Soukromí

ÚVOD DO OCHRANY SOUKROMÍ V DATECH



Tiffany Lewis
Security and Privacy Instructor

datacamp

Počátky soukromí

- 1. století – debaty o technologii a soukromí:
  - Práva jednotlivců
  - Bulvární zpravodajství
- **Soukromí** – právo být ponechán o samotě, bez vnějšího zasahování.



[1] Samuel D. Warren and Louis D. Brandeis, "The Right to Privacy," Harvard Law Review, 4 (5), (1890): 193-220, p. 195, citing Judge Cooley in Cooley on Torts, 2nd ed.

Dnešní definice soukromí

- *Data Privacy* – kontrola nad tím, jak jsou osobní data sbírána a používána.
- „Autorizované a oprávněné zpracování osobních údajů.“



[1] Bhajaria, Nishant, and Neil Hunt. Data Privacy: A Runbook for Engineers. Manning Publications Co., 2022.

Osobní data

- ***Osobní data*** – data související s osobou nebo umožňující identifikovat jednotlivce.
  - Příklady:
    - Datum narození (DOB)
    - Jméno
    - Geolokace
- Cílem je chránit osobní data



Rozšiřující se význam soukromí

- Více diskuzí ve 21. století kvůli:
  - Internetu
  - Aplikacím
  - Větší datové stopě
- Obavy o soukromí zahrnují:
  - Sledování
  - Big data analýzu
  - Poskytovatele třetích stran



Stav soukromí dnes

- Více než 59 % Američanů neví, co se s jejich daty děje.
- 81 % Američanů říká, že rizika sběru dat o nich převažují nad přínosy.
- Možné příčiny:
  - Nedostatek znalostí o soukromí
  - Nedostatek důvěry
  - Chybějící standardizovaná regulace



Dopady soukromí

Soukromí má různé dopady na různé skupiny

Role	Proč je soukromí důležité	Důsledky
Uživatel	• Důvěra uživatele • Jistota	• Porušení práv jednotlivce • Zvýšené riziko zneužití dat
Společnost	• Dodržování předpisů • Ochrana uživatelů	• Finanční ztráta • Právní důsledky
Regulátor	• Standardizace • Ochrana uživatelů	• Ztráta důvěry veřejnosti • Vykořisťování

PREACH

- **P (Purpose / účel)** – Proč firma žádá o použití tvých dat?
- **R (Right to Request / právo na změnu)** – Máš možnost požádat o změny svých informací?
- **E (Easy to understand / srozumitelnost)** – Jsou zásady firmy snadno pochopitelné?
- **A (Alerting / upozornění)** – Budeš upozorněn/a, pokud firma s tvými daty zachází nesprávně?
- **C (Consent / souhlas)** – Dal/a jsi souhlas (tj. povolení) s použitím svých informací?
- **H (How / jak)** – Jak firma nebo služba plánuje tvá data využít?

Pojďme si to vyzkoušet!

ÚVOD DO OCHRANY SOUKROMÍ V DATECH

Bezpečnost

ÚVOD DO OCHRANY SOUKROMÍ V DATECH



Tiffany Lewis
Security and Privacy Instructor

datacamp

Proč mluvíme o bezpečnosti?

- Bezpečnost je předpokladem soukromí.
- Programy bezpečnosti a soukromí jsou jako zmrzlinový pohár:
  - Bezpečnost = zmrzlina
  - Soukromí = poleva



Co je informační bezpečnost?

> ***Information Security (InfoSec)*** – „Ochrana informací a informačních systémů před neautorizovaným přístupem, použitím, zveřejněním, narušením, úpravou nebo zničením s cílem zajistit důvěrnost, integritu a dostupnost.“



[1] https://www.nist.gov/blogs/cybersecurity-insights/next-generation-security-and-privacy-controls-protecting-nations

CIA Triad

- Populární bezpečnostní model
- *CIA Triad* pomáhá firmám rozpoznat a pochopit bezpečnostní opatření
- **Poznámka:** Existuje mnoho bezpečnostních modelů
  - Příklad – *DIE*
    - Distributed
    - Immutable
    - Ephemeral



Rozbor CIA Triad

- CIA Triad zahrnuje:
  - **Confidentiality** (důvěrnost) – data jsou chráněna a nedostupná neoprávněným osobám.
  - **Integrity** (integrita) – data nejsou neočekávaně měněna.
  - **Availability** (dostupnost) – datové systémy fungují podle očekávání.



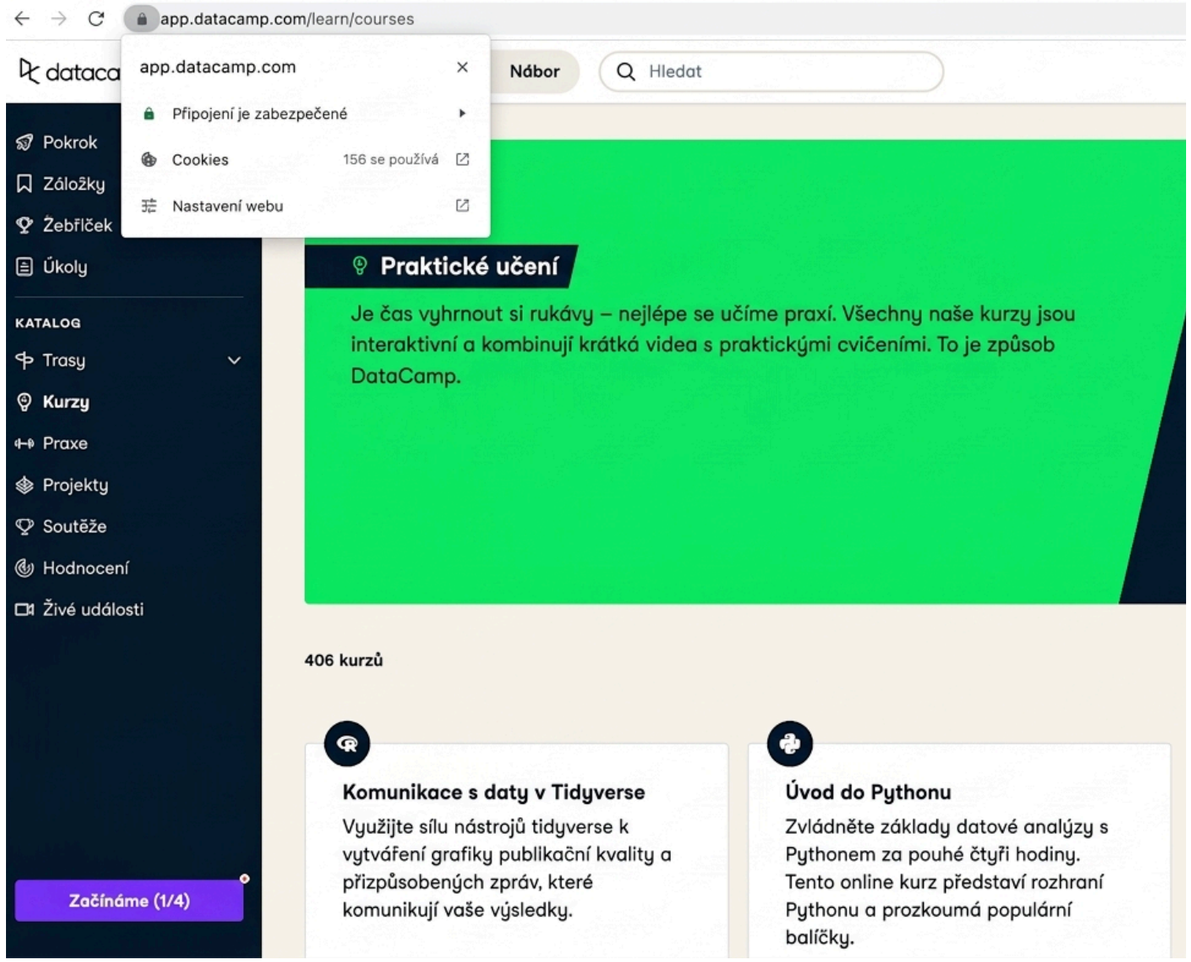
Confidentiality – Identity Access Management (IAM)

- **Confidentiality** – schopnost systému zajistit, aby k informacím měli přístup jen správní uživatelé.
- **Identity Access Management (IAM)**
  - Zajišťuje, aby správní lidé měli přístup ke správným zdrojům ve správný čas.
- Příklad z praxe – omezení přístupu zaměstnanců ke zdrojům:
  - Firemní e-mail
  - Přístup do firemní sítě
  - Přístup v pracovní době – od 8 do 17 h



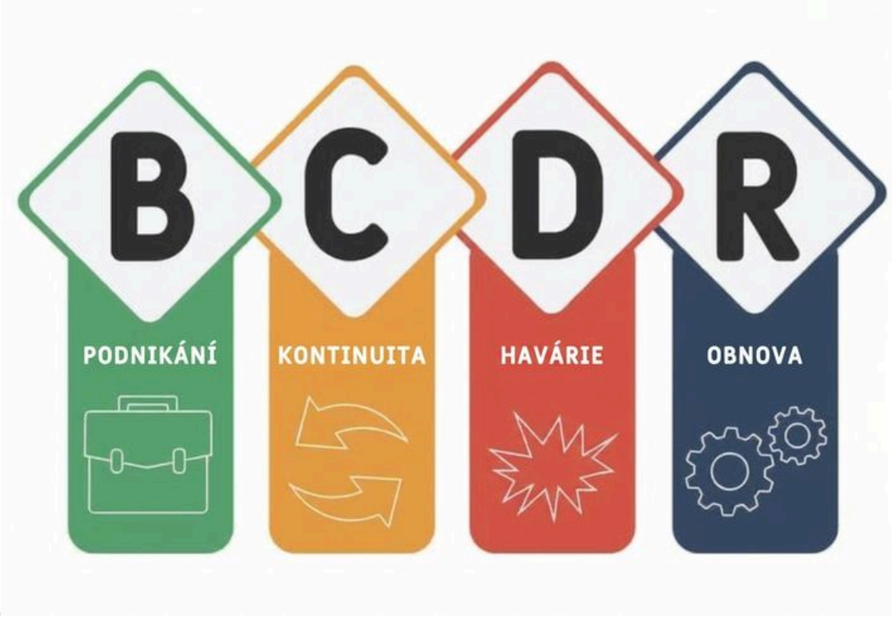
Integrity – šifrování a hashování

- **Integrity** – datům lze důvěřovat a nebyla nevhodně upravena
  - **Encryption** (šifrování) – proces, který činí čitelná data nečitelnými.
    - „midnight“ -> „Y!lay.ig“
  - **Hashing** (hashování) – převod dat na standardizovaný algoritmický výstup
- Z praxe: HTTPS komunikace



Availability – Business Continuity and Disaster Recovery

- **Availability** – systémy jsou přístupné a dostupné.
- **Business Continuity and Disaster Recovery (BCDR)** – procesy, zásady a lidé, kteří firmě pomáhají fungovat při neplánovaných událostech.
- Příklad – povodeň poškodí datové centrum



Pojďme si to vyzkoušet!

ÚVOD DO OCHRANY SOUKROMÍ V DATECH

Vztah mezi bezpečností a ochranou soukromí

ÚVOD DO OCHRANY SOUKROMÍ V DATECH

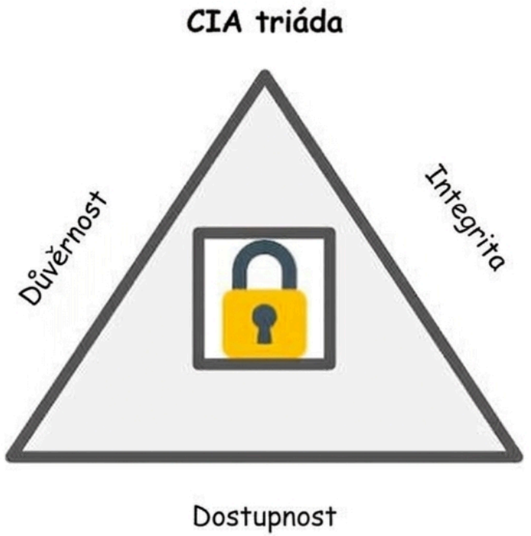


Tiffany Lewis
Security and Privacy Instructor

datacamp

Základy bezpečnosti

- Prevence neoprávněného použití, zpřístupnění a změny dat:
  - Triáda CIA
- Příklady:
  - Šifrování
  - Správa přístupu k identitám

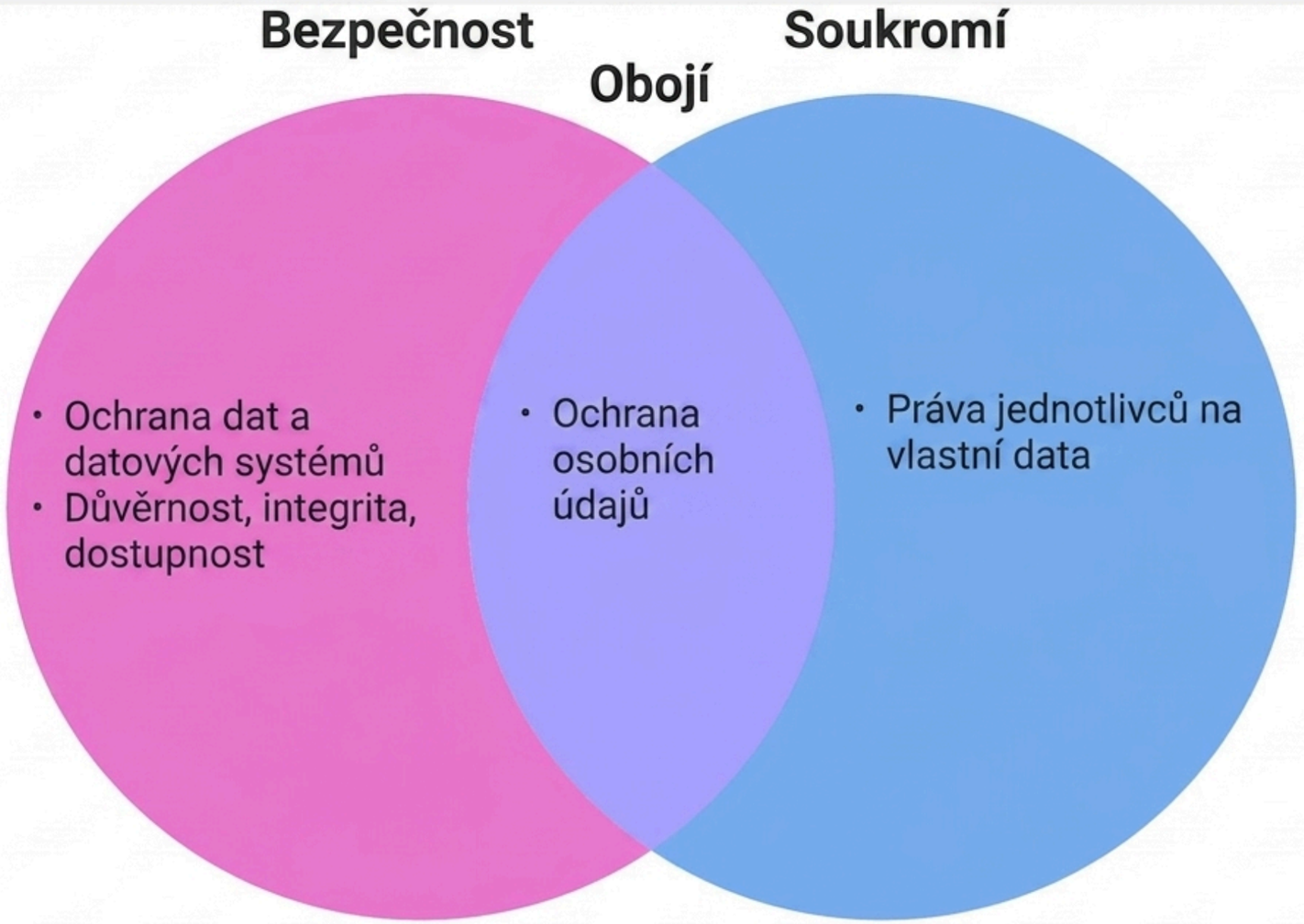


Základy ochrany soukromí

- Data zpracovávaná platným způsobem, který byl uživatelem autorizován
- Příklady:
  - Oznámení
  - Šifrování



Vennův diagram bezpečnosti a soukromí



Aplikace získaných znalostí

- Startup Backpack
- Otázky bezpečnosti a ochrany soukromí
- Analýza:
  - Produktová data
  - Osobní údaje



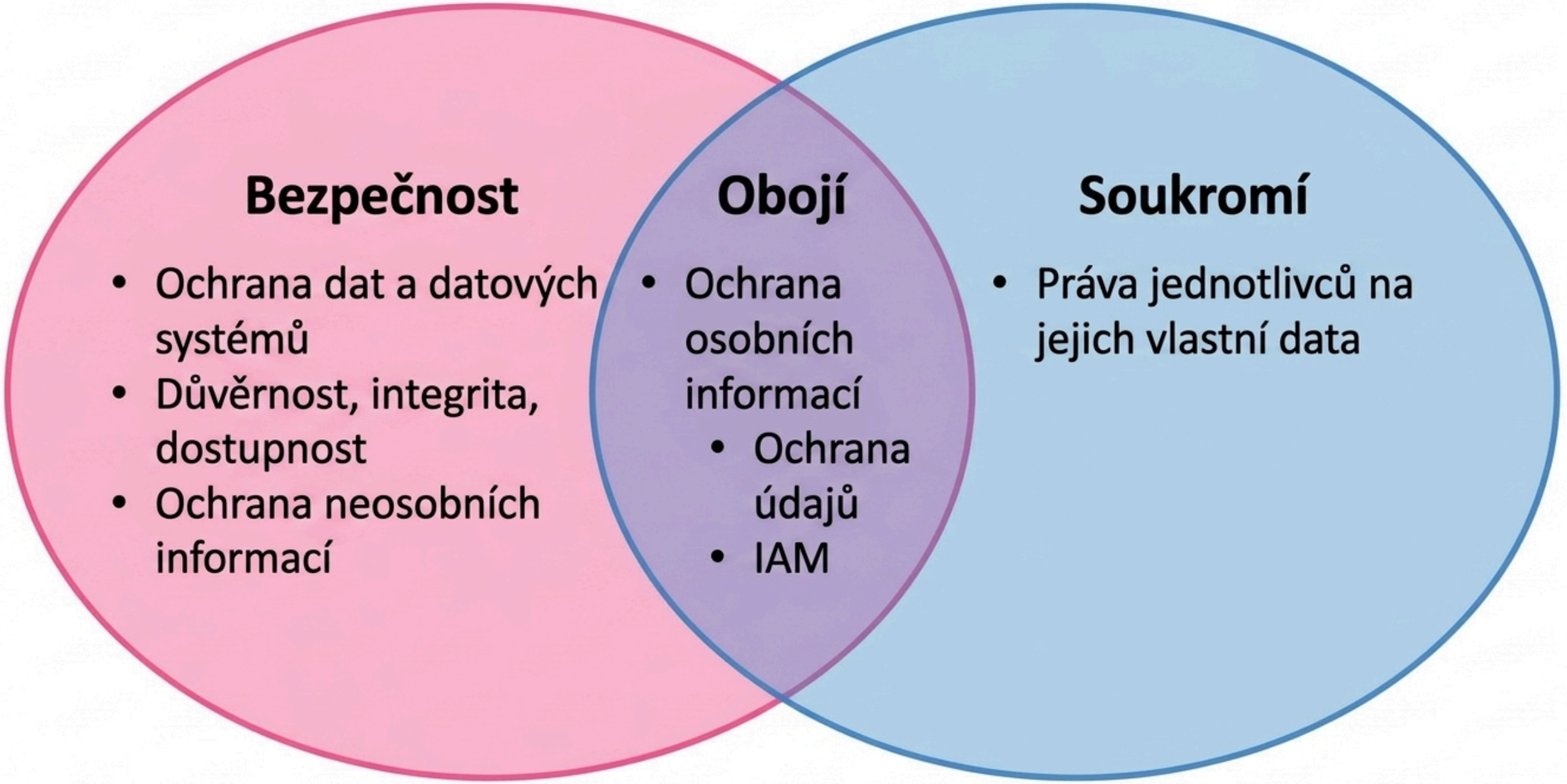
Bezpečnostní kontroly



Kontroly ochrany soukromí



Vennův diagram bezpečnosti a soukromí



Selhání bezpečnosti a ochrany soukromí

- Ochrana soukromí vyžaduje výslovný souhlas uživatelů k:
  - zpřístupnění
  - změně
  - změně způsobu použití dat
- Odcizená data – bez souhlasu nebo oprávnění uživatelů



Únik dat

> **Únik dat** – bezpečnostní incident, při němž jsou data neoprávněně zpřístupněna, pozměněna nebo odcizena.



- Příklad: únik dat Yahoo v roce 2013
  - Zasáhl přes 3 miliardy uživatelů
  - Hackeři se pokusili data prodat

[1] https://www.nytimes.com/2017/10/03/technology/yahoo-hack-3-billion-users.html

Pojďme si procvičit!

ÚVOD DO OCHRANY SOUKROMÍ V DATECH