Evergreen v českých knihovnách 2017

bezpečnostní certifikáty zdarma v praxi

Ing. Václav Jansa
ÚISK FF, Univerzita Karlova

9. 10. 2017

GDPR

- Obecné nařízení o ochraně osobních údajů
- technické a organizační potřeby pro implementaci:
  - organizační záležitosti – kdo, kdy a za jakých podmínek nakládá s osobními údaji
  - technické zabezpečení přístupu – přístupová oprávnění a zabezpečení serveru
  - bezpečnost a autenticita přenosového kanálu od serveru k uživateli – využívání SSL/TSL (Secure Sockets Layer / Transport Layer Security)

Řešení zabezpečení přenosového kanálu

- přesměrování komunikace (WWW a poštovní servery) na jiné porty s použitím SSL/TLS
  - drobná úprava nastavení
  - vynucování komunikace po šifrovaném kanálu
  - u zastaralých systémů použití šifrovaného tunelu realizovaného dalším programem
- použití uznávané veřejné certifikační autority
  - veřejně akceptovaný certifikát nemusí koncový uživatel ručně akceptovat; ověří se přes kořenové certifikáty uložené v operačním systému nebo prohlížeči
  - certifikační autorita má vlastní uznávaná bezpečnostní pravidla (splnění podmínek GDPR)

Uznané certifikační autority

- komerční certifikáty
  - v Česku například I.CA, Post Signum, certifikát pro server na jeden rok za 800 až 1 200 Kč
  - výhodou je ověření autenticity organizace a odpovědných osob
- akademické certifikáty CESNET PKI
  - bezplatné pro akademické členy a uživatele CESNETu
  - zajištěná autenticita odpovědných osob a organizací
  - ne každý na ně dosáhne
- Let‘s Encrypt
  - vydáváno neziskovou organizací, za níž stojí technologičtí vůdci v oboru (Facebook, Google, Mozilla a Linux Foundation, Akamai, Cisco atd.)
  - ověření autenticity je nepřímé – přes přístup k DNS záznamům
  - je zdarma, s cílem, že všichni mají mít možnost se zabezpečit

Let‘s Encrypt

- nezisková společnost financovaná špičkami v oboru i dobrovolníky
- v červnu 2017 překročeno 100 milionů vydaných certifikátů
- jednoduché automatizované obnovy certifikátů
- od ledna 2018 budou i doménové (neboli *) certifikáty
- primárně chrání přenosový kanál (jediným ověřením autenticity je DNS záznam, který pochopitelně spravují jen pověřené osoby v každé organizaci)

Let‘s Encrypt – jak to funguje

- speciální program (například certbot) vygeneruje žádost o certifikát a tu odešle spolu se seznamem domén pro tento certifikát certifikační autoritě
- certifikační autorita ověří na všech doménách ze seznamu, zda na nich běží certbot, který má soukromý klíč odpovídající žádosti o certifikát
- po úspěšném ověření všech domén autorita předá podepsaný certifikát s platností 90 dní certbotu a ten jej uloží pro použití službami spuštěnými na serveru
- pravidelně spouštěný certbot potom automaticky aktualizuje certifikáty, zbývá-li do vypršení platnosti méně než 30 dní

Certbot – představení

- podporované systémy
  - Linux (různé distribuce)
  - BSD
  - MacOS
- možnost samostatné činnosti
- integrační moduly pro
  - Apache httpd
  - NGINX
  - HAProxy
  - Plesk

Certbot – instalace v Linuxu

- doporučuji standalone režim (neskrývá žádné překvapení z nadbytečné automatizace)
- RHEL/CentOS 7
  - povolit repozitář EPEL a nainstalovat (yum install certbot)
  - https://certbot.eff.org/#centosrhel7-other
- Debian 8 – Jessie
  - povolit repozitář Jessie Backports a nainstalovat (apt-get install certbot -t jessie-backports)
  - https://certbot.eff.org/#debianjessie-other

Certbot – žádost o certifikát v standalone režimu

- nastavíme DNS server a zkontrolujeme pomocí nslookup, že je správně resolvována IP adresa serveru
- zkontrolujeme, že je na firewallu otevřen port 443 (https) a žádný jiný program nenaslouchá na tomto portu
- spustíme žádost o certifikát

```
certbot certonly --standalone -d osobni.osvobozena-knihovna.cz
```

- potvrdíme licenční pravidla a zadáme adresu, na kterou mají chodit upozornění na končící certifikáty

Přidání certifikátu do konfigurace

- vytvořený certifikát (pár soukromý klíč a certifikát nebo certifikát včetně vložených certifikátů) je třeba přidat do konfigurace serveru
- využití linků z původní lokace
  - Evergreen má podle instalačního manuálu certifikáty na adrese

    `/etc/apache2/ssl`
  - linky jsou potom:

```
server.crt -> /etc/letsencrypt/live/osobni.osvobozena-knihovna.cz/fullchain.pem
server.key -> /etc/letsencrypt/live/osobni.osvobozena-knihovna.cz/privkey.pem
```

Automatická aktualizace certifikátu

- v Linuxu se spouští certbot jednou týdně cronem
- rozklíčování položky (řádky) cronu:
  - `25 5 * * sun`
    každou neděli v 5:25 ráno
  - `certbot renew –standalone`
    spustí se certbot ve standalone režimu a ověří, zda není třeba aktualizovat certifikáty
  - `--pre-hook 'systemctl stop apache2 apache2-websockets'`
    před spuštěním se vypou webové servery, aby neblokovaly port
  - `--post-hook 'systemctl start apache2 apache2-websockets'`
    po aktualizaci certifikátu se nastartují webservery s novým certifikátem

Děkuji za pozornost

- Otázky?

- vaclav.jansa@gmail.com