

TLS-Sicherheit in der Praxis

# Nicht abschließend

Johannes Meng, Norbert Pohlmann



Das Institut für Internet-Sicherheit if(is) hat zahlreiche Webseiten untersucht und ein aktuelles Bild der Sicherheitslage bei der verschlüsselten Datenübertragung im Internet erstellt. Das vom if(is) entwickelte Testwerkzeug steht für eigene Tests öffentlich zur Verfügung.

Die im Mai 2018 in Kraft getretene Datenschutz-Grundverordnung (DSGVO) verpflichtet alle in der EU tätigen Unternehmen, den „Datenschutz durch Technikgestaltung“ zu ge-

währleisten. Dazu zählt insbesondere, personenbezogene Daten beim Übertragen durchs Internet mittels TLS (Transport Layer Security) zu schützen. Das zwar veraltete, aber zum Teil immer noch einge-



- TLS, das Nachfolgeprotokoll von SSL, dient der Verschlüsselung des Datentransports im Internet. Insbesondere zwischen Webservern und -browsern schützt TLS den Großteil aller Verbindungen.
- Da Webbrowser oft ab Werk unsicher konfiguriert sind, kommt den Server-Betreibern eine besondere Verantwortung zu, die Datensicherheit mittels geeigneter TLS-Konfiguration sicherzustellen.
- Ein öffentlich verfügbares Testwerkzeug verdeutlicht die Sicherheitslage von Webservern in Bezug auf TLS.

setzte Vorgängerprotokoll SSL (Secure Sockets Layer) ist im Folgenden einbezogen.

Die Verschlüsselung der zu übertragenden Daten mittels TLS dient dreierlei Zielen: Sie verhindert erstens den Zugriff durch Dritte während des Transports. Zweitens findet die Kommunikation integritätsgesichert statt; niemand kann den Datenverkehr unbemerkt manipulieren. Die dritte Funktion ist die Authentifizierung der Kommunikationspartner. TLS gewinnt also aus gutem Grund rasch an Beliebtheit: Von 2016 bis 2019 hat sich der Anteil der damit im Web geschützten Verbindungen auf über 75 % ungefähr verdreifacht (siehe Abbildung 1).

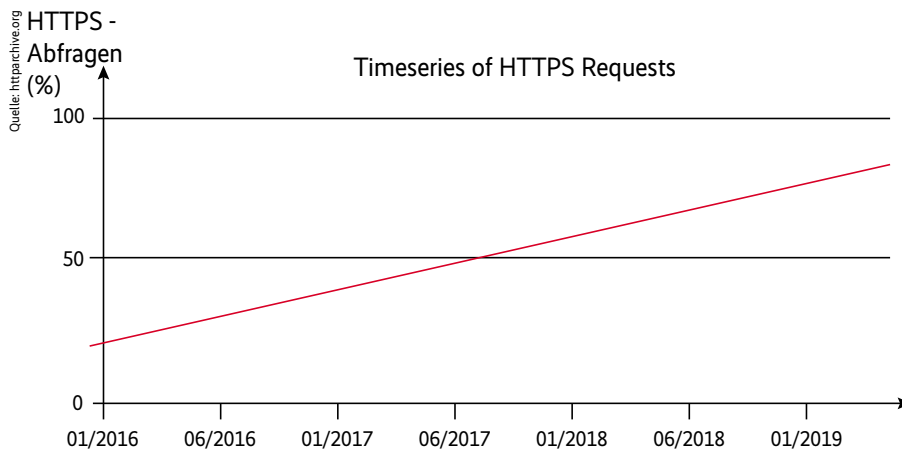
TLS kommt also bei Milliarden von Verbindungen täglich zum Einsatz. Das im Folgenden beschriebene Testverfahren bestätigt jedoch den Eindruck, dass die Sicherheit häufig zu wünschen übrig lässt – lauern doch einige Fallen beim Konfigurieren: Überholte Protokollversionen lassen einige Angriffsmöglichkeiten zu, der Einsatz veralteter Verschlüsselungsmethoden (Cipher Suites) gefährdet die Datensicherheit und falsch konfigurierte Parameter lassen Einfallstore für Angreifer offen (siehe Abbildung 2).

## Sichere Protokollversionen und Einstellungen

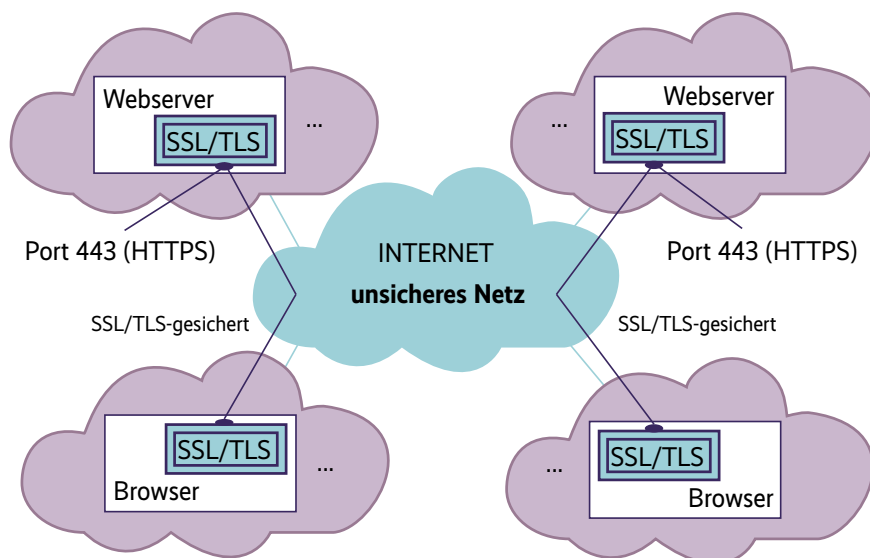
Die Verbindungsparameter stellt der Server in der ersten von zwei Phasen ein: beim Aufbau der Verbindung. Er berücksichtigt dabei die vom Client angegebenen Konfigurationsmöglichkeiten. Diese „Handshake-Phase“ entscheidet über die Sicherheit der Verbindung (siehe Abbildungen 3 und 4).

In der Regel leitet der Client die Handshake-Phase ein und sendet die Nachricht „ClientHello“. Diese enthält eine Liste der Cipher Suites, die der Client – meist ein Webbrowser – beherrscht [1]. Der Server entscheidet, welche davon zum Einsatz kommt, im Idealfall die sicherste Variante. Er kann die Verbindung ablehnen, wenn er keine vom Client vorgeschlagene Cipher Suite akzeptiert.

Das hier vorgestellte Testwerkzeug simuliert einen Client, der viele unterschiedliche Verbindungen nacheinander aufbaut (siehe Kasten „Das Testtool im Überblick“). Es verwendet dabei jeweils unterschiedliche Parameter (TLS-Version, Cipher Suites) in einer „ClientHello“-Nachricht. So gibt es zum Beispiel vor, dass der Client nur die veraltete SSL-Version 2.0 beherrscht, um herauszufinden, ob der Server dieses Protokoll akzeptiert (siehe Abbildung 5).



Der Anteil der TLS-Verbindungen im Web steigt seit Jahren rasch (Abb. 1).



Mit TLS (ehemals SSL) lassen sich sichere und vertrauenswürdige Kommunikationskanäle im Internet aufbauen – wenn Server und Client geeignet konfiguriert sind (Abb. 2).

Der Server antwortet dem Testtool per „ServerHello“-Nachricht, ob er die Verbindung annimmt. Für die Sicherheit ist es entscheidend, dass der Server keine alten und unsicheren Protokollversionen und Cipher Suites akzeptiert. Wenn er eine Verbindung mit SSL 2.0 aufzubauen bereit ist, offenbart dies gravierende Mängel. Der Test beantwortet also die Frage: Welches sind die unsichersten Parameter, die der Webserver akzeptiert?

Beim Laden einer Webseite über eine TLS-gesicherte Verbindung initiiert der Webbrowser den Verbindungsaufbau. Anwender richten nur in Ausnahmefällen ihr Augenmerk auf die TLS-Konfiguration – zum Beispiel, wenn ein Zertifikat des Servers abgelaufen ist und der Browser einen entsprechenden Warnhinweis gibt. Die meisten Nutzer befassen sich nicht mit den Details, sondern belassen es bei den Voreinstellungen des Browsers. Diese Standardkonfigurationen lassen oft veraltete Protokolle wie TLS 1.0 zu, was im Hinblick auf die Sicherheit unverantwortlich ist. Umso mehr Verantwortung liegt bei den Website-Betreibern, beim Konfigurieren des Servers auf sichere TLS-Einstellungen zu achten (siehe Kasten „TLS serverseitig sicher konfigurieren“).

Das Testtool bewertet die TLS-Konfigurationen anhand von Zertifikat und Schlüssel, Protokollversionen, HTTP-Header sowie weiterer Kriterien. Zunächst prüft es, ob die in die Adresszeile des Browsers eingegebene Domain mit derjenigen im Zertifikat übereinstimmt. Jede Instanz, die eine TLS-Verbindung aufbaut, enthält einen Zertifikatsspeicher (Trust Store) mit sogenannten Wurzelzertifikaten (Root Certificates). Bei diesen Instanzen handelt es sich beispielsweise um Webbrowser wie Firefox. Die müssen eine Vertrauenskette (Chain of Trust) vom Wurzelzertifikat bis zum Zertifikat des besuchten Webservers aufbauen. Zu den geprüften Kriterien gehört das Online Certificate Status Protocol (OCSP), mit dessen Hilfe sich ein Zertifikat auch vor Erreichen des ursprünglich vorgesehenen Ablaufdatums widerrufen lässt.

Besonderes Augenmerk gilt Zertifikaten vom Typ Extended Validation. Hierbei muss der Antragsteller Nachweise erbringen, dass er berechtigt ist, das Zertifikat für eine bestimmte Domain zu beantragen, dass er physisch existiert und eine aktive Organisation unterhält. Das stellt die Identität des Zertifikatinhabers sicher und ob der Betreiber einer Webseite die im Zertifikat genannte Domain verwenden darf. Die Domain teletrust.de zum Beispiel gehört offenbar tatsächlich TeleTrust, dem Bundesverband der IT-Sicher-

heit, weil D-Trust als ausgebende Stelle diesen Zusammenhang sicherlich intensiv geprüft hat.

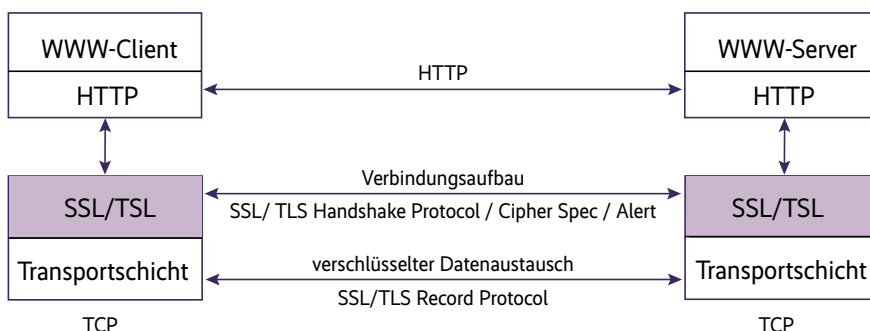
Ein Teil des Schlüsselpaares, der geheime Schlüssel (Private Key), ist praktisch der Generalschlüssel des Servers und hat einen hohen Schutzbedarf. Er bildet die Basis zum Generieren temporärer Schlüssel, die für den Aufbau genau einer TLS-Verbindung nötig sind.

Die Sicherheit der TLS-Verbindung beruht auch auf der in Bit angegebenen Länge der Schlüssel. Je länger die Schlüssel sind, desto besser ist die Kommunikati-

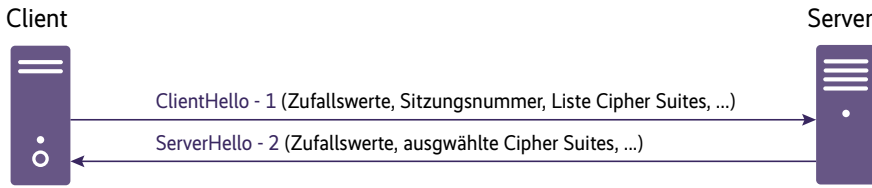
onsverbindung geschützt, desto mehr Rechenaufwand erfordert die Datenübertragung aber auch.

## Vor 25 Jahren erschien SSL

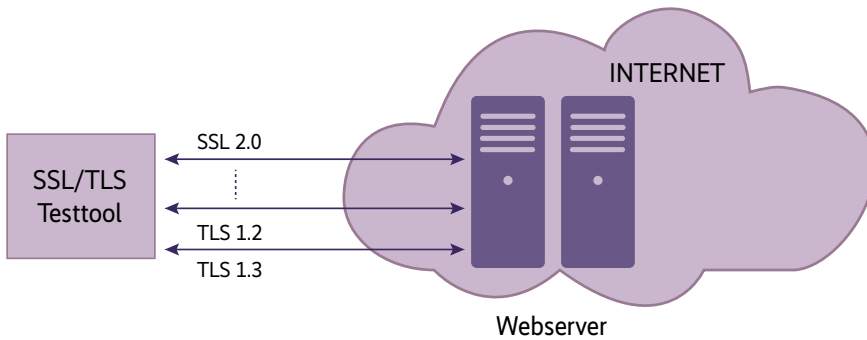
Zum Verschlüsseln existieren heute sechs Protokollversionen. Die ersten beiden, SSL 2.0 und SSL 3.0, hat Netscape 1994 und 1995 veröffentlicht. Eine Version 1.0 wurde rechtzeitig als unsicher erkannt, sodass sie niemals erschien. Auch SSL 2.0 hat klare Schwächen, gilt aber erst seit



TLS fügt der Kommunikation im Internet – nicht nur im Web – eine zusätzliche Kommunikationsschicht hinzu (Abb. 3).



Beim Aufbau einer TLS-Verbindung nennt der Client die Verschlüsselungsverfahren, die er beherrscht, der Server wählt eine davon aus (Abb. 4).



Das Testtool sendet viele Anfragen mit unterschiedlichen Parametern an den Webserver und ermittelt so die unsicherste Konfiguration, die er zu akzeptieren bereit ist (Abb. 5).

2011 offiziell als veraltet und sollte spätestens seitdem nicht mehr zum Einsatz kommen, SSL 3.0 seit 2015. Die nachfolgenden Versionen TLS 1.0 bis 1.3 obliegen der Internet Engineering Task Force (IETF); die aktuelle Version gibt es seit August 2018. Nur diese, TLS 1.3, wird den heutigen Sicherheitsanforderungen

gerecht, weil sie unsichere Algorithmen wie RC4 von vornherein ausschließt (siehe iX 8/2018, S. 110).

Das TLS-Testtool widmet sich neben Zertifikaten und Protokollen auch dem HTTP-Header: Jedes Datenpaket enthält darin Meta-Informationen über die Verbindung, etwa, ob HTTP Strict Transport

Security (HSTS) zum Einsatz kommt. HSTS legt fest, dass Inhalte ausschließlich über gesicherte Verbindungen geladen werden dürfen. Außerdem prüft das Tool das HTTP Public Key Pinning (HPKP), das einen Webserver darüber informiert, dass nur bestimmte Certificate Authorities (CAs) Zertifikate für die entsprechende Domain ausstellen dürfen.

Zu den weiteren Testkriterien gehört der SCSV-Fallback-Mechanismus (Signaling Cipher Suite Value). Er verhindert, dass der Server während der Handshake-Phase eine niedrigere Protokollversion als nötig auswählt. Das Testtool überprüft außerdem, ob die folgenden bekannten Sicherheitslücken behoben sind: Im Fall eines erfolgreichen Angriffs der CSS-Injection-Schwachstelle kann der Master-Key auf die Länge null schrumpfen; mithilfe der Heartbleed-Schwachstelle können Angreifer den privaten Schlüssel des Servers auslesen.

## Bewertung der Testergebnisse

Im Rahmen des Tests erhalten die einzelnen Kriterien Bewertungen auf einer Skala von 0 (höchst unsicher) bis 10 (bestmögliche Sicherheit). Schlechte Bewertungen in einem der Teilbereiche schlagen auf das Gesamtergebnis durch: Wenn nur einer angreifbar ist, stellt das den gesamten Schutz der Verbindung infrage. Im Folgenden finden sich einige Beispiele für konkrete Bewertungen.

Das Zertifikat erhält eine 0, wenn es nicht für die entsprechende Domain gilt, da dies eine grundlegende Voraussetzung für das Vertrauen ist. Mittels Hash-Wert kann man prüfen, ob ein Zertifikat nach der Ausstellung modifiziert wurde. Kommt dazu jedoch der unsichere SHA1-Algorithmus zum Einsatz, wird das Ergebnis auf 2 herabgestuft. Ist in der mitgelieferten Zertifikatskette das Wurzelzertifikat nicht enthalten, kann die Bewertung nicht besser sein als 8; mehr als eine 9 ist nicht drin, wenn kein Extended-Validation-Zertifikat zum Einsatz kommt.

Auch für das Akzeptieren veralteter Protokollversionen gibt es kräftige Abschlüsse, bei SSL 2.0 auf 1, beim ebenfalls anerkannt unsicheren SSL 3.0 auf 2. Auch TLS 1.0 und 1.1 sind veraltet; die Bewertung bei aktiviertem TLS 1.0 kann daher nicht besser sein als 7. Akzeptiert der Server unsichere oder veraltete Cipher Suites, liegt sie je nach Angreifbarkeit noch darunter. Für eine NULL-Verschlüsselung, also eine Übertragung im Klartext, gibt es natürlich eine 0.

Ein Server sollte auf jeden Fall mindestens die TLS-Version 1.2 beherrschen, für

## Das Testtool im Überblick

Das auf vom if(is) zur Verfügung gestellte Online-Werkzeug [2] überprüft die TLS-Konfiguration von Webservern und simuliert zu diesem Zweck einen Client, der mehrmals und mit wechselnden Parametern Verbindungen aufbaut. Der Anwender gibt die Webseiten-Adresse ein und startet den Test, worauf das Tool die Einstellungen der getesteten Website anzeigt.

Auf der Test-Webseite finden sich zum Vergleich einige bereits ermittelte Bewertungen



Das if(is) bringt ausführliche Bewertungen der gewünschten Website sowie zahlreicher zuvor getesteter Server (Abb. 6).

in drei Kategorien: die Top 50 der in Deutschland abgerufenen Webseiten, die Top 30 der kleinen und mittelständischen Unternehmen sowie die Top 20 der Hochschulen.

Das Frontend des Testtools stammt vom Institut für Internet-Sicherheit if(is). Es nimmt Namen des zu testenden Hosts entgegen und stellt das Ergebnis inklusive Bewertung grafisch dar. Bereits vorliegende Ergebnisse dreier verschiedener Anbieterkategorien sind ebenfalls verfügbar.

Das funktionale Gerüst bildet das Python-Framework django. Es erleichtert das Erstellen von Webanwendungen, denn häufig verwendete Funktionen sind bereits implementiert, was zum Beispiel den Umgang mit URLs im Python-Code erleichtert.

Django steuert den technischen Teil des Tests, der auf dem als Library eingebundenen Open-Source-Tool slyze basiert [2]. Dieses kann gezielt einzelne Protokollversionen testen oder der gesamten TLS-Konfiguration eines Servers auf den Zahn fühlen.

## TLS serverseitig sicher konfigurieren

die keine schwerwiegende Schwachstelle bekannt ist. Der Test bewertet die Website anderenfalls mit 3. Die Verwendung der aktuellen TLS-Version 1.3 wird ebenfalls getestet und visuell hervorgehoben, allerdings erhöht sie noch nicht die Bewertung.

Ohne HTTP Strict Transport Security im Header sinkt die Bewertung auf maximal 5, da dies erhebliche Sicherheitseinbußen mit sich bringt. Ein deaktiviertes HTTP Public Key Pinning senkt die Bewertung um einen Punkt auf 9. Ist der SCSV-Fallback-Mechanismus OCSP nicht aktiviert, ist höchstens eine 7 drin. Besteht die CSS-Injection-Schwachstelle, gibt es höchstens die 4; die Heartbleed-Lücke, die ebenfalls längst behoben sein sollte, resultiert in maximal 2.

### Öffentliche Webserver im Test

Das if(is) hat die Top 50 der relevantesten Webseiten in Deutschland, die Top 20 der kleinen und mittelständischen Unternehmen sowie die Top 20 der deutschen Hochschulen getestet. Die Ergebnisse sind auf den Seiten des Instituts abrufbar [2]. Die beste Gesamtbewertung in dieser Kategorie, eine 7, wurde siebenmal erreicht; das schlechteste Ergebnis ist eine 2, bei einer Durchschnittsbewertung von 5,1. Die besonders vertrauenswürdigen Extended-Zertifikate erfreuen sich unverständlicherweise keiner großen Beliebtheit: Sie waren lediglich bei zwei Domains zu finden. Bei allen getesteten Domains war noch TLS 1.0 aktiviert, was die Sicherheit unnötig gefährdet. Die zum Facebook-Konzern gehörenden Domains whatsapp.com und facebook.com lassen jeweils eine unsichere Cipher Suite zu.

Auch die getesteten 30 kleinen und mittelständischen Unternehmen in Deutschland erreichen als beste Bewertung in dieser Kategorie eine 7 (dreimal). Die schlechteste Bewertung 2 wurde zweimal vergeben, weil veraltete Verschlüsselungsalgorithmen wie RC4 im Einsatz waren. Ein Extended-Validation-Zertifikat fand sich lediglich bei einer einzigen Domain. Die Durchschnittsbewertung bei kleinen und mittelständischen Unternehmen beträgt 4,9. Damit ist sie noch etwas niedriger als bei den Top-50-Webseiten Deutschlands. Der überwiegende Teil der Domains ist nicht sicher genug konfiguriert und teilweise zeugen die Konfigurationen von Nachlässigkeit.

Für die Webseiten deutscher Hochschulen waren bessere Ergebnisse zu erwarten, weil dort häufig einiges frische Know-how im Bereich IT-Sicherheit zur Verfügung

steht. Doch auch hier konnten nur drei Domains die Bestnote 7 erreichen. Die schlechteste Uni-Bewertung war eine 3 (Durchschnitt: 4,6). Nur für eine einzige Domain ist derzeit die neueste Version TLS 1.3 konfiguriert. Die Hochschulen scheinen das informationstechnische Know-how im eigenen Haus nicht praktisch auf die Konfiguration der eigenen IT-Infrastruktur anzuwenden.

### Sicherheitslage: knapp ausreichend

Die Tests des if(is) ergaben bisher durchschnittliche Bewertungen zwischen 4,9 und 5,1 von 10. Das ist aus Sicht der IT-Sicherheit und Vertrauenswürdigkeit nicht akzeptabel. Auffälligkeiten wegen nicht geschlossener Schwachstellen gab es immerhin nicht. Es ist jedoch grundsätzlich notwendig, dass die Server-Betreiber veraltete Protokollversionen bis hin zu TLS 1.0 deaktivieren. Aktuelle Webbrowser beherrschen bereits TLS 1.3. Aus sicherheitstechnischer Sicht dürfen eigentlich nur noch TLS 1.2 mit sicheren Verschlüsselungsalgorithmen und TLS 1.3 aktiviert sein. Alle anderen Konfigurationen sind eine unnötige Gefährdung der IT-Sicherheit.

Zertifikate vom Typ „Extended Validation“ (EV) kommen leider kaum zum Einsatz. Hier besteht dringender Handlungsbedarf. Insbesondere Webseiten mit hoher Relevanz könnten damit den Schutz vor Phishing-Angriffen erhöhen. Ein EV-Zertifikat verursacht zusätzliche Kosten und einen erweiterten Aufwand, jedoch sind

das Profil TLS\_ECDHE\_ECDSA\_WITH\_AES\_256\_CBC\_SHA384 vor [2]. Es gibt weitere Profile, die eine vergleichbare Sicherheit bieten. Auf keinen Fall dürfen anerkannt unsichere Algorithmen wie die „Null-Verschlüsselung“ (TLS\_RSA\_WITH\_NULL\_SHA256) zum Einsatz kommen.

**HSTS** (HTTP Strict Transport Security) muss aktiviert sein, damit garantiert kein Klartext über die Leitung geht.

**HPKP** (HTTP Public Key Pinning) gilt es korrekt zu konfigurieren, inklusive „Backup-Pin“, damit keine dubiosen CAs zum Zuge kommen.

Der **SCSV** (Signaling Cipher Suite Value) stellt den Einsatz der stärkstmöglichen Protokollversion sicher.

Zum Prüfen und Widerrufen von Zertifikaten muss das **OCSP** (Online Certificate Status Protocol) korrekt konfiguriert sein.

dies wichtige Investitionen in die IT-Sicherheit und Vertrauenswürdigkeit der angebotenen Webdienste.

### Fazit


Offenbar besteht noch keine Einigkeit darüber, welchen Mindestschutz TLS überhaupt gewährleisten soll. Die Hersteller der Software-Komponenten und die Betreiber der Websites sollten klare Angaben über das Schutzniveau als selbstverständlichen Service gegenüber den Anwendern sehen.

Eine sichere Konfiguration von TLS erfordert einiges an Know-how und unterliegt ständigen Änderungen. Regelmäßiges Überprüfen und Anpassen sind deshalb notwendig – und das nicht nur im festen Turnus: Dringender Änderungsbedarf kann sehr plötzlich entstehen, wenn etwa eine neue Schwachstelle bekannt wird. Daher ist es notwendig, einen Konsens von Anbietern

### Johannes Meng

studiert im Master Internet-Sicherheit am Institut für Internet-Sicherheit – if(is) an der Westfälischen Hochschule Gelsenkirchen.

### Norbert Pohlmann

ist Professor für Informationssicherheit und Leiter des Instituts für Internet-Sicherheit – if(is) an der Westfälischen Hochschule in Gelsenkirchen, Vorstandsvorsitzender des Bundesverbands IT-Sicherheit TeleTrusT sowie Mitglied im Vorstand des Internetverbands eco. 

und Herstellern herbeizuführen, den alle anhand fundierter und eindeutiger Anweisungen umsetzen können. (un@ix.de)

### Quellen

- [1] Norbert Pohlmann; Cyber-Sicherheit; Springer Vieweg, Wiesbaden 2019
- [2] Alle URLs zum Artikel unter [ix.de/zzep](http://ix.de/zzep)