását közvetlenül az alkalmazáson belül. A modern megoldások többsége titkosított tárolást, mentést, és bizonyos esetekben platformok közötti szinkronizációt is biztosít.

Ez a fajta integrált megközelítés ideális lehet azoknak, akik centralizált digitális identitáskezelést keresnek, ugyanakkor fontos, hogy csak megbízható, nyílt forráskódú vagy jól auditált szolgáltatót válasszunk, és gondoskodjunk az alkalmazások rendszeres frissítéséről.

Hardveres tokenek, hardverkulcsok

A **hardveres hitelesítő eszközök** olyan fizikai biztonsági kulcsok, amelyek különösen magas szintű védelmet biztosítanak a többtényezős hitelesítés során. Ezek az eszközök – például a **Yubico YubiKey**, a **Token2**, vagy a **Feitian ePass** – egyedi, dinamikusan változó kódokat generálnak, amelyeket a felhasználó manuálisan vagy automatikusan használ fel a bejelentkezési folyamat során.

A hardverkulcsok működésének alapja lehet **TOTP** (időalapú egyszeri jelszó), **HOTP** (számláló alapú egyszeri jelszó), vagy a **FIDO2 / U2F** (Universal 2nd Factor) protokoll, amelyek erős titkosítással biztosítják az azonosítás folyamatát. A modern eszközök gyakran **USB-A/C**, **Lightning**, vagy **NFC** (Near Field Communication) interfészen keresztül csatlakoznak a hitelesítendő eszközhöz, legyen szó számítógépről vagy mobiltelefonról.

Az ilyen eszközök egyik legnagyobb előnye, hogy a biztonsági titok soha nem hagyja el a hardverkulcsot, és offline környezetben is használható, mivel a hitelesítés nem igényel hálózati kapcsolatot. A fizikai jelenlét követelménye pedig jelentősen csökkenti az olyan támadások sikerességét, mint a phishing, session hijacking vagy man-in-the-middle (MITM) támadások.

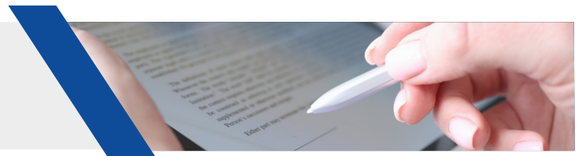
A hardveres megoldások kompatibilisek a legtöbb nagy szolgáltatóval, például a **Google**, **Microsoft**, **Facebook**, **GitHub**, vagy **Amazon** platformjaival. A hitelesítési folyamat során a kulcs az eszközbe történő csatlakoztatás vagy NFC érintés után **egyedi, titkosított választ küld** a szerver részére, amely ellenőrzi annak érvényességét és a felhasználó jogosultságát.

Legfőbb előnyei:

- **Maximális biztonság**: fizikai hozzáférés nélkül a kulcs használhatatlan;
- **Phishing-ellenállás**: FIDO-alapú kulcsok nem engedélyeznek bejelentkezést hamis weboldalakon;
- **Széles kompatibilitás**: támogatott a legtöbb modern platformon.

Hátrányai közé tartozik, hogy további hardver beszerzésére van szükség, valamint az eszköz elvesztése esetén problémát okozhat a hozzáférés visszaállítása – emiatt célszerű több kulcsot regisztrálni vagy helyreállítási opciókat is biztosítani.

Digitális aláírás



A **digitális aláírás** nem csupán hitelesítési módszer, hanem egy **kriptográfiai művelet**, amely egyszerre szolgál a felhasználó azonosítására, valamint a dokumentum integritásának biztosítására. Míg a klasszikus kétfaktoros hitelesítési módszerek célja elsősorban a felhasználói hozzáférés ellenőrzése, a digitális aláírás ezen túlmenően képes bizonyítani a dokumentum eredetiségét és sértetlenségét is, ezáltal kulcsszerepet játszik az elektronikus ügyintézésben, szerződéskötésben, pénzügyi tranzakciókban és archiválásban.

A digitális aláírás **aszimmetrikus titkosításon alapul,** amely egy publikus és egy privát kulcsból álló kulcspárt használ. A folyamat során a felhasználó a dokumentumból egy egyedi kriptográfiai lenyomatot (hash) képez egy hash-algoritmus segítségével, majd ezt az értéket a saját privát kulcsával titkosítja. Ez a titkosított hash képezi magát a digitális aláírást.

Az aláírás ellenőrzésekor a fogadó fél ugyanazzal a hash-algoritmussal újraszámítja a dokumentum hash értékét, majd a felhasználó publikus kulcsával visszafejti az aláírásként kapott hash-t. Amennyiben a két hash érték megegyezik, a dokumentum hitelesnek és érintetlennek tekinthető. Fontos azonban, hogy ez az ellenőrzés nem azonosítja automatikusan a személyt, csak akkor, ha az aláírás egy tanúsítványalapú hitelesítésszolgáltató (CA) által kibocsátott digitális tanúsítvánnyal párosul, amely igazolja az aláíró kilétét.

A digitális aláírás használatának **legfőbb előnye**, hogy **az aláírt dokumentum nem módosítható anélkül, hogy az ne lenne** észlelhető, továbbá lehetőséget biztosít az időbélyegzésre és a nem-megtagadhatóság elvének érvényesítésére. Ez azt jelenti, hogy az aláíró nem tagadhatja le hitelt érdemlően, hogy ő írta alá a dokumentumot.

Szabványos formái közé tartozik az **X.509 tanúsítványokon alapuló PKI** (Public Key Infrastructure), valamint az **eIDAS-rendelet** által szabályozott minősített elektronikus aláírás, amely joghatással egyenértékű a kézzel írott aláírással az Európai Unió területén.

A digitális aláírás egyre inkább integrálódik az üzleti és államigazgatási folyamatokba, és fontos eszköze a papírmentes, biztonságos digitális környezet kialakításának. Ennek ellenére használata technikai tudást és infrastruktúrát igényel, így a bevezetése tudatos előkészítést és szabályozási megfelelést kíván.

Blokklánc-alapú autentikáció

A **blokklánc alapú hitelesítés** egy decentralizált azonosítási megközelítés, amely a blokklánc-technológia fő jellemzőire – változtathatatlanság, átláthatóság és kriptográfiai integritás – épül. E módszer célja, hogy kiváltsa a központi azonosítási rendszerek (pl. jelszószerverek, identitáskezelő platformok) szükségességét azáltal, hogy a felhasználói azonosítási információk **elosztott főkönyvi technológiára** kerülnek.

A hitelesítési folyamat során a felhasználó először létrehoz egy publikus és privát kulcspárból álló **azonosítási egységet**, ahol a publikus kulcs egy azonosítható entitásként, a privát kulcs pedig az adott identitás bizonyításához szükséges kriptográfiai eszközként szolgál. A publikus kulcs rögzítésre kerül a blokkláncon, így az nyilvánosan elérhető és ellenőrizhető. Amikor a felhasználó hitelesíteni szeretné magát, digitális aláírással lát el egy kihívást (challenge), amelyet a rendszer a publikus kulcs alapján ellenőriz, és összeveti a blokkláncon tárolt információval.

A blokklánc alapú autentikáció előnye, hogy nem igényel **központi bizalmi horgonyt**, vagyis nincs szükség megbízható harmadik félre, aki tanúsítványokat állít ki vagy hitelesítéseket végez. Emellett minden hitelesítési esemény **nyilvános főkönyvön** rögzül, így visszakövethető, auditálható és nem visszavonható.

Legfőbb előnyei:

- **Decentralizáció:** nincs központi támadási pont;
- **Megváltoztathatatlanság:** az azonosítási események kriptográfiai védelemmel, visszamenőleg módosíthatatlanul kerülnek rögzítésre;
- **Átláthatóság és ellenőrizhetőség:** minden hitelesítés visszakereshető a blokklánc állapotából.

Ugyanakkor a blokklánc-alapú hitelesítés használata jelentős technikai feltételeket igényel, beleértve a folyamatos internetkapcsolatot, a blokklánc node-ok elérhetőségét, valamint az egyes rendszerek integrálhatóságát. A hitelesítési sebesség és költség függhet a blokklánc hálózat aktuális terheltségétől és működési mechanizmusától (pl. proof-of-work vagy proof-of-stake konszenzus).

Ezeket a rendszereket jelenleg elsősorban kutatási, fejlesztési vagy szűkebb körű üzleti pilotprojektek keretében alkalmazzák, de elméleti megalapozottságuk és biztonsági előnyeik miatt kiemelt szerepet kaphatnak a jövő identitáskezelési megoldásaiban, különösen a self-sovereign identity (SSI) koncepció megvalósítása során.

Milyen platformokon állítsunk be 2FA-t?

A kétlépcsős hitelesítés alkalmazása napjainkra nemcsak ajánlott, hanem sok esetben **elengedhetetlen lépés** az online identitás és érzékeny adatok védelme érdekében. Bármely olyan digitális fiók vagy szolgáltatás, amely hozzáférést biztosít személyes, pénzügyi vagy üzleti jellegű információkhoz, potenciális célpontja lehet illetéktelen hozzáférési kísérleteknek – ezek ellen a többtényezős azonosítás hatékony védelmet nyújt.

Kiemelten javasolt a 2FA bekapcsolása minden olyan platformon, ahol egy esetleges jogosulatlan hozzáférés **súlyos adatvesztéssel**, **anyagi kárral** vagy **hírnévbeli veszteséggel járhat**. Nem elegendő csupán az e-mail fiókokra gondolni – fontos végiggondolni, milyen alkalmazásokban, rendszerekben tárolunk értékes információkat.

A leggyakoribb és legkritikusabb kategóriák, ahol a kétlépcsős azonosítás **különösen ajánlott**, a következők:

- **Online pénzügyi szolgáltatások:** Ilyen például a PayPal, a Revolut, valamint a mobilbanki alkalmazások, ahol egyetlen jogosulatlan belépés is súlyos pénzügyi következményekkel járhat.
- **E-mail szolgáltatók:** Az e-mail fiók gyakran a digitális identitás központja, ezért kiemelten fontos a Gmail, az Outlook, a Yahoo Mail vagy a Hotmail fiókok védelme. Egy feltört postafiók lehetőséget ad más rendszerekhez való hozzáférés visszaszerzésére is (pl. jelszó-visszaállítási linkeken keresztül).

- **Közösségi média platformok:** A Facebook, az Instagram, a LinkedIn és hasonló szolgáltatások nemcsak személyes adatokat tárolnak, hanem társadalmi és üzleti jelenlétünk integrált részei, így kompromittálásuk komoly károkat okozhat.
- **Fájlmegosztó és felhőtároló rendszerek:** A Google Drive, a Dropbox vagy a OneDrive gyakran tartalmaznak érzékeny dokumentumokat, szerződéseket vagy mentéseket, amelyek illetéktelen kézbe kerülve jelentős kockázatot jelentenek.
- **Jelszókezelő alkalmazások:** Mivel ezek az eszközök minden más jelszóhoz és hitelesítő adatunkhoz hozzáférnek, kiemelten fontos a 2FA engedélyezése a Bitwarden, a 1Password, a LastPass vagy a KeePass használata esetén.
- **Felhőalapú és fiókkezelő rendszerek:** Olyan átfogó szolgáltatások esetén, mint a Microsoft-fiók, a Google-fiók, az Apple ID, valamint vállalati rendszerek, mint az AWS vagy a Microsoft Azure, a többtényezős hitelesítés bevezetése üzleti kontinuitási és compliance szempontból is elengedhetetlen.

A 2FA nem csupán egy technikai megoldás, hanem egy proaktív biztonságtudatossági lépés, amellyel jelentősen csökkenthető az adatszivárgások, fiókfeltörések és social engineering támadások sikeressége. Ahol lehetőség van rá, a kétfaktoros azonosítás bevezetését azonnali prioritásként érdemes kezelni – különösen a fenti, kritikus kategóriákban.

Összefoglalás

A **kétfaktoros hitelesítés (2FA)** egy olyan megbízható és hatékony biztonsági mechanizmus, amely jelentősen csökkenti a felhasználói fiókokhoz történő jogosulatlan hozzáférés kockázatát. A rendszer lényege, hogy a bejelentkezéshez két, egymástól független hitelesítési tényezőt kell megadni, ami **többlépcsős védelmet biztosít** még akkor is, ha az egyik tényező – például a jelszó – kompromittálódik.

Az elmúlt években a 2FA használata széles körben elterjedt: e-mail szolgáltatók, pénzügyi alkalmazások, felhőalapú rendszerek, közösségi médiafelületek és jelszókezelők egyaránt lehetővé teszik a többtényezős azonosítás beállítását. Ezek a megoldások nem közvetlenül a felhasználó személyét, hanem a fiókját védik, ezzel akadályozva meg az adatlopást, visszaélést vagy illetéktelen hozzáférést.

A kétfaktoros hitelesítés **proaktív biztonsági intézkedés**, amely kulcsszerepet játszik abban, hogy a felhasználók és szervezetek csökkentsék a jelszólopás, az adathalászat és a célzott támadások sikerességét. A 2FA nem csupán technológiai megoldás, hanem a kiberbiztonsági tudatosság és érettség fontos eleme is.

A **többtényezős hitelesítés (MFA)** bevezetése különösen indokolt érzékeny adatokat kezelő rendszerek, üzletkritikus alkalmazások vagy kritikus infrastruktúrák esetében. A fejlődő technológiák – beleértve a biometrikus azonosítást, a hardverkulcsokat vagy a blokklánc-alapú hitelesítést – lehetővé teszik, hogy rugalmasan és testre szabottan alkalmazzuk ezeket a megoldásokat különböző környezetekben.

Összességében elmondható, hogy a többfaktoros hitelesítés a modern információbiztonság egyik alappillére, amelynek alkalmazása **elkerülhetetlen** a megbízható digitális környezet kialakításához, különösen olyan esetekben, ahol a **digitális identitás és az adatok védelme elsődleges prioritás**.

Források

- **Nemzetbiztonsági Szakszolgálat Nemzeti Kibervédelmi Intézet.** (2023) *Kulcs a digitális élethez – a biztonságos jelszókezelésről.* https://nki.gov.hu/it-biztonsag/elemzesek/kulcs-a-digitalis-elethez-a-biztonsagos-jelszokezelesrol/ (Letöltve: 2025. április 28.)
- **ICTglobal.** (2023) *Kétfaktoros hitelesítés: módszerek és mítoszok.* https://ictglobal.hu/technologia/ketfaktoros-hitelesites-modszerek-es-mitoszok/ (Letöltve: 2025. április 28.)
- **Biztonságosan a Neten!** (2020) *A kétlépcsős azonosítás és fontossága.* https://biztonsagosananeten.hu/a-ketlepcsos-azonositas-es-fontossaga/ (Letöltve: 2025. április 28.)
- **Microsoft Entra.** (2025) *A Microsoft Authenticator használata ellenőrzött azonosítóval.* https://learn.microsoft.com/hu-hu/entra/verified-id/using-authenticator (Letöltve: 2025. április 28.)
- **Fortinet.** (2023) *A biztonságos jelszó és kétfaktoros hitelesítés fontosságáról.* https://fortinet.hrp.hu/a-biztonsagos-jelszo-es-ketfaktoros-hitelesites-fontossagarol/ (Letöltve: 2025. április 28.)
- **Microsoft.** *Mi az a kétfaktoros hitelesítés?* https://www.microsoft.com/hu-hu/security/business/security-101/what-is-two-factor-authentication-2fa?msockid=0d45e4732d2264d43752f1092cfb653f (Letöltve: 2025. április 28.)
- **Mav-IT.** (2024) *Mi az a kétfaktoros hitelesítés, és miért fontos?* https://rendszer-informatikus.hu/mi-az-a-ketfaktoros-hitelesites-es-miert-fontos (Letöltve: 2025. április 30.)
- **KangaDesign.** (2025) *2FA kétfaktoros hitelesítés szerepe a kiberbiztonságban.* https://kangadesign.hu/ketfaktoros-hitelesites.html (Letöltve: 2025. április 30.)
- **Fortinet.** *Multi-Factor Authentication: Benefits, Best Practices & More.* https://www.fortinet.com/resources/cyberglossary/multi-factor-authentication (Letöltve: 2025. április 29.)
- **Fortinet.** *Two-Factor Authentication: How Does 2FA Protect User Logins & Data?* https://www.fortinet.com/resources/cyberglossary/two-factor-authentication (Letöltve: 2025. április 29.)

- **TechTarget.** (2024) *What is two-factor authentication (2FA)?* https://www.techtarget.com/searchsecurity/definition/two-factor-authentication (Letöltve: 2025. április 29.)
- **Digitaltrends.** (2017) *Two-factor security is the best lock for your digital life, but it's not perfect.* https://www.digitaltrends.com/computing/why-2-factor-security-is-flawed/ (Letöltve: 2025. április 29.)
- **Paloalto.** *What is the Evolution of Multi Factor Authentication.* https://www.paloaltonetworks.com/cyberpedia/what-is-the-evolution-of-multi-factor-authentication (Letöltve: 2025. április 30.)
- **TechTarget.** (2025) *What is SAML (Security Assertion Markup Language)?* https://www.techtarget.com/searchsecurity/definition/SAML (Letöltve: 2025. április 30.)
- **FIDO Alliance.** (2024) *User Authentication Specifications Overview.* https://fidoalliance.org/specifications/ (Letöltve: 2025. május 6.)
- **Auth0.** *What is OAuth 2.0?* https://auth0.com/intro-to-iam/what-is-oauth-2 (Letöltve: 2025. május 7.)
- **OpenID.** (2023) *What is OpenID Connect.* https://openid.net/developers/how-connect-works/ (Letöltve: 2025. május 7.)
- **Microsoft.** *What is SAML?* https://www.microsoft.com/en-us/security/business/security-101/what-is-security-assertion-markup-language-saml (Letöltve: 2025. május 6.)

- **How to Geek.** (2017) *U2F Explained: How Google and Other Companies Are Creating a Universal Security Token.* https://www.howtogeek.com/232314/u2f-explained-how-google-microsoft-and-others-are-creating-universal-two-factor-authentication-tokens/ (Letöltve: 2025. május 6.)
- **AuthX.** (2024) *What is SMS Authentication? A Beginner's Guide to Secure Verification.* https://www.authx.com/blog/what-is-sms-authentication/ (Letöltve: 2025. május 6.)
- **NIST.** (2025) *Digital Identity Guidelines.* https://pages.nist.gov/800-63-3/sp800-63-3.html (Letöltve: 2025. május 12.)
- **1Kosmos.** (2023) *What Is an HMAC-Based One-Time Password (HOTP)? How it Works.* https://www.1kosmos.com/security-glossary/hmac-based-one-time-password-hotp (Letöltve: 2025. május 6.)
- **Em360tech.** (2024) *What is Biometric Authentication? Benefits and Risks.* https://em360tech.com/tech-articles/what-biometric-authentication-benefits-and-risks (Letöltve: 2025. május 7.)
- **How to Geek.** (2024) *Microsoft Authenticator vs Google Authenticator: Which One Should You Use for 2FA?* https://www.howtogeek.com/microsoft-authenticator-vs-google-authenticator-which-one-should-you-use-for-2fa/ (Letöltve: 2025. május 6.)

NEMZETI
KIBERVÉDELMI INTÉZET

nki.gov.hu

titkarsag@nki.gov.hu

+36 (1) 325 7672

Nemzeti Kibervédelmi Intézet

@ nki.gov.hu

Kibertámadás!
podcast

2025