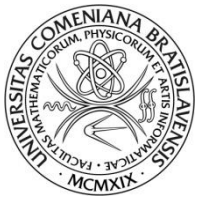
Ministerstvo financií
Slovenskej republiky

Fakulta matematiky, fyziky
a informatiky Univerzity
Komenského v Bratislave



Analýza stavu nasadenia SSL/TLS na zabezpečenie WWW stránok inštitúcií verejnej správy v Slovenskej republike v roku 2011

MINISTERSTVO FINANCIÍ SLOVENSKEJ REPUBLIKY
FAKULTA MATEMATIKY, FYZIKY A INFORMATIKY UK

2011

Analýza stavu nasadenia SSL/TLS na zabezpečenie WWW stránok inštitúcií verejnej správy v Slovenskej republike v roku 2011

Ministerstvo financií SR

Štefanovičova 5
P. O. BOX 82
817 82 Bratislava

tel.: (+421 2) 5958 1111
fax: (+421 2) 5958 3048

Ján Hochmann
riaditeľ odboru legislatívy, štandardov a bezpečnosti informačných systémov

tel.: (+421 2) 5958 2427
e-mail: jan.hochmann@mfsr.sk

Ivan Vazan
tel.: (+421 2) 5958 2449
e-mail: ivan.vazan@mfsr.sk

Fakulta matematiky, fyziky a informatiky UK

Mlynská dolina
842 48 Bratislava

tel.: (+421 2) 60295 111
fax: (+421 2) 65412 305

Jaroslav Janáček
Katedra informatiky FMFI UK

tel.: (+421 2) 60295 578
fax: (+421 2) 65427 041
e-mail: janacek@dcs.fmph.uniba.sk

Obsah

Zoznam grafov

Zoznam tabuliek

Úvod

So zvyšovaním dostupnosti pripojenia k Internetu v slovenských domácnostiach a firmách logicky rastie aj využívanie Internetu na získavanie informácií z orgánov verejnej správy. Zároveň sa postupne zvyšuje aj množstvo služieb verejnej správy, ktoré je možné využiť prostredníctvom elektronickej komunikácie. Základným prostriedkom používaným na zverejňovanie a poskytovanie informácií je systém WWW[1]. Okrem zverejňovania informácií prostredníctvom web-stránok tento systém umožňuje aj implementáciu interaktívnych elektronických služieb bez potreby špecifického vybavenia na strane používateľa týchto služieb.

Systém WWW je založený na klient-server architektúre. Pozostáva z WWW serverov a WWW klientov (prehliadačov), ktorí medzi sebou komunikujú prostredníctvom Internetu protokolom HTTP. WWW prehliadače sú v súčasnosti štandardnou výbavou bežných počítačov a mobilných zariadení.

Protokol HTTP prenáša údaje cez Internet v nezabezpečenej podobe, čo so sebou prináša bezpečnostné riziká – najmä nemožnosť overiť si identitu druhej strany, možnosť „odpočúvania“ komunikácie treťou stranou a možnosť modifikácie prenášaných údajov treťou stranou. Tieto nedostatky je možné odstrániť správnym nasadením kryptografickej ochrany. V systéme WWW sa takáto ochrana štandardne realizuje použitím protokolov SSL/TLS[2] na vytvorenie zabezpečeného komunikačného kanála, cez ktorý sa následne prenáša protokol HTTP[3]. Táto kombinácia HTTP a SSL/TLS je označovaná ako HTTPS.

Bezpečné použitie protokolov SSL/TLS (a teda aj HTTPS) si vyžaduje splnenie viacerých predpokladov. Nesplnenie týchto predpokladov môže mať za následok zníženie úrovne bezpečnosti až na úroveň rovnakú ako bez použitia SSL/TLS. Pre nedostatočne informovaného používateľa môže byť situácia paradoxne aj ešte horšia, nakoľko takýto používateľ môže vnímať samotné použitie SSL/TLS ako a-priori bezpečné, a preto môže stratiť ostražitosť, ktorú by v prípade čistého HTTP mohol mať.

Cieľom tohto prieskumu je analyzovať nasadenie protokolu SSL/TLS na zabezpečenie web stránok inštitúcií verejnej správy na vzorke cca 100 subjektov, identifikovať a klasifikovať nedostatky v konfigurácii SSL/TLS na príslušných serveroch a odporučiť opatrenia na ich odstránenie.

[1] World Wide Web, celosvetová sieť
[2] Secure Socket Layer, Transport Layer Security – protokoly pre bezpečnú transportnú vrstvu
[3] Hyper-text Transfer Protocol – protokol na prenos hypertextu

Charakteristika možností protokolov SSL/TLS

Ako sme spomenuli v úvode, komunikácia napr. protokolom HTTP cez Internet nie je chránená proti odpočúvaniu ani modifikácii, a neumožňuje spoľahlivo overiť identitu komunikujúcich strán. Cieľom protokolov SSL/TLS je použitím kryptografických prostriedkov vytvoriť medzi klientom (napr. WWW prehliadač) a serverom (napr. WWW server) komunikačný kanál, ktorý zabezpečí:

- autentifikáciu servera,
- voliteľne aj autentifikáciu klienta,
- ochranu dôvernosti prenášaných údajov a
- ochranu integrity prenášaných údajov.

Autentifikácia servera

Úlohou autentifikácie servera je poskytnúť používateľovi vysokú mieru istoty, že server, s ktorým komunikuje, je skutočne tým, za ktorý sa vydáva. Bez autentifikácie servera je prakticky zbytočné zaoberať sa ochranou dôvernosti a integrity prenášaných údajov, nakoľko bez autentifikácie servera klient, a teda ani používateľ, nemá možnosť overiť si, či komunikuje so želaným serverom alebo so serverom útočníka.

Autentifikácia v SSL/TLS je založená na asymetrickej kryptografii (kryptografii s verejnými a súkromnými kľúčmi). Základom je schopnosť servera preukázať znalosť súkromného kľúča, ktorý prislúcha k verejnému kľúču. Verejný kľúč je zviazaný s identitou servera (v prípade WWW minimálne s doménovým menom servera) formou certifikátu verejného kľúča. Certifikát verejného kľúča je elektronický dokument v definovanom formáte, ktorým jeho vydavateľ – certifikačná autorita potvrdzuje skutočnosť, že v certifikáte uvedený verejný kľúč patrí v certifikáte uvedenému držiteľovi. Certifikát je digitálne podpísaný, aby bolo možné overiť, že ho skutočne vydala certifikačná autorita, ktorá je v ňom uvedená ako vydavateľ. Na overenie digitálneho podpisu certifikačnej autority je potrebné poznať verejný kľúč tejto certifikačnej autority, ktorý býva taktiež distribuovaný v podobe certifikátu verejného kľúča. Postupnosť certifikátov, kde nasledujúci certifikát obsahuje verejný kľúč potrebný na overenie digitálneho podpisu predchádzajúceho certifikátu sa označuje ako certifikačná cesta alebo reťaz certifikátov (certificate chain). Posledný certifikát reťaze certifikátov (tzv. koreňový certifikát) je podpísaný súkromným kľúčom prislúchajúcim k verejnému kľúču uvedenému v tomto certifikáte – jedná sa o tzv. self-signed certifikát. Tento posledný certifikát reťaze certifikátov musí byť klientovi známy ako tzv. dôveryhodný certifikát, pretože platnosť jeho podpisu nemožno ďalej overiť (je na to potrebná informácia obsiahnutá v tomto certifikáte, ktorá pred jeho overením nie je dôveryhodná).

Server počas vytvárania komunikačného kanála protokolmi SSL/TLS posiela klientovi reťaz certifikátov. Ak klient nepozná žiadny certifikát tejto reťaze ako dôveryhodný, nie je schopný overiť digitálny podpis na certifikáte servera, a teda nie je schopný spoľahlivo získať verejný kľúč servera, a teda autentifikácia servera nie je možná.

Certifikáty verejných kľúčov majú obmedzenú dobu platnosti z dôvodu, že s dlhšou dobou používania páru verejného a súkromného kľúča rastie pravdepodobnosť úspešného odhalenia súkromného kľúča prislúchajúceho k verejnému kľúču uvedenému v certifikáte. Odhalenie súkromného kľúča by útočníkovi umožnilo falšovať digitálne podpisy certifikátov alebo autentifikáciu servera.

Autentifikácia klienta

Protokoly SSL/TLS umožňujú voliteľne vykonať aj autentifikáciu klienta založenú, rovnako ako autentifikácia servera, na asymetrickej kryptografii. Táto možnosť sa niekedy využíva na autentifikáciu používateľov v systémoch, kde používatelia majú na tento účel vydané certifikáty na svoje verejné kľúče. V takom prípade môže klient dokázať svoju identitu (resp. identitu používateľa) serveru – hovoríme o obojstranne autentifikovanom komunikačnom kanále (keďže autentifikácia servera je v SSL/TLS povinná). Autentifikácia klienta v rámci protokolu SSL/TLS sa využíva v rôznych informačných systémoch prístupných len vymedzenému okruhu používateľov a nie je určená pre WWW stránky prístupné širokej verejnosti.

Ochrana dôvernosti prenášaných údajov

V systéme WWW sa údaje prenášajú dvoma smermi:

- od servera ku klientovi,
- od klienta k serveru.

Od servera ku klientovi sa prenášajú všetky údaje, ktoré predstavujú obsah WWW stránky (či už sa jedná o statickú WWW stránku alebo WWW stránku dynamicky vygenerovanú na základe požiadavky od klienta) a pomocné údaje (napr. tzv. cookies). Od klienta k serveru sa prenášajú najmä požiadavky v podobe URL (adresy stránky s prípadnými parametrami), vyplnené polia vo formulároch, autentifikačné údaje (prihlasovacie mená a heslá) a pomocné informácie (napr. cookies). Tieto údaje môžu vyžadovať ochranu dôvernosti, t.j. zabránenie, aby ich bolo možné „odpočuť“ na ceste medzi klientom a serverom. Vždy by mala byť chránená dôvernosť autentifikačných údajov používateľa (najmä prihlasovacích hesiel).

Ochrana dôvernosti sa v SSL/TLS realizuje použitím symetrického šifrovania. Na tento účel je potrebné, aby medzi klientom a serverom došlo k dohodnutiu šifrovacieho kľúča, čo sa deje počas vytvárania komunikačného kanála protokolmi SSL/TLS. Výsledkom dohadovania šifrovacieho kľúča musí byť šifrovací kľúč známy len serveru a klientovi. Presnejšie v SSL/TLS dôjde počas vytvárania komunikačného kanála k dohodnutiu zdieľaného (medzi serverom a klientom) tajomstva, z ktorého sa následne odvodí šifrovací kľúč. Zdieľané tajomstvo sa v SSL verzie 3 a TLS verzie 1.0 dohaduje jedným z dvoch principiálnych spôsobov:

- použitím algoritmu na dohadovanie kľúčov (napr. algoritmus Diffie-Hellman), alebo
- vygenerovaním tajomstva u klienta a jeho zaslaním serveru v zašifrovanej podobe pomocou verejného kľúča servera. Na dešifrovanie takto preneseného tajomstva je potrebný príslušný súkromný kľúč. Úspešným dešifrovaním preto server preukáže znalosť príslušného súkromného kľúča, čím sa spojí autentifikácia a dohadovanie zdieľaného tajomstva.

Ochrana integrity prenášaných údajov

Úlohou ochrany integrity je zabezpečiť odhalenie situácie, kedy došlo k pozmeneniu prenášaných údajov medzi klientom a serverom. Ochrana integrity je minimálne rovnako dôležitá ako ochrana dôvernosti – často však dôležitejšia. Aj údaje, ktorých charakter nie je dôverný (napr. zverejnené informácie na WWW stránkach úradov), je zväčša potrebné chrániť proti neoprávneným zmenám. Údaje, ktorých integrita nie je chránená, môžu mať len informatívny charakter, nakoľko ich príjemca nemôže zistiť, či získané údaje neboli cestou pozmenené. Z tohto dôvodu má nasadenie protokolov SSL/TLS význam aj na WWW serveroch, ktoré len zverejňujú údaje, a neprichádzajú do styku so žiadnymi údajmi, ktorých dôvernosť je potrebné chrániť.

Ochrana integrity prenášaných údajov je v SSL/TLS zabezpečovaná pomocou hašovacích funkcií s kľúčom (známych tiež ako Keyed-Hash Message Authentication Code, skrátene HMAC). Podobne ako pri šifrovaní, aj v tomto prípade je potrebné medzi klientom a serverom zdieľať kľúč, ktorý sa kontrolu integrity použije. Ten sa, rovnako ako šifrovací kľúč, odvodí zo zdieľaného tajomstva dohodnutého pri vytváraní komunikačného kanála.

Predpoklady na správne použitie protokolov SSL/TLS pre WWW

Aby bolo použitie protokolov SSL/TLS v systéme WWW účinné, je potrebné, aby bolo splnených niekoľko predpokladov:

1. Klient musí byť schopný overiť reťaz certifikátov (overiť digitálne podpisy certifikátov), aby získal verejný kľúč servera.

2. Meno servera uvedené v certifikáte musí zodpovedať menu servera, s ktorým má klient komunikovať.

3. Na zabezpečenie ochrany komunikačného kanála a na digitálne podpisy certifikátov nesmú byť použité „slabé“ algoritmy, t.j. algoritmy, u ktorých sa v súčasnosti pozná alebo predpokladá možnosť ich úspešnej kryptoanalýzy, resp. nesmú byť použité kľúče, ktorých dĺžka sa v súčasnosti nepovažuje za dostatočnú.

4. Nesmie byť možné použiť protokol SSL verzie 2, ktorá má známe bezpečnostné slabiny.

5. Server nesmie akceptovať nebezpečné dohadovanie nových parametrov (renegotiation), ktoré vedie k známej metóde na vkladanie útočníkom zvolených údajov na začiatok komunikácie.

Nesplnenie predpokladu 1 alebo 2 má za následok situáciu, kedy nie je možná autentifikácia servera, a teda protokoly SSL/TLS nemôžu zabezpečiť ochranu komunikácie. Všetky bežné WWW prehliadače na túto skutočnosť používateľa upozornia, no veľká väčšina používateľov, podľa našich praktických skúseností, tieto varovania ignoruje a prehliadač prinúti pokračovať v spojení. Výsledkom je úroveň zabezpečenia porovnateľná s úrovňou klasického protokolu HTTP bez SSL/TLS. Navyše, používateľ si môže mylne myslieť, že spojenie je bezpečné alebo aspoň bezpečnejšie (keďže je zabezpečené protokolom SSL/TLS), a preto môže mať falošný pocit bezpečia a stratiť ostražitosť. Úspešná realizácia útoku, ktorý umožní „odpočúvanie“ a modifikáciu komunikácie, je v tomto prípade pomerne jednoduchá a zvládne ju bežný útočník bez špeciálneho vybavenia.

Nesplnenie predpokladu 3 alebo 4 môže dostatočne motivovanému útočníkovi umožniť vykonať úspešný kryptoanalytický útok, čo môže mať za následok prekonanie ochrany dôvernosti a/alebo integrity prenášaných údajov, alebo umožnenie falošnej autentifikácie servera a následné jednoduché „odpočúvanie“ a/alebo modifikáciu prenášaných údajov. Úspešná realizácia tohto typu útoku si však môže vyžadovať útočníka s dostatočným výpočtovým výkonom alebo inými zdrojmi a je rozhodne náročnejšia ako realizácia útokov pri nesplnení predpokladu 1 alebo 2.

Nesplnenie predpokladu 5 umožňuje útočníkovi vkladať na začiatok komunikácie od klienta k serveru ľubovoľné dáta. V závislosti od kontextu to môže umožniť realizáciu nepriameho odpočúvania časti komunikácie alebo zaslanie požiadaviek útočníka, ktoré bude server interpretovať ako pochádzajúce od legitímneho klienta. Realizácia tohto útoku je pomerne jednoduchá, no jeho reálna využiteľnosť je značne závislá na vlastnostiach aplikácie na serveri, voči ktorej je útok vedený. Preto ho v našom prieskume budeme považovať za menej závažný ako útoky realizovateľné pri nesplnení predpokladov 1 alebo 2.

Metodika vyhodnocovania nasadenia SSL/TLS

Testované skutočnosti

V rámci tohto projektu budú skúmané nasledovné skutočnosti s cieľom preveriť splnenie predpokladov uvedených v predchádzajúcej časti:

1. Zhoda WWW stránky prístupnej cez HTTPS s WWW stránkou prístupnou cez HTTP – cieľom je vylúčiť situáciu, kedy je HTTPS serverom síce podporované, no zobrazená stránke nie je predpokladanou stránkou.

2. Úplnosť reťaze certifikátov – cieľom je preveriť, či server posiela celú reťaz certifikátov a nie len certifikát servera. Špecifikácia protokolu TLS pripúšťa, aby v reťazi certifikátov, ktoré server pošle klientovi, bol vypustený posledný certifikát, ktorý aj tak klient musí mať k dispozícii ako dôveryhodný. Oba prípady (úplná reťaz a reťaz bez koreňového certifikátu) budeme považovať za korektné.

3. Certifikačná autorita (CA), ktorá vydala koreňový certifikát – pre úspešnú autentifikáciu servera je nevyhnutné, aby klient poznal koreňový certifikát ako dôveryhodný. WWW prehliadače sú štandardne vybavené zoznamom koreňových certifikátov známych svetových certifikačných autorít, ktoré považujú za dôveryhodné. Do prehliadačov je možné inštalovať ako dôveryhodné aj ďalšie koreňové certifikáty. Budeme rozlišovať nasledujúce prípady:

1. CA štandardne známa v bežných prehliadačoch – OK.

2. Slovenská CA (v zmysle zákona o elektronickom podpise), ktorá nie je štandardne známa v bežných prehliadačoch – problematická overiteľnosť pre bežného používateľa, ktorý nie je klientom tejto CA.

3. Neznáma/vlastná CA – neoveriteľnosť mimo uzavretej skupiny používateľov.

4. Self-signed certifikát servera – neoveriteľnosť mimo uzavretej skupiny používateľov.

   Prípady 3 a 4 budeme považovať za zásadnú prekážku overiteľnosti certifikátu, keďže sa zameriavame na servery poskytujúce informácie a služby širokej verejnosti (a nie uzavretej skupine používateľov so špecifickým vzťahom k prevádzkovateľovi servera). Prípad 2 budeme považovať za komplikáciu pre overenie, nakoľko nemožno predpokladať, že každý používateľ má vo svojom prehliadači inštalované koreňové certifikáty všetkých slovenských certifikačných autorít.

4. Meno servera uvedené v certifikáte – správne meno servera uvedené v certifikáte je kľúčovým predpokladom pre úspešnú autentifikáciu servera. Budeme rozlišovať 3 prípady:

1. správne meno – OK

2. iné meno v rovnakej doméne – problematická overiteľnosť

3. nesprávne meno – neoveriteľnosť

5. Dátum platnosti certifikátu – pokiaľ je aktuálny dátum a čas mimo rozsah platnosti certifikátu, WWW prehliadač bude používateľa varovať. Neplatnosť certifikátu budeme považovať za komplikáciu pre overenie.

6. Dĺžka RSA[4] kľúča servera – podľa aktuálnych odporúčaní by dĺžka RSA kľúča mala byť minimálne 2048 bitov. Kľúče s dĺžkou menšou ako 1024 bitov budeme považovať za bezpečnostný problém umožňujúci realizáciu netriviálnych útokov, kľúče s dĺžkou aspoň 1024 bitov ale menej ako 2048 budeme považovať za nesplnenie odporúčaní.

7. Použitie algoritmu MD5[5] na podpisy v certifikátoch – algoritmus MD5 je v súčasnosti považovaný za nevyhovujúci pre účely podpisovania certifikátov (už boli demonštrované úspešné útoky na SSL/TLS v prípadoch, kde certifikačná autorita používala MD5 pri podpisovaní certifikátov). Preto budeme jeho použitie v reťazi certifikátov považovať za nedostatok umožňujúci realizáciu netriviálnych útokov.

8. Prípustnosť slabých šifrovacích algoritmov (dĺžka kľúča < 128 bitov) – ak server pripúšťa slabé šifrovacie algoritmy, budeme to považovať za situáciu, ktorá umožňuje netriviálne útoky.

9. Prípustnosť protokolu SSL verzie 2 – prípustnosť protokolu SSL verzia 2 budeme považovať za

[4]RSA – asymetrický šifrovací a podpisovací algoritmus
[5]MD5 – hašovací algoritmus

nedostatok umožňujúci netriviálne útoky.

10. Prípustnosť nebezpečnej renegociácie SSL/TLS parametrov – nebezpečná renegociácia SSL/TLS parametrov umožňuje realizáciu útoku vkladania útočníkom zvolených údajov na začiatok komunikácie – budeme ju považovať za nedostatok umožňujúci realizáciu netriviálnych útokov.

11. Podpora bezpečnej renegociácie SSL/TLS parametrov – bezpečná renegociácia SSL/TLS parametrov odstraňuje problémy s nebezpečnou renegociáciou a je preto odporúčaná. Ak však server akceptuje renegociáciu iniciovanú klientom, vytvára zvýšený potenciál na útok na dostupnosť servera (Denial of Service). Nepodporovanie bezpečnej renegociácie ako aj akceptáciu klientom iniciovanej renegociácie budeme preto považovať na nesplnenie odporúčaní.

12. Použitie známych slabých kompromitovaných RSA kľúčov – existuje množina dobre známych dvojíc verejných a súkromných RSA kľúčov – ich použitie umožňuje jednoduché falšovanie identity servera, preto ho budeme považovať za zásadný problém.

Spracovanie zistených skutočností

Na základe zistených skutočností popísaných vyššie budú identifikované a v protokole z testovania individuálne popísané zistené problémy a navrhnuté opatrenia na ich odstránenie. Zároveň bude každému testovanému WWW serveru pridelené hodnotenie úrovne bezpečnosti – celkové hodnotenie a zvlášť hodnotenie certifikátu a hodnotenie konfigurácie SSL/TLS parametrov servera.

Na hodnotenie úrovne bezpečnosti bude použitá nasledujúca stupnica:

- X – server nepodporuje protokol HTTPS alebo WWW stránka prístupná cez HTTPS nezodpovedá WWW stránke prístupnej cez HTTP.

Ak server nepodporuje HTTPS (nie je možné sa pripojiť, na porte 443 nie je použitý protkol HTTPS, spojenie zlyhá chybou), neboli hodnotené žiadne ďalšie parametre. Ak server HTTPS podporuje a je možné sa k nemu pripojiť, boli vyhodnotené aj ostatné parametre, no ich hodnotenie nemusí byť relevantné, nakoľko zobrazovaná WWW stránka nezodpovedá očakávanej stránke (rovnakej, ako je na rovnakej adrese prístupná cez HTTP) a je niekedy stránkou úplne iného subjektu (napr. poskytovateľa služby prevádzky WWW servera).
Pre servery s týmto hodnotením odporúčame zvážiť nasadenie SSL/TLS minimálne za účelom autentifikácie servera a zabezpečenia integrity prenášaných údajov, čím by používatelia získali vysokú mieru istoty, že zobrazené informácie pochádzajú skutočne zo servera danej organizácie.

- E – zistené závažné nedostatky – nasadenie SSL/TLS na tomto serveri neposkytuje z pohľadu používateľa z radov širokej verejnosti žiadnu ochranu.

Do tejto kategórie sú zaradené servery, ktoré majú certifikát vystavený na cudzie meno, neoveriteľný certifikát (vydaný neznámou certifikačnou autoritou, self-signed certifikát, neúplná reťaz certifikátov) alebo používajú známy kompromitovaný RSA kľúč. Taktiež sú do tejto kategórie zaradené servery, ktoré po pripojení na stránku protokolom HTTPS spôsobia presmerovanie klienta na prístup cez protokol HTTP.
Odstránenie nedostatkov si vyžaduje úpravu konfigurácie alebo získanie správneho a overiteľného certifikátu pre server. V súčasnosti je možné u niektorých známych certifikačných autorít získať postačujúci certifikát aj bezplatne.

- D – parametre certifikátov alebo vlastnosti a nastavenie servera umožňujú realizáciu netriviálnych útokov.

Do tejto kategórie sú zaradené servery, pri ktorých bola detekovaná podpora nebezpečných algoritmov (SSL verzia 2, šifrovanie s kľúčmi kratšími ako 128 bitov), podpora nebezpečnej renegociácie SSL/TLS parametrov alebo použitie certifikátu podpísaného použitím algoritmu MD5.
Odstránenie nedostatkov je zväčša záležitosťou bezplatnej aktualizácie softvéru a úpravou konfigurácie.

- C – pri použití sa vyskytujú varovania, no nie je bezprostredne ohrozená bezpečnosť.

Do tejto kategórie sú zaradené servery, ktoré používajú (inak bez problémov overiteľný) certifikát s vypršanou platnosťou alebo certifikát vystavený na meno iného servera v tej istej doméne. Taktiež sú do tejto kategórie zaradené servery, ktoré používajú certifikát vydaný slovenskou certifikačnou autoritou (registrovanou podľa Zákona o elektronickom podpise).
Odstránenie nedostatkov si vyžaduje získanie obnoveného certifikátu, resp. získanie certifikátu so správnym menom. V súčasnosti je možné u niektorých známych certifikačných autorít získať postačujúci certifikát aj bezplatne.

- B – server nespĺňa niektoré súčasné odporúčania.

Do tejto kategórie sú zaradené servery, ktoré používajú RSA kľúče kratšie ako 2048 bitov, nepodporujú bezpečnú renegociáciu SSL/TLS parametrov alebo akceptujú klientom iniciovanú bezpečnú renegociáciu SSL/TLS parametrov. Tieto nedostatky v súčasnosti nepredstavujú ohrozenie bezpečnosti, no odporúčame ich odstrániť pre udržanie bezpečnostnej úrovne v budúcnosti.

- A – bez zistených nedostatkov.

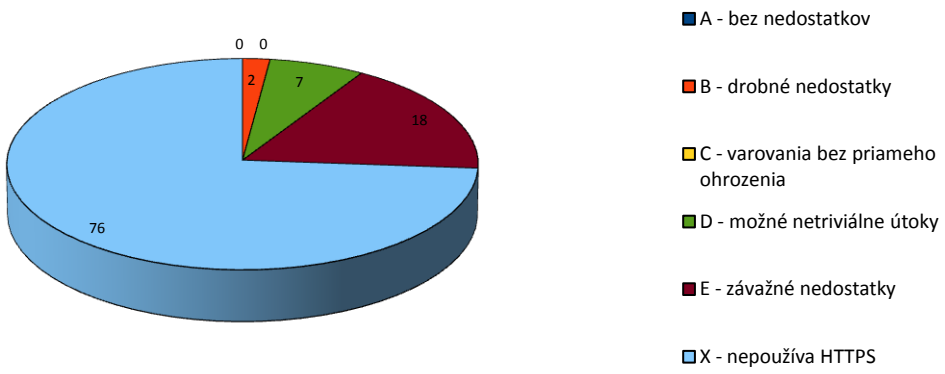
Do tejto kategórie sú zaradené servery, pri ktorých neboli zistené žiadne nedostatky v rozsahu preverovaných skutočností.

Sumár výsledkov vyhodnocovania nasadenia SSL/TLS

Celkovo bolo preverovaných 103 WWW serverov uvedených v prílohe 1. V tabuľke sú uvedené počty serverov v jednotlivých skupinách.

skupina	počet	podiel
Ministerstvá	14	14%
Iné orgány verejnej správy	36	36%
VÚC	8	8%
Mestá a obce	33	32%
Iné inštitúcie	11	11%
Spolu	**103**	

Tabuľka 1: Rozdelenie analyzovaných WWW serverov

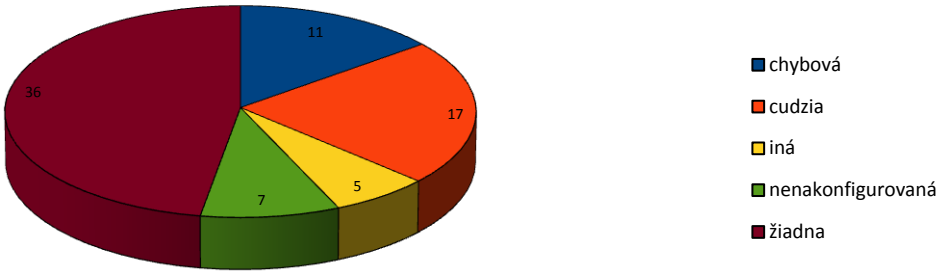


Graf 1: Celkové hodnotenie

V grafe 1 je zobrazený počet serverov v jednotlivých kategóriách celkového hodnotenia.

Ako vidno, len 27 testovaných serverov (26%) sprístupňuje protokolom HTTPS rovnakú WWW stránku ako protokolom HTTP. Zvyšných 76 serverov (74%) bolo zaradených do kategórie X, teda nevyužívajú protokol HTTPS na sprístupnenie rovnakého obsahu.

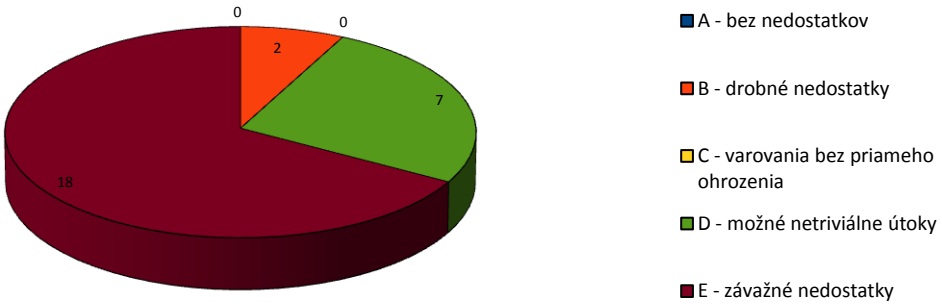
Podrobnejšie rozdelenie dôvodov zaradenia do kategórie X je zobrazené v grafe 2.



Graf 2: Dôvody pre hodnotenie X - zobrazená stránka

Takmer polovica zo serverov v kategórii X nesprístupňuje protokolom HTTPS žiadnu stránku. Takmer štvrtina zobrazuje stránku nesúvisiacu s danou inštitúciou – väčšinou sa jedná o stránku poskytovateľa služieb prevádzky WWW servera, v niektorých prípadoch o stránku jeho iného klienta. To môže pôsobiť značne mätúco na používateľa. V 11 prípadoch (14%) bola zobrazená chybová stránka, v 5 prípadoch (7%) iná stránka rovnakej inštitúcie a v 7 prípadoch (9%) bola na serveri ponechaná pôvodná konfigurácia z inštalácie.

V ďalšom sa budeme venovať len serverom, ktoré protokolom HTTPS sprístupňujú očakávanú WWW stránku. V



Graf 3: Celkové hodnotenie (mimo X)

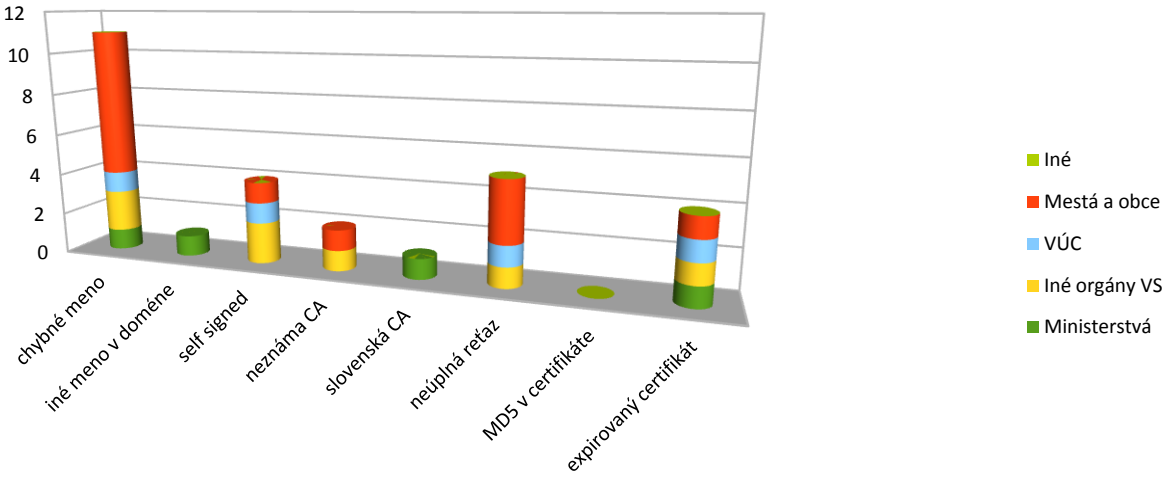
grafe 3 je uvedený počet takýchto serverov v jednotlivých kategóriách celkového hodnotenia.

Z nich žiadny nebol zaradený do kategórie A, 2 servery (7%) boli zaradené do kategórie B, 7 serverov (26%) do kategórie D a až 18 serverov (67%) do kategórie E.

6 serverov v kategórii D malo certifikáty na úrovni A alebo B, 1 server na úrovni C. Hodnotenie D získali z dôvodov nevhodnej konfigurácie, takže úpravou konfigurácie je možné výrazné zlepšenie ich hodnotenia.

Dôvodom hodnotenia E boli (až na 2 prípady) problémy s overiteľnosťou certifikátu.

V grafe 4 je uvedený prehľad chýb v certifikátoch serverov, ktoré neboli v celkovom hodnotení zaradené do kategórie X.



Graf 4: Chyby v certifikátoch

Ako vidno z grafu, 11 serverov (41%) používa certifikát vydaný na nesúvisiace meno, čo je závažný problém, nakoľko to spôsobuje rovnaké príznaky ako pokus o falšovanie identity servera útočníkom. Najviac serverov (7) s týmto problémom bolo v skupine mestá a obce.

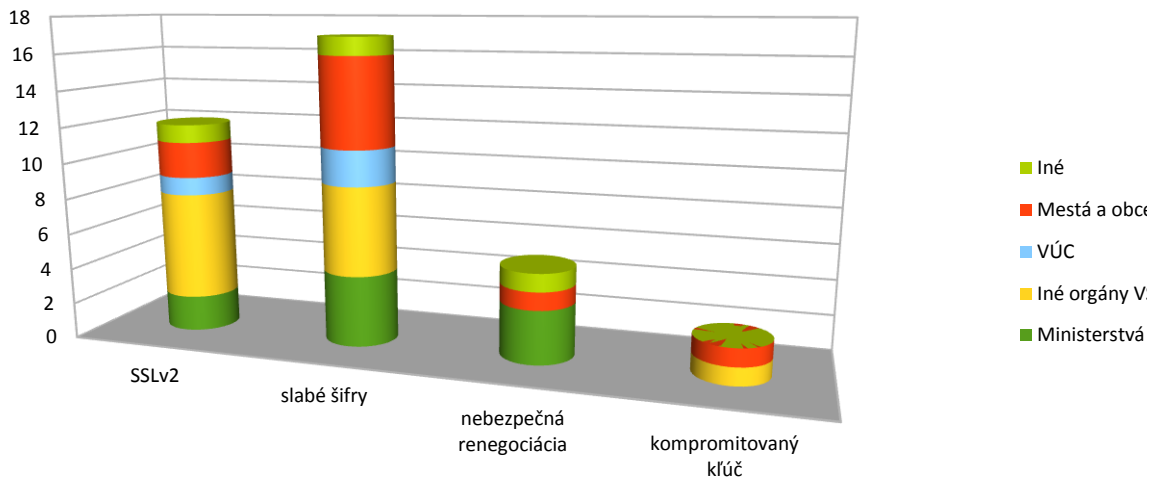
6 serverov (22%) používa self-signed certifikáty alebo certifikáty vydané neznámou certifikačnou autoritou, čo spôsobuje, že bežný používateľ z radov širokej verejnosti si nemôže overiť identitu servera. V tejto súvislosti musíme poznamenať, že získať certifikát pre server od známej certifikačnej autority je v súčasnosti možné aj bezplatne.

5 serverov (19%) má chybnú konfiguráciu – neposielajú správnu reťaz certifikátov, čím znemožňujú overenie svojho certifikátu aj v prípade, že je vydaný známou certifikačnou autoritou (takéto prípady boli 2).

4 servery (15%) prezentovali už neplatný certifikát, čo spôsobí varovanie v prehliadači.

Potešujúce bolo, že žiadny zo serverov mimo kategóriu X nepoužíva certifikát podpísaný použitím algoritmu MD5.

Okrem parametrov certifikátu boli detailne hodnotené aj vlastnosti a nastavenia WWW servera z pohľadu parametrov protokolu SSL/TLS. V grafe 5 je uvedený prehľad nedostatkov v konfigurácii serverov, ktoré neboli v celkovom hodnotení zaradené do kategórie X.



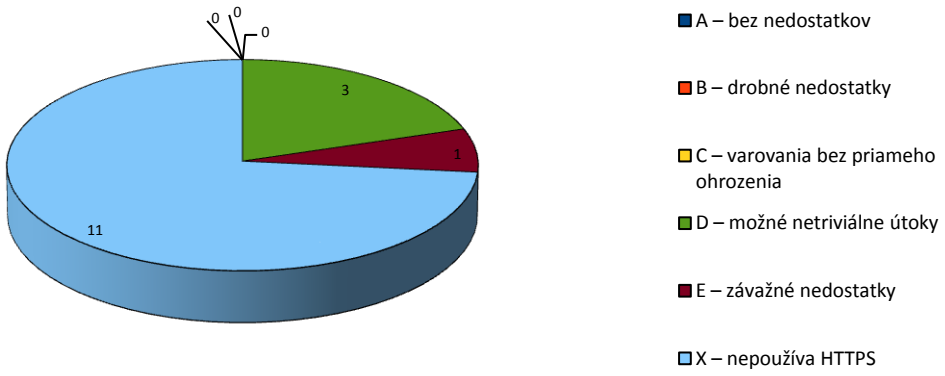
Graf 5: Chyby v konfigurácii

Najčastejším problémom bolo povolenie použitia slabých šifier (17 serverov) a protokolu SSL verzia 2 (12 serverov). Tieto nedostatky sú triviálne odstrániteľné úpravou konfigurácie serverov.

Vážnejší problém, ktorého zneužitie nemusí byť (v závislosti na konkrétnych podmienkach) zložité, je podpora nebezpečnej renegociácie SSL/TLS parametrov. Tento nedostatok bol zistený na 5 (19%) serveroch mimo kategóriu X. Signalizuje to používanie neaktualizovaných verzií softvéru, keďže po zverejnení tejto slabiny v minulosti boli vydané aktualizácie pre všetky bežne používané WWW servery, ktoré nebezpečnú renegociáciu zakázali.

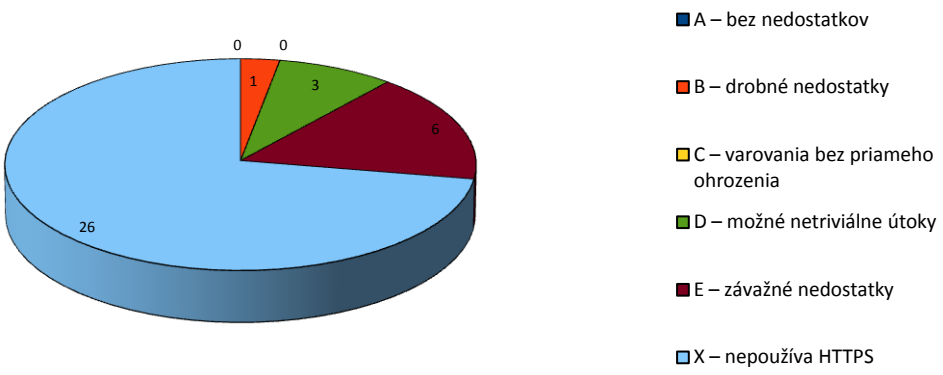
Za osobitnú zmienku stojí nález dvoch serverov, ktoré používajú známy kompromitovaný RSA kľúč. Identita týchto serverov môže byť ľahko sfalšovaná, resp. dôvernosť a integrita prenášaných údajov narušená. Takéto kľúče je potrebné okamžite zmeniť a získať nové certifikáty.

V grafoch 6 až 10 je zobrazené rozdelenie serverov v jednotlivých skupinách inštitúcií do jednotlivých kategórií celkového hodnotenia.



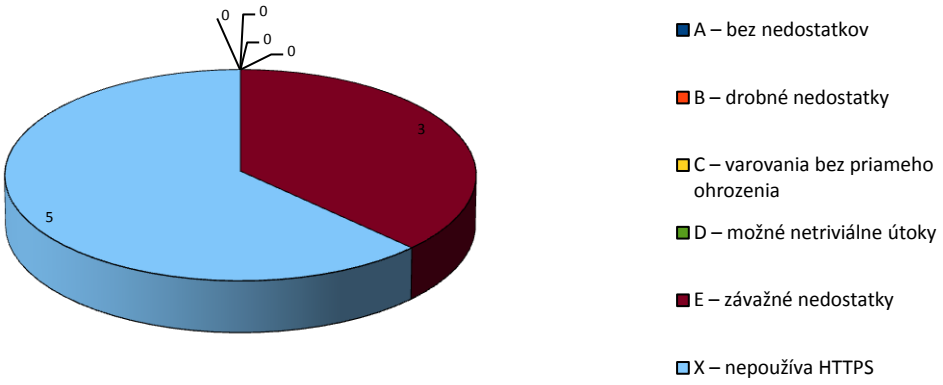
Graf 6: Celkové hodnotenie - ministerstvá

4 z 15 ministerstiev (27%) sprístupňujú testované stránky aj cez protokol HTTPS, pričom 3 z nich získali hodnotenie lepšie ako E.



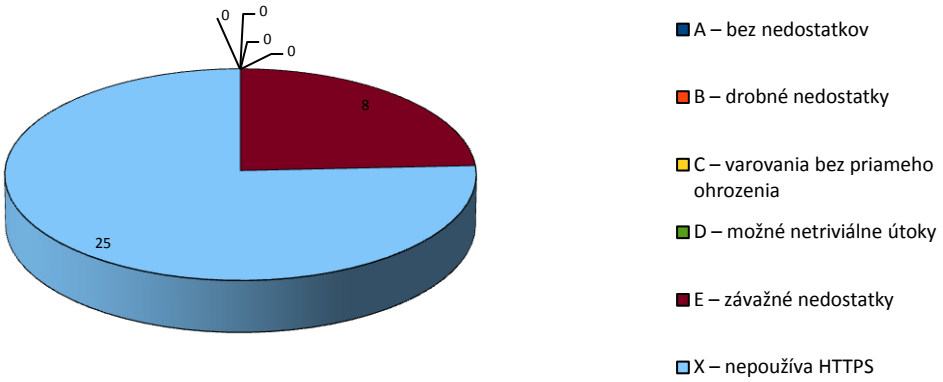
Graf 7: Celkové hodnotenie - iné orgány verejnej správy

V skupine iných orgánov verejnej správy využíva protokol HTTPS na sprístupnenie svojich stránok 10 z 36 inštitúcií (28%). Len 4 z nich však získali hodnotenie lepšie ako E.



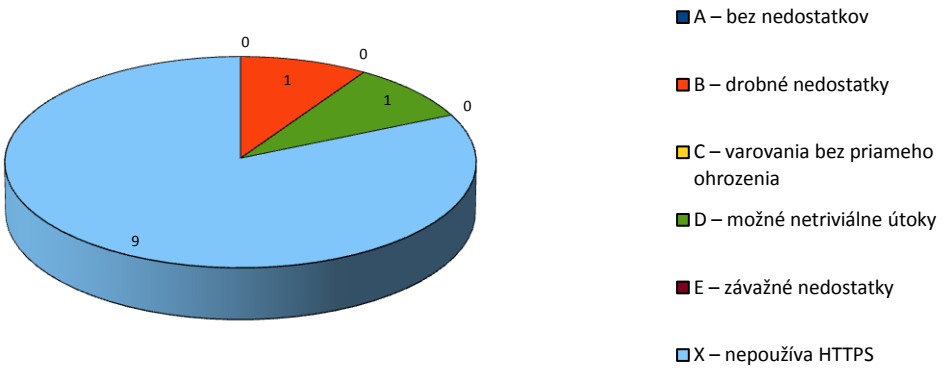
Graf 8: Celkové hodnotenie - VÚC

3 z 8 VÚC (38%) využívajú protokol HTTPS na sprístupnenie svojich WWW stránok, no žiadny nezískal hodnotenie lepšie ako E, teda použitie HTTPS na stránkach žiadneho VÚC v skutočnosti neprináša žiadnu ochranu.



Graf 9: Celkové hodnotenie - mestá a obce

8 z 33 testovaných miest a obcí (24%) používa HTTPS na sprístupnenie svojich WWW stránok, ale rovnako ako v prípade VÚC, žiadny z týchto serverov nezískal hodnotenie lepšie ako E, a teda neposkytuje žiadnu ochranu.



Graf 10: Celkové hodnotenie - iné inštitúcie

2 z 11 testovaných serverov v skupine iné inštitúcie (18%) používajú protokol HTTPS, jeden získal hodnotenie D a jeden hodnotenie B.

Celkovo možno konštatovať, že používanie protokolov SSL/TLS na zabezpečenie WWW stránok vo verejnej správe v Slovenskej republike je využívané pomerne málo. Navyše, s výnimkou 3 ministerstiev, 4 iných orgánov verejnej správy a 2 iných inštitúcií, vykazuje použitie SSL/TLS závažné nedostatky. Najhoršia situácia je v skupinách VÚC a mestá a obce, kde boli závažné nedostatky odhalené na všetkých testovaných serveroch.

Príloha 1 – zoznam WWW serverov zahrnutých do hodnotenia

Ministerstvá	
Ministerstvo dopravy, výstavby a regionálneho rozvoja SR	https://www.telecom.gov.sk/
Ministerstvo financií Slovenskej republiky	https://www.finance.gov.sk/
Ministerstvo hospodárstva SR	https://www.economy.gov.sk/
Ministerstvo kultúry SR	https://www.culture.gov.sk/
Ministerstvo obrany SR	https://www.mosr.sk/
Ministerstvo pôdohospodárstva SR	https://www.land.gov.sk/
Ministerstvo práce sociálnych vecí a rodiny	https://www.employment.gov.sk/
Ministerstvo školstva, vedy, výskumu a športu SR	https://www.minedu.sk/
Ministerstvo spravodlivosti SR	https://www.justice.gov.sk/
Ministerstvo vnútra SR	https://www.minv.sk/
Ministerstvo zahraničných vecí SR	https://www.foreign.gov.sk/
Ministerstvo zahraničných vecí SR	https://www.mzv.sk/
Ministerstvo zdravotníctva SR	https://www.health.gov.sk/
Ministerstvo životného prostredia SR	https://www.enviro.gov.sk/
Iné orgány verejnej správy	
Colná správa	https://www.colnasprava.sk/
Daňové riaditeľstvo	https://www.drsr.sk/
Fond národného majetku SR	https://www.natfund.gov.sk/
Generálna prokuratúra SR	https://www.genpro.gov.sk/
Jednotný automatizovaný systém právnych informácií	https://jaspi.justice.gov.sk/
Katastrálny portál Úradu geodézie, kartografie a katastra SR	https://www.katasterportal.sk/
Národná banka Slovenska	https://www.nbs.sk/
Národný bezpečnostný úrad	https://www.nbusr.sk/
Národný inšpektorát práce	https://www.nip.sk/
NKU - Najvyšší kontrolný úrad SR	https://www.nku.gov.sk/
NRSR - Národná rada SR	https://www.nrsr.sk/
Pamiatkový úrad	https://www.pamiatky.sk/
Poštový regulačný úrad	https://www.posturad.sk/
Prezident SR	https://www.prezident.sk/
Protimonopolný úrad SR webové sídla	https://www.antimon.gov.sk/
Slovenská informačná služba	https://www.sis.gov.sk/
Slovenský metrologický ústav	https://www.smu.gov.sk/
Slovenský metrologický ústav	https://www.smu.sk/
Slovenský ústav technickej normalizácie	https://www.sutn.gov.sk/
Slovenský ústav technickej normalizácie	https://www.sutn.sk/
Štátna pokladnica	https://www.pokladnica.sk/
Štátna správa hmotných rezerv SR	https://www.reserves.gov.sk/
Telekomunikačný úrad Slovenskej republiky	https://www.teleoff.gov.sk/
ÚPN - Ústav pamäti národa	https://www.upn.gov.sk/
Úrad geodézie, kartografie a katastra SR	https://www.geodesy.gov.sk/
Úrad jadrového dozoru	https://www.ujd.gov.sk/
Úrad na ochranu osobných údajov SR	https://www.dataprotection.gov.sk/
Úrad pre normalizáciu, metrológiu a skúšobníctvo SR	https://www.normoff.gov.sk/
Úrad pre normalizáciu, metrológiu a skúšobníctvo SR	https://www.unms.sk/
Úrad pre verejné obstarávanie	https://www.uvo.gov.sk/
Úrad priemyselného vlastníctva SR	https://www.indprop.gov.sk/
Úrad Vlády SR	https://www.government.gov.sk/
Úrad Vlády SR	https://www.vlada.gov.sk/
ÚRSO - Úrad pre reguláciu sieťových odvetví	https://www.urso.gov.sk/
Ústavný súd SR	https://www.concourt.sk/
Verejný ochranca práv	https://www.vop.gov.sk/
Vyššie územné celky	
Banskobystrický samosprávny kraj	https://www.vucbb.sk/
Bratislavský samosprávny kraj	https://www.region-bsk.sk/
Košický samosprávny kraj	https://www.vucke.sk/
Nitriansky samosprávny kraj	https://www.unsk.sk/
Prešovský samosprávny kraj	https://www.vucpo.sk/

Trenčiansky samosprávny kraj	https://www.tsk.sk/
Trnavský samosprávny kraj	https://www.trnava-vuc.sk/
Žilinský samosprávny kraj	https://www.regionzilina.sk/
Mestá a obce	
Banská Bystrica	https://www.banskabystrica.sk/
Bardejov	https://www.bardejov.sk/
Bernolákovo	https://www.bernolakovo.sk/
Bratislava - Oficiálne stránky hlavného mesta	https://www.bratislava.sk/
Bystrička	https://www.bystricka.sk/
Častá	https://www.obec-casta.sk/
Ducové	https://www.ducove.sk/
Haniska	https://www.haniska-ke.sk/
Humenné	https://www.humenne.sk/
Kamanová	https://www.kamanova.ocu.sk/
Komárno	https://www.komarno.sk/
Košice	https://www.kosice.sk/
Košice Západ - Mestská časť	https://www.kosicezapad.sk/
Levoča	https://www.levoca.sk/
Liptovský Mikuláš	https://www.mikulas.sk/
Lučenec	https://www.lucenec.sk/
Nitra	https://www.nitra.sk/
Nová Dubnica	https://www.novadubnica.eu/
Podbiel	https://www.podbiel.sk/
Podhájska	https://www.obecpodhajska.sk/
Poprad	https://www.poprad.sk/
Považská Bystrica	https://www.povazska-bystrica.sk/
Prešov	https://www.presov.sk/
Rožňava	https://www.roznava.sk/
Šahy	https://www.sahy.sk/
Spišská Nová Ves	https://www.spisskanovaves.eu/
Stropkov	https://www.stropkov.sk/
Šuňava	https://www.sunava.sk/
Trávnica	https://www.travnica.sk/
Trenčín	https://www.trencin.sk/
Ždiar	https://www.zdiar.eu/
Žilina	https://www.zilina.sk/
Zvolen	https://www.zvolen.sk/
Iné inštitúcie	
Centrálny depozitár cenných papierov SR	https://www.cdcp.sk/
Inštitút pre výskum práce a rodiny	https://www.sspr.gov.sk/
Rada pre vysielanie a retransmisiu	https://www.rada-rtv.sk/
Slovenská advokátska komora	https://www.sak.sk/
Slovenská kancelária poisťovateľov	https://www.skp.sk/
Slovenská obchodná inšpekcia	https://www.soi.sk/
Slovenská živnostenská komora	https://www.szk.sk/
Sociálna poisťovňa	https://www.socpoist.sk/
Únia miest Slovenska	https://www.unia-miest.sk/
Úrad pre dohľad nad zdravotnou starostlivosťou	https://www.udzs.sk/
Ústredný portál verejnej správy	https://portal.gov.sk/

Príloha 2 – protokoly z hodnotenia

Protokoly z hodnotenia sú k dispozícii na Sekcii informatizácie spoločnosti Ministerstva financií Slovenskej republiky.