Bundesamt
für Sicherheit in der
Informationstechnik

Deutschland
Digital•Sicher•BSI•

Mindeststandard des BSI für Schnittstellenkontrollen

nach § 8 Absatz 1 Satz 1 BSIG – Version 1.3 vom 07.07.2021

Änderungshistorie

Version	*Datum*	*Beschreibung*
1.0	16.11.2016	Erste Version des Mindeststandards
1.1	28.11.2017	Redaktionelle Anpassungen
1.2	14.01.2020	Redaktionelle Anpassungen, Anpassungen an aktualisierten Grundschutz
1.3	07.07.2021	Redaktionelle Anpassungen

Tabelle 1: Versionsgeschichte des Mindeststandards für Schnittstellenkontrollen. Eine ausführliche Änderungsübersicht zum Mindeststandard erhalten Sie unter: https://www.bsi.bund.de/dok/453464

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

Vorwort

Das Bundesamt für Sicherheit in der Informationstechnik (BSI) erarbeitet Mindeststandards für die Sicherheit der Informationstechnik des Bundes auf der Grundlage des § 8 Abs. 1 BSIG. Als gesetzliche Vorgabe definieren Mindeststandards ein konkretes Mindestniveau für die Informationssicherheit. Der Umsetzungsplan Bund 2017 legt fest, dass die Mindeststandards des BSI auf Basis § 8 Abs. 1 BSIG zu beachten sind.[1] Die Definition erfolgt auf Basis der fachlichen Expertise des BSI in der Überzeugung, dass dieses Mindestniveau in der Bundesverwaltung nicht unterschritten werden darf. Der Mindeststandard richtet sich primär an IT-Verantwortliche, IT-Sicherheitsbeauftragte (IT-SiBe)[2] und IT-Betriebspersonal.

IT-Systeme sind in der Regel komplex und in ihren individuellen Anwendungsbereichen durch die unterschiedlichsten (zusätzlichen) Rahmenbedingungen und Anforderungen gekennzeichnet. Daher können sich in der Praxis regelmäßig höhere Anforderungen an die Informationssicherheit ergeben, als sie in den Mindeststandards beschrieben werden. Aufbauend auf den Mindeststandards sind diese individuellen Anforderungen in der Planung, der Etablierung und im Betrieb der IT-Systeme zusätzlich zu berücksichtigen, um dem jeweiligen Bedarf an Informationssicherheit zu genügen. Die Vorgehensweise dazu beschreiben die IT-Grundschutz-Standards des BSI.

Zur Sicherstellung der Effektivität und Effizienz in der Erstellung und Betreuung von Mindeststandards arbeitet das BSI nach einer standardisierten Vorgehensweise. Zur Qualitätssicherung durchläuft jeder Mindeststandard mehrere Prüfzyklen einschließlich des Konsultationsverfahrens mit der Bundesverwaltung.[3] Über die Beteiligung bei der Erarbeitung von Mindeststandards hinaus kann sich jede Stelle des Bundes auch bei der Erschließung fachlicher Themenfelder für neue Mindeststandards einbringen oder im Hinblick auf Änderungsbedarf für bestehende Mindeststandards Kontakt mit dem BSI aufnehmen. Einhergehend mit der Erarbeitung von Mindeststandards berät das BSI die Stellen des Bundes[4] auf Ersuchen bei der Umsetzung und Einhaltung der Mindeststandards.

[1] Vgl. Umsetzungsplan Bund 2017 (BMI 2017), S. 4
[2] Analog „Informationssicherheitsbeauftragter (ISB)“
[3] Siehe FAQ zu den Mindeststandards (BSI 2021a)
[4] Zur besseren Lesbarkeit wird im weiteren Verlauf für „Stelle des Bundes“ der Begriff „Einrichtung“ verwendet.

Inhalt

1 Beschreibung

Der vorliegende Mindeststandard fordert die Kontrolle von externen Schnittstellen[5] von IT-Systemen[6] der Bundesverwaltung. Somit können die Schnittstellen, im Sinne der IT-Sicherheit, angemessen überwacht werden und Aktionen und Datenfluss können nachvollziehbar protokolliert werden. Die Schnittstellenkontrolle (SSK) regelt Registrierung, Freigabe, Blockierung und Protokollierung des Zugriffs von Daten, Applikationen und Geräten[7]. Sie gewährt die Umsetzung einer Sicherheitsrichtlinie für Schnittstellen nach dem Stand der Technik. Zu diesem Zweck können betriebssystemeigene Lösungen, organisatorische Maßnahmen oder Softwareprodukte von Drittherstellern -auch in Kombination - eingesetzt werden. Wird eine Softwarelösung zur Schnittstellenkontrolle genutzt, gibt dieser Standard Mindestsicherheitsanforderungen vor, die die Einrichtungen bei Beschaffung und Betrieb unterstützen.

Weitere Schutzmaßnahmen, wie etwa physische Beschränkungen, werden in diesem Mindeststandard nicht betrachtet. Auch Risiken, die direkt auf das Bussystem des IT-Systems zielen und derart auf andere angeschlossene Komponenten zugreifen, liegen außerhalb des Geltungsbereichs des Mindeststandards.[8]

Dieser Mindeststandard gibt Maßnahmen vor, um gängige Risiken zu reduzieren oder zu vermeiden. Auch bei Nutzung einer Schnittstellenkontrolle, die diesen Mindeststandard erfüllt, verbleiben Risiken, die in diesem Mindeststandard nicht betrachtet werden (z. B. Attacken direkt auf Hardware-Niveau, Angriff via DMA). Die in diesem Mindeststandard definierten Sicherheitsanforderungen bieten keinen vollständigen Schutz gegen alle denkbaren Angriffsszenarien. Das bedeutet jedoch nicht, dass die Einrichtung keinerlei Maßnahmen gegen diese Risiken zu ergreifen hat. Vielmehr muss die Einrichtung entsprechende technische, organisatorische (z. B. Dienstanweisungen) oder physische Maßnahmen gemäß eigener Risikoabschätzung zur Behandlung der verbleibenden Risiken auswählen und umsetzen. Beispiele für physische Maßnahmen sind:

- Ausschluss nicht benötigter Schnittstellen bei der Beschaffung,
- Entfernen nicht benötigter Schnittstellen,
- Verschließen von Schnittstellenanschlüssen.

Die Entscheidung zum Umgang mit diesen Risiken ist zu dokumentieren und von der Hausleitung mitzutragen.

Zur Umsetzung des Mindeststandards ist zu prüfen, ob die umgesetzten Maßnahmen zur Schnittstellenkontrolle alle Sicherheitsanforderungen (siehe Kapitel 2) vollständig erfüllen. Grundsätzlich lassen sich viele Regelungen auch durch z. B. entsprechende Konfigurationen der Betriebssysteme, bestehende Sicherheitslösungen oder organisatorische sowie andere technische Maßnahmen umsetzen. Gegebenenfalls müssen noch ergänzende Softwareprodukte beschafft werden. Eigene Prüfungen nach Teststellung und Installation in einer dem geplanten Einsatzszenario entsprechenden Umgebung werden empfohlen.

---

[5] Im Sinne des Mindeststandards: Externe Schnittstellen nach Stand der Technik, insbesondere USB, LAN, WLAN, Mobilfunk, Bluetooth, eSATA, PCMCIA, Firewire, Express-Card, Thunderbolt, NFC, Smartcard

[6] Computer mit dynamischer Gerätekonfiguration; dazu zählen bspw. Arbeitsplatzrechner, virtuelle Maschinen, Thin Clients/Remote Desktops, Laptops, mobile Kommunikationsgeräte sowie Server in normalen Büroumgebungen. Server, die in gemäß Grundschutz des BSI abgesicherten Serverräumen und abgeschlossenen Serverschränken betrieben werden, können auch über entsprechende Zugangskonzepte gesichert werden, müssen aber grundsätzlich ebenfalls alle aufgeführten Maßnahmen abdecken. Dies gilt ebenso für administrative Arbeitsplätze im Bereich Remote-Desktop bzw. Kernel-based Virtual Machine (KVM), die lokal angeschlossene Geräte an andere Systeme weiterreichen können.

[7] Im Sinne des Mindeststandards: Alle an externe Schnittstellen angeschlossene Geräte (z. B. Speichermedien, Ein-/Ausgabegeräte, Gadgets) außer weiterer IT-Systeme

[8] Z. B. direktes Schreiben in den Arbeitsspeicher via Direct Memory Access (DMA), wie es etwa bei Serial AT Attachment (S-ATA)-Schnittstellen möglich ist

In Anlehnung an den IT-Grundschutz[9] werden die Sicherheitsanforderungen mit den Modalverben MUSS und SOLLTE sowie den zugehörigen Verneinungen formuliert. Darüber hinaus wird das Modalverb KANN für ausgewählte Prüfaspekte verwendet. Die hier genutzte Definition basiert auf RFC 2119[10] und DIN 820-2: 2018[11].

MUSS / DARF NUR

bedeutet, dass diese Anforderung zwingend zu erfüllen ist. Das von der Nichtumsetzung ausgehende Risiko kann im Rahmen einer Risikoanalyse nicht akzeptiert werden.

DARF NICHT / DARF KEIN

bedeutet, dass etwas zwingend zu unterlassen ist. Das durch die Umsetzung entstehende Risiko kann im Rahmen einer Risikoanalyse nicht akzeptiert werden.

SOLLTE

bedeutet, dass etwas umzusetzen ist, es sei denn, im Einzelfall sprechen gute Gründe gegen eine Umsetzung. Bei einem Audit muss die Begründung vom Auditor auf ihre Stichhaltigkeit geprüft werden können.

SOLLTE NICHT / SOLLTE KEIN

bedeutet, dass etwas zu unterlassen ist, es sei denn, es sprechen gute Gründe für eine Umsetzung. Bei einem Audit muss die Begründung vom Auditor auf ihre Stichhaltigkeit geprüft werden können.

KANN

bedeutet, dass die Umsetzung oder Nicht-Umsetzung optional ist und ohne Angabe von Gründen unterbleiben kann.

[9] Vgl. BSI-Standard 200-2 (BSI 2017), S. 18
[10] Vgl. Key words for use in RFCs (IETF 1997)
[11] Vgl. DIN-820-2: Gestaltung von Dokumenten (DIN 2018)

2 Sicherheitsanforderungen

Nachfolgend werden Sicherheitsanforderungen an das Produkt gestellt (Kapitel 2.1). Darauf folgen Sicherheitsanforderungen an den Betrieb (Kapitel 2.2).

2.1 Sicherheitsanforderungen an das Produkt

SSK.2.1.01: Vertrauenswürdiger Kanal

a) Die Schnittstellenkontrolle MUSS einen gesicherten Kanal zu Administrationszwecken und zur Übertragung der Protokollierungsdaten bereitstellen.

b) Die Schnittstellenkontrolle MUSS die jeweils gültige Version des Mindeststandards des BSI „Verwendung von Transport Layer Security“[12] mit gegenseitiger zertifikatsbasierter Authentisierung oder Mechanismen mindestens gleicher Stärke (siehe jeweils gültige Versionen von TR-02102-1[13], TR-02102-3[14], TR-02102-4[15]) zum Schutz der Integrität, Authentizität und Vertraulichkeit des Administrationskanals unterstützen.

SSK.2.1.02: Identifikation und Authentisierung der Benutzer

Die Benutzeridentifikation/-authentisierung stellt sicher, dass der Zugriff auf Ressourcen und Schnittstellen entsprechend der Vorgaben (Richtlinien, Policies) des Betriebssystems im Zusammenwirken mit der Schnittstellenkontrolle umgesetzt wird.

a) Die Schnittstellenkontrolle MUSS eine Benutzeridentifikation/-authentisierung durchführen. Diese KANN auch mittels Single Sign-on, etwa über die Benutzeranmeldung am Betriebssystem umgesetzt werden.

b) Nur nach erfolgreicher Benutzeridentifikation/-authentisierung des Administrators DÜRFEN Anpassungen an der Konfiguration der Schnittstellenkontrolle durch einen Administrator möglich sein.

SSK.2.1.03: Identifikation der Geräte

a) Die Schnittstellenkontrolle MUSS die eindeutige Identifizierung einzelner Geräte leisten; bei USB-Devices etwa anhand von Geräteklasse, Vendor-ID[16] und Hardware-ID[17].

SSK.2.1.04: Identifikation der Daten

a) Die Schnittstellenkontrolle MUSS Daten auf angeschlossenen Geräten anhand ihrer Metadaten (etwa Dateiendung, Dateisignatur/Magic Number) identifizieren können.

b) Die Schnittstellenkontrolle MUSS die Identifizierung von geschachtelten bzw. eingebetteten (unverschlüsselten) Daten gewährleisten; zum Beispiel anhand von Dateisignatur und -endung.

c) Die Schnittstellenkontrolle MUSS die Definition individueller Dateiformate zulassen; beispielsweise um Dateien interner Fachanwendungen in die Schnittstellenkontrolle zu integrieren.

SSK.2.1.05: Autonome Arbeitsweise

a) Wenn die Schnittstellenkontrolle ihre Konfiguration von anderen IT-Systemen (Servern) bezieht, MUSS diese auch nach Trennung von jenen IT-Systemen funktionsfähig bleiben.

b) Freigaben MÜSSEN auch im Offline-Betrieb geschützter Rechner eingerichtet werden können, beispielsweise durch telefonische/schriftliche Challenge-Response-Verfahren.

---

[12] Vgl. Mindeststandard des BSI zur Verwendung von TLS (BSI 2021b)
[13] Vgl. TR-02102-1: “Kryptographische Verfahren: Empfehlungen und Schlüssellängen“ (BSI 2021c)
[14] Vgl. TR-02102-3: “Kryptographische Verfahren: Empfehlungen und Schlüssellängen, Teil 3 (BSI 2021d)
[15] Vgl. TR-02102-4: „Kryptographische Verfahren: Empfehlungen und Schlüssellängen, Teil 4 (BSI 2021e)
[16] Vendor-Identifikator
[17] Hardware-Identifikator

SSK.2.1.06: Schnittstellen

a) Die Schnittstellenkontrolle MUSS die Erkennung und Behandlung der nach dem Stand der Technik offerierten Schnittstellen ermöglichen. Alle anderen SOLLTEN gesperrt werden (Whitelisting).

SSK.2.1.07: Applikationen

a) Die Schnittstellenkontrolle MUSS die Ausführung von Programmen und Skripten, die sich auf den angeschlossenen Geräten im Sinne dieses Standards befinden, steuern[18], überwachen und protokollieren.

SSK.2.1.08: Daten

a) Die Schnittstellenkontrolle MUSS den Zugriff auf Daten, die sich auf einem Gerät befinden, steuern, überwachen und protokollieren.

SSK.2.1.09: Management von Sicherheitsattributen

a) Die Schnittstellenkontrolle MUSS gemäß Regelwerk

- eine granulare Einstellung der Aktionen „Lesen“, „Schreiben“ und „Ausführen“,
- eine (konditionale) Gerätefreigabe nach physischen und logischen Attributen,
- ein Anlegen selbstdefinierter Geräteklassen mit dem entsprechenden Regelwerk und
- die Kontrolle des Zugriffs eines installierten Hypervisors auf die überwachten Schnittstellen

ermöglichen.

b) Sofern die Kontrolle des Zugriffs vom Hypervisor nicht unterstützt wird, SOLLTE auf Ebene des Virtual-Machine-Monitors (VMM) oder im Gastsystem eine Absicherung stattfinden.

SSK.2.1.10: Generieren von Protokollierungsdaten

a) Die Schnittstellenkontrolle MUSS eine vollständige und unmittelbare Protokollierung der Informationsflüsse gewährleisten. Diese umfasst mindestens:

- Zeitpunkt der Aktion,
- Aktion,
- Quelle des Informationsflusses,
- Übertragungsweg (betroffene Schnittstelle),
- Ziel des Informationsflusses,
- die von dem Informationsfluss betroffene Applikationen,
- die mit dem Informationsfluss verbundene Benutzeridentität sowie deren Gruppenzugehörigkeit.

b) Die Protokollierung MUSS sich von berechtigten Personen abschalten, pseudonymisieren und feingranular konfigurieren lassen.

c) Die Schnittstellenkontrolle MUSS entweder die Protokollierungsfunktionen des Betriebssystems nutzen oder die Protokolle strukturiert an einen zentralisierten Protokollierungsspeicher zur Auswertung übertragen können.

d) Eine darüberhinausgehende Protokollierung MUSS per Konfiguration festlegbar sein.

SSK.2.1.11: Zentrale Verwaltung

a) Die Schnittstellenkontrolle MUSS die Möglichkeit zum Import von zentral erstellten Konfigurationen bereitstellen.

[18] Im Sinne des Mindeststandards: Ausführung erlauben/verbieten, Zugriff auf Ressourcen einschränken

SSK.2.1.12: Patch-Management

a) Der Anbieter des Produktes MUSS vertraglich zusichern, dass er nach Bekanntwerden einer kritischen Schwachstelle[19] in einer angemessenen Frist, spätestens nach 4 Wochen, ein Software-Update zur Verfügung stellt; im Falle der aktiven Ausnutzung (Proof of Concept) binnen 7 Tagen. Die Auslieferung der Updates MUSS integritätsgesichert erfolgen. Weiterhin gelten die Anforderung der jeweils gültigen TR-02102-1[20].

b) Der Betreiber MUSS derartige Updates unverzüglich einspielen.

c) Unabhängig von der Verfügbarkeit eines Updates MUSS der Betreiber nach spätestens 7 Tagen Maßnahmen zur Mitigation ergreifen.

2.2 Sicherheitsanforderungen an den Betrieb

Die Wirksamkeit von Sicherheitsmechanismen einer softwaregestützten Schnittstellenkontrolle hängt auch vom jeweiligen Betrieb ab. Eine grundlegende Voraussetzung ist die Bereitstellung einer sicheren Grundkonfiguration. Die im IT-Grundschutzkompendium beschriebene Standard-Absicherung definiert dafür umzusetzende Sicherheitsmaßnahmen (z. B. bieten hier die Bausteine SYS.2.1. „Allgemeiner Client“ und OPS.1.1.4[21] „Schutz vor Schadprogrammen“ eine gute Hilfestellung).

Der Betreiber MUSS die nun folgenden Sicherheitsanforderungen umsetzen.

SSK.2.2.01: Physische Zugriffsbegrenzung

a) Extern zugängliche physische Schnittstellen des IT-Systems KÖNNEN bei Nichtgebrauch versiegelt werden oder sind bei der Beschaffung auszuschließen. Empfohlen wird diese Maßnahme vor allem bei Schnittstellen mit direktem Zugriff auf andere Geräte/Schnittstellen über das Bus-System.

b) Alternativ wäre auch die Deaktivierung in der jeweiligen Firmware möglich, dies MUSS jedoch im Einzelfall auf Wirksamkeit überprüft werden.

SSK.2.2.02: Fernadministration

a) Die Fernadministration der Schnittstellenkontrolle DARF NUR auf einem kryptographisch abgesicherten Kanal erfolgen (vertraulich, integer, authentisch).

b) Die Vorgaben der Technischen Richtlinie TR-02102-1[22] in der jeweils aktuellen Version MÜSSEN beachtet werden.

SSK.2.2.03: Administration

a) Die Schnittstellenkontrolle DARF NUR von geschulten Administratoren oder Benutzern verwaltet werden.

SSK 2.2.04 Einsatzumgebung

a) IT-Systeme und/oder ihre zugelassenen Schnittstellen MÜSSEN in einer kontrollierten Ausführungsumgebung betrieben werden. Zu einer kontrollierten Ausführungsumgebung gehören mindestens:

- zeitnahes Einspielen sicherheitsrelevanter Patches und Updates (siehe Anforderung „SSK.2.1.12: Patch-Management“),
- Erkennung und Behandlung von Schadprogrammen bei Datenträgeraustausch und –übertragung,

[19] Eine Schwachstelle wird als kritisch bezeichnet, wenn sie nach dem Industriestandard Common Vulnerability Scoring System (CVSS) v3.1 mit High (7.0 - 8.9) oder Critical (9.0 -10.0) bewertet wird (vgl. FIRST 2019).
[20] Vgl. TR-02102-1: “Kryptographische Verfahren: Empfehlungen und Schlüssellängen“ (BSI 2021c)
[21] Vgl. IT-Grundschutz-Kompendium (BSI 2021f)
[22] Vgl. TR-02102-1: “Kryptographische Verfahren: Empfehlungen und Schlüssellängen“ (BSI 2021c)

- Richtlinien zur Steuerung des Umgangs mit externen Datenträgern,
- Richtlinien zur Steuerung des Umgangs mit ausführbaren Dateien auf externen Datenträgern,
- Deaktivierung oder Deinstallation nicht benutzter Schnittstellen,
- Deaktivierung oder Deinstallation nicht benötigter Dienste, Module, Protokolle, funktionaler Erweiterungen,
- Deaktivierung nicht benötigter Benutzerkonten,
- Einsatz aktueller Software- und Firmwarekomponenten,
- umgesetzte Rechte und Rollenkonzepte.

b) Außerdem MUSS es einen zyklischen Prozess zur Erkennung, Analyse, Bewertung und Bereinigung von Schwachstellen geben (Schwachstellenmanagement).

SSK.2.2.05: Protokolle

a) Bei der Auswertung der Protokolle MÜSSEN Informationssicherheit und der Datenschutz berücksichtigt werden.[23]

SSK.2.2.06: Meldesystem

a) Audit-/Log-Daten der Schnittstellenkontrolle MÜSSEN die Meldung sicherheitskritischer Ereignisse und Handlungsaufforderungen nach Dringlichkeitsstufen ermöglichen.

b) Dies KANN über softwareeigene Funktionen oder Zugriff auf Application Programming Interfaces (APIs) oder Log-Daten realisiert werden.

SSK.2.2.07: Auditdaten

a) Beim Ausrollen MUSS die Schnittstellenkontrolle dem jeweiligen Datenschutzkonzept entsprechend so konfiguriert sein, dass die unter SSK.2.1.10 generierten Protokollierungsdaten erzeugt werden.

b) Es MÜSSEN Prozesse definiert und abgestimmt sein, in welchen Fällen die erweiterte Protokollierung dokumentiert aktiviert wird.

[23] Bzgl. Protokolle siehe SSK.2.1.10

Literaturverzeichnis

BMI (2017) Bundesministerium des Innern, für Bau und Heimat: Umsetzungsplan Bund 2017 – Leitlinie für die Informationssicherheit in der Bundesverwaltung, 2017, https://www.bmi.bund.de/SharedDocs/downloads/DE/publikationen/themen/it-digitalpolitik/up-bund-2017.html, abgerufen am 26.05.2021

BSI (2017) Bundesamt für Sicherheit in der Informationstechnik: BSI-Standard 200-2 – IT-Grundschutz-Methodik, Version 1.0, 2017, https://www.bsi.bund.de/dok/128640, abgerufen am 26.05.2021

BSI (2021a) Bundesamt für Sicherheit in der Informationstechnik: Mindeststandards – Antworten auf häufig gestellte Fragen zu den Mindeststandards, https://www.bsi.bund.de/dok/453194, abgerufen am 09.06.2021

BSI (2021b) Bundesamt für Sicherheit in der Informationstechnik: Mindeststandard des BSI zur Verwendung von Transport Layer Security (TLS), Version 2.2, 2021, https://www.bsi.bund.de/dok/903226, abgerufen am 26.05.2021

BSI (2021c) Bundesamt für Sicherheit in der Informationstechnik: TR-02102-1: “Kryptographische Verfahren: Empfehlungen und Schlüssellängen“, Version: 2021-01, https://www.bsi.bund.de/dok/405540, abgerufen am 26.05.2021

BSI (2021d) Bundesamt für Sicherheit in der Informationstechnik: TR-02102-3: “Kryptographische Verfahren: Empfehlungen und Schlüssellängen, Teil 3 – Verwendung von Internet Protocol Security (IPsec) und Internet Key Exchange (IKEv2)“, Version: 2021-01, https://www.bsi.bund.de/dok/405536, abgerufen am 26.05.2021

BSI (2021e) Bundesamt für Sicherheit in der Informationstechnik: TR-02102-4: „Kryptographische Verfahren: Empfehlungen und Schlüssellängen, Teil 4 – Verwendung von Secure Shell (SSH) “, Version: 2021-01, https://www.bsi.bund.de/dok/405538, abgerufen am 26.05.2021

BSI (2021f) Bundesamt für Sicherheit in der Informationstechnik: IT-Grundschutz-Kompendium, Edition 2021, https://www.bsi.bund.de/dok/128568, abgerufen am 26.05.2021

DIN (2018) Deutsches Institut für Normung e.V.: Normungsarbeit – Teil 2: Gestaltung von Dokumenten, DIN 820-2:2018-09, Edition 2021

FIRST (2019) Common Vulnerability Scoring System (CVSS), Version 3.1, 2019, https://www.first.org/cvss/specification-document, abgerufen am 26.05.2021

IETF (1997) Internet Engineering Task Force: Key words for use in RFCs to Indicate Requirement Levels, RFC 2119, 1997, https://tools.ietf.org/html/rfc2119, abgerufen am 09.06.2021

Abkürzungsverzeichnis

API	Application Programming Interface
BSI	Bundesamt für Sicherheit in der Informationstechnik
BSIG	Gesetz über das Bundesamt für Sicherheit in der Informationstechnik
DIN	Deutsches Institut für Normung
DMA	Direct Memory Access
eSATA	External Serial Advanced Technology Attachment
ID	Identifikator
KVM	Kernel-based Virtual Machine
LAN	Local Area Network
NFC	Near Field Communication
PCMCIA	Personal Computer Memory Card International Association
RFC	Request for Comments
S-ATA	Serial AT Attachment
SSK	Schnittstellenkontrolle
TR	Technische Richtlinie
USB	Universal Serial Bus
VMM	Virtual Machine Monitor
WLAN	Wireless Local Area Network