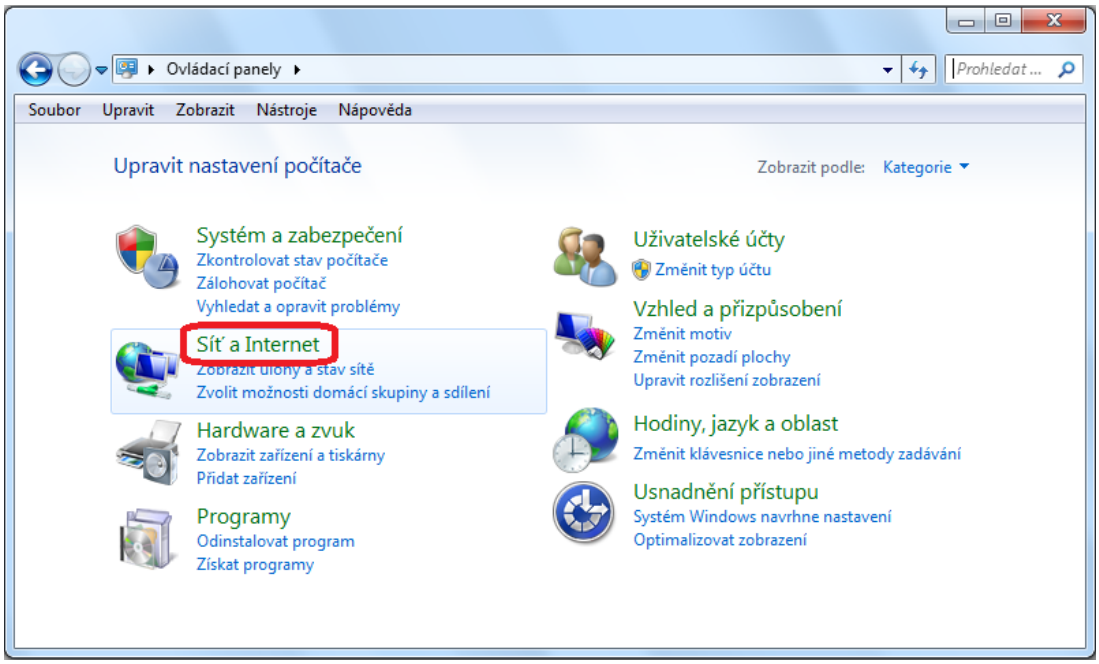
Vážení uživatelé informačních systémů ČNB,
dne 15. 10. 2014 byla zveřejněna zpráva o zranitelnosti protokolu https (resp. jeho varianty SSLv3), který je využíván i v informačních systémech ČNB (REGIS, SIPRES). Jedná se o velmi starý typ šifrovaného protokolu, který je ovšem ještě částí klientů (dle celosvětové statistiky 1% klientů) využíván. Obecné doporučení je zranitelnost eliminovat vypnutím varianty protokolu SSLv3 a používat pouze novější variantu TLSv1, kterou již řada klientů používá. O tom, jaký protokol klient využije pro komunikaci, si rozhoduje webový prohlížeč klienta sám – vybírá vždy nejkvalitnější šifrování. Vypnutí starší verze protokolu na serveru (na straně ČNB) může mít za následek nedostupnost některých klientů, pokud mají ve svém Internetovém nastavení povolený pouze tento protokol.

Bližší informace o zranitelnosti je např. na stránce https://technet.microsoft.com/en-us/library/security/3009008.aspx

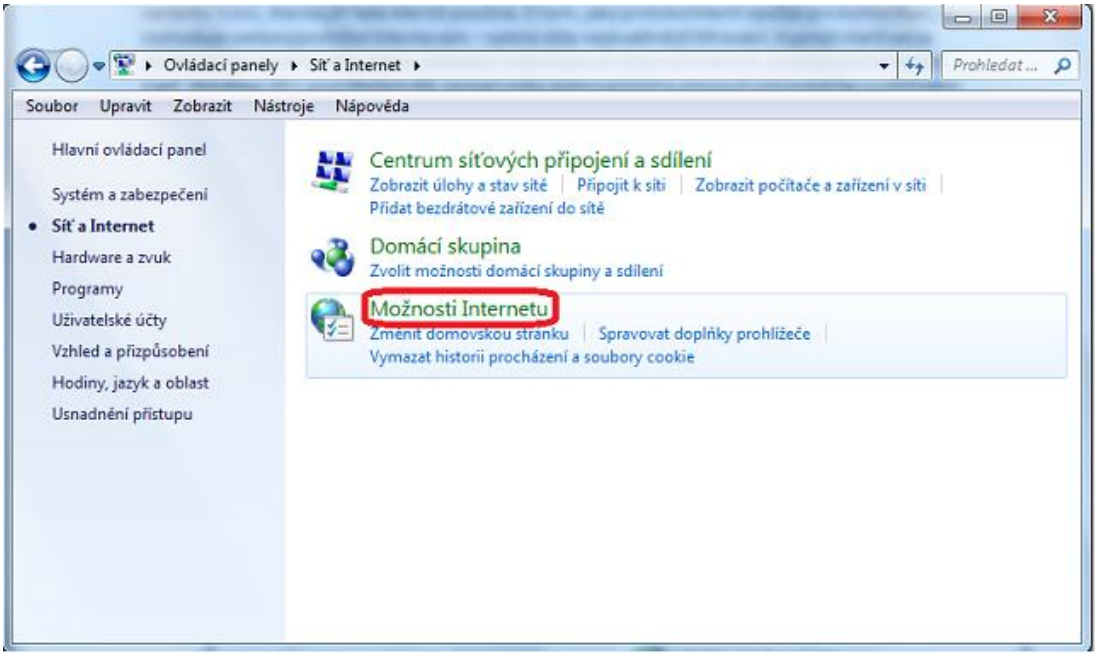
Z bezpečnostních důvodů přistoupila ČNB k zakázání přístupu k aplikacím pro uživatele používající protokol SSLv3.

Postup pro ruční nastavení protokolů:

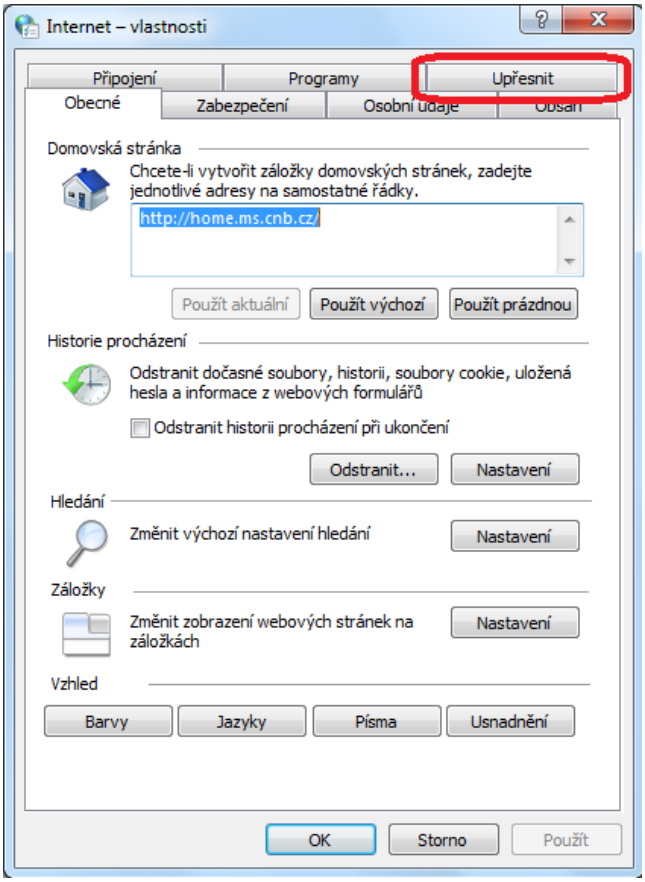
1. V PC najděte stránku *Ovládací panely*.



2. Na stránce *Síť a Internet* zvolte *Možnosti Internetu*.



3. Otevře se dialog *Možnosti Internetu*, na kterém je třeba zvolit kartu „Upřesnit“.



4. Na kartě *Upřesnit* je třeba vyhledat v *Nastavení* sekci *Zabezpečení* a nastavit používání protokolů tak, aby byly označeny pouze protokoly TLS. Poté vše potvrdit tlačítkem Použít.