Ústřední knihovnická rada ČR Klementinum 190, 110 00 Praha 1

Poradní orgán ministra kultury ČR

Webové stránky knihoven - přechod na protokol HTTPS

Doporučení Ústřední knihovnické rady ČR

Přes 2000 knihoven v ČR zpřístupňuje svůj katalog na internetu a významná část z nich umožňuje uživatelům se do tohoto katalogu přihlásit a využívat jeho služeb. Přihlášení je přitom realizováno většinou formou přímého zadání jména a hesla, jen některé knihovny využívají pro přihlášení MojeID nebo eduID. Velká většina knihovních katalogů (adresář knihoven ČR eviduje ke konci dubna 2017 více než 2153 odkazů na katalogy knihoven) je přitom zpřístupňována prostřednictvím protokolu http[1], jen několik desítek knihoven využívá protokolu HTTPS[2] (43 odkazů). Přestože je pravděpodobné, že reálný počet katalogů využívajících HTTPS bude vyšší, je tento nepoměr alarmující.

Hrozby

Největší hrozbou při používání protokolu HTTP je únik citlivých informací, který může poškodit uživatele knihovny. Mimo úniku informací o tom, co daný uživatel čte nebo četl, o jaká témata se zajímá apod. je největší hrozbou únik uživatelského jména a hesla. Ačkoli většina knihoven používá jako uživatelské jméno pro přihlášení číslo čtenářského průkazu, je součástí profilu uživatele i jeho e-mail. Uživatel si může nastavit libovolné heslo, což vede k tomu, že si řada z nich nastaví heslo shodně s účty u jiných online portálů nebo služeb, kde se jako přihlašovací jméno používá pro změnu e-mail uživatele. Útočník se může pokusit prostřednictvím získaných údajů zaútočit přímo na infrastrukturu zaměstnavatele daného uživatele knihovny (i když údaje o zaměstnavateli nejsou knihovnami obvykle sbírány, lze zaměstnavatele odhadnout, pokud uživatel v knihovně uvede svůj služební mail).

Na první pohled se může zdát, že riziko takového odposlechnutí není velké. Většina knihoven ale nabízí uživatelům připojení přes Wi-Fi. Uživatelé také často využívají volné Wi-Fi připojení v dopravních prostředcích, restauracích apod. I tyto Wi-Fi sítě jsou velmi často nešifrované, takže jakákoli komunikace, která přes ně prochází a není sama šifrovaná, například právě s využitím HTTPS místo HTTP, je velmi snadno odposlechnutelná. Ani zašifrované Wi-Fi přenosy však dnes už nelze považovat za bezpečné, a proto je v těchto případech šifrování pomocí HTTPS nezbytností. Nesmíme zapomínat ani na vysoké pokuty, kterými hrozí evropské nařízení pro ochranu osobních údajů GDPR[3], které má vstoupit v platnost 25. 5. 2018.

Ochrana osobních údajů uživatelů je však jen jednou stranou mince. Druhou její stranou je všeobecný technický vývoj. Google již začal v prohlížeči Chrome, který je s více než 50 % nejpoužívanějším prohlížečem internetu, označovat webové stránky, které přes protokol HTTP chtějí přenášet hesla nebo čísla kreditních karet za nezabezpečené. Nakonec ale začne za nezabezpečené označovat jakékoli stránky přístupné přes protokol HTTP.

Co s tím?

Ještě nedávno by přechod na HTTPS znamenal i pravidelné finanční výdaje na periodicky obnovovaný serverový certifikát a s tím spojenou manuální práci související s jeho výměnou za nový. Dnes je již možné

[1] HTTP (Hypertext Transfer Protocol) je internetový protokol určený pro výměnu hypertextových dokumentů ve formátu HTML. Viz podrobněji: https://cs.wikipedia.org/wiki/Hypertext_Transfer_Protocol.

[2] HTTPS (Hypertext Transfer Protocol Secure) je v informatice protokol umožňující zabezpečenou komunikaci v počítačové síti. Viz podrobněji: https://cs.wikipedia.org/wiki/HTTPS.

[3] Nařízení Evropského parlamentu a Rady (EU) 2016/679 ze dne 27. dubna 2016 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a volném pohybu těchto údajů ("Nařízení") neboli General Data Protection Regulation ("GDPR") má zásadní dopad na všechny subjekty, které osobní údaje pro různé účely a v různém rozsahu v rámci svého podnikání zpracovávají. Blíže o GDPR: https://www.uoou.cz/obecne-narizeni-eu/ds-3938/p1=3938

díky službě LetsEncrypt získat serverové certifikáty zdarma a jejich aktualizaci zcela zautomatizovat. Návodů je na Internetu nepřeberné množství, např.

https://www.jakpsatweb.cz/https.html
http://jecas.cz/https
http://blog.poski.com/dulezitost-ssl-certifikatu-a-https/
http://www.shockworks.eu/cz/prechod-e-shopu-na-https/
https://napoveda.seznam.cz/cz/fulltext-hledani-v-internetu/protokol-https/
https://support.google.com/webmasters/answer/6073543?hl=cs
https://cs.wikipedia.org/wiki/HTTPS

Pro většinu webových serverů navíc existují na míru připravené návody, jak HTTPS případně i včetně automatické aktualizace certifikátů LetsEncrypt zprovoznit. Jeden z nejjednodušších klientů na rozběhnutí (bohužel jen pro Linux) je asi acme.sh (https://www.root.cz/clanky/acme-sh-snadna-cesta-k-certifikatu-od-let-s-encrypt/), pro servery běžící na Windows může pomoci návod https://letsencrypt.org/docs/client-options/. Další možnosti jsou k nalezení na stránce https://certbot.eff.org.

Pozor! Pokud je knihovna zapojena do portálu **Knihovny.cz**, nebo z jiného důvodu provozuje strojové rozhraní pro zprostředkování služeb uživatelům (NCIP nebo jiné API), je nezbytné, aby toto rozhraní bylo také provozováno na https! Zároveň je třeba zajistit, aby k tomuto rozhraní nemohl nikdo získat neoprávněný přístup.

Doporučení

Významná část knihoven se pravděpodobně při nasazování HTTPS obrátí na svého správce nebo dodavatele knihovního systému, který zajistí vše potřebné. Není ale vyloučeno ani to, že bude výhodnější se v tomto případě obrátit na specialistu, který zároveň může prověřit i celkové zabezpečení knihovní infrastruktury. Přechod na HTTPS není pro zkušeného správce nikterak náročný a je realizovatelný dle složitosti daného systému během jedné nebo několika hodin. Co může práci významně prodražit je však nutnost instalace bezpečnostních aktualizací operačního systému, webového serveru a dalších souvisejících komponent, která se může v případě starších systémů výrazně protáhnout a v případě webserverů běžících na Windows může obnášet i nutnost zakoupení licencí na nové verze Windows. Další možností je před existující knihovní systém předřadit ještě jeden webserver (např. volně dostupný Apache či nginx), jehož úkolem bude fungovat jako brána mezi HTTPS komunikací zvnějšku a stávajícím katalogem běžícím interně nadále na HTTP.

V rámci přechodu na HTTPS je vhodné zajistit, aby zůstaly funkční všechny stávající odkazy do doby, než budou postupně všude na internetu změněny. To je možné zajistit například tak, že webserver knihovního systému bude nastaven tak, aby všechna URL poskytovaná protokolem HTTP přesměrovával na jejich zabezpečenou variantu. Další doporučeným krokem pak je použití HTTP Strict Transport Security (ve zkratce HSTS) - nastavením hlavičky je možné prohlížeči sdělit, že z příslušného serveru už nesmí zobrazovat obsah načtený přes nezabezpečené HTTP, ale vždy pouze přes zabezpečené HTTPS.

Pokud váš katalog používá cookies, je potřeba i u nich nastavit aby byly posílány výhradně přes HTTPS (nastavit jim security flag).

Kontrolu toho, že je webový server nastaven správně, lze provést prostřednictvím https://www.ssllabs.com/ssltest/index.html. Testovaný server by měl získat známku A+ nebo přinejhorším A. Vedlejším efektem tohoto nastavení bude znepřístupnění katalogu knihovny uživatelům používajícím Internet Explorer na Windows XP.

Pozor! Pokud vaše knihovna provozuje jako součást svého webu nějaké speciální rozhraní typu NCIP nebo SIP2, přes které jsou předávány i osobní informace uživatelů, mělo by toto rozhraní být také adekvátně zabezpečeno! Mimo použití HTTPS je v takovém případě nezbytné zabránit zneužití tohoto rozhraní i omezením přístupu dle IP adres a navíc i pomocí jména a hesla nebo přístupového klíče.

Při nasazování HTTPS je možné s minimálními náklady dosáhnout i nezanedbatelných přínosů. Lze zejména významně urychlit stahování webových stránek uživateli díky **zapnutí podpory protokolu HTTP/2**

(https://en.wikipedia.org/wiki/HTTP/2), který je dnes už podporován všemi rozšířenějšími prohlížeči internetu, který ale pro své fungování potřebuje právě HTTPS. Toto zrychlení se může projevit například při stahování většího množství obrázků - třeba náhledů obálek ze serveru obalkyknih.cz. Součástí zprovoznění HTTP/2 musí být i zprovoznění rozšíření ALPN, což je rozšíření urychlující rozhodnutí, zda se při komunikaci může HTTP/2 použít. Funkčnost HTTP/2 pak lze otestovat na adrese https://tools.keycdn.com/http2-test. Rozdíl v rychlosti mezi běžným HTTP/1.1 a HTTP/2 je pak možné vidět například na stránce https://http2.akamai.com/demo.

Pro lepší analýzy chování uživatelů (např. s využitím Google Analytics) je také vhodné, aby všechny webové stránky na vašem serveru, které neobsahují v URL citlivé údaje a odkazují na stránky nezabezpečené protokolem HTTPS měly nastaveno <meta name="referrer" content="unsafe-url”/>. To umožní, že taková nezabezpečená stránka se “dozví”, z jaké adresy přesně uživatel přichází a díky tomu může například analyzovat chování uživatelů na svém webu.

Přestože je toto doporučení zaměřeno především na katalogy knihoven, vztahuje se i na veškeré další weby - například zavedení HTTPS v kombinaci s HTTP/2 v digitální knihovně Kramerius velmi výrazně urychlí načítání náhledů stránek.

3. 8. 2017