TLS/SSL: eine Frage der Implementierung

Sicherheit zwischen Klick und Webseite

Die Kommunikation im Internet ist grundsätzlich offen, die Wahrscheinlichkeit eines Angriffs daher permanent sehr hoch. Die Nutzung einer verschlüsselten und integritätsgesicherten Kommunikation zwischen Client und Server ist daher von besonderer Bedeutung. Der vorherrschende Ansatz für die Transportverschlüsselung im Web ist die Verwendung von TLS (Transport Layer Security)/SSL (Secure Socket Layer) – TLS/SSL. TLS/SSL ist ein anwendungsunabhängiges Cybersicherheitsprotokoll, das logisch auf einem Transportprotokoll aufsetzt. Dieser Beitrag untersucht die TLS/SSL-Konfiguration populärer Webseiten in Deutschland: Wie gut ist die Kommunikation mit Webseiten durch TLS/SSL gesichert? Setzen die Webserver nur sichere Cipher Suites (Verschlüsselungsmethoden) und Protokollversionen ein? Das für die Tests genutzte Tool und Ergebnisse aus drei damit durchgeführten Testreihen werden im Verlauf des Beitrags näher vorgestellt.

TLS/SSL ist weit verbreitet und wird täglich von Milliarden Internet-Nutzern verwendet: Der Anteil der TLS/SSL-Verbindungen hat sich seit Anfang 2016 von etwa 25 Prozent auf heute rund 75 Prozent der gesamten Verbindungen im Internet erhöht.

TLS/SSL bietet eine Reihe von Cybersicherheitsfunktionen:

- Authentifikation von Server und Client unter Verwendung von asymmetrischen Verschlüsselungsverfahren und elektronischen Zertifikaten.
- Vertrauliche Client-to-Server-Datenübertragung mithilfe symmetrischer Verschlüsselungsverfahren unter der Nutzung eines gemeinsamen Sitzungsschlüssels.
- Sicherstellung der Integrität der transportierten Daten unter Verwendung des HMAC-Verfahrens (Hash-based Message

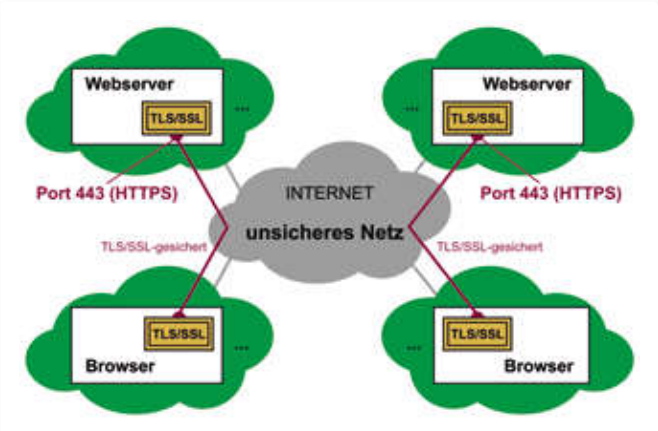

Bild 1: Sichere und vertrauenswürdige Kommunikation durch TLS/SSL.

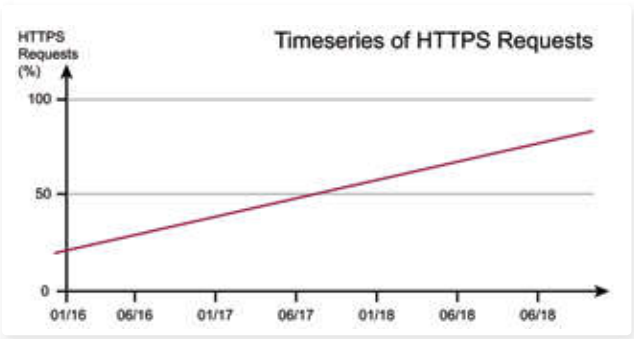

Bild 2: Entwicklung des Anteils der TLS/SSL-Verbindungen. (Quelle: httparchive.org)

Authentication Code, ein Hash-Verfahren, bei dem durch das Einbeziehen des privaten Schlüssels gleichzeitig Integrität und Authentizität gewährleistet werden können).
- In bestimmten Versionen bietet TLS/SSL auch die Komprimierung der Daten an.

Beschreibung des TLS-SSL-Testtools

Das unter https://tls-ssl-test.internet-sicherheit.de/ (in der aktuellen Phase unter Umständen noch: http://tls-ssl-test.internet-sicherheit.de/preview/) verfügbare Werkzeug dient der Überprüfung der TLS/SSL-Konfiguration von Webseiten. Der Nutzer kann eine beliebige Webseiten-Adresse (Domain) in das TLS-SSL-Testtool eingeben und den Test starten. Daraufhin zeigt das TLS-SSL-Testtool die Konfiguration der getesteten Webseite an. Als zusätzliches Feature wird die ermittelte Konfiguration bewertet.

Darüber hinaus sind unter der oben genannten Adresse auch bereits ermittelte Bewertungen von drei Anbieterkategorien bereitgestellt. Eine Kategorie ist die Top 50 der in Deutschland aufgerufenen Webseiten, die zweite Kategorie bilden die Top 30 der kleinen und mittelständischen Unternehmen sowie die dritte Kategorie die Top 20 der Hochschulen.

Prinzipielle Darstellung des Testablaufs

Beim Aufrufen einer Webseite wird grundsätzlich eine Verbindung zwischen dem IT-System des Nutzers (Client) und dem Webserver hergestellt. Beim Herstellen einer mit TLS/SSL gesicherten Verbindung werden dabei zu Beginn zunächst die zu verwendenden Parameter ausgehandelt, wie Cipher Suites und Protokollversion. Diese erste sogenannte Handshake-Phase ist entscheidend für die IT-Sicherheit der darauffolgenden Verbindung.

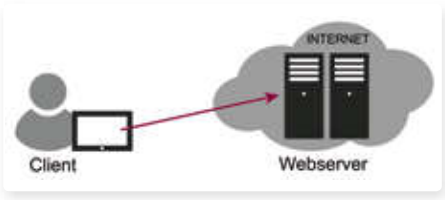

Bild 3: Anfrage des Clients an den Webserver beim Aufruf einer Webseite

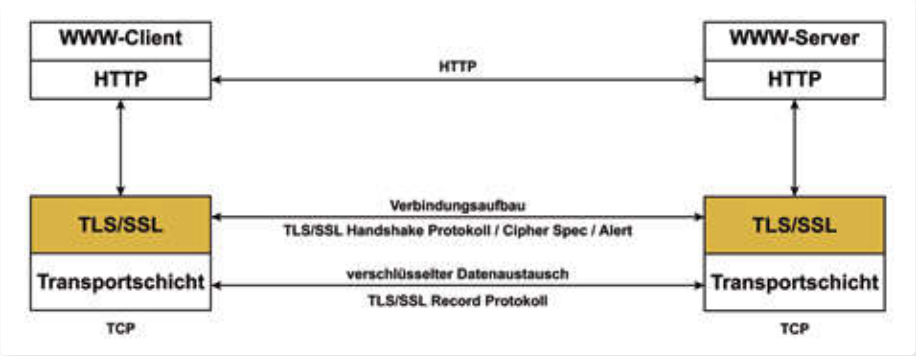

Bild 4: Schematische Darstellung zur Einordnung von TLS/SSL innerhalb des Schichtenmodells.

In der Handshake-Phase beginnt in der Regel der Client mit der ersten Nachricht „ClientHello". Im Inhalt der Nachricht sind Listen mit möglichen Cipher Suites enthalten, die vom Client (Browser) aus zur Verfügung stehen.[1] Der Server wählt dann aus, welche Cipher Suite tatsächlich verwendet wird. Im Idealfall wählt der Server die sicherste Variante aus. Darüber hinaus hat er auch die Möglichkeit, die Verbindung abzulehnen, wenn er keine Cipher Suite aus der vorgeschlagenen Liste akzeptiert.

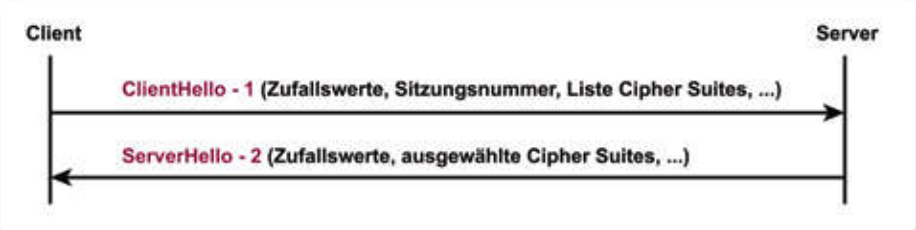

Bild 5: Verbindungsaufbau der TLS/SSL-Verbindung

Im vorgestellten Test wird der Client dabei durch das Testtool simuliert: Es werden sehr viele unterschiedliche Verbindungen aufgebaut. Dabei verwendet das Testtool jeweils unterschiedliche Parameter (TLS/SSL-Version, Cipher Suites), in einer „ClientHello"-Nachricht. So wird beispielsweise simuliert, dass vom Client nur die alte Version SSL 2.0 unterstützt wird, um herauszufinden, ob der Server diese Protokollversion akzeptiert. Das Testtool simuliert also einen Client, der bei unterschiedlichen Verbindungen verschiedene Cipher Suites nicht unterstützt.

Der Server antwortet daraufhin mit der „ServerHello"-Nachricht. Diese wird vom Testtool überprüft: Der Server kann die Verbindung annehmen oder ablehnen. Für die Sicherheit entscheidend ist in diesem Fall, inwieweit der Server noch alte und unsichere Protokollversionen und Cipher Suites akzeptiert. Ist er beispielsweise bereit, eine TLS/SSL-Verbindung der Protokollversion SSL 2.0 aufzubauen, zeigt dies gravierende Sicherheitsmängel. Der Test beantwortet also die Frage: Welches sind die unsichersten Parameter, die der Webserver noch bereit ist auszuwählen?

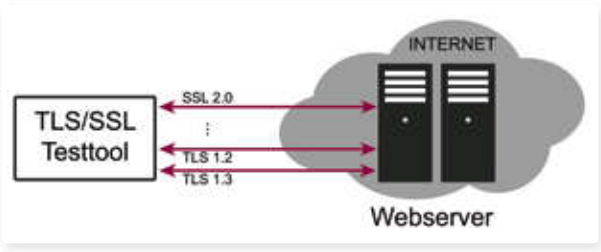

Bild 6: Das Testtool sendet viele Anfragen mit unterschiedlichen Parametern an den Webserver.

Nach dem erfolgreichen Abschließen der Handshake-Phase beginnt die zweite Phase, in der die zu übertragenden Daten (Payload) übermittelt werden. In dieser Phase werden also die Parameter verwendet, die zuvor ausgehandelt wurden. Die Daten werden in Serien von Datenfragmenten aufgeteilt und je unabhängig voneinander verschlüsselt. Da sich hier jedoch keine weiteren Änderungen der kryptografischen Parameter mehr ergeben, wird diese Phase hier nicht weiter beachtet.

Architektur des TLS-SSL-Testtools

Das genannte TLS-SSL-Testtool wurde mit dem Python-Framework Django entwickelt. Dies vereinfacht den Aufwand zur Erstellung von Webanwendungen, da viele häufig verwendete Funktionen bereits implementiert sind. So lassen sich beispielsweise Uniform Resource Locators (URLs) innerhalb des Projekts recht einfach im Python-Code konfigurieren.

Für den tatsächlichen Test der TLS/SSL-Server-Konfiguration ist das OpenSource-Tool sslyze (verfügbar unter https://github.com/nabla-c0d3/sslyze/) in das TLS-SSL-Testtool eingebettet. sslyze ist ebenfalls in Python geschrieben und wird als Bibliothek (library) zur Verfügung gestellt, die im vergangenen Jahr regelmäßig gepflegt wurde.

Auswahl der Testbereiche

Das TLS-SSL-Testtool bewertet die TLS/SSL-Konfigurationen anhand von vier Testbereichen. Es handelt sich um die Bereiche „Zertifikat und Schlüssel", „TLS/SSL-Protokollversionen", „HTTP-Header" und „weitere Kriterien". Nachfolgend werden die Testkriterien kurz vorgestellt.

Zertifikat und Schlüssel

Fundamentale Säule der Sicherheit auf Seiten des Servers ist die Nutzung eines starken Schlüsselpaares und ein vertrauenswürdiges Zertifikat. Zunächst wird deshalb in Bezug auf das Zertifikat überprüft, ob die in die Adresszeile eingegebene Domäne mit der im Zertifikat eingetragenen Domäne übereinstimmt. Dies ist sehr wichtig, da dies das Fundament allen weiteren Vertrauens auf TLS-SSL-Ebene ist.

In jeder Instanz, die eine TLS-Verbindung aufbaut, ist ein Trust Store (Zertifikatsspeicher) mit sogenannten Wurzelzertifikaten (root certificates) enthalten. Bei diesen Instanzen handelt es sich üblicherweise um Webbrowser wie Mozilla Firefox. Die Zertifikatsspeicher stellen die Ausgangsbasis für das Vertrauen in die Zertifikate der Webserver beziehungsweise der Domains dar. Der Webbrowser muss in der Lage sein, eine chain of trust (Vertrauenskette) vom beinhalteten Wurzelzertifikat bis zum Zertifikat des besuchten Webservers aufzubauen. Mit dem Zertifikat des Webservers werden in der Regel alle weiteren Zertifikate zur Verfügung gestellt, die benötigt werden, um die Vertrauenskette aufzubauen. Beim Test wird deshalb überprüft, ob in der bereitgestellten Vertrauenskette auch das Wurzelzertifikat enthalten ist.

Besonders ausführlich und umfangreich ist die Prüfung des Antragstellers bei Zertifikaten vom Typ Extended-Validated. Hierbei muss der Antragsteller Nachweise erbringen, dass er berechtigt ist, das Zertifikat für eine bestimmte Domäne zu beantragen, dass er physisch existiert und eine tatsächlich funktionierende Organisation unterhält. Darüber hinaus werden je nach Rechtsform des Antragstellers weitere Nachweise angefordert, beispielsweise ein entsprechender Handelsregisterauszug. Die Überprüfung dient dem Zweck der Sicherstellung der Identität des Zertifikatsinhabers, also, ob der Betreiber einer Webseite die im Zertifikat genannte Domain verwenden darf. Wir können also sicher sein, dass die Domain teletrust.de tatsächlich dem Bundesverband der IT-Sicherheit – TeleTrusT – gehört, weil dieser Zusammenhang von der D-Trust als ausgebender Stelle intensiv geprüft worden ist.

In Bezug auf das Zertifikat wird außerdem überprüft, ob das Endgerät, zum Beispiel ein Smartphone mit Android-Betriebssystem oder ein iPhone mit iOS, beziehungsweise ob die Software, zum Beispiel Mozilla Firefox oder Google Chrome, den Zertifikaten vertraut. Dazu wird eine Chain of Trust vom Zertifikat der Webseiten-Adresse bis hin zu den entsprechenden Trust Stores aufgebaut, der in der Software enthalten ist. Es wird somit also die Frage beantwortet: Sehe ich die Behauptung der Identität als wahr an? Im Beispiel bedeutet das: Gehe ich – das heißt, der verwendete Webbrowser – davon aus, dass sich hinter der Adresse https://www.teletrust.de/ der Kommunikationspartner Bundesverband der IT-Sicherheit verbirgt?

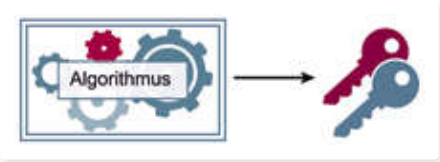

Bild 7: Schematische Darstellung eines Schlüsselpaares des Servers.

Alle mit dem vorgestellten TLS-SSL-Testtool getesteten Webseiten verwenden einen der beiden etablierten Algorithmen, wie das RSA-Verfahren oder die Elliptische-Kurven-Kryptografie (Elliptic Curve Cryptography – ECC). Der geheime Schlüssel (Private Key) stellt den Generalschlüssel des Servers dar und hat einen hohen Schutzbedarf. Dieser stellt die Ausgangsbasis für die Generierung von temporären Schlüsseln dar. Solch ein temporärer Schlüssel wird beim Aufbau einer TLS/SSL-Verbindung erzeugt und nur für diese eine Verbindung verwendet.

Vorwärtsgeheimhaltung (Forward Secrecy) bedeutet in diesem Zusammenhang, dass das temporär genutzte kryptografische Material nicht nachträglich ermittelt werden kann, selbst bei Bekanntwerden des geheimen Schlüssels des Servers. Die Sicherheit der TLS/SSL-Verbindung beruht jedoch nicht nur auf dem genutzten kryptografischen Algorithmus, sondern auch auf der Länge der Schlüssel. Die Länge der Schlüssel wird in Anzahl von Bits angegeben. Je länger diese Schlüssel sind, desto besser ist die Kommunikationsverbindung geschützt.

Protokollversion

Bei diesem Testkriterium, der TLS/SSL-Protokollversion, wird überprüft, welche Versionen des Protokolls vom getesteten Server unterstützt werden. Die Protokollversion ist ein entscheidender Faktor, weil bestimmte Versionen nicht mehr den aktuellen Sicherheitsanforderungen entsprechen.

Derzeit existieren von TLS/SSL insgesamt sechs Protokollversionen. Die erste öffentliche Version von TLS/SSL stammt aus dem November 1994. Sie hieß SSL 2.0 und war Bestandteil von Netscape. Die darauffolgende Version SSL 3.0 kam im März 1995. Ab dann gingen Weiterentwicklung und Veröffentlichung des Protokolls in die Hände der Internet Engineering Task Force (IETF) über. Von dort folgten im Januar 1999 TLS 1.0, im April 2006 TLS 1.1 und im August 2008 wurde schließlich TLS 1.2 veröffentlicht. Zwischen der neuesten Protokollversion TLS 1.3 und der Veröffentlichung der direkten Vorgängerversion liegen zehn Jahre. Nur die im August 2018 veröffentlichte Version TLS 1.3 wird den enorm gestiegenen Sicherheitsanforderungen gerecht. Der Unterschied zwischen den Bezeichnungen TLS und SSL bezieht sich also lediglich auf die Version derselben Protokollfamilie.

Die wesentlichen Änderungen zwischen TLS 1.2 und TLS 1.3 sind, dass unsichere Algorithmen, wie RC4 und schwache Export-Verschlüsselungsvarianten, nicht mehr konfiguriert werden können. Darüber hinaus kommt nun ausschließlich die Vorwärtsgeheimhaltung zum Einsatz, welche eine deutliche Verbesserung der Datensicherheit zur Folge hat.

Das Testtool überprüft unabhängig von der Protokollversion, ob veraltete oder unsichere Cipher Suites akzeptiert werden. Beispielhaft sind hier NULL-Verschlüsselung, welche faktisch keine Verschlüsselung anbietet, oder die unsichere RC4-Verschlüsselung zu nennen.

HTTP-Header

Das TLS-SSL-Testtool untersucht im dritten Testbereich den HTTP-Header. Der HTTP-Header beinhaltet Informationen, die jedem einzelnen Datenpaket als Meta-Informationen mitgeschickt werden. Diese beinhalten „HTTP Strict Transport Security", „HTTP Public Key Pinning" und „HPKP-Backup-Pin".

1. HTTP Strict Transport Security: Es wird getestet, ob HTTP Strict Transport Security (HSTS) bei der entsprechenden Webseite konfiguriert ist. Wenn dies der Fall ist, können Inhalte der gesamten Seite ausschließlich über gesicherte Verbindungen geladen werden.

2. HTTP Public Key Pinning: Mit HTTP Public Key Pinning (HPKP) wird der Client, also beispielsweise der Webbrowser, informiert, dass nur bestimmte Certificate Authorities (CAs) Zertifikate für eine bestimmte Domain ausstellen dürfen. Die Technik hat allerdings Nachteile, insbesondere das virtuelle „Zumauern" der eigenen Seite, wenn die Kontrolle über die Instanz verloren wird.

3. HPKP-Backup-Pin: Die oben beschriebene Gefahr kann mithilfe eines konfigurierten Backup Pins abgemildert werden, sodass auch noch beim Verlust der Kontrolle der Hauptinstanz eine weitere Instanz angegeben werden kann, die im Falle des Verlusts zum Einsatz kommt. Daher wird auch das Vorhandensein eines gültigen Backup Pins überprüft.

Weitere Kriterien

SCSV-Fallback-Mechanismus: Mit aktiviertem TLS Fallback Signaling Cipher Suite Value (SCSV) wird bei einem Cyberangriff verhindert, dass in der Handshake-Phase des Protokolls eine niedrigere Protokollversion als nötig ausgewählt wird.

Angreifbar entsprechend der CSS Injection-Schwachstelle: Das TLS-SSL-Testtool überprüft, ob die Schwachstelle mit der Kennung CVE-2014-0224 geschlossen ist. Diese Schwachstelle führte bei bestimmten Versionen[1] der serverseitigen Software OpenSSL[2] dazu, dass ein Master Key der Länge 0 verwendet und somit der Schutz aufgehoben wird.

Angreifbar gemäß der Heartbleed-Schwachstelle: Ebenfalls prüft das TLS-SSL-Testtool das Vorhandensein der Sicherheitslücke CVE-2014-0160. Diese Sicherheitslücke betrifft wiederum bestimmte Versionen von OpenSSL[3]. Durch das Einschleusen bestimmter Datenpakete ist es hierbei möglich, sensible Daten, wie den privaten Schlüssel des Servers, auszulesen.

Übertragungskompression: Zu Informationszwecken wird überprüft, ob die Übertragungskompression aktiviert ist. Durch das Einschalten der Übertragungskompression wird der CRIME-Angriff unter bestimmten Voraussetzungen möglich, bei dem es möglich ist, den HTTP-Header trotz TLS auszulesen. In TLS Version 1.3 ist die Kompression auf TLS-Ebene daher grundsätzlich nicht mehr möglich.

OCSP: Das Online Certificate Status Protocol (OCSP) ermöglicht es, bei Anwendungen den Zustand eines Zertifikats abzufragen. Dadurch kann ein Zertifikat beispielsweise auch vor Ablauf des vorgesehenen Ablaufdatums widerrufen werden. Das TLS-SSL-Testtool überprüft, ob OCSP konfiguriert ist und bewertet die OCSP-Antwort, zum Beispiel, dass einem Zertifikat weiterhin vertraut werden kann.

Erläuterung der Bewertung

Das Ergebnis der genannten Testkriterien wird auf einer Skala von „0" bis „10" bewertet. Eine „10", stellt das beste und „0" das schlechteste Ergebnis dar. Ist die Bewertung in einem der vier Teilbereiche sehr niedrig, wirkt sich dies überproportional auf das Gesamtergebnis aus. Denn wenn nur ein Teilbereich der getesteten Verbindung angreifbar ist, dann ist die gesamte Verbindung unsicher.

Bewertung Zertifikat

Die Bewertung des Zertifikats wird auf die schlechteste Bewertung „0" abgewertet, wenn das Zertifikat nicht für die entsprechende Domain ausgestellt wurde, da dies eine grundlegende Voraussetzung für das Vertrauen ist. Mit einem Hash-Wert kann leicht überprüft werden, ob ein Zertifikat nach der Ausstellung modifiziert wurde. Wird dazu jedoch der unsichere SHA1-Algorithmus verwendet, wird das Ergebnis auf „2" herabgestuft.

Ist in der mitgelieferten Zertifikatskette das Wurzelzertifikat nicht enthalten, wird die Bewertung auf „8" heruntergestuft. Die Wahrscheinlichkeit ist dann etwas geringer, dass die Vertrauenskette erfolgreich aufgebaut werden kann.

Die Bewertung wird auf eine „9" herabgestuft, wenn kein Extended-Validated-Zertifikat zum Einsatz kommt.

Bewertung TLS/SSL-Protokollversion

SSL 2.0 ist unsicher und darf nicht mehr verwendet werden. Deshalb wird für das Akzeptieren dieser Protokollversion die Bewertung „1" ausgestellt. Auch SSL 3.0 darf nicht mehr eingesetzt werden, da es hierfür wirksame Angriffe gibt. Aktiviertes SSL 3.0 wird mit einer „2" bewertet.

TLS Versionen 1.0 und 1.1 sind ebenfalls veraltet und sollten nicht mehr angeboten werden. Bei der Bewertung wird für aktiviertes TLS 1.0 daher eine „7" vergeben. Das PCI Council[4] hat entschieden, dass TLS 1.0 ab dem 30. Juni 2016 nicht mehr für Zahlungsdienste verwendet werden darf.

Werden unsichere oder veraltete Cipher Suites vom Server akzeptiert, wird je nach Angreifbarkeit eine geringere Bewertung vergeben. Für eine NULL-Verschlüsselung beispielsweise wird die Bewertung „0" vergeben, da dies faktisch keine Verschlüsselung darstellt, und für angebotene 3DES-Verschlüsselung die Bewertung „5".

Für die TLS Version 1.2 liegt keine schwerwiegende bekannte Schwachstelle vor. Diese Version bietet die aktuellen und sicheren Cipher Suites an. Daher wird im Test eine „3" vergeben, wenn TLS Version 1.2 nicht angeboten wird. Im Fall von aktivierten unsicheren Verschlüsselungsalgorithmen innerhalb der Protokollversion wird die Bewertung ebenfalls abgewertet. Die Verwendung der jüngsten TLS Version 1.3 wird aktuell noch nicht in der Bewertung berücksichtigt. In den Testergebnissen wird das Ergebnis allerdings grün hervorgehoben.

Bewertung HTTP-Header

Ist HTTP Strict Transport Security im Header nicht aktiv, wird die Bewertung auf „5" herabgestuft, da dies eine gewichtige Sicherheitseinbuße darstellt. Für deaktiviertes HTTP Public Key Pinning wird die Bewertung auf „9" herabgestuft.

Bewertung der weiteren Kriterien

Ist der SCSV-Fallback-Mechanismus oder OCSP nicht aktiviert, wird die Bewertung „7" vergeben. Bei der Anfälligkeit auf die CSS-Injection-Schwachstelle wird die davon ausgehende Gefahr mit einer „4" bewertet. Bei der Verwundbarkeit entsprechend der Heartbleed-Schwachstelle wird die Bewertung auf „2" verringert.

Testdurchführung

Das vorgestellte Testtool prüft und bewertet die TLS/SSL-Konfiguration von öffentlich erreichbaren Webservern. Die Ergebnisse der einzelnen Testkriterien wurden daraufhin wie oben beschrieben bewertet. Die Gesamtbewertung ergibt sich aus der niedrigsten Teilbewertung. Der Test zeigt also, welches die unsichersten Parameter sind, die ein Server noch bereit ist zu akzeptieren.

Test 1: Top-50-Domains in Deutschland

Um einen Einblick in die TLS/SSL-Sicherheit der 50 meist verwendeten Webseiten in Deutschland zu bekommen, wurden diese im Rahmen der Erstellung des TLS-SSL-Test-

tools getestet und stehen nun unter https://tls-ssl-test.internet-sicherheit.de/rangliste/de-liste/ zur Verfügung.

Ergebnis Test 1

Die am besten bewerteten Webseiten haben eine Gesamtbewertung von „7" erreicht. Dazu gehören die Domains wikipedia.org, ebay-kleinanzeigen.de, ok.ru und paypal.com. Insgesamt haben sieben von 50 Domains diese Bewertung erreicht. Insbesondere wikipedia.org und yahoo.com sind hierbei positiv hervorzuheben, da OCSP korrekt eingerichtet wurde. Die Schlüsselstärke des Schlüssel-Paares ist häufig 2.048 Bits für den RSA-Algorithmus und 256 Bits für die Elliptische-Kurven-Kryptografie.

Das schlechteste Ergebnis wurde bei den Domains whatsapp.com und yandex.ru mit einer „2" festgestellt, da beide Domains die Protokollversion SSL 3.0 aktiviert haben. Zusätzlich sind für diese Domains unsichere Verschlüsselungsverfahren aktiviert, beispielsweise RC4 bei whatsapp.com.

Extended-Zertifikate wurden lediglich bei zwei Domains festgestellt, dies sind otto.de und postbank.de. Die durchschnittliche Bewertung liegt bei 5,1.

Diskussion der Ergebnisse Test 1

Bei allen getesteten Domains war noch TLS 1.0 aktiviert, was die Sicherheit unnötig gefährdet. Weiterhin ist auffällig, dass die zum Facebook-Konzern gehörenden Domains whatsapp.com und facebook.com jeweils eine unsichere Cipher Suite zulassen. Ein möglicher Grund dafür ist eine Verfügbarkeit für eine breitere Masse, allerdings auf Kosten der IT-Sicherheit und des Datenschutzes!

Die Domain paypal.com erzielte eine relativ gesehen gute Gesamtbewertung, was für Webseiten mit Geld-Transaktionen notwendig ist. Allerdings wird auch dort nach wie vor TLS 1.0 zugelassen.

Einen unhaltbaren Zustand stellt die kaum vorhandene Verwendung von Extended-Zertifikaten dar. Gerade bei Webseiten dieser Reichweite ist es unabdingbar, die IT-Sicherheit und Vertrauenswürdigkeit zu erhöhen, indem dem Nutzer vermittelt wird, dass die vorgegebene Domain tatsächlich zu der entsprechenden Organisation gehört. Es ist geradezu fahrlässig, diesen Sicherheitsgewinn nicht zu nutzen.

Test 2: Top-30-Webseiten von kleinen und mittelständischen Unternehmen in Deutschland[5]

Eine andere mit dem TLS-SSL-Testtool getestete Kategorie ist eine Liste mit 30 kleinen und mittelständischen Unternehmen in Deutschland, die potenziell höhere Anforderungen an die IT-Sicherheit haben, dafür jedoch meist geringere Kapazitäten zur Verfügung stellen.

Ergebnis Test 2

Die beste Bewertung in dieser Kategorie ist eine „7", welche dreimal erreicht wurde. Die schlechteste Bewertung „2" wurde zweimal vergeben, verursacht durch die Verwendung von SSL 3.0 in Verbindung mit der unsicheren Verschlüsselungsmethode RC4. Die zweitschlechteste Bewertung „3" wurde für die Verwendung von RC4 bei aktiviertem TLS 1.0 als älteste Protokollversion vergeben.

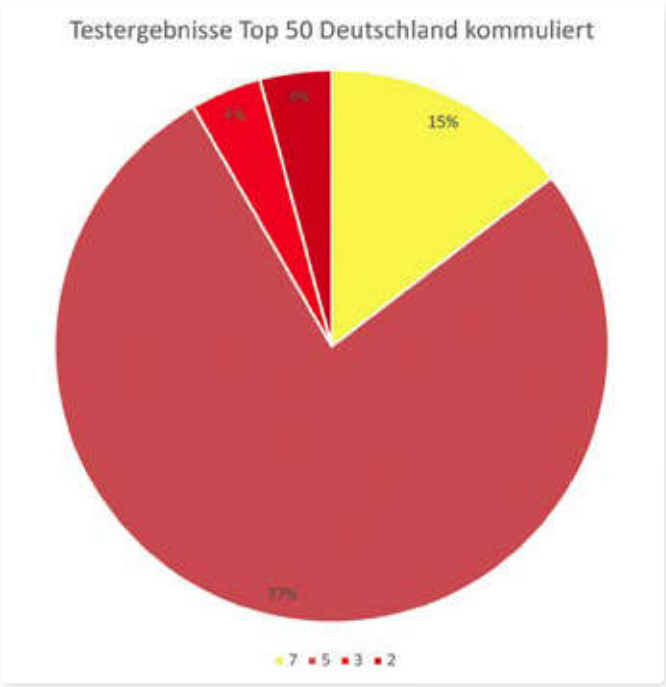

Bild 8: Testergebnisse der Top 50 Domains in Deutschland, nach Gesamtbewertung gruppiert.

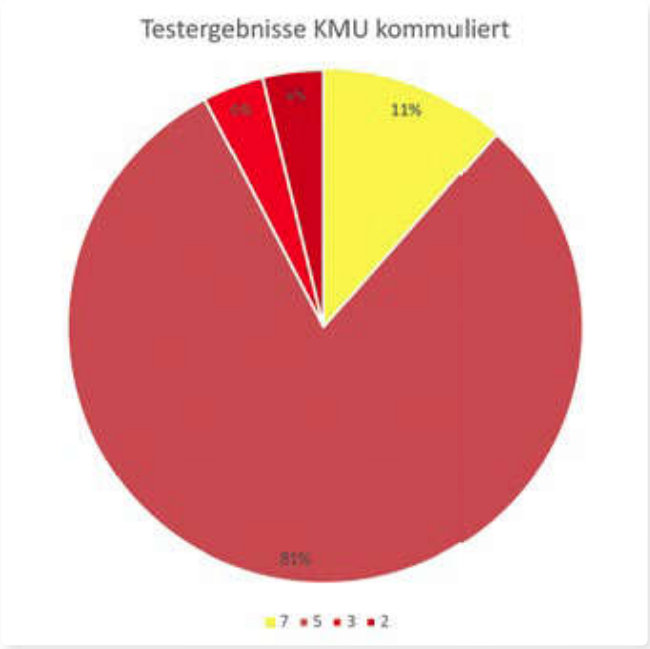

Bild 9: Testergebnisse der KMUs nach Gesamtbewertung.

Ein Extended-Validated-Zertifikat konnte ausschließlich bei der Domain www.rimowa.com festgestellt werden. Im Bereich der Schlüsselstärke wurde nur bei knapp einem Drittel der Domains starke 4.096 Bits für die RSA-Verschlüsselung ermittelt. Die Durchschnittsbewertung bei kleinen und mittelständischen Unternehmen beträgt 4,9.

Diskussion der Ergebnisse Test 2

Insgesamt sind die Bewertungen dieser Kategorie etwas schlechter als bei den Top 50 Webseiten Deutschlands. Hervorzuheben ist hier ebenfalls der mangelnde Einsatz von Extended-Validated-Zertifikaten, welche nur bei einer einzigen getesteten Domain zum Einsatz kommen.

Allerdings weist die überdurchschnittliche Schlüsselstärke der asymmetrischen Verschlüsselung darauf hin, dass bereits ein Bewusstsein für die Sicherheit der Domains besteht. Der Einsatz von SSL 3.0 bei www.mapal.com und www.bitzer.de stellt jedoch ein Sicherheitsrisiko dar, ebenso wie die Verwendung von RC4 bei den beiden genannten Domains sowie www.hansgrohe.de. Ein positives Beispiel bei den Protokollversionen ist www.advaoptical.com, bei der ausschließlich TLS 1.2 aktiviert ist.

Insgesamt ergibt sich ein durchwachsenes Bild. Es gibt einerseits gute Ansätze von Domains wie www.brueckner.com, bei der wesentliche Merkmale einer sicheren Konfiguration umgesetzt wurden. Der überwiegende Teil der Domains ist jedoch nicht sicher genug konfiguriert und teilweise zeugen die Konfigurationen von Nachlässigkeit. Insbesondere bei den genutzten Protokollversionen sowie bei der Verwendung von HSTS wurden schlechte Testergebnisse erzielt.

Test 3: Top 20 Webseiten deutscher Hochschulen[6]

Hier legen wir das Augenmerk auf die Webseiten deutscher Hochschulen, die sich in ihrer Organisation in der Regel erheblich von Unternehmen unterscheiden und bei denen teils auch theoretisches Know-how im Bereich IT-Sicherheit zur Verfügung steht.

Ergebnis Test 3

Drei Domains wurden mit „7" bewertet, welche in dieser Kategorie die höchste vergebene Bewertung ist. Dabei fällt die Domain www.fau.de besonders positiv auf, da für diese als einzige im Test bereits TLS 1.3 angeboten wird. Gut ein Drittel der getesteten Domains weist eine hohe Schlüsselstärke von 4.096 Bits auf.

Die in diesem Testgang schlechteste Bewertung „3" wurde für die Domain www.fernuni-hagen.de vergeben, weil sich die TLS/SSL-Verbindung nur über die Version TLS 1.0 aufbauen lässt und die aktuellen Protokollversionen nicht unterstützt werden. Der Grund für die schlechte Bewertung ist hier, dass TLS 1.2 nicht aktiviert ist. Die Durchschnittsbewertung der getesteten Domains beträgt 4,6.

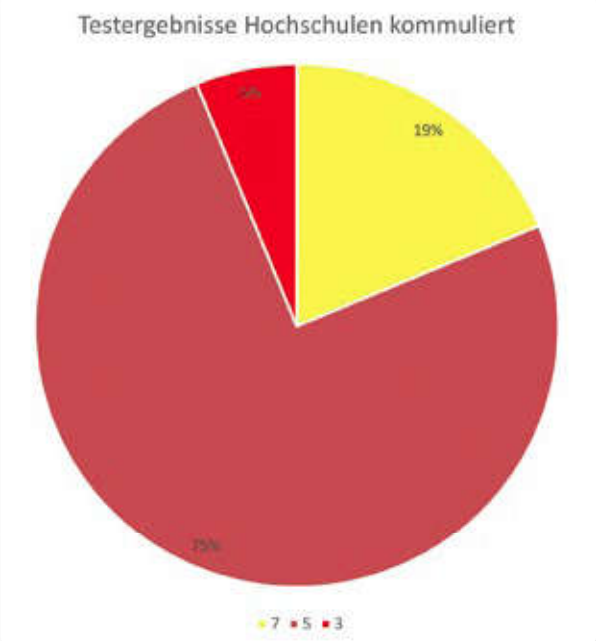

Bild 10: Top 20 Hochschulen nach Gesamtergebnis

Diskussion der Ergebnisse Test 3

Das veraltete TLS 1.0 wird für fast alle Domains angeboten, was ein großes Nachbesserungspotenzial für den Großteil der Domains dieser Gruppe offenlegt. Ebenfalls großes Nachbesserungspotenzial liegt im Bereich OCSP, welches nur für zwei Domains konfiguriert (www.fau.de, www.uni-muenster.de) ist. Dies sorgt im Falle des Missbrauchs des Zertifikats für erhöhte IT-Sicherheit.

Wenige Domains haben die neueste Version TLS 1.3 konfiguriert (nur www.fau.de). Hochschulen verfügen in der Regel über ein hohes Maß an informationstechnischem Know-how, welches auch für die Konfiguration der eigenen IT-Infrastruktur genutzt werden sollte.

Etwas besser zeigt sich die Sicherheitslage bei der Aktivierung von HSTS. Vier der getesteten Domains sind dementsprechend konfiguriert, was insgesamt jedoch trotzdem wenig ist. Ein kleiner Lichtblick: Die Schlüsselstärke ist überdurchschnittlich hoch. Außerdem konnte keine Angreifbarkeit über die getesteten Schwachstellen festgestellt werden.

Einschätzung der gegenwärtigen TLS/SSL-Sicherheitslage

Nach der Durchführung der drei Testläufe lagen die durchschnittlichen Bewertungsergebnisse zwischen 4,9 und 5,1. Ein solches Ergebnis ist aus Sicht der IT-Sicherheit und Vertrauenswürdigkeit nicht akzeptabel. Auffälligkeiten wegen nicht geschlossener Schwachstellen wurden nicht festgestellt. Es ist jedoch grundsätzlich notwendig, dass insbesondere TLS 1.0 deaktiviert wird. Aktuelle Webbrowser unterstützen schon TLS 1.3.

Es ist erkennbar, dass es zwischen den einzelnen Kategorien, wie der Hochschul- und der Deutschland-Liste, keine gravierenden Unterschiede gibt. Daraus lässt sich ab-

leiten, dass die Administratoren ähnliche Konfigurationen als praktikabel und für die Praxis als sicher genug ansehen.

Es ist also dringend notwendig, die veralteten Protokollversionen zu deaktivieren. Aus sicherheitstechnischer Sicht darf nur noch TLS 1.2 mit sicheren Verschlüsselungsalgorithmen sowie TLS 1.3 aktiviert sein. Alle anderen Konfigurationen sind eine unnötige Gefährdung der IT-Sicherheit.

Zertifikate vom Typ „Extended Validated" (EV) kommen quasi kaum zum Einsatz. Hier besteht dringender Handlungsbedarf. Insbesondere Webseiten mit hoher Relevanz können an dieser Stelle den Schutz vor Phishing-Angriffen erhöhen. Ein EV-Zertifikat verursacht zusätzliche Kosten und einen erweiterten Aufwand, jedoch sind dies wichtige Investitionen in die IT-Sicherheit und Vertrauenswürdigkeit der angebotenen Webdienste.

Es ist notwendig, ein Bewusstsein im Bereich TLS/SSL zu schaffen, so dass ein gemeinsamer Konsens der akzeptierten Konfigurationen erzielt wird. Mit einer konkreten, von der Mehrheit akzeptierten Konfiguration von TLS/SSL können Hersteller der einzelnen Komponenten und Betreiber von Webservern durch gezielte Umsetzung reagieren. Die praktische Verantwortung liegt letztlich bei den technischen Ansprechpartnern, die für eine Domain eingetragen sind. Dies ist als Service gegenüber den Nutzern (Kunden) der Webseite zu sehen, mit dem mehr IT-Sicherheit und Vertrauenswürdigkeit geschaffen werden kann.

Es ist eine Tatsache, dass sichere und fachlich-begründbare Konfigurationen von TLS einiges an Hintergrundwissen bedürfen. Es ist jedoch notwendig, in diesem Punkt in die IT-Sicherheit zu investieren. Da Internet und TLS/SSL sich ständig wandeln, kann es keine dauerhaft gültige Konfiguration geben. Ein regelmäßiges Überprüfen und Anpassen ist deshalb notwendig. Insgesamt benötigt das Thema TLS/SSL einen höheren Stellenwert. Einerseits wird Sicherheitsbewusstsein benötigt, andererseits Fachwissen, um dies korrekt anzuwenden. Daher ist es notwendig, einen Konsens von Anbietern und Herstellern herbeizuführen, der dann mit fachlich präzisen und eindeutigen Anweisungen von allen umgesetzt werden kann.

Ausblick

Da die TLS/SSL-Technologie einen sehr hohen praktischen Stellenwert bezüglich der IT-Sicherheit und Vertrauenswürdigkeit im Internet hat, ist ein grundsätzliches Umdenken notwendig. Weg von einer statischen, einmaligen Konfiguration, hin zu einem, an das sich dynamisch entwickelnde Themenfeld angepassten, Einspielen von kontinuierlichen Verbesserungen in der Konfiguration unter Berücksichtigung aktueller Technologien.

Das wiederholte Testen von Webseiten der hier vorgestellten Kategorien kann dazu beitragen, die verantwortlichen Organisationen und Personen für das Thema sensibel zu machen. Das verwendete Webtool selbst kann weiterentwickelt werden, indem weitere Testkriterien in die Bewertung mit aufgenommen werden, um ein noch umfangreicheres Bild der Sicherheitskonfiguration zu erhalten. ■

JOHANNES MENG,
studiert im Master Internet-Sicherheit am Institut für Internet-Sicherheit – if(is) an der Westfälischen Hochschule Gelsenkirchen und beschäftigte sich im Rahmen des Studiums mit der IT-Sicherheit und Vertrauenswürdigkeit von TLS/SSL.

NORBERT POHLMANN,
Informatikprofessor für Informationssicherheit und Leiter des Instituts für Internet-Sicherheit – if(is) an der Westfälischen Hochschule in Gelsenkirchen sowie Vorstandsvorsitzender des Bundesverbands IT-Sicherheit – TeleTrusT und im Vorstand des Internetverbandes – eco.

Literatur

[1] N. Pohlmann: Lehrbuch „Cybersicherheit", Springer Vieweg Verlag, Wiesbaden 2019, ISBN 978-3-658-25397-4

Fußnoten

(1) Kleiner als Version 0.9.8za, Version 1.0.0 bis 1.0.0m und Version 1.0.1 bis 1.0.1h, Quelle: http://cve.circl.lu/cve/CVE-2014-0224, abgerufen am 14.11.2018

(2) Verfügbar unter https://www.openssl.org/source/

(3) OpenSSL-Version 1.0.1 bis 1.0.1f, Quelle: http://heartbleed.com/, abgerufen am 14.11.2018

(4) Globales Gremium, das weltweite Industrie-Standards für kartenbasierte Zahlungsdienste festlegt. https://www.pcisecuritystandards.org/about_us/

(5) Aus technischen Gründen konnten nur 27 der 30 KMU-Webseiten getestet werden.

(6) Aus technischen Gründen konnten die Domains www.tu-dresden.de, www.hu-berlin.de und www.uni-bonn.de nicht getestet werden.