Bundesamt
für Sicherheit in der
Informationstechnik

Deutschland
Digital•Sicher•BSI•

Hilfsdokument zum Mindeststandard des BSI zur Verwendung von Transport Layer Security V2.4

nach § 8 Absatz 1 Satz 1 BSIG – Version 2.4 vom 25.05.2023

Änderungshistorie

Version	*Datum*	*Beschreibung*
1.0	22.08.2019	Hilfsdokument zum MST-TLS (MST-TLS 2.0, IT-Grundschutz-Kompendium Edition 2019)
1.1	07.05.2020	Hilfsdokument zum MST-TLS (MST-TLS 2.1, IT-Grundschutz-Kompendium Edition 2020)
2.2	03.05.2021	Hilfsdokument zum MST-TLS (MST-TLS 2.2, IT-Grundschutz-Kompendium Edition 2021)
2.3	15.03.2022	Hilfsdokument zum MST-TLS (MST-TLS 2.3, IT-Grundschutz-Kompendium Edition 2022)
2.4	25.05.2023	Hilfsdokument zum MST-TLS (MST-TLS 2.4, IT-Grundschutz-Kompendium Edition 2023)

Tabelle 1: Versionsgeschichte des Hilfsdokumentes

Bundesamt für Sicherheit in der Informationstechnik
Postfach 20 03 63
53133 Bonn
Tel.: +49 22899 9582-6262
E-Mail: mindeststandards@bsi.bund.de
Internet: https://www.bsi.bund.de

Inhalt

1 Einleitung 4
2 Transport Layer Security im IT-Grundschutz 5
2.1 IT-Grundschutz-Bausteine mit direktem Bezug zu TLS 5
2.1.1 APP.1.2 Web-Browser 5
2.1.2 APP.2.1 Allgemeiner Verzeichnisdienst 5
2.1.3 APP.3.2 Webserver 5
2.1.4 APP.4.2 SAP-ERP-System 5
2.1.5 SYS.1.7 IBM-Z System 5
2.1.6 NET.1.2 Netzmanagement 6
3 Risikoanalyse 7
3.1 Ermittlung der zu betrachtenden Zielobjekte 8
3.2 Erstellung einer Gefährdungsübersicht 9
3.2.1 Schwachstellen von TLS 1.0 und TLS 1.1 9
3.2.2 Elementare Gefährdungen 11
3.2.3 Betrachtung zusätzlicher Gefährdungen 12
3.3 Einstufung von Risiken 12
3.3.1 Bewertung von Risiken 13
3.4 Behandlung von Risiken 14
Literaturverzeichnis 15
Abkürzungsverzeichnis 17

1 Einleitung

Werden Informationen ausgespäht oder manipuliert, erfolgt dies häufig beim Transport über Kommunikationsnetze. Eine geeignete Schutzmaßnahme vor solchen Cyber-Angriffen ist die Verwendung des Verschlüsselungsprotokolls Transport Layer Security (TLS). Vorgaben für die Verwendung einer sicheren Version mit sicheren kryptografischen Verfahren macht der Mindeststandard des BSI zur Verwendung von Transport Layer Security (MST-TLS).[1]

Der MST-TLS (Version 2.4) fordert, sobald TLS verwendet wird, den Einsatz von TLS 1.2 und/oder TLS 1.3 in Kombination mit Perfect Forward Secrecy (PFS). Ebenso fordert der MST-TLS bei Verwendung von TLS den Einsatz von in der Technischen Richtlinie TR-02102-2[2] empfohlenen kryptografischen Verfahren. Das heißt jedoch nicht, dass alle nicht empfohlenen kryptografischen Verfahren generell als unsicher zu bewerten sind.[3] Kapitel 2.0.03 des MST-TLS (Abweichungen und Risikomanagement) legt die Mindestsicherheitsanforderungen fest, unter denen sogenannte zum Mindeststandard nicht konforme TLS-Versionen und nicht konforme kryptografische Verfahren temporär eingesetzt werden können. Eine zentrale Sicherheitsanforderung ist die Durchführung einer Risikoanalyse.

Dieses Hilfsdokument unterstützt bei der Umsetzung des MST-TLS und gibt Hilfestellung insbesondere bei der Durchführung einer Risikoanalyse.

Dazu listet Kapitel 2 Bausteine aus dem IT-Grundschutz-Kompendium[4] auf, die einen direkten Bezug zur Transportverschlüsselung haben. Diese Auflistung kann als Hilfestellung dienen, um die Bereiche eines Informationsverbundes zu identifizieren, in denen Transportverschlüsselung eingesetzt wird. Stellt sich bei Betrachtung dieser Bereiche heraus, dass nicht konforme oder sogar als unsicher bekannte TLS-Versionen und/oder nicht konforme oder sogar als unsicher bekannte kryptografische Verfahren eingesetzt werden, muss zunächst überprüft werden, ob auf konforme und sichere Varianten aktualisiert werden kann. Ist dies nicht möglich, muss eine Risikoanalyse (z. B. auf Basis des BSI-Standards 200-3[5]) durchgeführt werden.

Kapitel 3 unterstützt bei der Durchführung einer solchen Risikoanalyse und folgt dabei dem im BSI-Standard 200-3[6] beschriebenen Ablauf. Kapitel 3.1 bietet Hilfestellung bei der Ermittlung von Zielobjekten. Kapitel 3.2 kann zur Erstellung einer Gefährdungsübersicht als Vorbereitung zur Einstufung der Risiken, wie in Kapitel 3.3 beschrieben, herangezogen werden. Hinweise zur Behandlung von Risiken werden in Kapitel 3.4 gegeben.

[1] Vgl. MST-TLS (BSI 2023a)
[2] Vgl. TR-02102-2 (BSI 2023b)
[3] Vgl. TR-02102-2 (BSI 2023b)
[4] Vgl. IT-Grundschutz-Kompendium (BSI 2023c)
[5] Vgl. BSI-Standard 200-3 (BSI 2017b)
[6] Vgl. BSI-Standard 200-3 (BSI 2017b)

2 Transport Layer Security im IT-Grundschutz

Das IT-Grundschutz-Kompendium[7] enthält keinen allgemeinen, übergreifenden Baustein zum Einsatz von TLS. Die Sicherheitsanforderungen zur Transportverschlüsselung mit TLS werden dort in verschiedenen spezifischen Bausteinen behandelt. Die folgende Auflistung dieser Bausteine kann zur Unterstützung bei der Analyse dienen, auf welchen IT-Systemen in einem Informationsverbund TLS implementiert sein könnte.

2.1 IT-Grundschutz-Bausteine mit direktem Bezug zu TLS

2.1.1 APP.1.2 Webbrowser

APP.1.2.A2 Unterstützung sicherer Verschlüsselung der Kommunikation (B)

Der Webbrowser MUSS Transport Layer Security (TLS) in einer sicheren Version unterstützen. Verbindungen zu Webservern MÜSSEN mit TLS verschlüsselt werden, sofern dies vom Webserver unterstützt wird. Unsichere Versionen von TLS SOLLTEN deaktiviert werden. Der Webbrowser MUSS den Sicherheitsmechanismus HTTP Strict Transport Security (HSTS) gemäß RFC 6797[8] unterstützen und einsetzen.

2.1.2 APP.2.1 Allgemeiner Verzeichnisdienst

APP.2.1.A13 Absicherung der Kommunikation mit Verzeichnisdiensten (S)

Werden vertrauliche Informationen übertragen, SOLLTE die gesamte Kommunikation mit dem Verzeichnisdienst über ein sicheres Protokoll entsprechend der Technischen Richtlinie TR-02102 des BSI (z. B. TLS) verschlüsselt werden. Der Datenaustausch zwischen Client und Verzeichnisdienst-Server SOLLTE abgesichert werden. Es SOLLTE definiert werden, auf welche Daten zugegriffen werden darf.

2.1.3 APP.3.2 Webserver

APP.3.2.A11 Verschlüsselung über TLS (B)

Der Webserver MUSS für alle Verbindungen durch nicht vertrauenswürdige Netze eine sichere Verschlüsselung über TLS anbieten (HTTPS). Falls es aus Kompatibilitätsgründen erforderlich ist, veraltete Verfahren zu verwenden, SOLLTEN diese auf so wenige Fälle wie möglich beschränkt werden. Wenn eine HTTPS-Verbindung genutzt wird, MÜSSEN alle Inhalte über HTTPS ausgeliefert werden. Sogenannter Mixed Content DARF NICHT verwendet werden.

2.1.4 APP.4.2 SAP-ERP-System

APP.4.2.A18 Abschaltung von unsicherer Kommunikation (S)

Die Kommunikation mit und zwischen SAP-ERP-Systemen SOLLTE mit SNC abgesichert werden. Sofern Datenbank und SAP-Applikationsserver auf verschiedenen Systemen betrieben werden, SOLLTE die Datenbankverbindung in geeigneter Weise verschlüsselt werden. Die internen Dienste des SAP-Applikationsservers SOLLTEN nur mittels TLS miteinander kommunizieren.

2.1.5 SYS.1.7 IBM-Z System

SYS.1.7.A6 Einsatz und Sicherung der Remote Support Facility (B)

Es MUSS entschieden werden, ob und gegebenenfalls wie RSF eingesetzt wird. Der Einsatz MUSS im Wartungsvertrag vorgesehen und mit dem Hardware-Support abgestimmt sein. Es MUSS sichergestellt

[7] Vgl. IT-Grundschutz-Kompendium (BSI 2023c)
[8] Vgl. RFC 6797(IETF 2012)

werden, dass die RSF-Konfiguration nur von hierzu autorisierten Personen geändert werden kann. Wartungszugriffe für Firmware-Modifikationen durch das herstellende Unternehmen MÜSSEN von Betreibenden explizit freigegeben und nach Beendigung wieder deaktiviert werden. Die RSF-Kommunikation MUSS über Proxy-Server und zusätzlich über gesicherte Verbindungen (wie TLS) stattfinden.

2.1.6 NET.1.2 Netzmanagement

NET.1.2.A10 Beschränkung der SNMP-Kommunikation (B)

Grundsätzlich DÜRFEN im Netzmanagement KEINE unsicheren Versionen des Simple Network Management Protocol (SNMP) eingesetzt werden. Werden dennoch unsichere Protokolle verwendet und nicht über andere sichere Netzprotokolle (z. B. VPN oder TLS) abgesichert, MUSS ein separates Managementnetz genutzt werden. Grundsätzlich SOLLTE über SNMP nur mit den minimal erforderlichen Zugriffsrechten zugegriffen werden. Die Zugangsberechtigung SOLLTE auf dedizierte Management-Server eingeschränkt werden.

3 Risikoanalyse

Die Risikoanalyse dient dazu, relevante Gefährdungen zu identifizieren und das Risiko, das von diesen Gefährdungen ausgeht, einzustufen und geeignet zu behandeln. Der BSI-Standard 200-3[9] beschreibt diesen allgemeinen Prozess im Detail. Das vorliegende Hilfsdokument konkretisiert die Anwendung des BSI-Standard 200-3[10] auf den Fall der Verwendung von TLS. Eine Risikoanalyse muss durchgeführt werden, sobald eine der drei nachfolgenden Bedingungen zutrifft:

- die Einrichtung verwendet von TLS 1.2 oder TLS 1.3 abweichende TLS-Versionen
- die Einrichtung verwendet kryptografische Verfahren, die nicht in der TR-02102-2 empfohlen werden[11]
- die Einrichtung verwendet kryptografische Verfahren, die nicht die Eigenschaft „Perfect Forward Secrecy“ erfüllen

Die Risikoanalyse macht die bestehenden Risiken für die Einrichtung transparent und eröffnet somit Möglichkeiten zu deren Behandlung. Die folgende Abbildung veranschaulicht, wann der MST-TLS erfüllt ist, und wann eine Risikoanalyse durchgeführt werden muss.

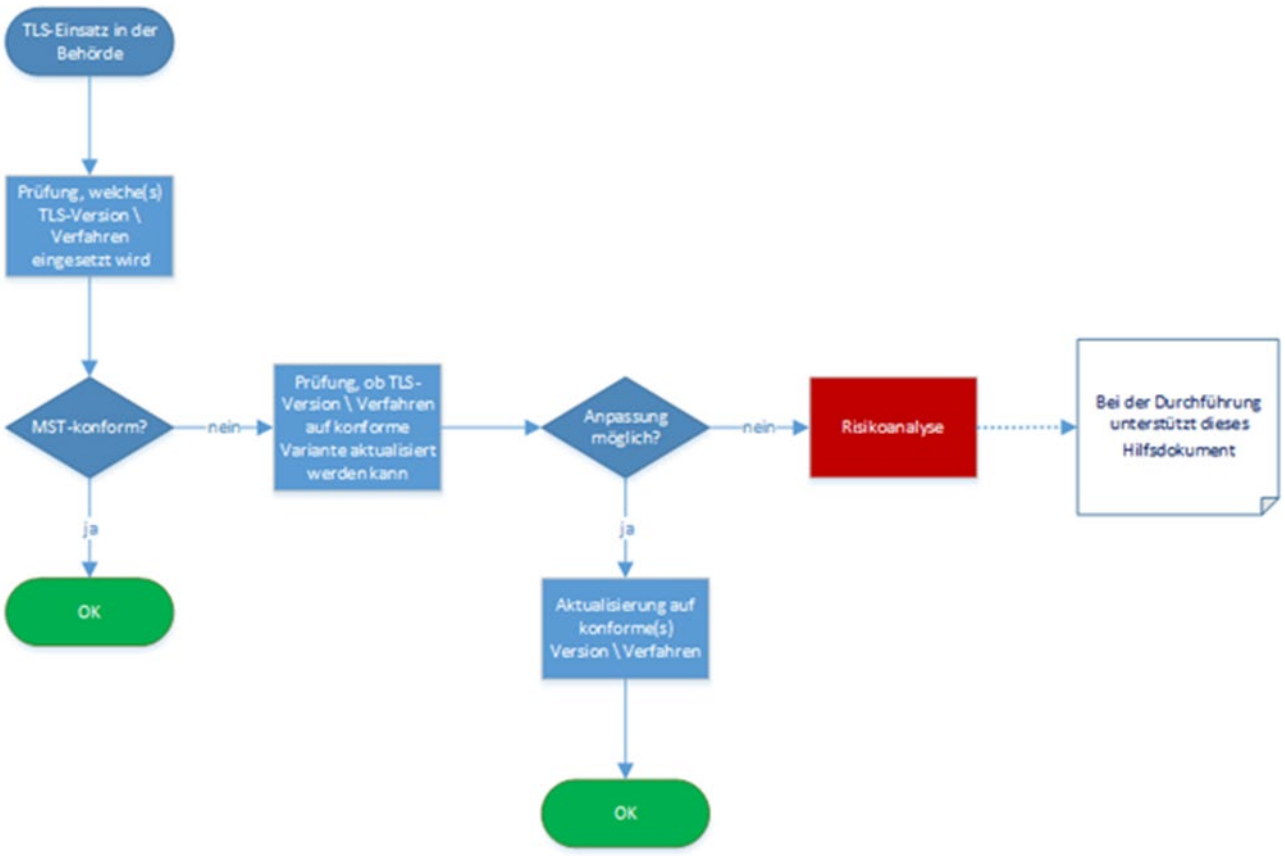

Abbildung 1: Vorgehensweise zur Erfüllung des MST-TLS

[9] Vgl. BSI-Standard 200-3 (BSI 2017b)
[10] Vgl. BSI-Standard 200-3 (BSI 2017b)
[11] Vgl. TR-02102-2 (BSI 2023b)

Zur Durchführung einer Risikoanalyse in Bezug auf die Verwendung von TLS empfiehlt sich, in Anlehnung an den BSI-Standard 200-3[12], folgende, im weiteren Text näher beschriebene, Vorgehensweise:

- Ermittlung der zu betrachtenden Zielobjekte (Kapitel 3.1)
- Erstellung einer Gefährdungsübersicht (Kapitel 3.2)
- Prüfung, ob für die eingesetzten Versionen/kryptografischen Verfahren Schwachstellen bekannt sind
- Betrachtung der elementaren Gefährdungen
- Analyse zusätzlicher Gefährdungen
- Einstufung von Risiken (Kapitel 3.3)
- Einschätzung von Risiken
- Bewertung von Risiken
- Behandlung von Risiken (Kapitel 3.4)

3.1 Ermittlung der zu betrachtenden Zielobjekte

Zur Ermittlung und Erfassung aller zu betrachtender Zielobjekte eines Informationsverbundes können z. B. folgende Verfahren, auch in Kombination, eingesetzt werden:

- Prüfung der für die Transportverschlüsselung relevanten Bausteine des IT-Grundschutzes (s. Kapitel 2)
- Sichtung der im Rahmen der Erstellung einer Sicherheitskonzeption nach IT-Grundschutz bereits durchgeführten und dokumentierten Strukturanalyse[13]
- Nachfragen bei Ansprechpersonen aus dem Bereich IT-Betrieb sowie bei Netz- und Verfahrensverantwortlichen

Die erfassten Zielobjekte können zur Arbeitserleichterung sinnvoll in Gruppen zusammengefasst werden. Im BSI Standard 200-2, Kapitel 8.1.1 (IT-Grundschutz-Methodik)[14] sind Kriterien für eine sinnvolle Gruppenbildung beschrieben.

So können z. B. Zielobjekte, die sich in einem nach außen und vom Produktionsnetz abgeschotteten, vor unbefugtem Zugriff geschützten Bereich befinden und die

- ähnlich in das Netz eingebunden sind (z. B. im gleichen Netzsegment) und
- ähnlichen administrativen und infrastrukturellen Rahmenbedingungen unterliegen,

als eine Gruppe betrachtet werden. Wurde im Rahmen der Erstellung eines Sicherheitskonzeptes bereits eine Gruppenbildung durchgeführt, so kann diese verwendet werden.

[12]Vgl. BSI-Standard 200-3 (BSI 2017b)
[13] Vgl. BSI Standard 200-2 (BSI 2017a)
[14] Vgl. BSI Standard 200-2 (BSI 2017a)

3.2 Erstellung einer Gefährdungsübersicht

Im nächsten Schritt der Risikoanalyse werden jedem erfassten Zielobjekt (bzw. jeder erfassten Gruppe) die relevanten Gefährdungen aus der Liste der elementaren Gefährdungen zugewiesen. Die Identifizierung der relevanten Gefährdungen muss aufgrund der heterogenen Systemlandschaft individuell von jeder Einrichtung durchgeführt werden.

Zur Ermittlung relevanter Gefährdungen beim Einsatz nicht konformer Versionen und/oder nicht konformer kryptografischer Verfahren ist zunächst zu prüfen, ob für diese Versionen und/oder kryptografischen Verfahren Schwachstellen bekannt sind. Dazu können z.B. folgende Quellen herangezogen werden:

- Warn- und Informationsdienst des CERT-Bund[15]
- Common Vulnerabilities and Exposures (CVE)[16]
- Fachpublikationen
- Herstellerdokumentationen

Zur Unterstützung bei der Feststellung von Gefährdungen werden in Kapitel 3.2.1 beispielhaft die derzeit bekannten Schwachstellen der Versionen TLS 1.0 und TLS 1.1 mit den entsprechenden kryptografischen Verfahren beschrieben. Darauf aufbauend können die elementaren Gefährdungen, die aufgrund dieser Schwachstellen relevant werden können, bestimmt werden.

Mit Veröffentlichung der RFC 8996 hat die Internet Engineering Taskforce (IETF) die Versionen TLS 1.0 und TLS 1.1 für veraltet (deprecated) erklärt.[17] Der Einsatz von TLS 1.0 und TLS 1.1 wird auf Grund mehrerer Schwachstellen auch in der TR-02102-2[18] nicht empfohlen.

3.2.1 Schwachstellen von TLS 1.0 und TLS 1.1

- In TLS 1.0 und TLS 1.1 können nur Signaturverfahren mit den Hashfunktionen MD-5 und SHA-1 für die Authentisierung im Handshake-Protokoll genutzt werden.[19,20] Diese Hashfunktionen sind anfällig für Kollisionsangriffe (zwei Eingaben erzeugen den gleichen Hashwert) und sind damit nicht fälschungssicher.[21 ,22, 23] Die Verwendung dieser Hashfunktionen zur Signierung von Zertifikaten kann dazu führen, dass TLS-Zertifikate durch Angriffe gefälscht werden. Dadurch kann es Angreifenden ermöglicht werden, aus einer Man-in-the-Middle-Position heraus den Datenverkehr von Kommunikationspartnern mitzulesen und zu manipulieren.

Durch das Ausnutzen weiterer Schwachstellen der TLS-Versionen 1.0 und 1.1 kann es Angreifenden ermöglicht werden, die Verschlüsselung teilweise aufzubrechen und somit an geheime Informationen zu gelangen. Die Vertraulichkeit der Informationen ist dadurch gefährdet.

- In TLS 1.0 werden für den CBC-Betriebsmodus (Cipher Block Chaining) vorhersagbare Initialisierungsvektoren (IV) gewählt.[24] Die TLS-Versionen 1.1 und höher sind nicht betroffen. Hier wird jedem Block ein zufällig gewählter Initialisierungsvektor vorangestellt. Beim CBC-Betriebsmodus

[15] Vgl. Warn- und Informationsdienst von CERT-Bund (BSI 2023d)
[16] Vgl. Common Vulnerabilities And Exposures (Mitre Corporation, 2023)
[17] Vgl. RFC 8996 (IETF 2021)
[18] Vgl. TR-02102-2 (BSI 2023b)
[19] Vgl. RFC 2246 (IETF 1999), Abschnitte 7.4.3 und 7.4.8
[20] Vgl. RFC 4346 (IETF 2006), Abschnitte 7.4.3 und 7.4.8
[21] Vgl. Short Chosen-Prefix Collisions for MD5 and the Creation of a Rogue CA Certificate (Stevens M. et al., 2009)
[22] Vgl. The First Collision for Full SHA-1 (Stevens M. et al., 2017)
[23] Vgl. SHA-1 is a Shambles - First Chosen-Prefix Collision on SHA-1 and Application to the PGP Web of Trust (Gaëtan Leurent and Thomas Peyrin, 2020)
[24] Vgl. RFC 2246 (IETF 1999), Abschnitte 6.1 und 6.2.3.2

werden Daten blockweise verschlüsselt. Der jeweils aktuelle Klartextblock wird vor seiner Chiffrierung mit dem Geheimtext des vorangegangenen Blocks XOR-verknüpft. Damit hängt das Resultat der Chiffrierung vom gerade verarbeiteten Klartextblock und von all seinen Vorgängern ab. Da der erste Block keinen Vorgängerblock hat, wird für diesen ein Initialisierungsvektor generiert. Dieser wird mit dem ersten Datenblock XOR- verknüpft. Vorhersagbare Initialisierungsvektoren erleichtern sogenannte Chosen-Plaintext Angriffe. Bei diesem Angriff werden frei gewählte Klartexte blockweise verschlüsseln. Durch den Vergleich der so erstellten Geheimtexte können Rückschlüsse auf unbekannte Klartexte gezogen werden. Bei zufällig generierten, also nicht vorhersagbaren Initialisierungsvektoren, ergibt die Verschlüsselung des gleichen Klartextes einen immer anderen Geheimtext. Eine Vergleichbarkeit der Geheimtexte wäre somit erschwert. Ein Beispiel für einen solchen durchgeführten Chosen-Plaintext-Angriff ist BEAST[25] (Browser Exploit Against SSL/TLS).

- Im CBC-Betriebsmodus verwendet TLS für die Verschlüsselung die Reihenfolge MAC-then-Encrypt (anstatt Encrypt-then-MAC). Dadurch können Padding-Oracle-Angriffe ermöglicht werden.[26] Zu einer sicheren Übertragung von Informationen gehören die Verschlüsselung der Informationen (Encrypt) und die Sicherstellung der Authentizität der Informationen (Message Authentication Code, MAC). Wichtig ist hier die Reihenfolge, in der Verschlüsselung und Authentifizierung stattfinden. Klassischerweise kombiniert TLS diese Verfahren in der Reihenfolge MAC-then-Encrypt. Dabei wird zunächst mittels HMAC[27] ein Authentifizierungstoken gebildet. Dieser wird an den zu verschlüsselnden Klartext gehängt. Die Nachricht und der HMAC-Token werden dann mittels eines Paddings[28] aufgefüllt und anschließend verschlüsselt. Das Padding ist demnach nicht durch den HMAC-Token geschützt. Angreifende können diesen Umstand ausnutzen, indem sie Geheimtexte manipulieren und anhand der zurückgegebenen Fehlermeldung herausfinden, ob das Padding oder die Überprüfung des HMAC-Hashes einen Fehler verursacht. In älteren Versionen verschickt TLS in diesen Fällen unterschiedliche Fehlermeldungen, aber auch unterschiedliche Antwortzeiten können Informationen darüber liefern.[29] So können Rückschlüsse auf den Klartext gezogen werden. Betroffen sind SSL und TLS bis Version 1.2, sofern eine Cipher Suite mit CBC verwendet wird. Alternativen zum CBC-Modus wie GCM oder CCM, die nicht anfällig für Padding-Oracle-Angriffe sind, können erst ab TLS 1.2 verwendet werden.
- In TLS 1.0 / TLS 1.1 ist die Implementierung der veralteten Cipher Suite TLS_DHE_DSS_WITH_3DES_EDE_CBC_SHA / TLS_RSA_WITH_3DES_EDE_CBC_SHA verpflichtend.[30] [31] Die Verwendung der enthaltenen 64-bit Blockchiffre Triple-DES (3DES) kann sogenannte Geburtstagsangriffe ermöglichen.[32] [33] Ziel dieser Angriffe ist es Kollisionen zwischen Geheimtextblöcken zu finden, also Geheimtexte zu finden, die gleich sind. Dadurch können Rückschlüsse auf den Klartext gezogen werden.

Diese beispielhaft aufgelisteten und beschriebenen Schwachstellen machen deutlich, warum der Mindeststandard auch das Deaktivieren dieser unsicheren TLS-Versionen und dieser unsicheren kryptografischen Verfahren fordert. Bleiben diese trotz des Einsatzes sicherer TLS-Versionen und sicherer kryptografischer Verfahren im Hintergrund aktiviert, so könnten unter Umständen sogenannte Downgrade-Angriffe erfolgreich durchgeführt werden. Beim Aufbau einer TLS-Verbindung zwischen

[25] Vgl. Here Come The XOR Ninjas (Duong, 2011)
[26] Vgl. Password Interception in a SSL/TLS Channel (Canvel et al., 2003)
[27] HMAC (Keyed-Hash Message Authentication Code): Message Authentication Code (MAC), dessen Konstruktion auf einer kryptografischen Hashfunktion basiert.
[28] In der Regel muss der letzte Block (beim Cipher Block Chaining, CBC) mit zusätzlichen Bytes aufgefüllt werden, da der Klartext ein Vielfaches der Blocklänge sein muss. Dieses Auffüllen wird als Padding bezeichnet.
[29] Vgl. Breaking the TLS and DTLS Record Protocols (AlFardan, Paterson, 2013)
[30] Vgl. RFC 2246 (IETF 1999), Kapitel 9
[31] Vgl. RFC 4346 (IETF 2006), Kapitel 9
[32] Der Name beruht auf dem statistischen Phänomen, dass bereits in einer sehr kleinen Gruppe wenigstens zwei Personen mit 50%iger Wahrscheinlichkeit am gleichen Tag Geburtstag haben.
[33] Vgl. On the Practical (In-)Security of 64-bit Block Ciphers (Karthikeyan Bhargavan, Gaëtan Leuren, 2016)

einem Client und einem Server oder einem Dienst werden Verbindungsparameter ausgehandelt. Dabei wird versucht, eine Verbindung mit der höchsten unterstützten Protokollversion aufzubauen. Schlägt dieser Versuch fehl, wird versucht, die Verbindung mit einer älteren Protokollversion aufzubauen. Durch gezielte Verbindungsstörungen können Angreifende somit den Aufbau einer Verbindung mit einer älteren unsicheren Protokollversion provozieren und anschließend die daraus resultierenden Sicherheitslücken dieser Verbindung ausnutzen (z. B. POODLE).[34]

3.2.2 Elementare Gefährdungen

Die in Kapitel 3.2.1 beschriebenen Angriffe konnten bereits größtenteils praktisch demonstriert werden. Durch den Einsatz unsicherer TLS-Versionen oder unsicherer kryptografischer Verfahren wird es Angreifenden erleichtert, sich z. B. durch Man-in-the-Middle-Angriffe unbefugten Zugriff auf Informationen zu verschaffen. Durch Ausnutzung von Schwachstellen unsicherer Versionen und/oder unsicherer kryptografischer Verfahren kann es Angreifenden ermöglicht werden, verschlüsselte Informationen im Klartext zu lesen.

Implementierungen unsicherer TLS-Versionen und/oder unsicherer kryptografischer Verfahren sollten demnach mindestens auf ihre Verwundbarkeit gegenüber bekannten Schwachstellen untersucht werden.

Daraus resultierend sind beim Einsatz dieser TLS-Versionen und kryptografischen Verfahren mindestens die im Folgenden aufgelisteten elementaren Gefährdungen für die entsprechenden Zielobjekte zu betrachten. Dem IT-Grundschutz folgend, betreffen die Gefährdungen dabei hauptsächlich folgende Schutzziele: Vertraulichkeit (C), Integrität (I) und Verfügbarkeit (A).[35]

- G 0.14 Ausspähen von Informationen (Spionage) (C)

Beispiel: Bei Verwendung einer unsicheren TLS-Version können Angreifende per Man-in-the-Middle-Angriff übertragene Daten unbefugt auslesen. Die Vertraulichkeit der Informationen ist damit gefährdet.

- G 0.15 Abhören (C)

Beispiel: s. G 0.14

- G 0.18 Fehlplanung oder fehlende Anpassung (C, I, A)

Beispiel: Schon bei der Planung eines IT-Verfahrens muss darauf geachtet werden, geeignete und sichere Übertragungsprotokolle auszuwählen. Ansonsten werden Angriffsflächen durch den Einsatz eines unsicheren Protokolls geboten, die zu einer Gefährdung der Vertraulichkeit, der Integrität und der Authentizität der übertragenen Informationen führen können. Das bedeutet auch, dass bei bestehenden Systemen mit unsicheren Protokollen eine Anpassung auf ein aktuelles, sicheres Transport-Verschlüsselungsprotokoll vorgenommen werden sollte.

- G 0.19 Offenlegung schützenswerter Informationen (C)

Beispiel: Vertrauliche Informationen müssen vor Offenlegung geschützt werden. Die Gefahr der Offenlegung dieser Informationen durch Angriffe besteht besonders bei der Übertragung von Daten, wenn diese nur unzureichend durch unsichere Transport-Verschlüsselungsprotokolle abgesichert wird.

- G 0.22 Manipulation von Informationen (I)

Beispiel: Beim Einsatz eines unsicheren Transport-Verschlüsselungsprotokolls ist es durch einen Angriff aus der Man-in-the-Middle-Position heraus möglich, übertragene Daten zu manipulieren. Durch einen solchen Angriff können z.B. Inhalte von Webseiten verändert oder auch unerwünschte Inhalte hinzugefügt werden. Die Integrität der Informationen ist damit gefährdet.

[34] Vgl. This POODLE Bites: Exploiting The SSL 3.0 Fallback (Möller, Duong, Kotowicz, 2014)
[35] Vgl. BSI-Standard 200-3 (BSI 2017b)

- G 0.23 Unbefugtes Eindringen in IT-Systeme (C, I)

Beispiel: Sobald es Angreifenden durch Ausnutzung von Schwachstellen eines unsicheren Transport-Verschlüsselungsprotokolls gelungen ist, schützenswerte Informationen zu erhalten, können sie mit Hilfe dieser Informationen eventuell in weitere IT-Systeme eindringen. Beispiele für schützenswerte Informationen sind Benutzername und Passwort.

- G 0.30 Unberechtigte Nutzung oder Administration von Geräten und Systemen (C, I, A)

Beispiel: s. G 0.23

- G 0.43 Einspielen von Nachrichten (C, I)

Beispiel: Angreifende in einer Man-in-the-Middle-Position können unbemerkt eine Vermittlungsposition in der Kommunikation zwischen verschiedenen Teilnehmern einnehmen. In der Regel täuschen sie hierzu der absendenden Person einer Nachricht vor, die eigentliche empfangende Person zu sein, und sie täuschen der empfangenden Person vor, die eigentliche absendende Person zu sein. Wenn dies gelingt, können die Angreifenden dadurch Nachrichten, die nicht für sie bestimmt sind, entgegennehmen und vor der Weiterleitung an die eigentliche empfangende Person auswerten und gezielt manipulieren. Die Vertraulichkeit und die Integrität der Informationen sind damit gefährdet.

- G 0.46 Integritätsverlust schützenswerter Informationen (I)

Beispiel: s. G.018, G.022, G.023, G.030

3.2.3 Betrachtung zusätzlicher Gefährdungen

Für die zu betrachtenden Zielobjekte kann es zusätzliche Gefährdungen geben, die über die elementaren Gefährdungen hinausgehen und sich aus dem spezifischen Einsatzszenario oder dem spezifischen Anwendungsfall ergeben. Diese Gefährdungen müssen von jeder Einrichtung individuell identifiziert, und nach dem in Kapitel 3.3 beschriebenen Verfahren eingeschätzt und bewertet werden. Hilfestellung zur Ermittlung zusätzlicher Gefährdungen gibt der im BSI-Standard 200-3 (Kapitel 4.2 und 9.3).[36]

3.3 Einstufung von Risiken

Nachdem die Gefährdungen für die jeweiligen Zielobjekte identifiziert wurden, müssen die Risiken, die von diesen Gefährdungen ausgehen, eingeschätzt und bewertet werden.

Um das Risiko einzuschätzen, das von einer Gefährdung ausgeht, muss ermittelt werden, wie häufig diese Gefährdung eintreten kann. In Bezug auf den Einsatz von unsicheren TLS-Versionen und/oder unsicheren kryptografischen Verfahren spielen bei der Einschätzung der Eintrittshäufigkeit mehrere Faktoren eine Rolle, z. B.

- Steht das entsprechende IT-System z. B. für die Öffentlichkeit zugänglich im Internet ist die Eintrittswahrscheinlichkeit höher einzustufen als für ein IT-System, das abgeschottet in einem vom Produktionsnetz abgetrennten Testnetz steht.
- Werden risikomindernde Maßnahmen (s. Kapitel 3.3.1) eingesetzt, so ist die Eintrittswahrscheinlichkeit niedriger einzustufen, als bei einem nicht in dieser Hinsicht ‚optimierten' IT-System.

Zur Einschätzung des Risikos gehört auch die Beurteilung des Schadens, den der Eintritt der Gefährdung verursachen kann. Auch hier müssen verschiedene Faktoren berücksichtigt werden, z. B.

- Ist nach einem Angriff die Arbeitsfähigkeit der Einrichtung gefährdet?
- Können schützenwerte Informationen an die Öffentlichkeit gelangen?
- Kann durch einen Angriff das Ansehen der Einrichtung geschädigt werden?

[36] Vgl. BSI-Standard 200-3 (BSI 2017b)

Der BSI-Standard 200-2[37] beschreibt Schadensszenarien mit beispielhaften Fragestellungen.

Eine detaillierte Beschreibung der Vorgehensweise liefert der BSI-Standard 200-3.[38] Dort gibt es Vorlagen für die Kategorisierung der Eintrittshäufigkeit und auch für die Festlegung der Schadenshöhe. Diese Vorlagen sollten von jeder Einrichtung individuell auf ihre spezifischen Gegebenheiten angepasst werden.

3.3.1 Bewertung von Risiken

Das eingeschätzte Risiko muss von jeder Einrichtung individuell bewertet werden. Dazu bietet der BSI-Standard 200-3[39] eine Vorlage zur Definition von Risikokategorien. Diese Vorlage sollte von jeder Einrichtung auf ihre spezifischen Gegebenheiten angepasst werden.

Als risikomindernd könnten dabei z. B. die nachgestellten Maßnahmen sowie das Betreiben der entsprechenden Anwendung in einem abgeschotteten Netz (z. B. in einem physisch vom Produktionsnetz abgetrennten Testnetz mit festgelegten Zutritts-, Zugangs- und Zugriffsregelungen anhand definierter Berechtigungen) angeführt werden.

- Verzicht auf JavaScript:

JavaScript ist eine eigene Programmiersprache. Sie kann in Webseiten eingebunden werden und so aktive Inhalte ermöglichen. Dadurch können Webseiten funktional gestaltet werden und das dynamische Verändern von Inhalten wird ermöglicht (z. B. bewegte Bilder, auf Anwenderaktionen reagierende Grafiken, Anzeige von Dialogfenstern, etc.). Der jeweilige Programmcode wird dabei auf Rechner der Anwendenden heruntergeladen und auch dort ausgeführt. Bösartiger Code kann dabei diese Rechner kompromittieren und Informationen abgreifen.

- Abschalten von Session Renegotiation:

Session Renegotiation ist eine Neuaushandlung der Parameter einer bestehenden HTTPS-Sitzung. Nach dem Aufbau einer verschlüsselten Verbindung zwischen Server und Client kann jede Seite eine Session Renegotiation initialisieren, die vollständig im verschlüsselten Kanal abläuft. Dabei besteht keine logische Verbindung zwischen der verschlüsselten Anfrage vor und nach der Session Renegotiation. Das heißt, durch einen Man-in-the-Middle-Angriff kann versucht werden, beliebige Inhalte in eine existierende HTTPS-Sitzung einzufügen. Im Request for Comments (RFC) 5746[40] werden der Hintergrund der Schwachstelle bei der Neuaushandlung von HTTPS-Verbindungen sowie die entsprechenden Gegenmaßnahmen beschrieben.

- Abschalten von Session Resumption:

Session Resumption dient der Beschleunigung der Wiederaufnahme einer Verbindung. Bei der Wiederaufnahme der Verbindung erfolgt hier keine Neuaushandlung der Parameter. Das kann dazu führen, dass Verbindungen nachträglich entschlüsselt werden können, was durch Forward Secrecy eigentlich verhindert werden sollte. Session Resumption kann über Session IDs oder Session Tickets erfolgen. Bei der Verwendung von Session IDs speichert der Server die TLS-Verbindungsdaten in einem Cache und liest sie wieder ein, sobald der Client sich wieder meldet. Beim Einsatz von Session Tickets verschlüsselt der Server die TLS-Verbindungsdaten mit einem Schlüssel und schickt diese dem Client. Sobald der Client sich wieder mit dem Server verbindet, gibt er dem Server das Ticket. Angreifende können, wenn sie Zugriff auf den Server erhalten, den Session Cache oder den Ticket Schlüssel auslesen und damit alle entsprechenden Verbindungen nachträglich entschlüsseln.

- Abschalten von TLS-Kompression:

Unter TLS-Kompression wird die Möglichkeit verstanden, die zu übertragenden Daten vor der Verschlüsselung zu komprimieren. Wenn Angreifende Teile des Klartextes wählen können, so lässt die

[37] Vgl. BSI-Standard 200-2 (BSI 2017a)
[38] Vgl. BSI-Standard 200-3 (BSI 2017b)
[39] Vgl. BSI-Standard 200-3 (BSI 2017b)
[40] Vgl. RFC 5746 (IETF 2010)

Größe der komprimierten Nachricht Rückschlüsse auf den den Angreifenden unbekannten Teil des Klartextes zu. Dadurch kann die Verwendung von TLS-Kompression Angriffe wie CRIME[41] [42] ermöglichen.

3.4 Behandlung von Risiken

Im Anschluss an die Risikobewertung muss, entsprechend der in der Einrichtung geltenden Richtlinien zur Risikobehandlung, der Umgang mit den bewerteten Risiken festgelegt werden. Ziel sollte dabei sein, das Risiko, welches durch den Einsatz von nicht zum Mindeststandard konformen TLS-Versionen und/oder nicht konformen kryptografischen Verfahren besteht, vollständig zu vermeiden. Da Angriffe auf Schwachstellen sich weiterentwickeln können, bietet der ausschließliche Einsatz von als sicher geltenden TLS-Versionen und -Verfahren den besten Schutz. Sollten die Risiken nicht vermieden, sondern durch mitigierende Maßnahmen nur reduziert werden können, so muss das Restrisiko, wie im Kapitel 3.2.3 des UP-Bund[43] vorgegeben, dokumentiert, der jeweiligen Leitung der Einrichtung bekannt gemacht und von dieser getragen werden.

[41] CRIME: Compression Ratio Info-leak Made Easy
[42] Vgl. The CRIME attack, Ekoparty (Duong, 2012)
[43] Vgl. UP-Bund (BMI 2017)

Literaturverzeichnis

AlFardan, Paterson (2013)	Lucky Thirteen: Breaking the TLS and DTLS Record Protocols. IEEE Symposium on Security and Privacy : s.n., 2013
BMI (2017)	Bundesministerium des Innern und für Heimat: Umsetzungsplan Bund 2017 (UP-Bund 2017), https://www.bmi.bund.de/SharedDocs/downloads/DE/publikationen/themen/it-digitalpolitik/up-bund-2017.html, abgerufen am 25.05.2023
BSI (2017a)	Bundesamt für Sicherheit in der Informationstechnik: BSI-Standard 200-2 – IT-Grundschutz-Methodik, Version 1.0, 2017, https://www.bsi.bund.de/dok/10027846, abgerufen am 25.05.2023
BSI (2017b)	Bundesamt für Sicherheit in der Informationstechnik: BSI-Standard 200-3 – Risikoanalyse auf der Basis von IT-Grundschutz, Version 1.0, 2017, https://www.bsi.bund.de/dok/407502, abgerufen am 25.05.2023
BSI (2023a)	Bundesamt für Sicherheit in der Informationstechnik: Mindeststandard zur Verwendung von Transport Layer Security V2.4, https://www.bsi.bund.de/dok/1086002, abgerufen am 25.05.2023
BSI (2023b)	Bundesamt für Sicherheit in der Informationstechnik: TR 02102-2: Kryptographische Verfahren: Empfehlungen und Schlüssellängen, Teil 2 – Verwendung von Transport Layer Security (TLS), Version 2023-01, https://www.bsi.bund.de/dok/433400, abgerufen am 25.05.2023
BSI (2023c)	Bundesamt für Sicherheit in der Informationstechnik: IT-Grundschutz-Kompendium, Edition 2023, https://www.bsi.bund.de/dok/1073656, abgerufen am 25.05.2023
BSI (2023d)	Bundesamt für Sicherheit in der Informationstechnik: Warn- und Informationsdienst von CERT-Bund, https://wid.cert-bund.de/portal/wid/start, abgerufen am 25.05.2023
Canvel et al. (2003)	Password Interception in a SSL/TLS Channel, CRYPTO 2003
Duong (2011)	Here Come The XOR Ninjas
Duong (2012)	The CRIME attack, Ekoparty 2012
Gaëtan Leurent and Thomas Peyrin (2020)	SHA-1 is a Shambles - First Chosen-Prefix Collision on SHA-1 and Application to the PGP Web of Trust, https://eprint.iacr.org/2020/014, abgerufen am 25.05.2023

IETF (1999)	The TLS Protocol Version 1.0, Dierks 1999, https://datatracker.ietf.org/doc/html/rfc2246, abgerufen am 25.05.2023
IETF (2006)	The Transport Layer Security (TLS) Protocol Version 1.1, Dierks. 2006, https://datatracker.ietf.org/doc/html/rfc4346, abgerufen am 25.05.2023
IETF (2010)	Transport Layer Security (TLS) Renegotiation Indication Extension, https://datatracker.ietf.org/doc/html/rfc5746, abgerufen am 25.05.2023
IETF (2012)	HTTP Strict Transport Security (HSTS), https://datatracker.ietf.org/doc/html/rfc6797, abgerufen am 25.05.2023
IETF (2021)	Deprecating TLS 1.0 and TLS 1.1, https://datatracker.ietf.org/doc/html/rfc8996, abgerufen am 25.05.2023
Karthikeyan Bhargavan, Gaëtan Leuren (2016)	On the Practical (In-)Security of 64-bit Block Ciphers. CCS 2016.
Mitre Corporation (2023)	Common Vulnerabilities and Exposures, https://cve.mitre.org/cve/, abgerufen am 25.05.2023
Möller, Duong, Kotowicz (2014)	This POODLE Bites: Exploiting The SSL 3.0 Fallback
Stevens M. et al. (2009)	Short Chosen-Prefix Collisions for MD5 and the Creation of a Rogue CA Certificate. In: Halevi, S. (eds) Advances in Cryptology - CRYPTO 2009. CRYPTO 2009. Lecture Notes in Computer Science, vol 5677. Springer, Berlin, Heidelberg. https://doi.org/10.1007/978-3-642-03356-8_4, abgerufen am 25.05.2023
Stevens M. et al. (2017)	Stevens, M., Bursztein, E., Karpman, P., Albertini, A., Markov, Y. (2017). The First Collision for Full SHA-1. In: Katz, J., Shacham, H. (eds) Advances in Cryptology – CRYPTO 2017. CRYPTO 2017. Lecture Notes in Computer Science(), vol 10401. Springer, Cham. https://doi.org/10.1007/978-3-319-63688-7_19, abgerufen am 25.05.2023

Abkürzungsverzeichnis

A	Availability (Schutzziel Verfügbarkeit)
BEAST	Browser Exploit Against SSL/TLS
BSI	Bundesamt für Sicherheit in der Informationstechnik
BSIG	Gesetz über das Bundesamt für Sicherheit in der Informationstechnik
C	Confidentiality (Schutzziel Vertraulichkeit)
CBC	Cipher Block Chaining
CCM	Counter with CBC-MAC
CERT	Computer Emergency Response Team
CRIME	Compression Ratio Info-leak Made Easy
CVE	Common Vulnerabilities and Exposures
DoS	Denial-of-Service
ERP	Enterprise Resource Planning
GCM	Galois/Counter Mode
HMAC	Keyed-Hash Message Authentication Code
HSTS	HTTP Strict Transport Security
HTTP	Hypertext Transfer Protocol
HTTPS	Hypertext Transfer Protocol Secure
I	Integrity (Schutzziel Integrität)
IETF	Internet Engineering Taskforce
IPsec	Internet Protocol Security
IV	Initialisierungsvektoren
MAC	Message Authentication Code
MD-5	Message-Digest Algorithm 5
MST-TLS	Mindeststandards des BSI zur Verwendung von Transport Layer Security
PFS	Perfect Forward Secrecy
POODLE	Padding Oracle On Downgraded Legacy Encryption
RFC	Request for Comments
RSF	Remote Support Facility
SAP-ERP	Enterprise Resource Planning
SHA-1	Secure Hash Algorithm 1
SNC	Secure Network Communications
SNMP	Simple Network Management Protocol
SSL	Secure Sockets Layer

SOA	Serviceorientierte Architektur
TLS	Transport Layer Security
TR	Technische Richtlinie
Triple-DES (3DES)	Triple Data Encryption Algorithm
VPN	Virtual Private Network
XOR	eXclusive OR