Zentrum für sichere Informationstechnologie – Austria
Secure Information Technology Center – Austria

A-1030 Wien, Seidlgasse 22 / 9
Tel.: (+43 1) 503 19 63–0
Fax: (+43 1) 503 19 63–66

A-8010 Graz, Inffeldgasse 16a
Tel.: (+43 316) 873-5514
Fax: (+43 316) 873-5520

http://www.a-sit.at
E-Mail: office@a-sit.at

DVR: 1035461
ZVR: 948166612
UID: ATU60778947

KURZSTUDIE

HTTPS (SSL, TLS) ANALYSE ÖSTERREICHISCHER GV.AT DOMÄNEN

PETER TEUFL – PETER.TEUFL@A-SIT.AT
ANDREAS REITER – ANDREAS.REITER@A-SIT.AT
ALEXANDER MARSALEK – ALEXANDER.MARSALEK@A-SIT.AT
SANDRA KREUZHUBER – SANDRA KREUZHUBER@A-SIT.AT

VERSION 1.3 - 26. SEPTEMBER 2014

Zusammenfassung: In diesem Projekt werden österreichische gv.at Domänen auf sicherheitsrelevante Aspekte im Zusammenhang mit HTTPS (SSL/TLS) untersucht: (1) Verfügbarkeit von HTTPS, (2) Eigenschaften der verwendeten Schlüssel, (3) angebotene TLS/SSL Versionen und (4) angebotenen Cipher-Suites.
Bei der Analyse wurde festgestellt, dass nur ein geringer Prozentsatz der untersuchten Services HTTPS anbietet. Bei den verfügbaren Services konnten Sicherheitsmängel in Bezug auf verwendete Cipher-Suites und TLS/SSL Versionen festgestellt werden.

Inhaltsverzeichnis

Inhaltsverzeichnis 1
1. Einleitung 2
1.1. Transport Security Layer 2
2. Methodik 3
3. Analyse 3
3.1. Hostnamen Übereinstimmung 3
3.2. Schlüssellängen Verteilung 4
3.3. Gültigkeitszeitraum der Zertifikate 5
3.4. SSL/TLS Versionen 5
3.5. Verwendete Cipher-Suites 6
4. Fazit 7
5. Referenzen 7

1. Einleitung

Bei HTTPS wird das Standard HTTP-Protokoll über eine Secure Socket Layer (SSL)/Transport Security Layer (TLS) [1] Verbindung durchgeführt. SSL/TLS bietet den darauf aufsetzenden Protokollen eine authentifizierte und verschlüsselte Verbindung und stellt die Datenintegrität sicher. Die Authentifizierung kann einseitig (nur serverseitige Authentifizierung) oder beidseitig (server- und clientseitige Authentifizierung) erfolgen. Eine beidseitige Authentifizierung ist im Web-Kontext eher unüblich.
Derzeit sind fünf Versionen von SSL/TLS im Umlauf die – wie in Kapitel 3 gezeigt – noch alle in Verwendung sind. Dadurch ergibt sich, dass einerseits SSL/TLS Protokolle mit bekannten Schwachstellen verwendet werden und andererseits nach wie vor bekanntlich schwache oder gebrochene Cipher-Suites im Einsatz sind.
Im Zuge dieses Projekts wurden bekannte *Domains von österreichischen eGovernment Services* hinsichtlich sicherheitsrelevanten SSL/TLS Aspekten untersucht.

1.1. Transport Security Layer

Dieses Kapitel bietet eine Übersicht über die SSL und TLS Standards in einem Maße wie es für das Verständnis für die Analyse benötigt wird.

TLS besteht aus zwei verschiedenen essentiellen Schichten: dem *Record Protocol,* das die Verbindungssicherheit bereitstellt und dem *Handshake Protocol* das es ermöglicht, dass sich Client und Server authentifizieren, sich auf einen Verschlüsselungsalgorithmus einigen und ein Sitzungsschlüssel etabliert wird. Die dazu verwendeten Algorithmen und Verfahren werden in einer Cipher-Suite repräsentiert. Die zur Verfügung stehenden Cipher-Suites können in folgende Kategorien gegliedert werden:

- ***Einteilung nach Stärke der Verschlüsselung:***
  - ***Ohne Verschlüsselung:***
    (z.B.: RSA_WITH_NULL_MD5, RSA_WITH_NULL_SHA*):* Cipher-Suites dieser Klasse bieten eine Authentifizierung der Gegenstelle und Integritätssicherheit. Die Daten werden jedoch unverschlüsselt übertragen. Generell kann festgehalten werden, dass Cipher-Suites aus dieser Gruppe niemals im Echtbetrieb verwendet werden dürfen.
  - ***Schwache Verschlüsselung:***
    (z.B.: RSA_WITH_RC4_128_MD5, RC2_128_CBC_WITH_MD5): Die unter Verwendung dieser Cipher-Suites übertragenen Daten sind gefährdet, da die verwendeten Algorithmen bereits gebrochen wurden oder kein adäquates Sicherheitsniveau für den Schutz von Daten bieten. Auch zu beachten ist, dass ein entsprechender Modus des symmetrischen Algorithmus gewählt wird (z.B. CBC, GCM bei AES).
  - ***Starke Verschlüsselung:***
    (z.B.: RSA_WITH_AES_256_CBC_SHA256,
    TLS_RSA_WITH_AES_256_GCM_SHA384): Sofern der symmetrische Schlüssel unter Verwendung eines sicheren Schlüsselaustauschverfahrens eingerichtet wurde, können Übertragungen unter Verwendung von starker Verschlüsselung als sicher angesehen werden. Es sollten nur Verbindungen mit starker Verschlüsselung verwendet werden.
- ***Einteilung nach Schlüsselaustauschverfahren:***
  - ***Statischer RSA Schlüsselaustausch:***
    (z.B.: *RSA_WITH_AES_128_CBC_SHA256, RSA_WITH_RC4_128_SHA*): Bei Cipher-Suites dieser Klasse basiert der symmetrische Schlüssel auf einem einseitig vom Client zufällig generierten und mit dem öffentlichen Schlüssel des Servers verschlüsselten Wert (in diesem Fall wird für diesen asymmetrischen Teil der Verschlüsselung das RSA-Verfahren benutzt).
  - ***Diffie-Hellman Schlüsselaustausch:***
    (z.B.: *DH_RSA_WITH_AES_128_CBC_SHA*): Hierbei wird ein Diffie-Hellman

Schlüsselaustausch durchgeführt. Äquivalente Cipher-Suites gibt es auch für Schlüssel die auf elliptischen Kurven basieren.

- ***Ephemeral Diffie-Hellman Schlüsselaustausch***
  *(z.B.: DHE_RSA_WITH_AES_256_CBC_SHA256**):*** Hierbei handelt es sich um die einzige Klasse von Cipher-Suites die die Eigenschaft der *Perfect Forward Secrecy (PFS)* besitzt. PFS sagt aus, dass es unter der Annahme dass der Serverschlüssel veröffentlich wird, nicht möglich ist alle bisherigen (evt. aufgezeichneten) Daten zu entschlüsseln. Dies wird dadurch erreicht, dass für jeden Schlüsselaustausch ein neues temporäres (ephemeral, flüchtig) Schlüsselpaar erzeugt wird, das exklusiv für einen Austausch verwendet und danach verworfen wird. Äquivalente Cipher-Suites gibt es auch für Schlüssel die auf elliptischen Kurven basieren.

2. Methodik

Die Analyse startet ausgehend von einer Liste von *1285* Domains zu denen jeweils eine HTTPS Verbindung aufgebaut wurde und folgende Informationen gesammelt wurden:

- Unterstützte SSL/TLS Versionen
- Unterstützte Cipher-Suites
- Angebotenes Zertifikat

Nach ersten Analysen hat sich gezeigt, dass diese Daten noch nicht ausreichend sind, da eine Vielzahl der Domains zwar per HTTPS erreichbar schienen, der dort angebotene Inhalt aber auf (a) Standardseiten des Providers, (b) Fehlerseiten oder (c) auf andere Seiten auf dem offensichtlich selben Server verwiesen hat. Das Verhalten von Punkt (c) bedarf einer Erläuterung: HTTP unterstützt seit Version 1.1 [3] mehrere virtuelle Hosts auf derselben IP-Adresse. Dazu wird der *Host-Header* in der HTTP-Anfrage verwendet. Da die TLS Verbindung vor dem Absetzen der HTTP-Anfrage aufgebaut wird, hat der Server keine Informationen darüber zu welchem Hostnamen eine Verbindung aufgebaut wurde. Um diesem Problem entgegenzuwirken, wurde eine TLS-Erweiterung definiert, die noch vor Aufbau der TLS Verbindung den entsprechenden Hostnamen entgegennimmt [2], aber offensichtlich von einigen Installationen nach wie vor nicht unterstützt wird.
Um nun zuverlässige Statistiken über tatsächlich per HTTPS angebotenen Seiten zu erhalten, wurden die Inhalte die per HTTP und die Inhalte die per HTTPS von derselben URL empfangen wurden unter Verwendung eines Ähnlichkeitsalgorithmus verglichen.[1]

3. Analyse

Es wurden Daten von insgesamt *1285* österreichischen eGovernment Services gesammelt, von denen *763* keine HTTPS-Konnektivität anbieten.
Die gesammelten Daten werden in den folgenden Abschnitten ausgewertet.

3.1. Hostnamen Übereinstimmung

Damit der Browser und in weiterer Folge der Benutzer die Vertrauenswürdigkeit der Gegenstelle bewerten kann, wird eine eindeutige Zuordnung von Server-Zertifikat auf die Webseite benötigt. Dafür werden im ausgestellten Zertifikat als *Common-Name (CN)* der entsprechende Hostname oder ein Wildcard in der Form *„*.domain“* angegeben.
In diesem Abschnitt wird die Gültigkeit dieser Zuordnung der einzelnen Server untersucht. Abbildung 1 zeigt die Ergebnisverteilung aller *522* eGovernment Services, die eine HTTPS Schnittstelle anbieten:

- *match-wildcard:* Im Zertifikat ist ein Wildcard Hostname angegeben der mit dem Host übereinstimmt.
- *match-exact:* Der im Zertifikat angegebene CN stimmt mit dem Hostname überein.
- *mismatch:* Der im Zertifikat angegebene CN stimmt nicht mit dem Hostnamen überein. Das Resultat daraus ist, dass der Browser den Benutzer eindringlich warnt diese Seite

[1] Diese Methodik der Gleichheitsprüfung kann auch dazu führen, dass Seiten die im Browser gleich angezeigt werden falsch klassifiziert werden wenn beispielsweise Javascript basierte Weiterleitungen verwendet werden. Außerdem wird nur die gelieferte Einstiegsseite überprüft und keine tiefere Analyse durchgeführt.

zu besuchen da es sich um einen Betrugsversuch handeln könnte. Es wird vom Browser eine Bestätigung vom Benutzer zum Fortfahren eingefordert.

- *catch-all-https:* Die oberen drei Werte beinhalten außerdem eine Überprüfung ob eine Übereinstimmung der über HTTP und HTTPS angeboten Seiten gegeben ist. Ist dies nicht der Fall so kann generell unterschieden werden zwischen (a) einer vom Hosting-Provider bereitgestellten Standardseite, die dem Benutzer mitteilt dass diese Seite nicht über HTTPS erreichbar ist oder (b) einer Weiterleitung auf eine andere (mit der ursprünglichen Domain nicht unbedingt direkt verwandten) Seite oder (c) Fehlerseiten. In keinem der Fälle ist eine Benutzung des Services möglich wie es über HTTP angedacht ist.

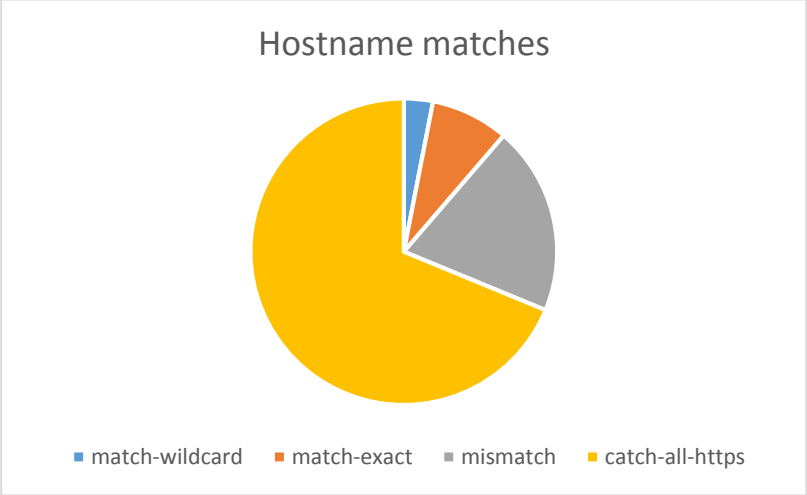

Abbildung 1 – Übereinstimmungen – Name des Hosts

Das Ergebnis der Auswertung zeigt dass eine Mehrheit der untersuchten Webseiten keine gültige HTTPS Anbindung aufweist. Insgesamt bieten somit von *1285* untersuchten eGovernment Services nur *59* oder **4,6%** (bzw. **19,2%** bezogen auf 522 Services) ein gültiges und verifizierbares HTTPS Interface an.

Alle weiteren Analysen beziehen sich nur noch auf die übrig gebliebenen 163 (*match-wildcard*, *match-exact*, *mismatch*) Services.

3.2. Schlüssellängen Verteilung

Die Schlüssellängen Verteilung in Abbildung 2 zeigt die Längen (in Bit) für den asymmetrischen Server-Schlüssel. Die Verwendung von Schlüsseln mit Schlüssellängen von 1024 Bit oder kleiner sollte dringend überdacht werden.

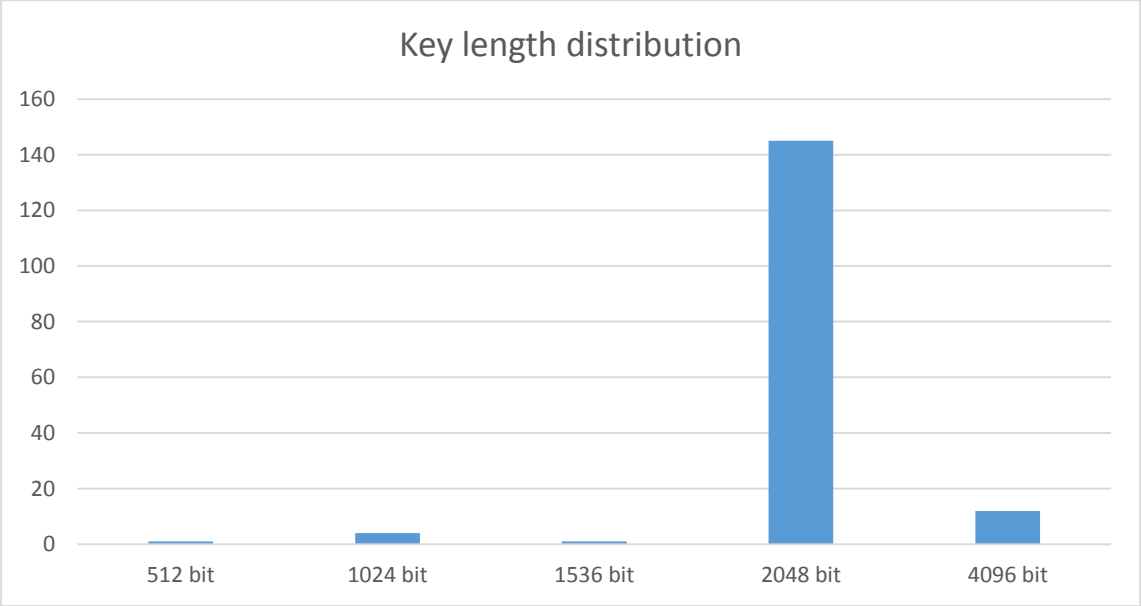

Abbildung 2 – Verteilung der Schlüssellängen

3.3. Gültigkeitszeitraum der Zertifikate

In dieser Analyse wurde nur das Gültigkeitsdatum der Zertifikate analysiert (ohne eine vollständige Zertifikatsprüfung inklusive Widerrufsprüfung durchzuführen). Es ist ersichtlich dass **12,5%** der Zertifikate bereits abgelaufen sind und nicht mehr gültig sind.

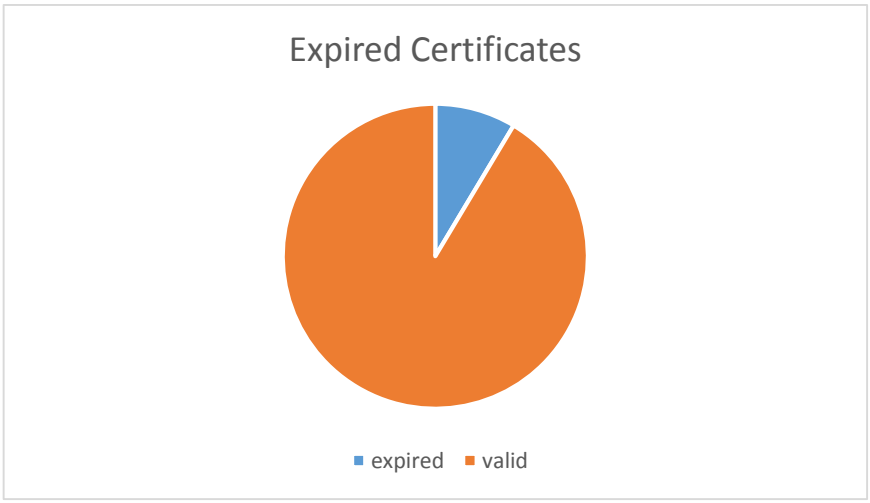

Abbildung 3 - Zertifikate in und außerhalb des Gültigkeitszeitraums

3.4. SSL/TLS Versionen

Abbildung 4 zeigt die unterstützen SSL und TLS Versionen pro Server. SSLv2 und SSLv3 weisen signifikante Sicherheitsprobleme auf und sollten nicht mehr verwendet werden. Auch wenn viele Server TLSv1.1 und TLSv1.2 unterstützen, werden oft trotzdem SSLv2 und SSLv3 unterstützt. Da in diesem Fall von einem potentiellen Angreifer ein Fallback auf die alten Versionen erzwungen werden kann, ist die Sicherheit der Services beeinträchtigt.

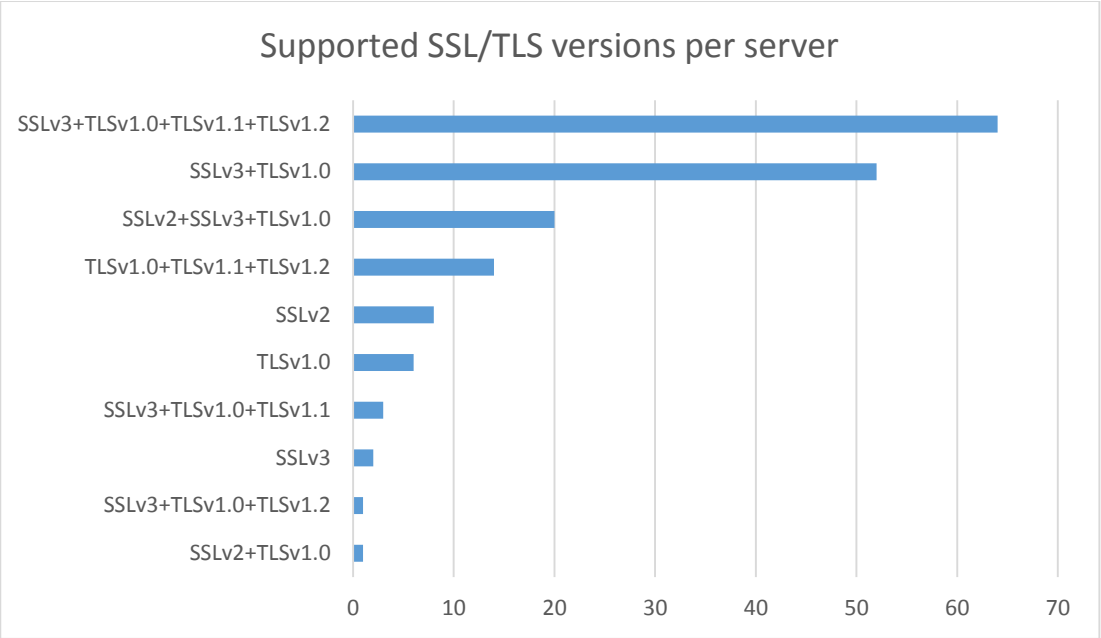

Abbildung 4 - SSL/TLS Versionsverteilung

3.5. Verwendete Cipher-Suites

Die Sicherheit und Vertrauenswürdigkeit einer HTTPS Verbindung ist maßgeblich von der verwendeten Cipher-Suite abhängig. Wie bereits in Kapitel 1.1 erläutert sollten Cipher-Suites ohne Verschlüsselung oder mit schwacher Verschlüsselung nicht verwendet werden. Abbildung 5 zeigt die unterstützten Cipher-Suites über alle Hosts hinweg. Auch *RSA_WITH_NULL_MD5* – also eine Cipher-Suite ohne Verschlüsselung – ist in der Auflistung im unteren Drittel vertreten.
Außerdem ist auffällig, dass einige Server anonyme Cipher-Suites unterstützen (z.B.: *DH_anon_WITH_AES_128_CBC_SHA*), bei denen zwar unter anderem ein Diffie-Hellman Key-Agreement durchgeführt wird, aber ohne Authentifizierung der Gegenstelle. In diesem Fall können sehr einfach Man-in-the-Middle Attacken durchgeführt werden.

Eine empfohlene, aber erst mit TLS1.2 eingeführte Cipher-Suite (*DHE_RSA_WITH_AES_128_GCM_SHA256*) – basierend auf ephemeral Diffie-Hellman mit AES im Gallois/Counter Mode – ist ebenfalls im Mittelfeld vertreten. Mittlerweile unterstützen alle aktuellen Browserversionen TLS1.2. Das Anbieten von dieser oder ähnlichen aktuellen Cipher-Suites muss daher als Basisvoraussetzung für einen aktuellen Web Server gesehen werden. In Zukunft sollte darauf geachtet werden, dass die Unterstützung für nicht unbedingt benötigte Versionen (SSLv2, SSLv3, TLS1.0) deaktiviert, sowie die Unterstützung für unsichere Cipher-Suites entfernt wird.

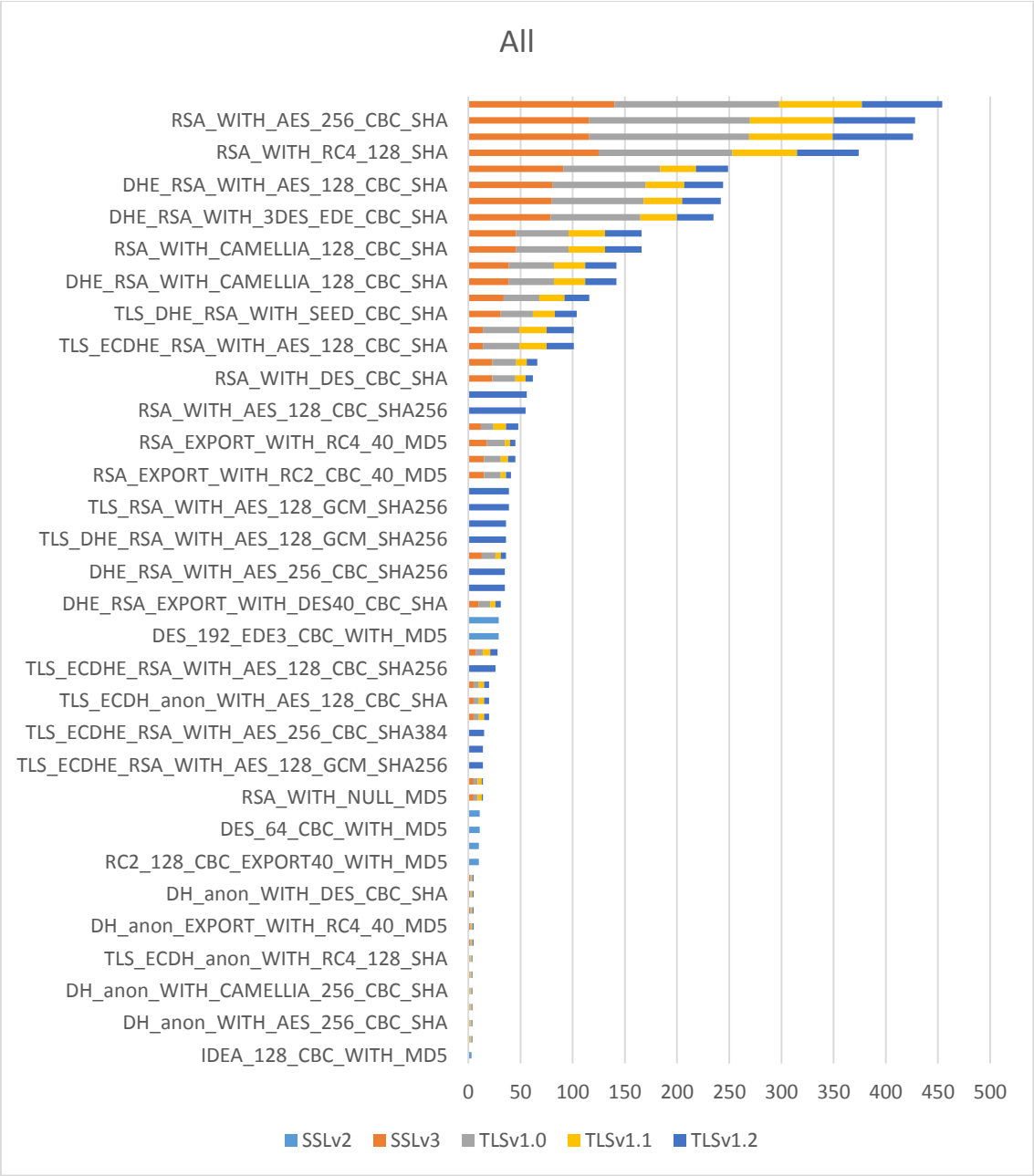

Abbildung 5 - Unterstützte Cipher Suites pro Server

4. Fazit

Die durchgeführte Kurzanalyse der österreichischen gv.at Domänen zeigt, dass (1) HTTPS von einem geringen Teil der verfügbaren Domänen angeboten wird (von 163/1285 Services) und (2) in vielen Fällen gravierende Sicherheitsmängel bei der Konfiguration des HTTPS-Servers bestehen. Diese Sicherheitsmängel beziehen sich vor allem auf die Verwendung von nicht sicheren Cipher-Suites und alten TLS/SSL Versionen. Bis auf einzelne Ausreißer werden von den über HTTPS verfügbaren Services Zertifikate mit akzeptablen und im Allgemeinen sicher geltenden Schlüssellängen verwendet.

5. Referenzen

[1] Rescorla, E., RTFM, I., Modadugu, N., & Google, I. (2012). RFC 6347 - Datagram Transport Layer Security Version 1.2.

[2] Eastlake 3rd, D. & Huaway (2011). RFC 6066 – Transport Layer Security (TLC) Extensions: Extension Definitions

[3] Fielding, R., UC Irvine, Gettys J., Compaq/W3C, Mogul, J., Compaq, Frystyk, H., W3C/MIT, Masinter, L., Xerox, Keach, P., Microsoft, Berners-Lee, T., (1999). RFC 2616 – Hypertext Transfer Protocol – HTTP/1.1