Lekce 6.1:

Digitální identita

Ing. Pavel Roubal

Kapitola 6:

BEZPEČNÉ DIGITÁLNÍ PROSTŘEDÍ

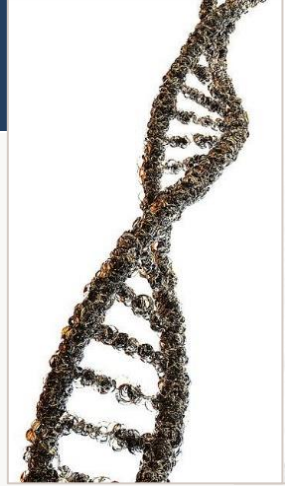
K této prezentaci jsou k dispozici cvičení. Pracovní sešit pro žáky objednávejte na webu:

www.opocitacich.cz

Pro pohodlné promítnutí prezentace v prohlížeči webu klepněte vpravo nahoře na Spustit prezentaci
a pak již pouze klepejte myší nebo mezerníkem…

Biologická identita

- **Identita = totožnost osoby.** Tedy moje identita = kdo jsem **JÁ**.
- Všichni máme svoji **biologickou identitu**.
- **Biologická identita** je dána naším **genomem** a dá se jednoznačně určit testem **DNA**.
- **Biologická identita** se navenek projevuje naší **fyziologií**, tedy **kombinací biologických vlastností** (tvář, výška postavy, tvar těla, otisky prstů, oční duhovka atd.).
- **Biologická identita** se dá určit také z hlasu člověka a dokonce i ze způsobu jeho pohybu (chůze).



Biometrie používá snímání našich biologických vlastností (zejména otisku prstu a skenu obličeje) pro určení **oprávnění přístupu** k počítačovým systémům.

Více je zmíněna v části *3.3 Bezpečnost na webu*.

Právní identita

- **Identita = totožnost osoby.** Tedy moje **identita** = kdo jsem **JÁ**.
- **Právní identita** určuje mne jako **člena společnosti**. Je určena zejména mým **jménem**, dále také **adresou** a mým **státním občanstvím**.
- Protože však jmen není tolik, jako lidí a identifikace člověka by nebyla **jednoznačná**, používají se státem určené identifikátory, například **rodné číslo**.
- **Fyzická identita** člověka je dána **spojením jeho biologické identity s jeho právní identitou**.
- **Doklady** určující moji právní identitu (občanský průkaz, pas) proto obsahují **biometrické prvky** (moji fotografii či sken obličeje a otisk prstu).

Z právní identity vyplývají má **práva** jako občana nějakého státu a také moje **povinnosti** vůči tomuto státu.

Právem je například právo na bezplatné základní vzdělání, právo na lékařskou péči, sociální zabezpečení atd.

Digitální identita (také někdy internetová identita)

- **Identita = totožnost osoby.** Tedy moje **identita** = kdo jsem **JÁ**.
- Uživatelské účty (e-mail, Facebook apod.) tuto podmínku **nesplňují**. (Viz dále v této lekci.)
- **Spojení digitální identity s fyzickou** musí **garantovat státem oprávněný subjekt**.
- Pro občany jsou k dispozici minimálně tyto zaručené způsoby prokázání digitální identity:
  - kvalifikovaný **osobní certifikát** (podpis),
  - **datová schránka**.
- Obojí poskytují za poplatek státem akreditované (schválené) instituce – **certifikační autority**. Největším poskytovatelem těchto služeb v ČR je **Česká pošta**.

Digitální identita, pokud to má být opravdu **identita**, musí být **spojena s naší fyzickou identitou**.

Kvalifikovaný osobní certifikát – elektronický podpis

- **Kvalifikovaný osobní certifikát** je **elektronický kód**, který je **spojen** s určitou **fyzickou osobou**.
- Toto spojení garantuje **certifikační autorita**, která certifikát vydala.
- Pro získání elektronického podpisu je zapotřebí:
  - Vygenerovat si předem žádost o elektronický podpis (certifikát),
  - zajít osobně k poskytovateli el. podpisu (např. na pobočku České pošty a.s.),
  - předložit svůj občanský průkaz (OP).
  - Pracovník certifikační autority **ověří** vaši **žádost** a vaši **totožnost** (fyzickou identitu) podle OP a vygeneruje váš elektronický podpis.

Elektronický podpis musí být uložen na tzv. **tokenu, nosiči certifikátů.**

Tokeny jsou speciální USB flash disky nebo elektronické čipy. Přístup k tokenu je **chráněn heslem**.

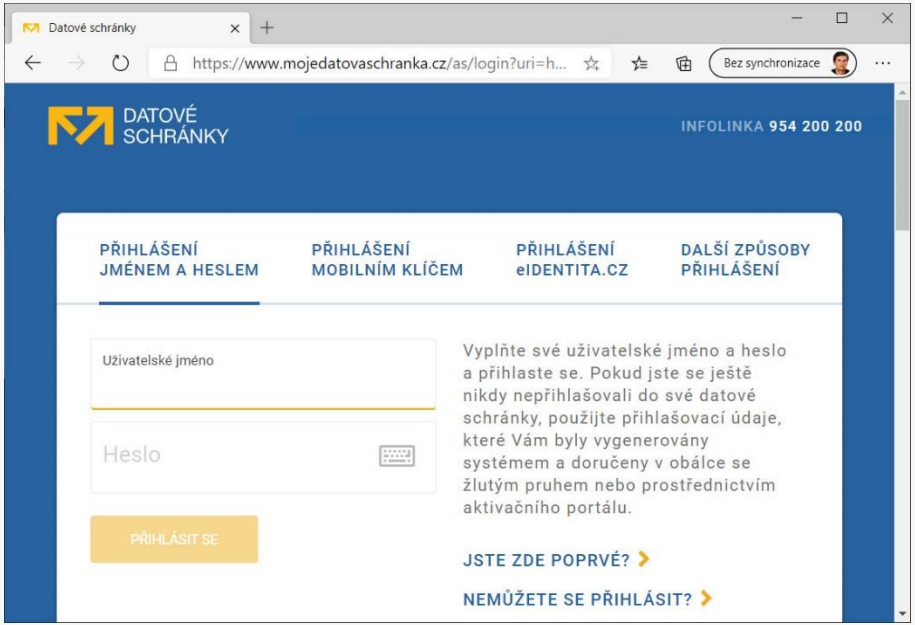
Všechny nově vydávané **občanské průkazy** obsahují čip pro uložení elektronického podpisu a mohou být tedy využity jako **uložiště osobních certifikátů**.

Datová schránka

- **Elektronický podpis** ověřuje **identitu**. Umožňuje podepsat e-mail nebo (PDF) dokument a certifikační autorita ověří, **kdo** dokument podepsal.
- Neověřuje však, **kdy** ho odeslal a odesilatel nemá jistotu, že dokument příjemce **četl**.
- **To vše řeší systém datových schránek (DS).**
- **Datové schránky** řeší vše důležité ještě lépe než elektronické podpisy, dnes se proto běžně používají.
- Datovou schránku si může zřídit i fyzická osoba.

Při zřízení datové schránky je nutné prokázat svoji fyzickou identitu. DS tedy také spojuje **digitální** identitu s identitou **fyzickou**.

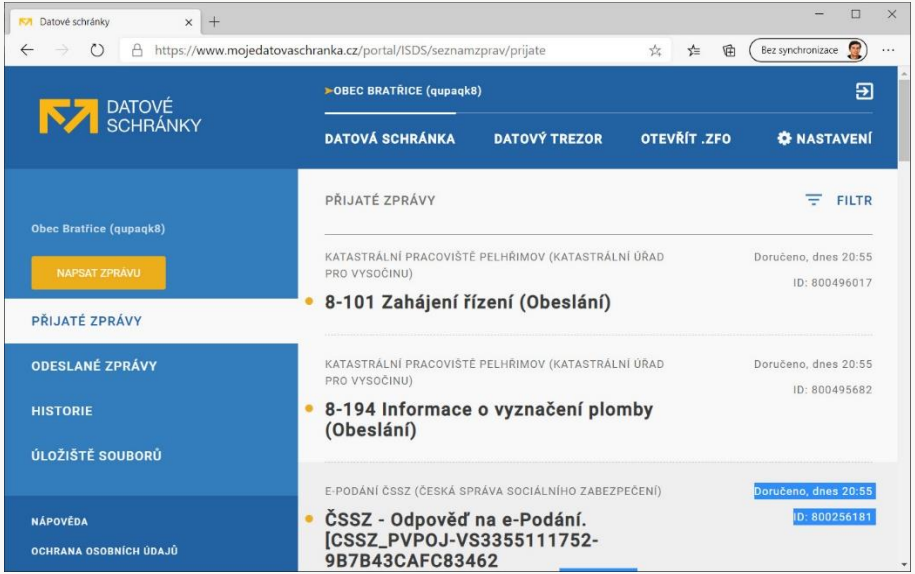
Datovou schránku musí povinně mít a používat všechny státní instituce (úřady, školy…) i všechny firmy (právnické osoby).



Systém datových schránek

- **Systém datových schránek** umožňuje vytvořit (napsat) datovou zprávu a odeslat ji do datové schránky příjemce.
- Systém zajistí a **nepopiratelně garantuje** vše potřebné pro bezpečnou a ověřenou komunikaci:
  - **Kdo** datovou zprávu poslal.
  - **Co** bylo předmětem zprávy a **jaké soubory** k ní byly přiloženy.
  - **Kdy** byla zpráva odeslána.
  - **Kdy byla doručena** příjemci.
- Přenos dat do/z datové schránky je samozřejmě šifrovaný.

Majitel DS je povinen číst její obsah. Pokud to nedělá, je to jeho chyba – po určité době (14 dnů) je zpráva **považována za doručenou/přečtenou** se všemi případnými **právními následky**.



Uživatelské účty – e-mail

- **Co již víme:**
- **E-mailová schránka** se fyzicky nachází na e-mailovém serveru připojeném k Internetu.
- Tento **server zajišťuje** také **odesílání** a **přijímání** pošty.
- **E-mailová adresa má danou strukturu**: **jmenoschranky@nazevpocitace.domena**
- To, že je v e-mailové adrese (často) **jméno** člověka, je zcela **volitelné** a nikým **neověřené**.
- Poštovní server navíc umožňuje uvedení **názvu odesilatele**, který se pak příjemci zobrazí nad nebo místo e-mailové adresy.

Název schránky se od názvu počítače odděluje znakem **@** (zavináč). Ten byl použit, protože se v žádném jazyku nepoužívá. Časem se z něho stal symbol elektronické komunikace.

Příklad adresy:
xyz007@seznam.cz

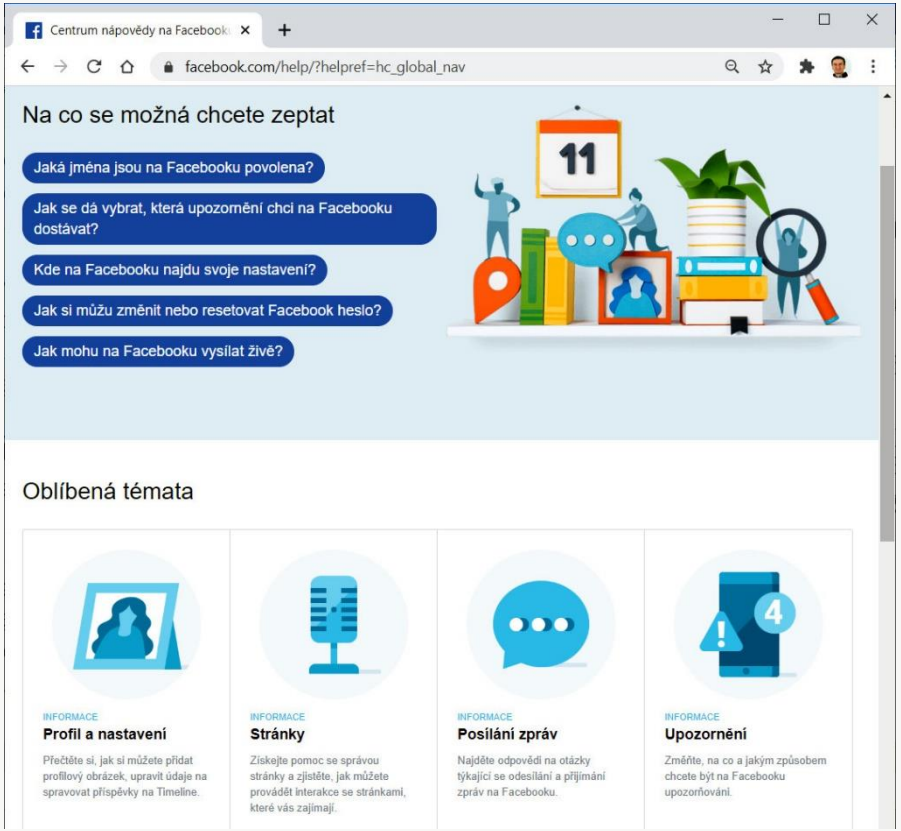
Schránka **xyz007** na serveru **seznam.cz**

E-mailová adresa je vlastníkem schránky určená kombinace znaků a **nemá žádnou přímou vazbu na jeho fyzickou identitu**.

Uživatelské účty – sociální sítě (Facebook, Instagram, Twitter)

- Při vytvoření účtu na sociální síti se sice **zadávají** další údaje (jméno, adresa, věk…), ale sociální sítě tyto údaje **neověřují**.
- Ověřují pouze e-mailovou adresu. Tu si však může vytvořit kdokoliv jakoukoliv.
- Například Facebook je určen pro děti od 13 let.
- Podle průzkumů je nejčastější věk registrace na tuto síť v ČR ve věku 11,5 roku.
- Část uživatelů tedy již při tvorbě svého účtu uvádí nepravdivé údaje.

Na sociálních sítích je možné a poměrně snadné vytvořit zcela **falešnou digitální identitu**.



Uživatelské účty – cloudové služby

- Současné **operační systémy** (MS Windows, Apple MacOS, Google Android) nabízejí (téměř vyžadují) přihlášení pomocí **cloudových přihlašovacích účtů**.
- **Účet Microsoft, Google či Apple** umožňuje současně přihlášení k počítačům (tabletům, mobilům) s příslušným operačním systémem i ke cloudovým službám uvedených firem.
- Díky **propojení zařízení přes cloudový účet** můžeme využívat několik digitálních zařízení s **jednou digitální identitou** a navíc **sdílet data** mezi těmito zařízeními.

Také cloudové služby velkých IT firem umožňují vytvořit **falešnou digitální identitu**.

Při zakládání cloudových účtů pro operační systémy jsou **vyžadovány** osobní údaje, nejsou však nijak **ověřovány**.

Cloudové účty proto **nejsou garantovaně provázány** s **fyzickou identitou** uživatelů.

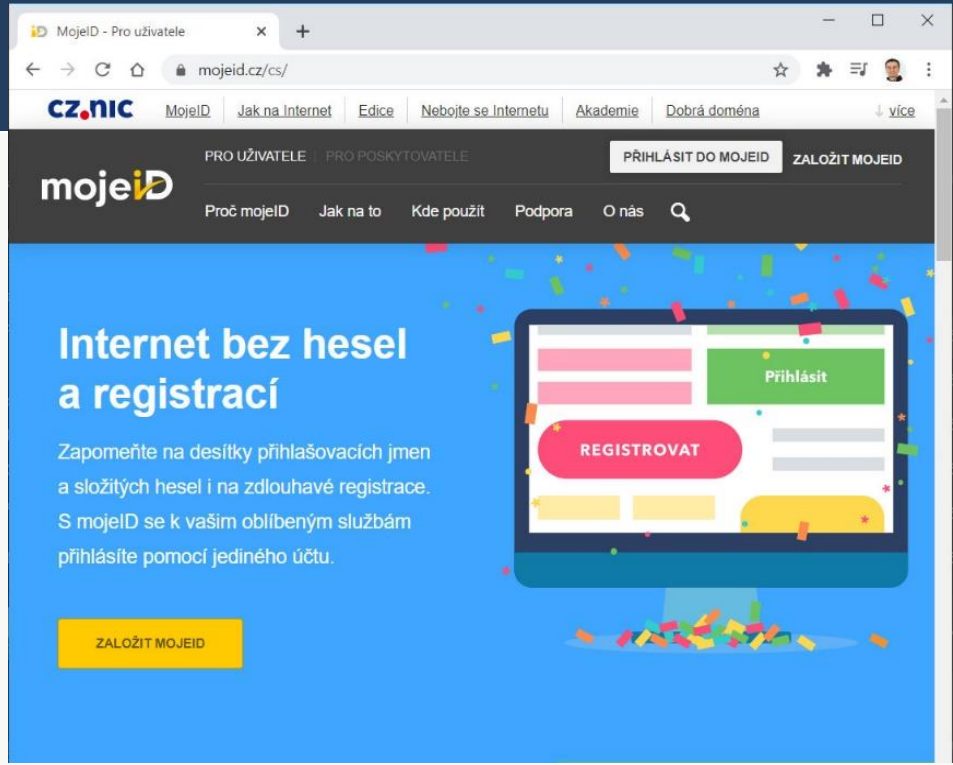
Moderní digitální zařízení často umožňují **přihlašování** přes otisk prstu nebo pomocí snímání obličeje.

Cloudové účty pro operační systémy jsou díky tomu **provázány s naší biologickou identitou**.

Nikoliv však s právní identitou.

Uživatelské účty – MojeID

- Společnost CZ.NIC, správce domény **.CZ**, nabízí službu **mojeID**, která alespoň **částečně spojuje digitální identitu s fyzickou identitou**.
- Při **registraci služby** mojeID je vyžadováno ověření přes telefonní číslo, a zejména
- na **adresu uživatele** je odeslán dopis s kódem, který musí následně zadat.
- Je tedy garantováno **spojení uživatele s fyzickou adresou** domu.
- **CZ.NIC** splňuje nejvyšší bezpečnostní standardy, je to firma, která spravuje české domény a (kořenové, základní) DNS záznamy.



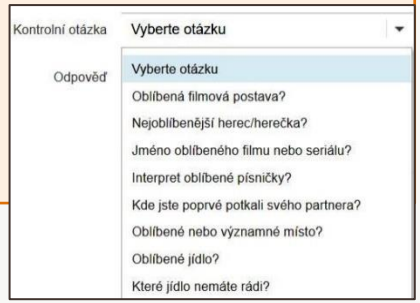
Více o službě mojeID najdete na webu tohoto projektu: https://www.mojeid.cz/cs/ .

Krádež digitální identity

- **Státem garantovanou digitální identitu**, tedy elektronický podpis nebo datovou schránku, je **velmi obtížné zneužít** a kromě profesionálních hackerských skupin to běžní uživatelé nedokáží. Podobné je to u platebních karet.
- **Negarantovanou digitální identitu**, tedy **uživatelský účet** k různým (cloudovým) službám, je možné zneužít mnohem snadněji.
- Zabezpečení účtů je totiž do značné míry **závislé na jednání jejich vlastníků**, uživatelů.
- Ti často **nedodržují bezpečnostní pravidla** (silná různá hesla, vícefaktorové ověření, nezveřejňování osobních informací) a kvůli tomu může případný útočník získat přístup k jejich účtu.

Nejčastěji jsou napadány e-mailové schránky uživatelů. Protože mnoho dalších služeb využívá e-mail k zasílání bezpečnostních zpráv (například při změně hesla), umožňuje útočníkovi získání přístupu k e-mailu oběti přístup i k dalším službám.

Příklad útoku: K obnově hesla k e-mailu se používají kontrolní otázky. Jestliže tato otázka zní: *„Moje nejoblíbenější hudební skupina?“* a na veřejném facebookovém profilu majitel schránky zveřejní své oblíbené hudební skupiny, nedá útočníkovi moc práce, změnit heslo k jeho e-mailové schránce.



Krádež digitální identity

- Útočník získaný přístup k účtu oběti může využít k tzv. **kyberšikaně**:
  - Získání a následnému **zneužití osobních (citlivých) dat** oběti i jejích přátel.
  - Poškození oběti **publikováním nevhodných příspěvků** a snímků jejím jménem.
- Cizím jménem je možné páchat i **kybernetickou trestnou činnost**:
  - **Rozesílání spamu** a využití ukradeného účtu pro phishingové útoky (*viz lekce 5.2*).
  - **Krádež firemních informací** (plány výrobků, databáze zákazníků apod.).

Krádež digitální identity a české zákony:

Pokud útočník **překoná zabezpečení** (heslo) a dále pod digitální identitou oběti vystupuje, může dojít k naplnění skutkové podstaty některého z těchto **trestných činů**:

- Neoprávněný přístup k počítačovému systému a nosiči informací (§ 230 trestního zákoníku).
- Opatření a přechovávání přístupového zařízení a hesla k počítačovému systému a jiných takových dat (§ 231 trestního zákoníku).
- Porušení tajemství dopravovaných zpráv (§ 182 trestního zákoníku).

Krádež digitální identity není zábava. Může naplnit podstatu trestného činu, řeší ji Policie ČR a pachateli hrozí pokuta i vězení.

Digitální identita – shrnutí

- **Digitální identita** současného uživatele IT je rozdělena mezi různé **uživatelské účty**. Např.:
  - E-mail.
  - Facebook, Instagram atd.
  - Účet Microsoft, Google, Apple.
  - Další cloudové služby, e-shopy atd.
- Digitální identitu jednoznačně **spojenou s fyzickou identitou** musí garantovat **státem určená autorita**.
- **Elektronický podpis** = kvalifikovaný osobní certifikát, elektronická (digitální) identita garantovaná **certifikační autoritou**.
- **Datová schránka** – **státem garantované** spojení digitální a fyzické identity.

Identita = **totožnost**, kdo jsem **já**.

Biologickou identitu člověka určuje jeho **DNA.**

Právní identitu člověka určuje **stát** pomocí jím určených identifikátorů (jméno, adresa, rodné číslo).

Fyzická identita = spojení biologické a právní identity.

Cloudové účty negarantují spojení mezi fyzickou identitou člověka a jeho identitou digitální.

Při komunikaci s lidmi přes zařízení IT známe pouze jejich **digitální identitu**. Ta je většinou negarantovaná a dá se kromě státem garantovaných identit poměrně jednoduše zfalšovat.

Z toho plyne potřeba určité (spíše velké) **opatrnosti a ověřování** toho, **kdo je skutečně** člověk, se kterým přes IT komunikujeme.

Zdroje

1. Pixabay.com. [online]. [cit. 2020-04-05]. Dostupný z URL: < https://pixabay.com/>. Fotky od OpenClipart-Vectors z Pixabay. OpenPhoto Gallery. [online]. [cit. 2009-04-05]. Dostupný z URL: < http://openphoto.net/gallery/index.html >.
2. Wikimedia Commons[online]. [cit. 2020-01-09]. Dostupný z https://commons.wikimedia.org/wiki/Main_Page
3. KRÁDEŽ IDENTITY [online]. [cit. 2020-07-12]. Dostupné z: https://www.internetembezpecne.cz/internetem-bezpecne/rizika-online-komunikace/kybersikana/kradez-identity/

Konec lekce

www.opocitacich.cz