VIAVIS střežíme podstatné

Digitální identita

Kybernetická a informační bezpečnost II

Vladimír Lazecký

vladimir.lazecky@viavis.cz

Bezpečnost v informačních systémech

- **Bezpečnost = záruka důvěrnosti, dostupnosti, integrity**
  - Nejde o tak triviální problém
  - *Dnes důvěrnost*
- **Důvěrnost** = k datům má přístup pouze ten, kdo je k tomu oprávněn
  - Autentizace přístupu = je přistupující tím, za koho se vydává
  - Autorizace přístupu = přístup je tam, kde má oprávnění
  - Auditovatelnost přístupu = vznik průkazných záznamů

Přístupy k definici bezpečnostní politiky

- **Co není zakázáno, je dovoleno**
  - **Maximální důvěra, maximum oprávnění**
  - Postupné zpřísňování pravidel
- **Co není povoleno je zakázáno**
  - Maximální restrikce, postupné uvolňování na základě oprávněných potřeb
- ***Výhody/nevýhody?***

Trend - Zero Trust – nulová důvěra

- **Zero Trust Architecture** (*odmysleme produktový marketing*):
  - Zásady a přístupy k řešení dosažení stanovené míry bezpečnosti
  - **Přístup založený na nedůvěře** – zařízení, uživatel, proces
  - Důvěra není poskytnuta “by default“, ale až na základě ověření
  - **Nikdy nevěř, vždy ověřuj**

Zero Trust – nulová důvěra

- Možný přístup k návrhům bezpečnostních politik
  - **Ověřování** – využití všech možných dat (identita, geolokace, stav, anomálie…)
  - **Minimální možné přístupy** – jen nezbytně nutné minimum, výluka výjimek
  - **Předpoklad incidentů** – systém je předpokládá, je schopen je detekovat a reagovat

Zero Trust

Klíčové principy:

- Jeden zabezpečený zdroj uživatelských identit – jeden vydavatel a správce
- Silná a vynucená autentizace uživatele
- Silná a vynucená autentizace technických prostředků
- Definovaná bezp. politika technicky vynutitelná a „zdravá“ zařízení
- Politika autorizace přístupu, technicky vynutitelná
- Řízení přístupu a generování auditních stop

Digitální identita

- Prostředek co nejjednoznačnější identifikace:
  - Osob - uživatelů
  - Připojených zařízení

Proč nejjednoznačnější a ne jednoznačné?

Vývoj digitální identity

- Základní předpoklady:
  - Řetězec důvěry – poskytovatel a příjemce digitální identity
  - Uzavřené systémy – za perimetrem:
    - Vzájemná znalost uživatelů
    - Identitní prostředky pod jednou kontrolou – jeden správce identit
    - Jméno + heslo

Rozvoj internetu x kyber prostoru

- Nové problémy:
  - **Problém – propojení uzavřených systémů různých vlastníků**
    - **Jak mohu důvěřovat identitě vydané jiným poskytovatelem?**
  - **Míra důvěry v identitní prostředek**
    - **Důvěryhodnost spojení emailová adresa x osoba**
    - **MAC adresa x zažízení**

Osobní digitální identita

- **Úřední digitální identita**
  - Komunikace se státními orgány
- **Soukromá digitální identita**
  - Bankovní identita
  - Uživatelská identita:
    - Přístup k soukromým zařízením
    - Webové a jiné služby
    - Komunikační platformy
    - Sociální sítě
- **Profesionální digitální identita**

Osobní digitální identita

- **Úřední x soukromá x profesionální digitální identita**
  - Požadavky na různou úroveň bezpečnosti
  - Aspekty digitální stopy
  - **NUTNOST ODDĚLENÍ DLE BEZPEČNOSTNÍCH POŽADAVKŮ**
- **Digitální identita pod kontrolou**
  - Rizika související s počtem identit
  - Systematické řešení
  - Řešením není mobilní telefon (popření vícefaktorové autentizace)

Digitální identita – elektronický podpis

- Snaha o jednoznačnou identifikaci osoby
  - Nahrazení „fyzického podpisu“
  - Vysoká míra důvěry
- Vlastnosti:
  - **Autenticita** – ověřitelnost identity subjektu že je tím, za koho se vydává
  - **Integrita** – průkaznost, že v podepsané zprávě nedošlo ke změně
  - **Nepopiratelnost** – subjekt nemůže popřít vytvoření podpisu
  - **Časové ukotvení** – časové razítko, obvykle vydává třetí strana, průkaznost času podepsání

Úřední digitální identita

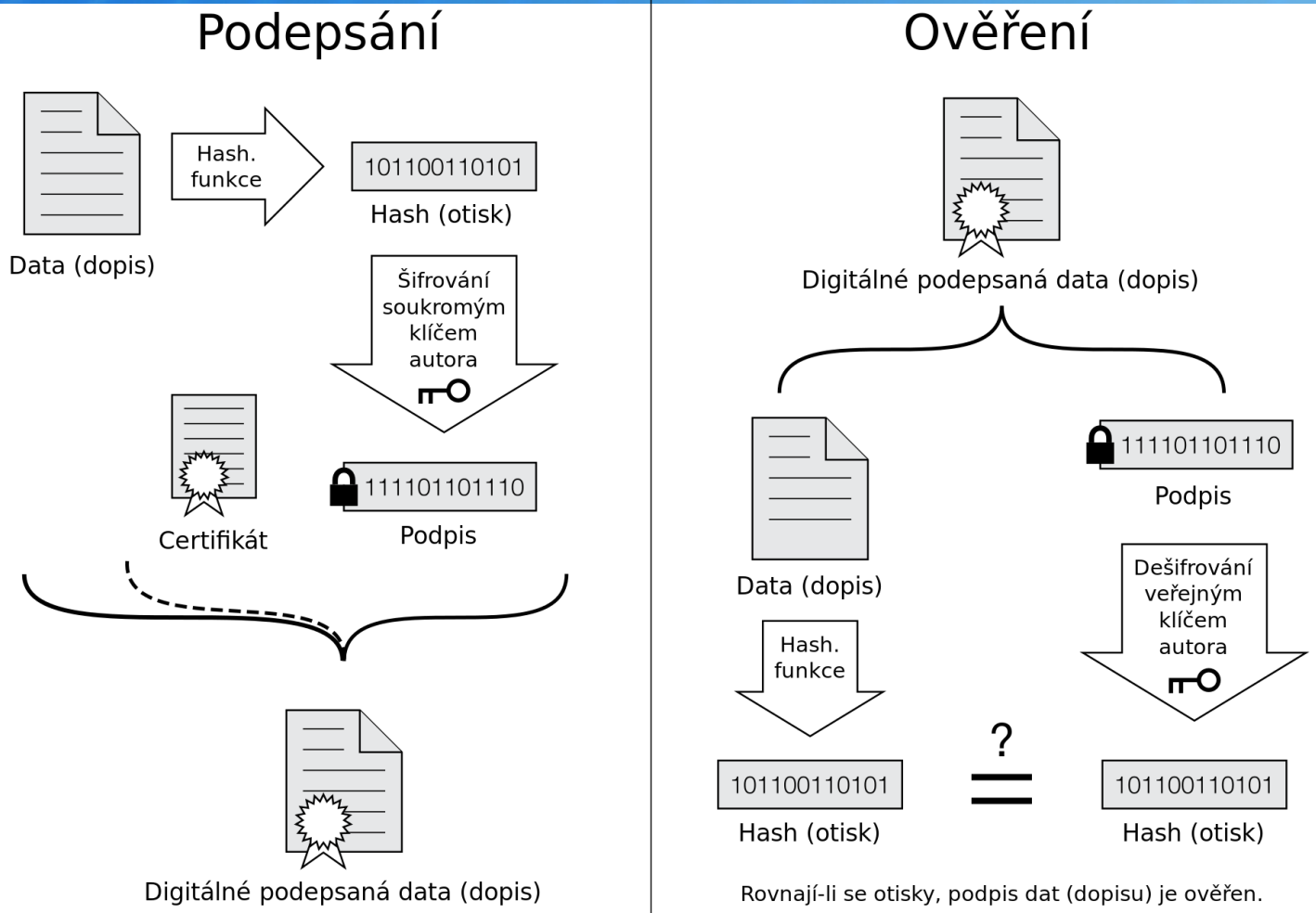
Úřední digitální identita

- Schopnost autentizace a autorizace úkonů se státní a veřejnou správou
- Právní úkony v oblasti soukromého práva
- Přístupy do IS státní správy

Elektronický podpis – snaha od roku 2000

- Kryptografický princip
  - **Asymetrická kryptografie**
  - **Subjekt vlastní dva klíče:**
    - **Veřejný klíč** – veřejně sdílený
    - **Soukromý klíč** – utajená data pouze pod kontrolou subjektu

Podpisování zpráv



https://cs.wikipedia.org/wiki/Elektronick%C3%BD_podpis#/media/Soubor:Digital_Signature_diagram_cs.svg

Řetězec důvěry

- **Kořenová (root) certifikační autorita – certifikační autorita pro certifikační autority**
  - Důvěryhodný subjekt
  - Vydávání certifikátů – veřejných klíčů s údaji o majiteli
  - Certifikáty certifikační autority jsou podepsány klíče uživatelů
  - Ověření platnosti klíčů
    - Nic složitého, stejný princip, jako u podepisování dokumentů, dokumentem je veřejný klíč subjektu

Bezpečnostní problémy certifikační autority

- **Ověření**:
  - Jak se ověřuje identita subjektu u vydání certifikátu (jde o IT problém?)
  - CA potvrdí veřejný klíč, soukromý si dopočítá subjekt sám – proces pod kontrolou subjektu
  - Kompromitace soukromého klíče subjektu
  - Ověření subjektu hlásící kompromitaci
- **Rychlost**:
  - Zneplatnění kompromitovaného certifikátu
    - Závažný a drahý procesní problém
- **Odolnost proti chybám**
  - Vícenásobné ověřování x rychlost

Bezpečnostní problémy subjektu

- **Privátní klíč**
  - **Ochrana klíče:**
    - Úložiště, zálohování
    - Autentizace subjektu
    - Autentizace operace s klíčem
    - Detekce kompromitace
    - Zneplatnění klíče
  - Složitost procesu
    - Se složitostí roste riziko chyb
      - Instalace kořenových certifikátů, řetězce důvěry, úložiště, autentizace, aktualizace
  - **Zařízení pod kontrolou – VÍRA a zase VÍRA**

Elektronické podpisy – typy zjednodušeně

- **Kvalifikovaný elektronický podpis**
  - Komunikace s „úřady“
  - Limity – šifrování, autentizace přístupu
- **Komerční certifikáty**
  - „Libovolný způsob použití“
  - Nižší úroveň záruky
  - Lze využít pro šifrování, autentizace
- ***Míra bezpečnosti je daná nejslabším článkem řetězce, kde jej vidíte?***

Stav v ČR

https://info.identitaobcana.cz/

Podporované identitní prostředky

- **Občanský průkaz s čipem** – vysoká úroveň záruky

- **NIA ID** – „státem poskytovaný identifikační prostředek založený na kombinaci jména, hesla a SMS kódu, dříve označovaný jako uživatelský účet“
- **Mobilní klíč** – „státem zdarma poskytovaný identifikační prostředek, který představuje využití přihlašování bez potřeby zadávání dalších ověřovacích kódů“

- Soukromí poskytovatelé – **bankovní identita**

- ***Diskuse – jaká je míra bezpečnost mobilních klíčů? Čím je dána?***

Úroveň záruky dle eIDAS

- eIDAS - Nařízení Evropského parlamentu a Rady (EU) č. 910/2014 ze dne 23. července 2014 o elektronické identifikaci a službách vytvářejících důvěru pro elektronické transakce na vnitřním trhu a o zrušení směrnice 1999/93/ES
- Úrovně důvěry:
  - Nízká
  - Značná
  - Vysoká
- Požadavky zahrnují celý systém e identit (vydávání, užívání, uznávání)

Digitální identita - trend

Rada EU Tisková zpráva 6. prosince 2022 11:15

Evropská digitální identita (elektronická identifikace): Rada pokročila s prací na digitální peněžence EU, což představuje změnu paradigmatu digitální identity v Evropě

Rada přijala společný postoj („obecný přístup“) k navrhovanému právnímu předpisu tykajícímu se rámce pro **evropskou digitální identitu** (eID). Revidované nařízení má za cíl zajistit všeobecný přístup občanů a podniků k **bezpečné a důvěryhodné elektronické identifikaci a autentizaci** prostřednictvím osobní digitální peněženky v mobilním telefonu.

> Digitální technologie mohou náš život velmi usnadnit. Jsem přesvědčen, že evropská peněženka digitální identity je pro naše občany a podniky nepostradatelná. Její zavedení bude znamenat obrovský pokrok ve způsobu, jakým lidé používají svou totožnost a pověření v každodenním kontaktu s veřejnými i soukromými subjekty a jak využívají digitální služby. A to vše při plném zachování kontroly nad svými údaji.
>
> — Ivan Bartoš, místopředseda vlády České republiky a ministr pro místní rozvoj a digitalizaci

https://www.consilium.europa.eu/cs/press/press-releases/2022/12/06/european-digital-identity-eid-council-adopts-its-position-on-a-new-regulation-for-a-digital-wallet-at-eu-level/

Digitální peněženka

- **Rozvíjí eIDAS z roku 2014**
  - Státy budou zdarma vydávat elektronické peněženky pro mobilní telefony
  - Vysoká úroveň záruky
  - Povinná certifikace poskytovatelů
- ***Diskuse – v čem vidíte bezpečnostní problémy?***

Digitální peněženka – plánované využití

- **Peněženka = kontejner**
  - Doklady – řidičák, erecepty…
  - Dokumenty
  - Platební karty
- ***Diskuse – opět, v čem vidíte bezpečnostní problémy?***

Soukromá digitální identita

- **Soukromá digitální identita**
  - Soukromé přístupy a úkony
  - Míru bezpečnosti si určuje uživatel sám
- **Soukromá digitální identita pod kontrolou**
  - Uživatel ji vytváří vědomě, má ji pod kontrolou
- **Soukromá digitální identita bez kontroly**
  - Vzniká u poskytovatele služby na základě digitálních stop

Soukromá digitální identita pod kontrolou

- **Stanovení bezpečnostních požadavků:**
  - Osobní BIA (Businness Impact Analysis)
  - Vysoká míra – bankovní přístupy, peněženky, doklady, zařízení s cennými daty, přístupy, certifikáty, soukromé LAN…
  - Střední míra – komunikační platformy, profily sociálních sítí…
  - Nízká míra – registrace u webových služeb

Soukromá digitální identita – vysoké nároky

- **Zásady pro autentizaci – prokazování identity**
  - **Split autentizačních dat:**
    - Nikdy nenechávat autentizační data a data na jednom zařízení
    - Digitální identita pod plnou kontrolou uživatele
    - Nastavení autorizačních pravidel (sdílené složky, více uživatelské systémy, cizí zařízení…)
  - **Více faktorová autentizace:**
    - Libovolná kombinace - mít, vědět, chovat se, být…
    - Pozor na biometriky – jaké je jejich omezení?
    - Časová omezení
    - Procesy detekce a řešení kompromitace identity

Soukromá digitální identita – střední nároky

- **Zásady pro autentizaci – prokazování identity**
  - **Oddělení identit s vysokými, středními a nízkými nároky**
    - Kompromitace jedné úrovně nesmí znamenat kompromitaci jiné
    - Bezpečnostním faktorem je složitost a komplikovanost
  - **Více faktorová autentizace:**
    - Je výhodou
    - Nespojovat s vysokými nároky
    - Bezpečnost je dána nejslabším článkem – pozor u emailových identit

Soukromá digitální identita – nízké nároky

- **Zásady pro autentizaci – prokazování identity**
  - Silná hesla
  - Zvážit dopady
  - Rozdělení identit a identity pod kontrolou

Profesionální digitální identita

- **Digitální identitu stanovuje vlastník systému**
  - Systém za perimetrem
  - Míra bezpečnosti musí odpovídat požadavkům na celkovou bezpečnost
    - Jméno + heslo ve zdravotnickém IS ☺

Profesionální digitální identita

- **Některé koncepty**
  - Single Sign On
    - Jedno přihlášení, autentizace a autorizace přístupů do všech systémů
    - Výhody/nevýhody?
  - Separed Sign On
    - Přihlašování do IS dle jejich bez. úrovní

Profesionální digitální identita

- **Bezpečnostní problémy**
  - Důvěryhodnost správce
  - Uživatelské role
  - Kontrola rozdělení identit uživatelů
  - Detekce a řešení kompromitace
- Přístup – striktní technická opatření bez možnosti obcházení

Digitální identita využívající behaviorální biometriky

- **Biometrika založená na porovnávání vzorců chování**
  - Předpoklad – dostatek behaviorálních dat
  - Využití AI
  - Nepřipravené bezpečnostní koncepty
    - Uložiště certifikátů může mít uživatel pod kontrolou
    - Uložiště behaviorálních dat?

Digitální identita využívající behaviorální biometriky

Běžně využívané mechanismy

- **KEYBOARD BEHAVIOR –** dynamika úhozu, způsob psaní, rychlost psaní, užívání speciálních kláves, klávesové zkratky
- **MOUSE BEHAVIOR** – způsob pohybování myší, pohyby do okrajů obrazovky, za obrazovku, rychlost pohybu…
- **PHONE BEHAVIOR** – svislé či podélné využívání obrazovky, způsob otáčení, rychlost pohybu, úhly natočení
- **TOUCHSCREEN BEHAVIOR –** způsob použití doteků, rychlost pohybu prstu, úhel prstu, obrys prstu, síla tlaku

Digitální identita využívající behaviorální biometriky

Bezpečnostní výhody

- Obtížnost prolomení - biometrika
- Jednoduchost, běží na pozadí, neobtěžuje uživatele
- Vysoká spolehlivost
- Snadnější detekce kompromitace

Digitální identita využívající behaviorální biometriky

- **Bezpečnostní nevýhody**
  - Limit biometrik – kompromitace jednou provždy
  - Dostatek dat pro vytvoření behaviorálního profilu
  - Kdo má nad identitou kontrolu, jak ji lze ověřit
  - Řešení anomálií

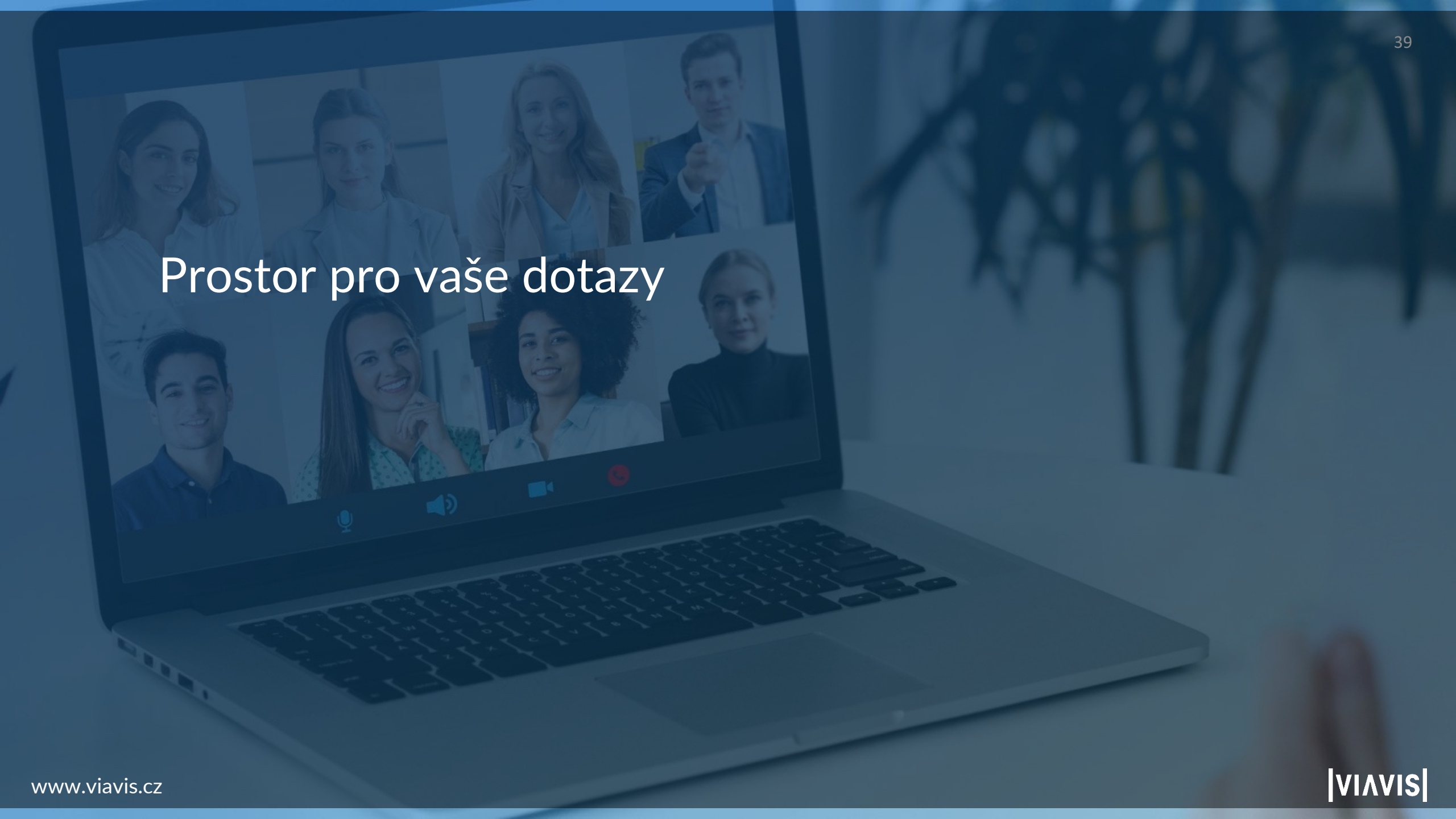
Co vlastně vlastníme v mobilním telefonu?

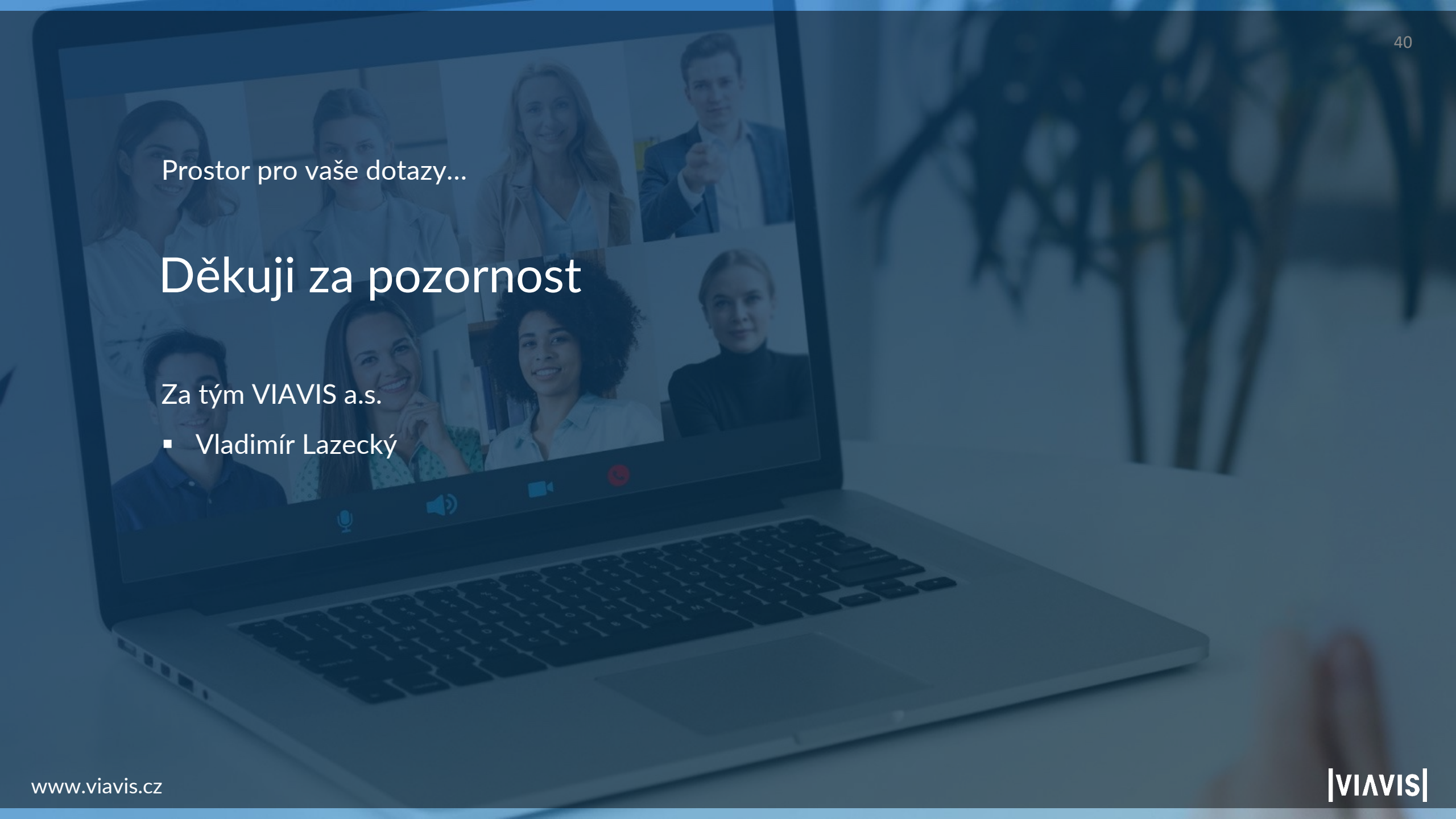
Digitální identita využívající behaviorální biometriky

- **Biometrika u nízké úrovně zabezpečení**
  - Webové a free služby – čím platíme?
  - Jakékoli služby s možnosti měření vzorců chování uživatelů
  - Aplikace v osobních zařízeních
  - Operační systémy, cloudové služby

Proč je obrovský marketingový tlak na využití cloudových služeb?

Prostor pro vaše dotazy





Prostor pro vaše dotazy…

Děkuji za pozornost

Za tým VIAVIS a.s.

- Vladimír Lazecký