Bundesamt
für Sicherheit in der
Informationstechnik

Mindeststandard des BSI für den Einsatz des SSL/TLS-Protokolls durch Bundesbehörden

nach § 8 Abs. 1 Satz 1 BSIG

Bundesamt für Sicherheit in der Informationstechnik
Postfach 20 03 63
53133 Bonn
Tel.: +49 22899 9582-0
E-Mail: referat-b25@bsi.bund.de
Internet: https://www.bsi.bund.de

Inhaltsverzeichnis

Vorwort

§ 8 Absatz 1 BSIG regelt die Befugnis des BSI, allgemeine technische Mindeststandards für die Sicherung der Informationstechnik des Bundes festzulegen. Mindeststandards können nach der Gesetzesbegründung etwa die IT-Grundschutz-Handbücher oder auch Prüfkriterien sein. Der Mindeststandard beschreibt die zu erfüllenden sicherheitstechnischen Anforderungen an eine Produkt- bzw. Dienstleistungskategorie oder Methoden, um eine angemessene Sicherheit für einen Mindestschutz gegen IT-Sicherheitsbedrohungen zu erreichen.

Mindeststandards stellen in diesem Sinne zunächst unverbindliche Empfehlungen dar. Allerdings kann das BMI nach Zustimmung des IT-Rats die dort formulierten Anforderungen ganz oder teilweise als allgemeine Verwaltungsvorschrift erlassen und dadurch für die Stellen des Bundes verbindlich erklären, vgl. § 8 Absatz 1 Satz 2 BSIG. Darüber hinaus kann der IT-Planungsrat Mindeststandards teilweise oder vollständig als gemeinsame Standards für den zur Aufgabenerfüllung zwischen dem Bund und den Ländern notwendigen Datenaustausch festlegen.[1]

Über die Stellen des Bundes hinaus sind Mindeststandards nach § 8 Absatz 1 BSIG damit von grundsätzlicher Bedeutung für den Einsatz von Informationstechnik auch in der öffentlichen Verwaltung der Länder und Kommunen, zur Sicherung kritischer Infrastrukturen und der Privatwirtschaft. Ziele, Anforderungen und Empfehlungen von Mindeststandards können dazu genutzt werden, eigene Sicherheitsanforderungen anzupassen oder zu überprüfen, auch bei der Erstellung von Leistungsbeschreibungen im Rahmen eigener Vergabeverfahren. Hersteller von Informationstechnik und IT-Dienstleister können Mindeststandards dazu nutzen, ihre angebotenen Produkte sicherer zu machen.

Inhalt des vorliegenden Dokuments sind Mindestsicherheitsanforderungen für den Einsatz des SSL/TLS-Protokolls in der öffentlichen Verwaltung. Ziel ist der zeitnahe und flächendeckende Einsatz von TLS 1.2 in allen entsprechenden Anwendungen.

1 Grundlage hierfür sind Artikel 91c GG und § 3 Abs.1 des Vertrages zur Ausführung des Artikel 91c GG zwischen dem Bund und den Bundesländern vom 01.04.2010.

1 Mindeststandardbezeichnung

1.1 Mindeststandardname

Das durch dieses Dokument beschriebene Mindeststandardobjekt (MSO) beinhaltet Vorgaben für die Sicherstellung von Vertraulichkeit, Authentizität und Integrität bei der Übertragung von Daten in Anwendungen des Bundes. Die Bezeichnung für dieses Mindeststandardobjekt lautet:

MSO.APP.TLS V1.5 vom 21.11.2014

1.2 Schlüsselwörter

Mindeststandard

SSL/TLS-Protokoll

Verschlüsselung

2 Inhalt des Mindeststandards

2.1 Anwendungsbereich des Mindeststandards

Dieser Mindeststandard gilt für die Transportverschlüsselung mit TLS (Transport Layer Security) bei der Kommunikation von Bundesbehörden mit anderen Behörden, Bürgern und der Wirtschaft.

Ein sicheres Netz hält für einen gegebenen Schutzbedarf technische und organisatorische Maßnahmen vor, welche eine Kenntnisnahme oder Veränderung der Informationen durch unautorisierte Dritte verhindert.

Ab normalem Schutzbedarf der Daten (analog IT-Grundschutz) und bei ihrer Übertragung in einem unsicheren Netz ist daher von den Bundesbehörden das Protokoll TLS 1.2 in Kombination mit Perfect Forward Secrecy[2] als Mindeststandard nach § 8 Abs. 1 Satz 1 BSIG zu verwenden.

Geprüfte Produkte, die diesen Mindeststandard erfüllen, sind vorrangig einzusetzen.

2.2 Technische Spezifikation

Für den Einsatz von TLS 1.2 mit PFS nimmt dieser Mindeststandard Bezug auf die jeweils geltende Fassung der Technischen Richtlinie TR-02102-2 „Kryptographische Verfahren: Empfehlungen und Schlüssellängen. Teil 2 – Verwendung von Transport Layer Security (TLS)“ [TR-02102-2]. Alle Anforderungen dieser Technischen Richtlinie sind einzuhalten.

Die TR-02102-2 verweist für Projekte des Bundes auf die TR-03116-4 „Kommunikationsverfahren im eGovernment“ [TR-03116-4].

Die Technische Richtlinie TR-02102-2 ist beim BSI unter https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/TechnischeRichtlinien/TR02102/BSI-TR-02102-2.pdf zu beziehen.

Die Technische Richtlinie TR-03116-4 ist beim BSI unter https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/TechnischeRichtlinien/TR03116/BSI-TR-03116-4.pdf zu beziehen.

2.3 Stufenplan und Übergangsfristen

Dieser Mindeststandard gilt ab dem Zeitpunkt seiner Verbindlichmachung für alle neuen Systeme mit TLS-Transportverschlüsselung. Bestandssysteme mit TLS-Transportverschlüsselung sind gemäß des im Folgenden dargestellten Sektormodells zu migrieren. Systeme, die Daten mit mindestens hohem Schutzbedarf gemäß IT-Grundschutz erheben und verarbeiten, sind vorrangig zu migrieren.

Die Anordnung der Sektoren in aufsteigender Folge ergibt die zeitliche Priorisierung der zu migrierenden Systeme.

Es werden die folgenden vier Sektoren festgelegt:

1. Bürger-Behörden-Kommunikation: Wenn Daten zwischen Bundesbehörden und Bürgern übertragen werden (z. B. durch Web-Server und Browser, E-Mail, FTP), müssen die Bestandssysteme bis zum 01.07.2015 migriert sein, sodass die Transportverschlüsselung mit TLS gemäß dieses Mindeststandards unter Beiziehung der TR-03116-4 angeboten wird.

2 PFS; die Bezeichnung Forward Secrecy kann synonym verwendet werden

2. Wirtschaft-Behörden-Kommunikation: Wenn Daten zwischen Bundesbehörden und der Wirtschaft über ein Fachverfahren übertragen werden, muss das Fachverfahren bis zum 31.12.2016 migriert sein, sodass die Transportverschlüsselung mit TLS gemäß dieses Mindeststandards verwendet wird.
3. Inter-Behördenkommunikation: Wenn Daten zwischen zwei oder mehreren Bundesbehörden über ein Fachverfahren übertragen werden, muss das Fachverfahren bis zum 31.12.2016 migriert sein, sodass die Transportverschlüsselung mit TLS gemäß dieses Mindeststandards verwendet wird.
4. Interne Behördenkommunikation: Wenn Daten innerhalb einer Bundesbehörde übertragen werden, müssen die Bestandssysteme bis zum 01.07.2017 migriert sein, sodass die Transportverschlüsselung mit TLS gemäß dieses Mindeststandards verwendet wird.

Sollten die Bestandssysteme innerhalb der angegebenen Fristen vollständig oder unter Hinzunahme von Alternativlösungen nicht migriert werden können, sind Abweichungen von diesem Mindeststandard spätestens 8 Wochen vor Ablauf der Migrationsfrist durch die jeweilige Bundesbehörde an das BSI oder an den für das Ressort zuständigen IT-Sicherheitsbeauftragten oder seine stellvertretend beauftragte Stelle zu notifizieren. Diese Notifikation soll folgende Angaben enthalten:

1. eine Benennung des nicht oder nur eingeschränkt migrierbaren Systems einschließlich seiner Zuordnung zu einem der oben genannten Sektoren, der betreibenden Dienststelle, des Schutzbedarfs der verarbeiteten Daten sowie der Art und Anzahl angeschlossener Nutzer,
2. einen Zeitplan zur Erfüllung des Mindeststandards für den Zeitraum eines Jahres ab Datum der Notifikation.

Die direkte Notifikation der Bundesbehörde an das BSI ist vom Behördenleiter zu unterschreiben. Bei Notifikation der Bundesbehörde an den IT-Sicherheitsbeauftragten des Ressorts oder seine stellvertretend beauftragte Stelle erfolgt dessen oder deren Notifikation an das BSI unverzüglich. Die Notifikation des IT-Sicherheitsbeauftragten des Ressorts an das BSI ist dann von diesem oder der von ihm stellvertretend beauftragten Stelle zu unterschreiben.

Die Verantwortung für die Umsetzung und Steuerung der Migration verbleibt davon unbesehen bei der Bundesbehörde bzw. dem IT-Sicherheitsbeauftragten des Ressorts.

3 Begründung des Mindeststandards

Das TLS-Protokoll (Transport Layer Security) dient der Sicherstellung von Vertraulichkeit, Authentizität und Integrität bei der Übertragung von Daten in unsicheren Netzwerken. TLS (Transport Layer Security) ist ein kryptographisches Protokoll zur Etablierung eines sicheren Kanals (verschlüsselt, authentisiert und integritätsgeschützt). Insbesondere ist die TLS-gesicherte Übertragung im Internet (mittels HTTPS) sehr wichtig und weit verbreitet. Heutzutage werden viele Anwendungen wie z. B. Homebanking, E-Commerce, E-Government etc. über das Internet abgewickelt, und gerade bei diesen Anwendungen ist es wichtig, dass die Daten (insbesondere Zugangsdaten, PINs, Passwörter) sicher übertragen werden können. Hier spielt das TLS-Protokoll eine wichtige Rolle. Es dient dazu, einen sicheren Kanal zwischen Sender und Empfänger (z. B. Webbrowser und Webserver) aufzubauen und alle Nutzdaten sicher durch diesen Kanal zu übertragen.

Der Spezifikationsstandard von TLS wird von der IETF (Internet Engineering Task Force) in RFCs (Request For Comment) in einem öffentlichen Diskussionsprozess standardisiert.

Das SSL-Protokoll existiert in den Versionen 1.0, 2.0 und 3.0, wobei die Version 1.0 nicht veröffentlicht wurde. SSL in der Version 2.0 wurde schon im Jahre 1996 wegen zahlreicher funktionaler Schwachstellen von der IETF abgekündigt und die Nutzung des von Netscape entwickelten SSL der Version 3.0 empfohlen. TLS 1.0 ist eine direkte Weiterentwicklung von SSL 3.0. Dessen Spezifikation wurde Anfang 1999 als [RFC2246] veröffentlicht. Des Weiteren gibt es für das TLS-Protokoll Sicherheitsanpassungen in den Versionen 1.1 und 1.2, welche 2006 als [RFC4346] bzw. 2008 als [RFC5246] spezifiziert wurden.

Seit 2011 sind mehrere Angriffe gegen SSL/TLS bekannt geworden. Die entsprechenden Schwachstellen können durch Nutzung entsprechender Cipher-Suites gemäß [TR-02102-2] in TLS 1.2 behoben werden.

Quellenverzeichnis

[RFC2246] IETF: T. Dierks, C. Allen: RFC 2246, The TLS Protocol Version 1.0, http://tools.ietf.org/html/rfc2246

[RFC4346] IETF: T. Dierks, E. Rescorla: RFC 4346, The Transport Layer Security (TLS) Protocol Version 1.1, http://tools.ietf.org/html/rfc4346

[RFC5246] IETF: T. Dierks, E. Rescorla: RFC 5246, The Transport Layer Security (TLS) Protocol Version 1.2, http://tools.ietf.org/html/rfc5246

[TR-02102-2] BSI: „Kryptographische Verfahren: Empfehlungen und Schlüssellängen. Teil 2 – Verwendung von Transport Layer Security (TLS)“, https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/TechnischeRichtlinien/TR02102/BSI-TR-02102-2.pdf

[TR-03116-4] BSI: „Vorgaben für Kommunikationsverfahren im E-Government“, https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/TechnischeRichtlinien/TR03116/BSI-TR-03116-4.pdf