Bevezetés

Az információbiztonsági képzéseken, tréningeken unalomig ismételt téma a jelszavak kiválasztása, tárolása, újrafelhasználásának kérdése. A közösségi média mellett a televízióban, rádióban, illetve hírportálokon is többször előkerül a téma, mikor kiberbiztonsági szakértők – általában nagyobb nyilvánosságot kapott jelszószivárgások után – felhívják a figyelmet a felhasználók jelszavainak biztonságára, azok komplexitására és gyakori cseréjének fontosságára.

Fontos kiemelni, hogy egyes szervezetek vonatkozásában egyenesen jogszabályi elvárások vonatkoznak az autentikációs megoldásokra, a jelszavak generálására (hosszára, komplexitására), tárolására, átadására és újra felhasználásának korlátozhatóságára.

De nézzük, miről is van szó, illetve mit tud megtenni az átlagfelhasználó a magánéletében használt jelszavak esetében, illetve milyen jogszabályi elvárások terhelik a szervezeteket, vagy éppen milyen jógyakorlatokat vezethetnek be a társaságok a jelszókezeléssel kapcsolatban, mellyel nagyobb eséllyel védhetőek meg az általa birtokolt nagy értékű üzleti-, pénzügyi- és akár személyes adatok.

A dokumentum felépítése

A dokumentum az alábbi – felhasználást és feldolgozást könnyítő – felosztásban készül:

Folyószövegként kerül feltüntetésre az egyes fejezetek alatt az információkat és összefüggéseiket magyarázó, részletes kifejtés.

Az egyes fejezetek végén, a lényeget összefoglaló részek egy keretes jelölőnégyzetben foglalnak helyet.

A jogszabályi előírásokat tartalmazó összefoglaló részek egy színes háttérrel ellátott keretes négyzet jelöli.

Autentikáció és autorizáció

A bevezetőben említett kérdés megválaszolásához nélkülözhetetlen egyes fogalmak megismerése.

Az **autentikáció** (hitelesítés) során a rendszer azonosítja a felhasználót, általában, amikor megadja a jelszavát, és a felhasználónevét.

Ezzel szemben az **autorizáció** (engedélyezés) a már korábban belépett felhasználót – jogosultságai szerint – a rendszer ellenőrzi, hogy amit megtekintene, amilyen műveletet végezne, ahhoz rendelkezik-e megfelelő jogosultsággal.

Az autentikációnak számos formáját ismerjük, de alapvetően háromféle jól körül határolt típusa ismeretes:

Tudásalapú: jellemzően jelszavak, melyek állhatnak betűkből, számokból, különleges karakterekből, vagy ezek kombinációjából;

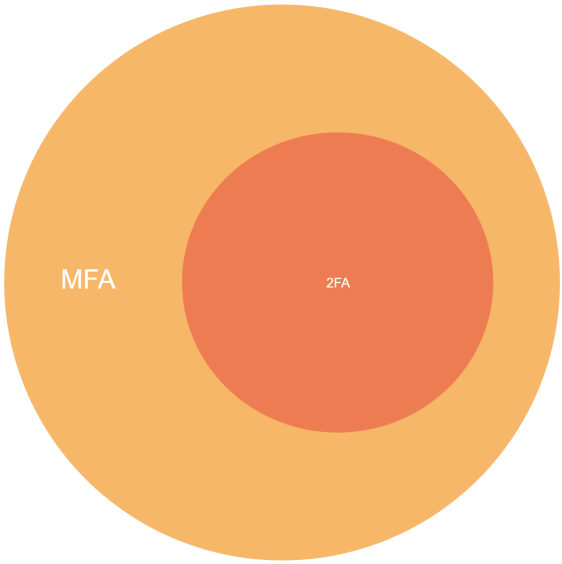
Birtoklásalapú: ezek jellemzően olyan tárgyak, melyek bemutatása, beolvasása szükséges az azonosításhoz, pl. RFID-s belépőkártya, vagy token;

Tulajdonságalapú azonosítás: ennek jellemzője, hogy kizárólag a felhasználóhoz köthető, nem megváltoztatható és nem hagyható el, nem másolható pl. arc-, vagy újnyomat azonosítás.

Hasonlóan az előzőekhez szükséges megértenünk az azonosítás folyamatát, melynek mentén értelmezhetővé válik a médiában és a tudatosító anyagokban oly népszerű kétfaktoros / két lépcsős azonosítás mibenléte.

A **kétfaktoros (2FA) hitelesítés** során a felhasználónak a fenti (jellemzően tudás alapú) autentikációs módszereken túl pontosan egy másik azonosítási megoldás alkalmazása (megerősítés) szükséges a belépési jogosultság megadásához.

A **többtényezős (MFA) hitelesítés** során a felhasználóknak – a fentiekhez hasonlóan – legalább kettő, vagy annál több hitelesítési faktor segítségével kell megerősíteniük az identitásukat. A kettő megoldás közti különbség abban foglalható össze, hogy itt a faktorok száma nem limitált, így akár kettőnél több módozat is épülhet egymásra.



Miért fontos a kettő (vagy több) faktor használata az azonosítás során? Van-e elvárás a szervezetek felé, hogy kötelezően alkalmazzanak ilyen megoldásokat? Megéri-e a társaságoknak efféle azonosítási módokat kidolgozni és bevezetni a szervezeten belül? Van-e olcsó és biztonságos módszer ennek kivitelezésére? Ezek és még számtalan kérdés merülhet fel ezen sorok olvasóiban, melyekre mind megpróbálunk választ adni a későbbiekben.

Miért fontos a 2FA/MFA alkalmazása?

Egyetlen hitelesítési tényező alkalmazása (jellemzően felhasználónév-jelszó pár) a legtöbb felhasználási helyen nem alkalmas a megfelelő szintű biztonság kialakítására és fenntartására, mivel ezen tudásalapú faktorok roppant egyszerűen megkerülhetőek. Egyrészt a felhasználói tudatosság alacsony szintjén a felhasználó egyszerűen kiírhatja valahova, ahol más elolvassa, vagy a felhasználónév/email cím és jelszó kombináció kiszivároghat, esetleg ugyanazt a jelszót használja a privát fiókjain, mint a szervezeti rendszereken. Ellenben, ha többtényezős hitelesítést alkalmazunk, úgy nem elég a felhasználónév és jelszó ismerete a belépéshez, mely önmagában drasztikusan csökkenti az illetéktelen elérések lehetőségét és számát. Minden szervezet úgy tekintsen a felhasználók részére kiadott felhasználónév-jelszó kombinációra, mint egy kulcsra, mely a legértékesebb társasági információkat rejtő széfet nyitja. Ha a kulcs elveszik, illetéktelen kezekbe kerül, onnantól a támadónak szabad bejárása van a „kincseskamrába”.

Hasonló a helyzet a birtoklásalapú azonosítók esetén is, hiszen azokat a felhasználó elveszítheti, azokat a támadó eltulajdoníthatja, lemásolhatja vagy egyéb módon rendelkezhet velük, így bejuthat a szervezet fizikai telephelyeire, vagy annak elektronikus információs rendszereibe.

A koronavírus-járvány alatt megugrott – és jórészt azóta is megmaradó – hibrid, illetve távoli munkavégzés esetén kiemelten fontossá vált a hitelesítés kérdése, hiszen amíg a munkavállaló korábban a munkahelyére érkezéskor a fizikai biztonsági megoldásokat alkalmazó létesítménybe történő belépése során a személyazonosságát kvázi igazolja, addig a távoli munkavégzés, vagy home office során annak ilyetén való bizonyítása, hogy ki ül a kiadott laptop mögött, alapvetően lehetetlen.

Mely szervezetek számára előírás a MFA alkalmazása?

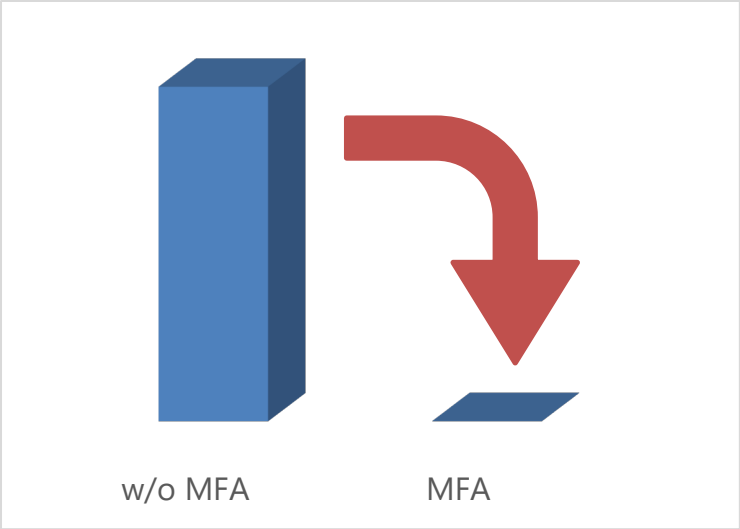
A hazai jogszabályi környezetben az alábbi szervezetek számára ír elő kötelezettséget a jogalkotó:

az állami és önkormányzati szervek elektronikus információbiztonságáról szóló 2013. évi L. törvény **(Ibtv.) hatálya alá tartozó szervezetek**, amennyiben a rendszer biztonsági osztálya 4, bizonyos esetekben 5 (távoli hozzáférés, helyi hozzáférés, privilegizált hozzáférés esetén)

az informatikai rendszer védelméről szóló 8/2020. (VI.22.) számú MNB ajánlás alapján a **pénzügyi közvetítőrendszer tagjai számára.**

Megéri-e a szervezeteknek MFA-t alkalmazniuk?

Ahogy a fentiekben kifejtésre került a társaságok számára – biztonságuk növelése érdekében – már rövidtávon is megéri a megoldás alkalmazása. A Microsoft 2019-ben közzétett tanulmánya szerint önmagában a MFA alkalmazása a **fiókkompromittáló támadások több mint 99,9 százalékát képes blokkolni**.



- A tudás- és a birtoklás alapú azonosítás több szempontból sem elégséges a megfelelő szintű védelemhez.
- Ahhoz, hogy magán-, illetve szervezeti adatainkat biztonságban tudjuk, mindenképpen érdemes beállítani az egyes fiókok esetében a többtényezős hitelesítést, mely önmagában a fiókkompromittáló támadások több mint 99,9 százalékát képes blokkolni.
- Egyes jogszabályok, illetve szabványok és ajánlások egyenesen kötelezővé tehetik az MFA alkalmazását.

Az Ibtv. hatálya alá tartozó szervezetek által üzemeltetett, legalább 4-es vagy 5-ös biztonsági osztályú elektronikus információs rendszerek esetében a helyi-, illetve távoli hálózati hozzáférés biztosításához (privilegizált és nem privilegizált) többtényezős hitelesítést kell alkalmazniuk.

A pénzügyi közvetítőrendszer tagjai számára a titkosítás és az adatszivárgás elleni védelem mellett az adatátvitelt biztosító eszközök esetében minden esetben, valamint a távoli felhasználók esetében szintén ki kell kényszeríteni a legalább kétfaktoros hitelesítést.

Jelszavak

Ma már mindenki használ jelszavakat. Ezek segítségével lépünk be a közösségimédia-fiókjainkba, azokat gépeljük be a hivatalos ügyintézéseink esetén, továbbá jelszavaink segítésével kezdhetjük meg a napi munkánkat. A jelszavakról mára mindenki igen sokat tud, azonban a tudás nem elég, ha nem használjuk a már unalomig ismételt frázisokat.

A rendszereinket feltörhetik, a készülékeinket elveszíthetjük, a jelszavainkat megszerezhetik, azokat akár mi magunk is kiadhatjuk, akár vétlen módon, akár meggondolatlanság okán. Így minden esetben törekednünk kell arra, hogy az eszközeinken tárolt adatok és információk biztonságát a lehető legjobban védeni tudjuk.

Annak megértésére, hogy miért fontosak a jelszavaink, lássunk két nagy port kavart példát a közelmúltból.

- 2021 legnagyobb adatszivárgása egy több korábbi szivárgás során szerzett felhasználónév és jelszókombinációkból álló hatalmas adatbázis volt, mely több milliárd felhasználót érintett. Képzeljük csak el, ha egy nap nem tudjuk használni kedvenc applikációinkat, közösségi médiás felületünket.
- De nem csak az egyszerű felhasználók vannak a célkeresztben, sok esetben a cégek is szenvedhetnek el hatalmas veszteségeket, legyen az közvetlen, vagy reputációt érintő veszteség. Ilyen volt a LinkedIn-t, vagy a Facebook-ot érintő adatszivárgás.

Az ilyen adatszivárgásoknak számtalan oka lehet, melyek egy része teljesen banális (például egy elhagyott eszközről származó információk), de lehetnek figyelmetlenségből eredő, vagy rossz logikai beállításokból adódó hibák, esetleg

olyanok, melyek a sérülékenységekre kiadott frissítések telepítésének elmaradásából adódnak.

A számítási kapacitások felfoghatatlan mértékű bővülésével, a mesterséges intelligencia alkalmazásával, valamint a gyakorlatban is megvalósult kvantumszámítógépek megjelenésével a jelszavak ún. brute force feltörésére fordított idő folyamatosan és nagymértékben csökken. Így a jelszavaink generálása során törekednünk kell a minél hosszabb és komplexebb jelszavak megalkotására.

Megfelelő jelszavak kiválasztása

A jelszavak kiválasztásával kapcsolatban az alábbi tanácsokat fogadjuk meg:

- jelszavaink legyenek hosszúak (legalább 12 karakter),
- legyenek komplexek, bonyolultak (kis és nagybetűk, számok és különleges karakterek),
- az előre beállított (alapértelmezett) jelszavakat mindig változtassuk meg, legyen szó munkahelyi fiókról, vagy egy szolgáltató által kapott routerről,
- azokat soha ne adjuk tovább,
- soha ne írjuk le őket (papírra, jegyzettömbbe, vagy nem védett, ún. plain text formátumban se tároljuk őket),
- ne válasszunk szavakat a szótárból, illetve ne magunkra, vagy a használt rendszerre, szervezetre jellemző jelszót adjunk meg (pl. név, születési dátum, évszám, rendszer neve, etc.)
- jelszavakat soha ne használjuk többször,
- használjunk jelszótároló alkalmazásokat, melyek a komplex és akár véletlen generált jelszavainkat is tárolni tudják,
- minden esetben állítsunk be többtényezős hitelesítést.

Előírások és előremutató gyakorlatok a szervezetek részére

Számtalan kötelező érvényű jogszabály, ajánlás vagy egyéb norma, szabvány ír elő a jótanácsokon túl olyan kötelezően alkalmazandó szabályokat, melyek hiányában az adott szervezet jókora pénzbírságok elé is nézhet.

Emellett számtalan jógyakorlat is létezik, melyek betartásával a társaság és annak üzemeltetési, valamint információbiztonságért felelő szervezeti egysége sokat tehet az általuk kezelt személyes és üzleti adatok védelme érdekében.

A teljesség igénye nélkül nézzünk pár megfontolásra érdemes ajánlást:

- jelszavakra vonatkozó szabályzatok és jelszó házirend kialakítása (minimális követelmények),
- bejelentkezési kísérletek számának maximalizálása, késleltetési idő beállítása,
- fiókzárolás hibás bejelentkezés után,
- jelszavak mentése kizárólag megfelelő kritpográfiai védelemmel, autentikációval és autorizációval ellátott jelszókezelőben történjen,
- jelszóadatbázisok biztonságos mentése,
- kétfaktoros azonosítás kikényszerítése,
- előre beállított jelszavak megváltoztatásának kikényszerítése,
- bejelentkezések és hibás bejelentkezi kísérletek naplózásának beállítása, valamint
- a felhasználók tudatosságának növelése és folyamatos oktatás.

- Mind az átlagfelhasználók, mind a szervezetek számára roppant fontos a megfelelő jelszavak generálása és használata.
- A szervezetek direkt (bírságok, beruházási- és kárenyhítési költségek) és indirekt költségekkel (reputációvesztés, elmaradt haszon) is szembesülhetnek egy felelőtlen vagy kevésbé tudatos felhasználó tevékenységének következtében.
- Ezért a felhasználók folyamatos edukációja, biztonságtudatosságuk és általános kiberhigiéniájuk kialakítása a szervezetek részéről hosszútávon komoly költségmegtakarítást is eredményezhet.

Most lássunk pár konkrét jogszabályi elvárást, melyet az egyes, normák által meghatározott szereplőknek teljesíteniük kell.

Az Ibtv. hatálya alá tartozó szervezetek esetében jogszabályi elvárás

- kis- és nagybetűk megkülönböztetése,
- a karakterek számának meghatározása,
- a kisbetűk, nagybetűk, számok és speciális karakterek megkövetelése,
- minimális jelszóhosszúság maghatározása,
- meghatározott szám karakterváltozást kikényszerítése új jelszó létrehozásakor,
- a jelszavak tárolásának tiltása (kivéve hash),
- minimális és maximális élettartam korlátozás előírása és kikényszerítése,

- meghatározott számú új jelszóig a jelszavak ismételt felhasználásának tiltása,
- első lépést lehetővé tevő ideiglenes jelszó lecserélésének előírása és kikényszerítése,
- meghatározott esetszám korlát alkalmazása a felhasználó meghatározott időtartamon belül egymást követő sikertelen bejelentkezési kísérleteire,
- amennyiben a felállított esetszám korlátot a felhasználó túllépi, automatikusan zárolja a felhasználói fiókot, vagy késleltesse a belépést,
- annak biztosítása, hogy a jelszavak a képernyőkön nem látszódhatnak (pl. csak * a jelszó helyett), valamint
- annak kikényszerítése, hogy amennyiben sikertelen a bejelentkezés, úgy a rendszer csak limitált információt osszon meg a sikertelenség miértjéről (tehát nem mondja meg hogy a karakter hiányzik a jelszóból, csak annyit, hogy "sikertelen belépés", illetve nem ad információ arról, hogy a felhasználónév vagy a jelszó nem megfelelő-e).

A pénzügyi közvetítőrendszer tagjai számára jogszabályi elvárás:

- a jelszókomplexitási és lejárati szabályok meghatározása, valamint kikényszerítése (kockázatarányosan),
- a felhasználói fiók be- és kilépés, jelszóváltoztatás és egyéb autentikációhoz kapcsolódó események adatait naplózza,
- a jelszó felhasználói szerepkörben minimum 12, adminisztrátori vagy technikai szerepkörben min. 15 karakterben történő minimalizálásnak előírása és kikényszerítése,
- a jelszó nem lehet szótár alapú,
- a jelszó nem lehet könnyen kitalálható (nem utalhat a felhasználóra, rokonára, tulajdonára stb.),
- a legutoljára használt 5 jelszó nem lehet ismételten beállítható,
- a jelszó lejárata legalább 1 nap és legfeljebb 90 nap
- legfeljebb 5 egymást követő sikertelen belépés esetén a fiók zárolásának előírása és kikényszerítése,

- az egymást követő sikertelen belépések közötti időtartamok (time-out period) növekedésének beállítása,
- a rendszergazdák, alkalmazásgazdák és más, több szerepkörben is a rendszerhez férő felhasználók belépési azonosítói szerepköreik szerint kerüljenek szétválasztásra,
- a jelszavak tárolása minden esetben rejtjelezetten történjen,
- a kezdeti jelszó megváltoztatását az informatikai rendszer általi kikényszerítése.

A jelszavak tárolása (jelszókezelők)

A korábbiakban láthattuk, hogy a jelszavak kiválasztása és az azokkal kapcsolatos központi beállítások alapvető fontosságúak annak érdekében, hogy az azokkal kapcsolatos biztonsági incidensek elkerülhetőek legyenek. A jelszavak helyes generálása és kezelése, valamint a gyakori jelszóváltoztatási kikényszerítés számtalan problémához vezethet, hiszen a felhasználók a különböző jelszavakat nehezen, vagy egyáltalán nem tudják megjegyezni, mely ahhoz vezethet, hogy azokat felírják, kiragasztják, vagy – hiányos jelszó házirend okán – csupán néhány karakter eltéréssel állítanak be új jelszavakat. Egyes iparági ajánlások egyenesen odáig merészkedtek, hogy azt tanácsolják, amíg az egyes szervezeti vagy felhasználói jelszavak nem szivárogtak ki, addig ne is változtassunk jelszót, tehát ne alkalmazzunk kötelező jelszócsere kikényszerítési időket szervezeti szinten, hiszen ezzel „több kárt okozunk, mint amennyi hasznot hajthatunk vele”.

Na de mi van ezeknek a jelszavaknak a tárolásával? Hogyan tudja megjegyezni az egyszeri felhasználó a sok különböző jelszót? Megoldás lehet erre az ún. jelszókezelő alkalmazások használata, mely egy erős kriptográfiai megoldással dolgozó applikáció, ahol az egyes fiókjaink és a hozzájuk tartozó jelszavak kerülnek tárolásra.

Ilyen megoldásokat kínálnak piaci szereplők, többek között a 1Password, a Lastpass, vagy a Keeper, hogy csak a három legismertebbet említsük. Ezek az alkalmazások nemcsak felhasználói, de üzleti megoldásokat is kínálnak, melyek a szervezet egészére alkalmazhatóak, így biztosítva a munkatársak helyes jelszókezelési tevékenységét. Nagyvállalati környezetben javasoljuk a privilegizált identitáskezelő (privileged access management, PAM) megoldásokat (pl. Thycotic, CyberArk, One Identity), melyek további funkcionalitásukkal (pl. session monitoring, privilegizált információk felhasználására vonatkozó adatok) kielégítik a nagyvállalati igényeket. Továbbá nyílt forráskódú, ingyenes jelszókezelő megoldások is rendelkezésre állnak (pl. KeePass).

A fizetős szolgáltatások mellett vannak a techóriások által kínált ingyenes megoldások is, mint a Google által kínált jelszókezelő, vagy az Apple kulcskarika elnevezésű megoldása. A két nagy techvállalkozás által kínált megoldás egyben – amennyiben a saját böngészőjét használjuk – képes figyelmeztetni minket, amennyiben az adott fiókhoz tartozó jelszó kiszivárgott korábban, így nem kell egyesével, manuálisan leellenőriznünk a fiókjainkhoz tartozó jelszószivárgásokat.

A fenti két (Google, Apple) vállalat az egyes felületeken történő regisztráció során emellett kínál olyan megoldást is, mely a jelszavakat egy általuk tervezett algoritmus mentén véletlenszerűen generálja (kis- és nagybetűk, számok, különleges karakterek), mely alapvetően biztonságosabb, mintha a felhasználó generálná szótáralapúan, továbbá kombinálva a saját jelszókezelő megoldásukkal egyben el is menti ezeket, így azok felírása vagy egyéb módon történő rögzítése nem szükséges. Természetesen ez feltételezi, hogy az adott rendszert és szolgáltatást kell használnunk a jelszavak automatikus beillesztésére.

- A jelszavak folyamatos változtatása – megfelelő jelszóházirend mellett – kontraproduktív lehet, a jelszavak felírásához vezethet.
- A jelszavaink tárolására (egyéni és szervezeti szinten) használjunk jelszókezelő alkalmazásokat.

Az Ibtv. hatálya alatt álló szervezetek számára a jelszavak tárolásával kapcsolatban a jogszabály az alábbiakat írja elő:

- a szervezet a jelszavakat nem tárolja (ide nem értve a jelszóból képzett hash tárolást), és nem továbbítja,

A pénzügyi közvetítőrendszer tagjai számára a vonatkozó MNB ajánlások az alábbi kötelezettségeket írják elő a jelszavak tárolásával kapcsolatban:

- a szervezet biztosítja, hogy az információs rendszerei a felhasználói fiók be- és kilépés, jelszóváltoztatás és egyéb autentikációhoz kapcsolódó események adatait naplózza, azzal, hogy a jelszó sem a kritikus, sem más rendszerekben nem kerülhet naplózásra,
- a jelszavak tárolása – a technikai jelszavak megfelelően kontrollált, vészhelyzetre történő kezelésén kívül – minden esetben rejtjelezetten történjen.

A jövő

Figyelemmel a rosszindulatú aktorok számára is elérhetőbbé váló és folyamatosan növekvő számítási kapacitásokra, a mesterséges intelligencia terjedésére és egyre sokrétűbb felhasználhatóságára, valamint a kvantumszámítógépek hadrendbe állására a hagyományos jelszavak kora hosszútávon leáldozni látszik.

Poszt-kvantumtitkosítás

Az Ibtv. 2023. január 1-jén hatályba lépő rendelkezése már ezekre a kihívásokra is felkészíti a hatálya alá tartozó szervezeteket, mikor előírja, hogy poszt-kvantumtitkosítást[1] (quantumproof) kell alkalmazniuk. Az alkalmazotti kör tekintetében a jogszabály a Szabályozott Tevékenységek Felügyeleti Hatósága (SZTFH) elnökének rendeletében meghatározott:

- kormányzati célú hálózatokról szóló kormányrendelet szerinti igénybevételre kötelezett szervezet,
- a hitelintézetekről és a pénzügyi vállalkozásokról szóló törvény szerinti bankok, valamint
- a földgázellátásról szóló törvény, a földgáz biztonsági készletezéséről szóló törvény, a villamos energiáról szóló törvény, a távhőszolgáltatásról szóló törvény, a víziközmű-szolgáltatásról szóló törvény, valamint a hulladékról szóló törvény hatálya alá tartozó közműszolgáltatók és közszolgáltatást nyújtó szervezek.

Figyelemmel arra, hogy ez a jogszabály törzsszövegében került szabályozásra, így független az egyes szervezetek biztonsági szintjétől, illetve azok által üzemeltetett elektronikus információs rendszerek biztonsági osztályától.

Jelszavak nélküli megoldások

A jövő számtalan kihívást tartogat számunkra. A jelszavak ideje ugyan leáldozni látszik, azonban a rendszerekbe beépített mivoltuk miatt még nagyon sokáig velünk maradnak. Azonban már most is elérhetőek olyan megoldások, melyek a jelszómentes

[1] poszt-kvantumtitkosítás: a matematikailag valószínűsíthetően igazolható, kvantumszámítógép által megvalósított támadás ellen a hagyományos kriptográfiai alkalmazáson felüli poszt-kvantum alkalmazást, illetve megoldást nyújtó titkosítás, amely során a két végpont közötti kommunikáció felhasználásával, az adatátvitellel megosztott kulcsot hoz létre a két végfelhasználó között, anélkül, hogy a kulcsot jogosulatlan harmadik fél megismerné.

világ képét vetítik elénk, csökkentve ezzel az azokkal kapcsolatos biztonsági problémákat. Az adatszivárgások és adatlopások 81%-a köthető gyenge vagy lopott jelszavakhoz.

A jelszómentes megoldások között számtalan lehetőség áll már most is a felhasználók, valamint a szervezetek rendelkezésére. Ezek bevezetése ugyan egyszeri nagyobb költséget generálhat a szervezeteknek, azonban a hosszútávon – beleértve a biztonsági incidensek számának szignifikáns csökkenését – megtérülnek.

A jelszavak hátrányai:

- biztonsági kockázat (elveszhet, kompromittálódhat),
- drága (szabályozások, jelszó házirendek kialakítása, fenntartása, konfiguráció és terméktámogatás, továbbá egy-egy elfelejtett jelszó visszaállítása alatti időben a felhasználó nem tud munkát végezni),
- felhasználói elégedetlenség (gyakori változtatási kikényszerítés negatívan hathat a felhasználók komfortérzetére, különösen, ha bonyolult jelszóházirendeket alkalmaz a szervezet).

Ezek a költségek nagyjából 87%-kal csökkenthetőek a Microsoft vonatkozó tanulmánya szerint.

Az egyes jelszómentes lehetőségek önmagukban, valamint más megoldásokkal együtt is alkalmazhatók, melyek együtt való alkalmazása többtényezős hitelesítésként szolgálhat. Nézzünk egy-két ilyen megoldást.

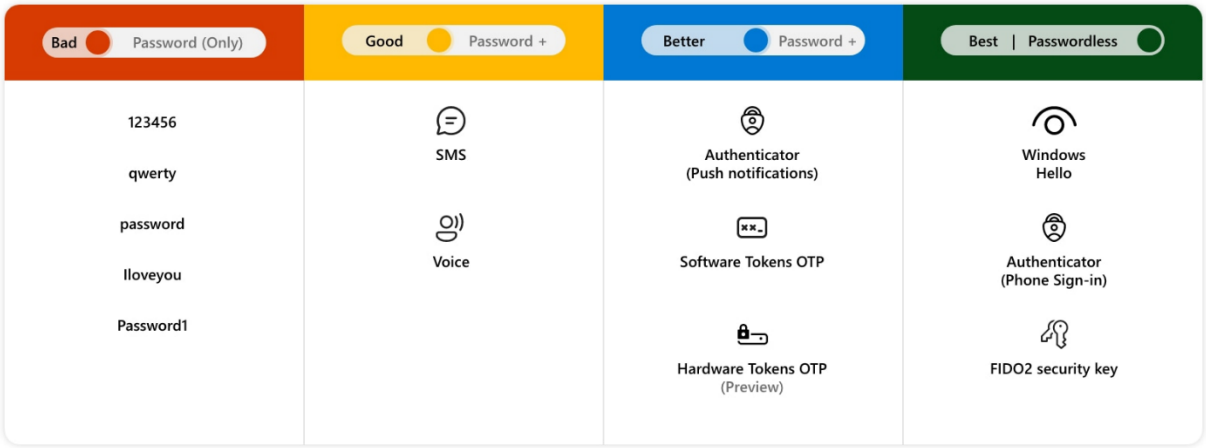
Birtoklásalapú megoldások

A birtoklás alapú azonosítás nem feltétlenül biztonságos, hiszen ilyen esetben az azonosítást végző faktor eltulajdonításával kompromittálódhat az azonosítás. Ilyen megoldás lehet az SMS alapú hitelesítés, vagy az OTP (One-time password).

Biometrikus megoldások

A biometrikus azonosítás, mint fent láthattuk sokkal biztonságosabb, mint bármely más azonosítási megoldás, figyelemmel arra, hogy az egyes testi jegyekkel (íriszkép, ujjlenyomat, arc, vénakép, etc.) kizárólag az egyes egyének rendelkeznek, így a felhasználói azonosítás tökéletesen biztonságos.

A Microsoft ilyen megoldásként kínálja a Hello for Business, vagy a Microsoft Authenticator applikációját (iOS, Android), vagy FIDO2 szabványon alapuló biztonsági kulcsok alkalmazását.

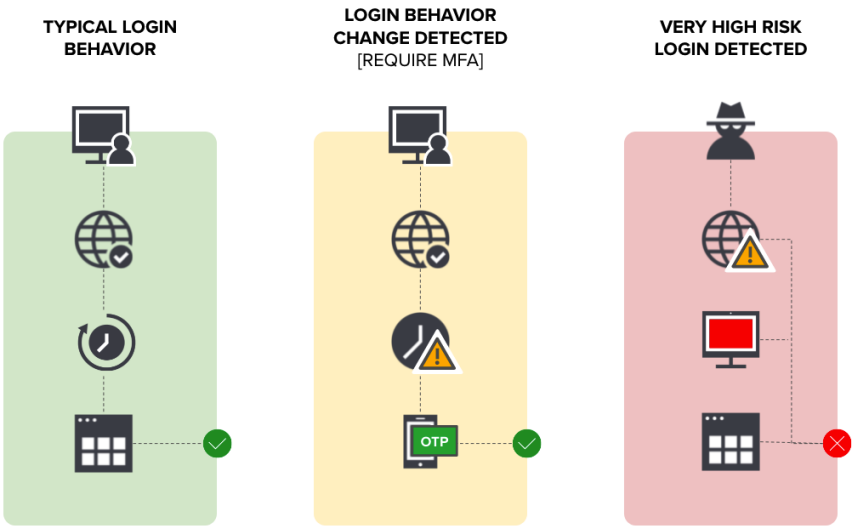


Az Apple iOS mobil operációs rendszerének nemrég megjelent új, 16-os frissítése lehetőséget nyújt olyan bejelentkezési megoldás alkalmazására, mely nem jelszavakat, hanem biometrikus adatokat generálva azonosítja a felhasználókat. Ez eltér a rendszer korábbi verzióiban megismert biometrikus azonosítást követő jelszóbeillesztési funkciótól. Ezt a funkciót egyelőre az egyes szolgáltatóknak és weboldal üzemeltetőknek kell engedélyezniük, így elterjedése hosszú folyamat lehet, azonban hosszútávon az ilyen és ehhez hasonló megoldások az egyre kevésbe biztonságos hagyományos jelszavak lecseréléséhez vezethetnek.

Adaptív (viselkedésalapú) autentikációs megoldások

Az ilyen jellegű megoldások a gépi tanuláson alapuló bejelentkezésekből alakítanak ki olyan viselkedési profilt, melytől való eltérés esetén – kockázatalapon – döntenek a bejelentkezés engedélyezéséről vagy tiltásáról.

Tehát ha a felhasználó általában hétköznap reggelente jelentkezik be otthonról a munkahelyi laptopjáról azt a rendszer engedélyezi. Ha ugyanez a felhasználó – szokásaival ellentétben – hétvégén is bejelentkezik otthonról a saját laptopjáról, a rendszer ezt már kockázatosnak ítélve már egy második tényezőhöz köti a bejelentkezést (pl. SMS, OTP, app, etc.). Amennyiben a felhasználó fiókjával és jelszavával egy másik országból próbálnak bejelentkezni, azt a rendszer automatikusan tiltja és a fiókot zárolja.


TYPICAL LOGIN BEHAVIOR
LOGIN BEHAVIOR CHANGE DETECTED
[REQUIRE MFA]
VERY HIGH RISK LOGIN DETECTED
OTP