# Multi-Factor Authentication (MFA)

Vícefázové ověřování (MFA – *Multi-Factor Authentication*) je bezpečnostní mechanismus, který od uživatele vyžaduje doložení dvou nebo více důkazů (faktorů) totožnosti předtím, než mu je udělen přístup do aplikace, sítě nebo k digitálnímu účtu. Slouží jako kritická vrstva ochrany, která kompenzuje inherentní slabiny tradičních textových hesel.

## Základní principy MFA

MFA je založeno na kombinaci zcela nezávislých kategorií (faktorů). Aby bylo ověření skutečně vícefázové, musí pocházet z různých skupin.

Něco, co znám (Faktor znalosti): Tradiční forma ověření. Patří sem textová hesla, číselné PIN kódy, gesta na obrazovce nebo odpovědi na předem definované bezpečnostní otázky. Samotný tento faktor je dnes kvůli riziku úniku dat, phishingu a útokům hrubou silou považován za nedostatečný.

Něco, co mám (Faktor vlastnictví): Fyzické zařízení, které má uživatel u sebe. Může jít o mobilní telefon (pro příjem SMS, potvrzení push notifikace nebo zobrazení kódu v aplikaci), hardwarový token (např. YubiKey), čipovou kartu nebo hardwarovou peněženku pro kryptoměny.

Něco, co jsem (Faktor inherence): Biometrické charakteristiky uživatele, které jsou unikátní a těžko zfalšovatelné. Zahrnuje otisky prstů, rozpoznání obličeje (Face ID, Windows Hello), skenování duhovky nebo analýzu hlasu. Řadí se sem i pokročilá behaviorální biometrie (styl a dynamika psaní na klávesnici, specifické pohyby myší).

## Běžné metody ověřování

V praxi se nasazují různé metody druhého faktoru, které se zásadně liší svou úrovní bezpečnosti a uživatelskou přívětivostí.

SMS a E-mailové kódy: Nejstarší a v současnosti nejméně bezpečná forma MFA. Systém zašle uživateli jednorázový kód (OTP – *One-Time Password*). Tato metoda je snadno nasaditelná, ale je silně zranitelná vůči phishingu, odposlechu telekomunikační sítě a útokům typu SIM Swapping. Experti doporučují od SMS autentizace ustupovat.

Autentizační aplikace (TOTP): Aplikace v chytrém telefonu (např. Google Authenticator, Microsoft Authenticator) generující časově omezené, obvykle šestimístné kódy (*Time-based One-Time Password*). Kódy jsou počítány lokálně na základě sdíleného tajného klíče (seed) a aktuálního času. Zásadní výhodou je, že nevyžadují mobilní signál ani internetové připojení.

Push notifikace: Po zadání hesla se na displeji spárovaného mobilního telefonu zobrazí výzva k potvrzení přihlášení (např. tlačítko „Povolit“). U bezpečnějších systémů se využívá takzvaný *Number Matching*, kdy uživatel musí na telefonu přepsat dvoumístné číslo zobrazené na obrazovce přihlašovaného počítače, aby se potvrdila jeho fyzická přítomnost u obou zařízení.

Hardwarové bezpečnostní klíče (FIDO2 / WebAuthn): Fyzická USB, NFC nebo Bluetooth zařízení. Jde o

aktuálně nejbezpečnější formu MFA, která je designována tak, aby byla odolná vůči phishingu (*Phishing-resistant MFA*). Klíč využívá asymetrickou kryptografii a kryptograficky ověřuje, zda se uživatel přihlašuje na skutečné (legitimní) webové doméně, čímž eliminuje hrozbu falešných přihlašovacích stránek.

## Zranitelnosti a útoky na MFA

Ačkoliv zavedení MFA dramaticky zvyšuje bezpečnost účtu a zabrání drtivé většině automatizovaných útoků, nejedná se o absolutní ochranu. Zkušení útočníci vyvinuli metody, jak tento mechanismus obcházet.

AiTM Phishing (Adversary-in-the-Middle): Útočník vytvoří falešnou přihlašovací stránku, která funguje jako transparentní proxy server. Jakmile uživatel zadá své jméno, heslo a následně i jednorázový MFA kód, útočníkův server tyto údaje okamžitě v reálném čase předá skutečné službě (např. Microsoft 365). Služba vygeneruje platnou relační sušenku (*Session Cookie*), kterou útočník ukradne. Pomocí této cookie pak přistupuje k účtu bez nutnosti znovu zadávat heslo nebo MFA.

MFA Fatigue (MFA Spamming / Bombing): Útok cílený na uživatele využívající push notifikace. Útočník, který již získal uživatelovo heslo, odesílá na jeho telefon desítky až stovky žádostí o potvrzení přihlášení, často v nočních hodinách. Cílem je oběť vyčerpat, frustrovat nebo zmást natolik, že v návalu zlosti či omylem stiskne „Povolit“. Obrana spočívá právě v zavedení *Number Matchingu*.

SIM Swapping: Sofistikovaná forma sociálního inženýrství, kdy útočník přesvědčí mobilního operátora, případně využije podplaceného zaměstnance na pobočce, aby převedl telefonní číslo oběti na novou, útočníkem vlastněnou SIM kartu. Útočník tak získá plný přístup ke všem ověřovacím SMS kódům.

## Závěr a Best Practices

Základním pravidlem moderní kyberbezpečnosti a digitální hygieny je zapnout MFA na všech online účtech, které tuto funkci podporují. Absolutní prioritou musí být e-mailové schránky, účty v bankovnictví, sociální sítě a správci hesel. V podnikovém prostředí by se mělo MFA spravovat centrálně v rámci systémů IAM (*Identity and Access Management*) a organizace by měly aktivně směřovat k implementaci bezheslového (*Passwordless*) ověřování, které spojuje vysokou bezpečnost s uživatelským komfortem.