cosmotron
Cosmotron Bohemia, s.r.o.

GDPR A INFORMAČNÍ SYSTÉM

Nadežda Andrejčíková
Libor Piškula

GDPR a informační systém

Obsah:

1. **Principy ochrany**
2. **Legitimnost zpracování osobních údajů**
3. **Praktické dopady GDPR**
4. **Technologické aspekty**

Principy ochrany

1. „Data protection by design“

- Zásada minimalizace údajů

- Technická řešení
  - Anonymizace – statistiky, trendy
  - Pseudonymizace – skrytí identity přes kód
  - Rozdělení oblastí s uloženými daty – fyzické nebo logické

- Personální a organizační opatření
  - kdo má přístup k jakým údajům
  - jaké jsou toky dat
  - definice rolí a přístupových práv do IS

Principy ochrany

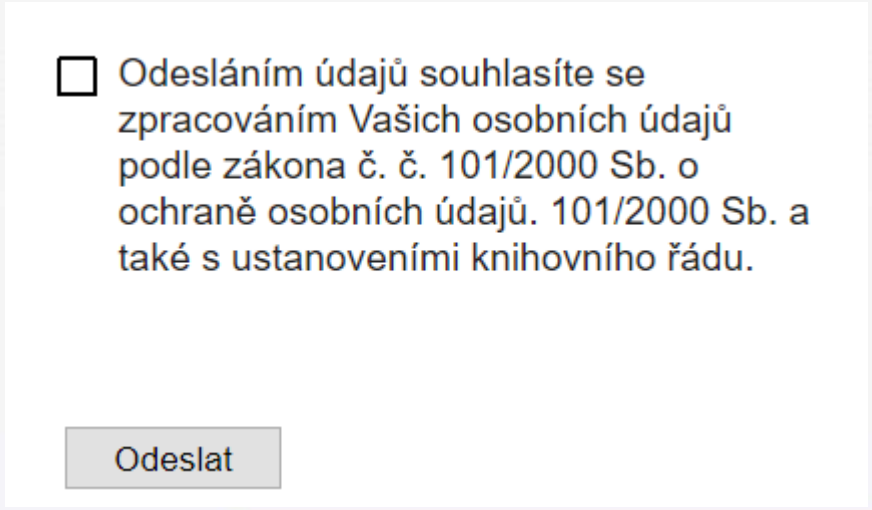
2. „Data protection by default“

- V základním nastavení služby jen osobní údaje, které jsou zcela nezbytné
  - Standardní pracovní formuláře pro evidenci uživatelů

Legitimnost zpracování osobních údajů

Souhlas se zpracováním osobních údajů

- **při registraci v knihovně**
- **online - předregistrace, konto čtenáře / profil uživatele**
  - **např. formou checkboxu, nesmí být defaultně vybraný**
- **zajistit uložení souhlasu do db**
- **zajistit možnost odvolání souhlasu**



Praktické dopady GDPR

Ochrana dat, bezpečné uložení

- **síťová infrastruktura (firewall, monitoring)**
- **databáze**
- **zálohování**
- **aplikační vrstva**
- **komunikační protokoly**

Zpracovatel dat musí uchovat kompletní historii změn a přístupů k datům

- **chronologie**
- **provozní logování**

Praktické dopady GDPR

Právo na změny osobních údajů

- **osobně v knihovně**
- **online – profil uživatele, formulář pro změnu údajů**

Právo na přenositelnost osobních údajů

- **možnost exportu 1 záznamu uživatele**
- **nařízení neurčuje konkrétní formát**

Právo na výmaz osobních údajů

- **online - profil uživatele, možnost odeslání požadavku na výmaz**
- **zajistit kompletní vymazání z databáze, resp. anonymizaci**
- **zálohy?**

Technologické aspekty

1. Zabezpečení komunikace
2. Bezpečná práce s prohlížečem
3. Šifrování, hashování
4. Síťová infrastruktura
5. Aplikační bezpečnost
6. Plánované úlohy, procesy na pozadí
7. Integrace

Technologické aspekty

1. **Zabezpečení komunikace**

- **Klíčový je kompletní přechod z http na https**
  - **tlustý klient ARL používá vynuceně https**
  - **tenký webový klient ARL a webové nástroje pro správce ARL používají vynuceně https**
  - **webový katalog OPAC (ARL IPAC) může kompletně běžet na https a probíhá postupné přepínání v knihovnách z http na https**
  - **ws služby (API) ARL používají vynuceně https**

- **Přechod od SSL k jeho bezpečnějšímu nástupci TLS**
  - **nastavení aplikačního webového serveru**

Technologické aspekty

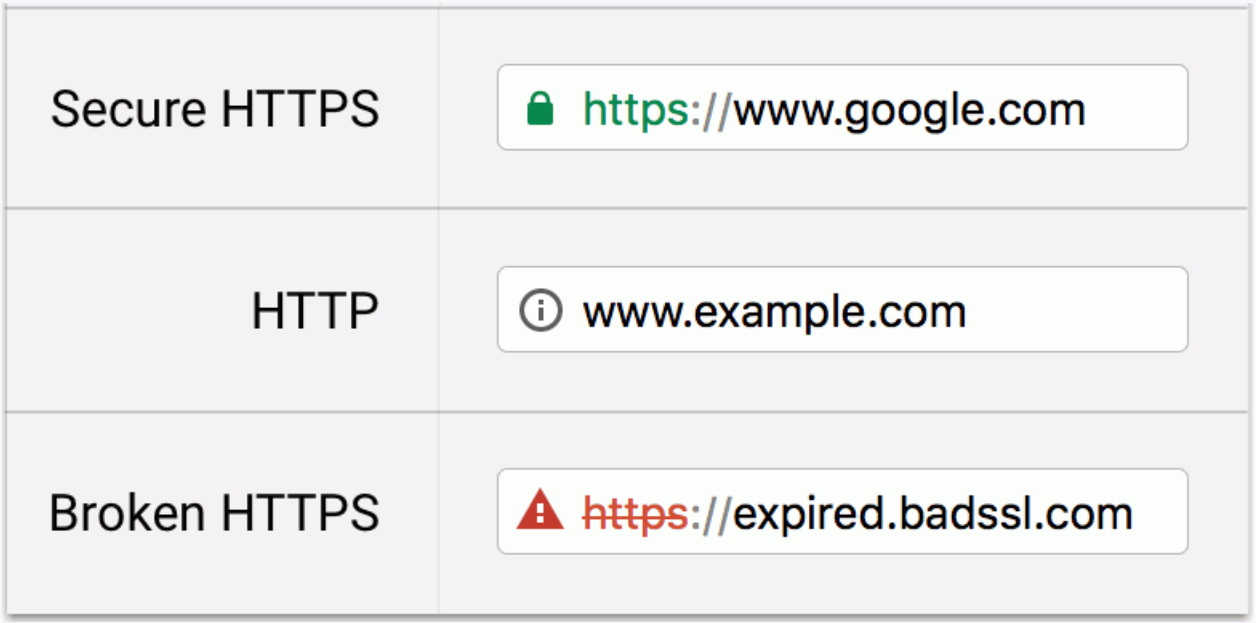
1. Zabezpečení komunikace

- Snadnější přístup k certifikátům
  - zdarma dostupný Let's Encrypt, automatizované obnovování
- Podpora pro reverzní https proxy
  - centrální certifikát instituce
- Aplikování nových technologií
  - HSTS - vynucení https, dokáže zabránit přesměrování na http
  - HPKP - dokáže zabránit výměně certifikačních autorit
  - …

Technologické aspekty

2. Bezpečná práce s prohlížečem

- **Nové verze webových prohlížečů**
  - **v adresním řádku graficky zvýrazňují zabezpečené stránky**



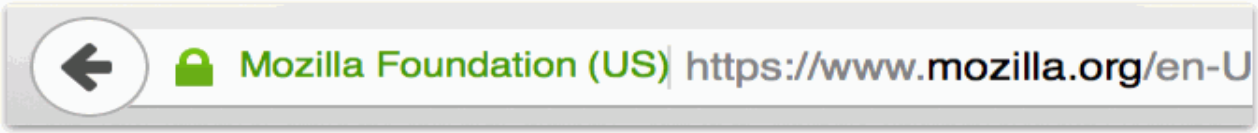
Technologické aspekty

2. Bezpečná práce s prohlížečem

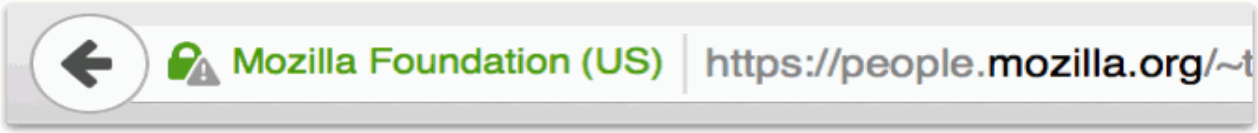
- **Nové verze webových prohlížečů**
  - v adresním řádku graficky zvýrazňují zabezpečené stránky
  - rozlišují úrovně certifikátů DV, OV, EV
  - stále více aktivně blokují nezabezpečené stránky

Sites with DV certificates

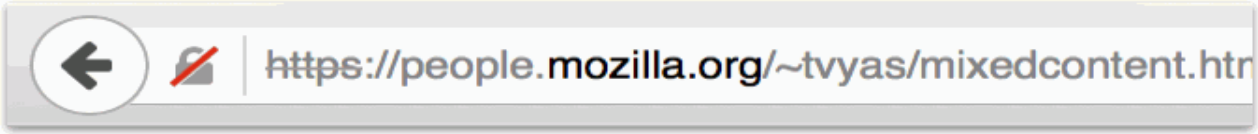
Sites with EV certificates



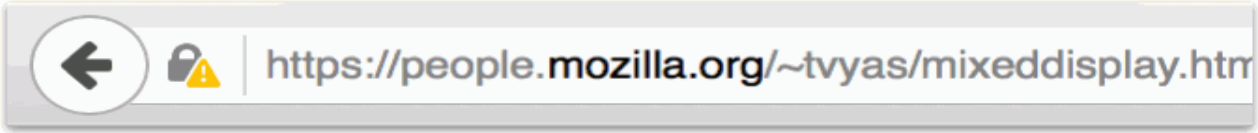
Sites with mixed active content blocked



Sites with mixed active content allowed



Sites with mixed passive content loaded



Technologické aspekty

2. **Bezpečná práce s prohlížečem**

- **Nové verze webových prohlížečů**
  - **v adresním řádku graficky zvýrazňují zabezpečené stránky**
  - **rozlišují úrovně certifikátů DV, OV, EV**
  - **stále více aktivně blokují nezabezpečené stránky**

- **Vzdělávání uživatelů IS**

Technologické aspekty

3. Šifrování, hashování

- GDPR neurčuje, že by šifrování bylo povinné
- Loginy, hesla, role, přístupová práva, apod.
  - ukládají se do šifrované části databáze

- Osobní údaje uživatelů
  - ukládat do šifrované části databáze

- Náhrada velmi rozšířeného, ale zastaralého hashování MD5 za SHA-512 (bcrypt, scrypt)
  - typicky hesla, z hashe nelze zpětně rekonstruovat heslo
  - stará hesla -> MD5 hash ještě navíc zabalíme do SHA-512 hashe

Technologické aspekty

4. **Síťová infrastruktura**

- **Firewall s proaktivní detekcí útoků a pokusů o průnik**
- **Aktivní monitoring hardwaru i softwarových služeb – PRTG**
- **Přístup správců na servery - pouze přes ssh tunely s certifikátem**

5. **Aplikační bezpečnost**

- **Penetrační testy a následná opatření - OWASP Top 10**
- **Logování všech aktivit v IS**

Technologické aspekty

6. Plánované úlohy, procesy na pozadí
- Rozesílání upomínek a různých notifikací k výpůjčním službám - email, SMS
- …

7. Integrace
- Synchronizace uživatelů IS s centrální správou identit
- Propojení na síťové tiskárny a kopírky (SafeQ)
- Propojení na turnikety
- Připojení selfchecku protokolem SIP
- Komunikace s CPK protokolem NCIP
- ...

Otazníky ???

- Výmaz osobních údajů ze záloh? –> obtížně realizovatelné
- Bude potřeba více samostatných souhlasů se zpracováním?
- Výměnný formát pro přenositelnost osobních údajů?