Správa hesel a MFA (Vícefaktorové ověřování)

V digitálním světě jsou identity uživatelů neustále pod útokem. Tradiční zabezpečení založené pouze na jednom heslu je v dnešní době považováno za nedostatečné kvůli hrozbám jako phishing, brute-force útoky nebo úniky databází ze služeb.

1. Problematika slabých hesel

Většina uživatelů se dopouští kritických chyb:

- **Opakované používání hesel:** Jedno heslo pro e-mail, banku i sociální sítě.
- **Malá komplexnost:** Používání jmen, dat narození nebo slovníkových výrazů (např. „heslo123“).
- **Předvídatelnost:** Změna hesla stylem „Leden2024“ na „Unor2024“.

2. Správci hesel (Password Managers)

Správce hesel je šifrovaná databáze (tzv. trezor), která generuje a ukládá unikátní, silná hesla pro každou službu. Uživateli stačí pamatovat si jedno **hlavní heslo (Master Password)**.

- **Lokální:** Databáze je uložena pouze na zařízení uživatele (např. **KeePassXC**).
- **Cloudoví:** Šifrovaná data se synchronizují mezi zařízeními (např. **Bitwarden**, **1Password**).
- **Bezpečnostní princip:** Využívají tzv. „Zero-knowledge“ architekturu – poskytovatel nemá přístup k vašemu hlavnímu heslu ani k datům v trezoru.

3. MFA: Vícefaktorové ověřování

MFA (Multi-Factor Authentication) přidává další vrstvu ochrany. I když útočník zjistí vaše heslo, k účtu se nedostane bez druhého faktoru. Faktory dělíme do tří kategorií:

```
1. **Něco, co vím:** Heslo, PIN, bezpečnostní otázka.
2. **Něco, co mám:** Mobilní telefon, hardwarový klíč, čipová karta.
3. **Něco, čím jsem:** Biometrika (otisk prstu, sken obličeje, duhovka).
```

4. Metody druhého faktoru (2FA)

Metoda	Úroveň bezpečnosti	Popis
SMS/E-mail	Nízká	Snadno zranitelné vůči útoku typu „SIM swapping“.
TOTP (Aplikace)	Střední	Generování kódů v aplikacích jako Google Authenticator nebo Bitwarden.
Push notifikace	Střední	Potvrzení přihlášení jedním kliknutím v mobilní aplikaci.

Metoda	Úroveň bezpečnosti	Popis
FIDO2 / U2F	**Vysoká**	Fyzické USB/NFC klíče (např. **YubiKey**). Odolné vůči phishingu.
Passkeys	**Vysoká**	Moderní standard nahrazující hesla biometrickým ověřením v zařízení.

5. Doporučená strategie zabezpečení

Pro maximální ochranu identity v IT encyklopedii doporučujeme:

- Používat správce hesel pro generování hesel o délce alespoň 16 znaků.
- Aktivovat MFA (ideálně TOTP nebo hardwarový klíč) na všech důležitých účtech (e-mail, banka, cloud).
- Vyhýbat se SMS kódům, pokud je k dispozici jiná metoda.
- Pravidelně kontrolovat e-mail v databázích uniklých hesel (např. služba *Have I Been Pwned*).

Související články:

- Kryptografie a šifrování
- Phishing a sociální inženýrství
- Biometrika a její rizika

Tagy: security passwords mfa 2fa bitwarden yubikey authentication