Bundesamt
für Sicherheit in der
Informationstechnik

Mindeststandard des BSI für Schnittstellenkontrollen

nach § 8 Absatz 1 Satz 1 BSIG – Version 1.1 vom 28.11.2017

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

Inhaltsverzeichnis

Vorwort

Das BSI als die nationale Cyber-Sicherheitsbehörde 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. Die Definition erfolgt auf Basis der fachlichen Expertise des BSI in der Überzeugung, dass dieses Mindestniveau in der Bundesverwaltung nicht unterschritten werden darf.

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[1] .

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 Prüfungszyklen einschließlich des Konsultationsverfahrens mit der Bundesverwaltung. 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 auf Ersuchen bei der Umsetzung und Einhaltung der Mindeststandards.

1 Vgl. BSI (2008).

1 Einordnung und Begründung

Der vorliegende Mindeststandard fordert die Kontrolle von externen Schnittstellen[2] von IT-Systemen[3] der Bundesverwaltung, damit diese im Sinne der IT-Sicherheit angemessen überwacht sowie Aktionen und Datenfluss nachvollziehbar protokolliert werden können. Hierzu 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 Stellen des Bundes bei Beschaffung und Betrieb unterstützen.

Dieser Mindeststandard richtet sich an IT-Verantwortliche, IT-Sicherheitsbeauftragte und IT-Fachkräfte sowie mit der Beschaffung beauftragte Stellen in der Bundesverwaltung. Anbieter, sowie weitere interessierte Personen, können diesen Mindeststandard zur Erhöhung der Informationssicherheit heranziehen.

Die Schnittstellenkontrolle (SSK) regelt Registrierung, Freigabe, Blockierung und Protokollierung des Zugriffs von Daten, Applikationen und Geräten[4]. Sie gewährt die Umsetzung einer Sicherheitsrichtlinie für Schnittstellen nach dem Stand der Technik. Sie bietet feingranulare Einstellungsmöglichkeiten für mindestens Zeit, logischen (IP-Adresse) oder physischen Ort, Benutzergruppen, Benutzertypen, Geräte und Gerätetypen.

Dieser Mindeststandard beschreibt Sicherheitsanforderungen für Konfiguration und Interaktion mit der Betriebssystemumgebung des IT-Systems, die eine softwaregestützte Schnittstellenkontrolle erfüllen muss. Bedrohungen, die z. B. durch fehlende Geräteidentifizierung oder -autorisierung oder durch fehlende Autorisierung von Applikationen entstehen können, werden durch Erfüllung dieser Anforderungen an eine Schnittstellenkontrolle reduziert. Die Protokollierung von mit Daten oder Datenformaten assoziierten Aktionen ist ein wesentlicher Bestandteil der Sicherheitsanforderungen an die Schnittstellenkontrolle. Unkontrollierter Datenzufluss und Datenabfluss muss verhindert werden. Besondere Anforderungen werden bei Einsatz einer Schnittstellenkontrolle an die Integrität der Konfigurationsdaten gestellt. Sowohl die Konfigurationsdaten selbst als auch eine eventuelle Übertragung müssen vor unbefugten Änderungen geschützt werden. Änderungen am Regelwerk müssen überwacht werden. Offensichtlich unsichere Konfigurationen der Schnittstellenkontrolle sollten erkannt und als solche auch kenntlich gemacht werden.

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.[5]

Die zentrale Aufgabe der Schnittstellenkontrolle besteht in der Umsetzung der folgenden Vorgaben und Regeln. Hierzu bedarf es nicht unbedingt einer zusätzlichen Software oder Hardware. Grundsätzlich lassen sich viele Regelungen durch z. B. entsprechende Konfigurationen der Betriebssysteme, bestehende Sicherheitslösungen oder organisatorische sowie andere technische Maßnahmen umsetzen. Dieser Mindeststandard setzt die Vorgehensweise gemäß IT-Grundschutz des BSI zum Management der Informationssicherheit voraus[6]. Er gilt für alle Schutzbedarfskategorien.

Zur Umsetzung des Mindeststandards ist zu prüfen, ob die umgesetzten Maßnahmen zur Schnittstellenkontrolle alle Sicherheitsanforderungen (siehe Kapitel 2) vollständig erfüllen oder ob ggf. noch ergänzende Softwareprodukte beschafft werden müssen. Eigene Prüfungen nach Teststellung und Installation in einer dem geplanten Einsatzszenario entsprechenden Umgebung werden empfohlen.

Auch bei Nutzung einer Schnittstellenkontrolle, die diesen Mindeststandard erfüllt, verbleiben Risiken, die in diesem Mindeststandard nicht betrachtet werden. Die in diesem Mindeststandard definierten Sicherheitsanforderungen bieten daher keinen vollständigen Schutz gegen alle denkbaren Angriffsszenarien. Daher ist

2 Definition von externen Schnittstellen siehe „Abkürzungsverzeichnis und Glossar“.
3 Definition von IT-Systemen siehe „Abkürzungsverzeichnis und Glossar“.
4 Definition von Geräten siehe „Abkürzungsverzeichnis und Glossar“.
5 Z. B. direktes Schreiben in den Arbeitsspeicher via Direct Memory Access (DMA), wie es etwa bei S-ATA-Schnittstellen möglich ist.
6 Vgl. BSI (2008), S.49f.

im Bedarfsfall auch denkbar, verbleibende Risiken mit Hilfe von organisatorischen (z. B. Dienstanweisungen) oder physischen Maßnahmen (Verkleben von Schnittstellen und Gehäusen) zu reduzieren.

In diesem Mindeststandard werden Maßnahmen vorgeschrieben, um gängige Risiken zu reduzieren oder zu vermeiden. Demnach bleiben Restrisiken übrig, für deren Behandlung nach Einschätzung des BSI derzeit unverhältnismäßiger Aufwand anfallen würde. Bereits erwähnt wurden Attacken direkt auf Hardware-Niveau (Angriff via DMA), die im Gegensatz zu USB-Geräten gar nicht erst vom Mindeststandard erfasst werden – im Sinne einer Restrisikobetrachtung aber denselben Stellenwert haben.

Die Wertung als Restrisiko bedeutet jedoch nicht, dass die Behörde keinerlei Maßnahmen gegen diese Risiken zu ergreifen hat. Vielmehr hat die Behörde entsprechende technische, organisatorische oder physische Maßnahmen gemäß eigener Risikoabschätzung auszuwählen. Die Entscheidung ist zu dokumentieren und von der Behördenleitung mitzutragen.

2 Sicherheitsanforderungen

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

2.1 Sicherheitsanforderungen an das Produkt

SSK.01: Vertrauenswürdiger Kanal

Die Schnittstellenkontrolle muss einen gesicherten Kanal zu Administrationszwecken und zur Übertragung der Protokollierungsdaten bereitstellen.

Die Schnittstellenkontrolle unterstützt die aktuell gültige Version des Mindeststandards SSL/TLS[7] mit gegenseitiger zertifikatsbasierter Authentisierung oder Mechanismen mindestens gleicher Stärke (siehe TR-02102-1[8], TR-02102-3[9], TR-02102-4[10]) zum Schutz der Integrität, Authentizität und Vertraulichkeit des Administrationskanals.

SSK.02: Identifikation und Authentisierung der Benutzer

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

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

SSK.03: Identifikation der Geräte

Die Schnittstellenkontrolle muss die eindeutige Identifizierung einzelner Geräte leisten; bei USB-Devices etwa anhand von Geräteklasse, Vendor-ID und Hardware-ID.

SSK.04: Identifikation der Daten

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

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

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

SSK.05: Autonome Arbeitsweise

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

Freigaben müssen auch im Offline-Betrieb geschützter Rechner einrichtbar sein, beispielsweise durch telefonische/schriftliche Challenge-Response-Verfahren.

SSK.06: Schnittstellen

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

7 Vgl. BSI (2015).
8 Vgl. BSI (2017).
9 Vgl. BSI (2017a).
10 Vgl. BSI (2017b).

SSK.07: Applikationen

Die Schnittstellenkontrolle muss die Ausführung von Programmen und/oder Skripten, die sich auf den angeschlossenen Geräten im Sinne dieses Standards befinden, steuern[11], überwachen und protokollieren.

SSK.08: Daten

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

SSK.09: Management von Sicherheitsattributen

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 (Sofern dies vom Hypervisor nicht unterstützt wird, sollte auf Ebene des Virtual Machine Monitors (VMM) oder im Gastsystem eine Absicherung stattfinden.)

ermöglichen.

SSK.10: Generieren von Protokollierungsdaten

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.

Die Protokollierung muss sich von berechtigten Personen abschalten, pseudonymisieren und feingranular konfigurieren lassen.

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

Eine darüber hinausgehende Protokollierung muss per Konfiguration festlegbar sein.

SSK.11: Zentrale Verwaltung

Die Schnittstellenkontrolle muss die Möglichkeit zum Import von zentral erstellten Konfigurationen bereitstellen.

SSK.12: Patch-Management

Der Anbieter des Produktes soll vertraglich zusichern, dass er nach Bekanntwerden einer kritischen Schwachstelle in einer angemessenen Frist, spätestens nach 48 Tagen, ein Software-Update zur Verfügung stellt; im Falle der aktiven Ausnutzung (Proof of Concept) binnen 7 Tagen. Die Auslieferung der Updates

11 Definition von Steuern siehe „Abkürzungsverzeichnis und Glossar“.

muss integritätsgesichert erfolgen. Es sollen hierbei die Anforderungen der ISO/IEC 30111[12] berücksichtigt werden. Weiterhin gelten die Anforderung der TR-02102[13].

Der Betreiber hat derartige Updates unverzüglich einzuspielen.

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. Der Betreiber hat daher folgende Sicherheitsanforderungen umzusetzen.

SSK.13: Komplementäre Maßnahmen

Auf dem IT-System müssen folgende Maßnahmen umgesetzt werden:

- Zeitnahes Einspielen sicherheitsrelevanter Patches und Updates (siehe Anforderung „SSK.12: Patch-Management“),
- Erkennung und Behandlung von Schadprogrammen bei Datenträgeraustausch und -übertragung.[14]

SSK.14: Physische Zugriffsbegrenzung

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

SSK.15: Fernadministration

Die Fernadministration der Schnittstellenkontrolle darf nur auf einem kryptographisch abgesicherten Kanal erfolgen (vertraulich, integer, authentisch). Die Vorgaben der Technischen Richtlinie TR-02102 „Kryptographische Verfahren: Empfehlungen und Schlüssellängen“ in der jeweils aktuellen Version sind zu beachten.[15]

SSK.16: Administration

Die Schnittstellenkontrolle ist nur von geschulten Administratoren oder Benutzern zu verwalten.

SSK.17: Einsatzumgebung

IT-Systeme und/oder ihre zugelassenen Schnittstellen sind in einer kontrollierten Ausführungsumgebung zu betreiben.

SSK.18: Protokolle

Protokolle sind im Hinblick auf die Informationssicherheit und unter Berücksichtigung des Datenschutzes auszuwerten.[16]

SSK.19: Meldesystem

Audit-/Log-Daten der Schnittstellenkontrolle müssen die Meldung sicherheitskritischer Ereignisse und Handlungsaufforderungen nach Dringlichkeitsstufen ermöglichen. Dies kann über softwareeigene Funktionen oder Zugriff auf Application Programming Interfaces (APIs) oder Log-Daten realisiert werden.

12 ISO/IEC (2013).
13 BSI (2017).
14 Gem. BSI (2014).
15 BSI (2017).
16 Bzgl. Protokolle siehe SSK.10.

SSK.20: Auditdaten

Die Schnittstellenkontrolle muss beim Ausrollen, dem jeweiligen Datenschutzkonzept entsprechend, so konfiguriert sein, dass die unter SSK.10 generierten Protokollierungsdaten erzeugt werden. Es müssen Prozesse definiert und abgestimmt sein, in welchen Fällen die erweiterte Protokollierung dokumentiert aktiviert wird.

Literaturverzeichnis

BSI (2008) Bundesamt für Sicherheit in der Informationstechnik: BSI-Standard 100–2, IT-Grundschutz-Vorgehensweise
https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzStandards/ITGrundschutzStandards100/Standard02/ITGStandard02_node.html

BSI (2014) Bundesamt für Sicherheit in der Informationstechnik: IT-Grundschutz-Kataloge, M 4.237 Sichere Grundkonfiguration eines IT-Systems, 13. Ergänzungslieferung, 2013
https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKataloge/Inhalt/_content/m/m04/m04237.html

BSI (2015) Bundesamt für Sicherheit in der Informationstechnik: Mindeststandard des BSI nach § 8 Absatz 1 Satz 1 BSIG für den Einsatz des SSL/TLS-Protokolls in der Bundesverwaltung, V1.0., 2015
https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Mindeststandards/Mindeststandard_BSI_TLS_1_2_Version_1_0.pdf?__blob=publicationFile&v=4

BSI (2017) Bundesamt für Sicherheit in der Informationstechnik: TR-02102-1, Kryptographische Verfahren: Empfehlungen und Schlüssellängen, Version 2017–01, 2017
https://www.bsi.bund.de/DE/Publikationen/TechnischeRichtlinien/tr02102/index_htm.htm

BSI (2017a) Bundesamt für Sicherheit in der Informationstechnik: TR-02102-3, Kryptographische Verfahren: Empfehlungen und Schlüssellängen, Version 2017–01, 2017
https://www.bsi.bund.de/DE/Publikationen/TechnischeRichtlinien/tr02102/index_htm.htm

BSI (2017b) Bundesamt für Sicherheit in der Informationstechnik: TR-02102-4, Kryptographische Verfahren: Empfehlungen und Schlüssellängen, Version 2017–01, 2017
https://www.bsi.bund.de/DE/Publikationen/TechnischeRichtlinien/tr02102/index_htm.htm

ISO/IEC (2013) International Organization for Standardization and International Electrotechnical Commission: ISO/IEC 30111: Information technology. Security techniques. Vulnerability handling processes, Version 2013-10-31, 2013

Abkürzungsverzeichnis und Glossar

API	Application Programming Interface
BMI	Bundesministerium des Innern
BSI	Bundesamt für Sicherheit in der Informationstechnik
BSIG	Gesetz über das Bundesamt für Sicherheit in der Informationstechnik
Daten	Menschen- oder maschinenlesbare Zeichen
Dateisignatur	Dateiinterne Bytefolge zur Identifizierung von Dateitypen; Magic Number
DMA	Direct Memory Access
Externe Schnittstelle	Im Sinne des Mindeststandards: Externe Schnittstellen nach Stand der Technik, insbesondere: USB, LAN, WLAN, Mobilfunk, Bluetooth, eSATA, PCMCIA, Firewire, Express-Card, Thunderbolt, NFC, SmartCard
Geräte	Im Sinne des Mindeststandards: Alle an externe Schnittstellen angeschlossene Geräte (bspw. Speichermedien, Ein-/Ausgabegeräte, Gadgets) außer weiterer IT-Systeme
GG	Grundgesetz der Bundesrepublik Deutschland
IT	Informationstechnik
IT-System	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/KVM, die lokal angeschlossene Geräte an andere Systeme weiterreichen können.
SSL	Secure Sockets Layer
Steuern	Im Sinne des Mindeststandards: Ausführung erlauben/verbieten, Zugriff auf Ressourcen einschränken
TLS	Transport Layer Security
VMM	Virtual Machine Monitor