Přístup přes nezabezpečený protokol HTTP či FTP

V dnešní době již neexistuje žádný argument pro poskytování obsahu na webu pomocí nezabezpečeného protokolu HTTP či ještě staršího FTP, které už v prohlížečích ztrácí podporu. Toto přirozeně platí i pro otevřená data, jakožto obsah poskytovaný přes web. Jelikož se ale jedná o běžnou součást provozu webového serveru, omezíme se na jasné doporučení: Pro svůj web, a tedy i přístup k otevřeným datům použijte protokol HTTPS. Při jeho implementaci dávejte pozor na nejčastější chyby při implementaci HTTPS.

Výhody protokolu HTTPS

- Uživatel si může být jist, že server je ten, za který se vydává
- Uživatel si může být jist, že data, která stáhne, jsou ta, která vystavil jejich poskytovatel
- Uživatel si může být jist, že to, o která data má zájem, zůstane mezi ním a cílovým serverem (nikdo nebude sledovat jeho chování po cestě)
- Google penalizuje weby nezabezpečené pomocí HTTPS
- Nejnovější protokol HTTP/2 už nezabezpečenou variantu ani neobsahuje

Nejčastější mýty podporující nezabezpečený protokol HTTP

Jedná se o otevřená data (případně veřejný web bez přihlašování). Proč tedy obsah šifrovat?

HTTPS neslouží jen pro šifrování, tedy zajištění toho, že při přenosu dat ze serveru na klienta si jejich obsah nepřečte třetí strana. Slouží i pro ověření, že server je ten, za který se vydává. To už má smysl i v případě otevřených dat a jiného webového obsahu. Klient (uživatel) si může být jist, že data či jiný obsah není podvržen. Další argumenty naleznete na stránce Why HTTPS Matters.

Zajištění certifikátu a jeho pravidelná obnova jsou drahé

To je nesmysl. Existuje například certifikační autorita Let's Encrypt, která certifikáty a jejich automatickou obnovu poskytuje v základní verzi zdarma. Její službu používá i tento web.