Bundesamt
für Sicherheit in der
Informationstechnik

Mindeststandard des BSI für Schnittstellenkontrollen

nach § 8 Absatz 1 Satz 1 BSIG – Version 1.0 vom 16.11.2016

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

Inhaltsverzeichnis

Tabellenverzeichnis

Vorwort

§ 8 Absatz 1 BSIG regelt die Befugnis des BSI, allgemeine technische Mindeststandards für die Sicherung der Informationstechnik des Bundes festzulegen. Ein Mindeststandard beschreibt die zu erfüllenden sicherheitstechnischen Anforderungen an eine Produkt- bzw. Dienstleistungskategorie oder Methoden, um eine angemessenen Mindestschutz gegen IT-Sicherheitsbedrohungen zu erreichen.

Mindeststandards sind Vorgaben des BSI für die Stellen des Bundes. Allerdings kann das BMI im Benehmen mit dem IT-Rat die dort formulierten Anforderungen ganz oder teilweise als allgemeine Verwaltungsvorschrift erlassen und dadurch für die Stellen des Bundes als verbindlich erklären.[1] Darüber hinaus kann der IT-Planungsrat Mindeststandards in Teilen oder als Ganzes als gemeinsame Standards für den zur Aufgabenerfüllung zwischen dem Bund und den Ländern notwendigen Datenaustausch festlegen.[2]

Über die Bundesverwaltung hinaus sind Mindeststandards nach § 8 Absatz 1 BSIG auch in der öffentlichen Verwaltung der Länder und Kommunen für den Einsatz von Informationstechnik und zur Sicherung kritischer Infrastrukturen von grundsätzlicher Bedeutung. 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. Anbieter von Informationstechnik und IT-Dienstleister können Mindeststandards dazu nutzen, ihre angebotenen Produkte sicherer zu machen.

1 Vgl. § 8 Absatz 1 Satz 2 BSIG

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

1 Einordnung und Begründung

Der vorliegende Mindeststandard fordert die Kontrolle von externen Schnittstellen[3] von IT-Systemen[4] der Bundesverwaltung, damit diese im Sinne der IT-Sicherheit angemessen überwacht, sowie Aktionen und Datenfluss nachvollziehbar protokolliert werden können. Hierzu können betriebssystemeigene Lösungen und organisatorische Maßnahmen oder Softwareprodukte von Drittherstellern eingesetzt werden. Wird eine Softwarelösung zur Schnittstellenkontrolle genutzt, gibt dieser Standard Mindestsicherheitsforderungen vor, die die Bundesverwaltung bei Beschaffung und Betrieb unterstützen.

1.1 Kurzbeschreibung

Die Schnittstellenkontrolle regelt Registrierung, Freigabe, Blockierung und Protokollierung des Zugriffs von Daten, Applikationen und Geräten. Sie gewährt die Umsetzung einer Sicherheitsrichtlinie für Schnittstellen nach dem Stand der Technik/Standardisierung. Diese bieten feingranulare Einstellungsmöglichkeiten für mindestens Zeit, logischen (IP-Adresse) oder physischen Ort, Benutzer (-gruppen/-typen) und Geräte (-typen).

1.2 Begründung des Handlungsbedarfs

Die Schnittstellen eines IT-Systems dienen naturgemäß dem Transfer von Daten auf das System oder von diesem – und bergen damit diverse Risiken bezüglich nicht autorisiertem Abfluss von Daten beziehungsweise dem Zufluss schädlicher Daten. Insbesondere vor dem Hintergrund aktueller Entwicklungen wie „Bring Your Own Device“ (BYOD) und „Company Owned Privatly Enabled“ (COPE), also der privaten Nutzung dienstlicher sowie der dienstlichen Nutzung privater Geräte, die sich nicht rein organisatorisch (z. B. über Verbote) verhindern lassen, ist hier Handlungsbedarf auszumachen. Betriebssysteme stellen mitunter Funktionen bereit, mit denen sich grundsätzlich – je nach System mehr oder weniger grobgranulare – Sicherheitsrichtlinien umsetzen lassen. Sind diese für den ermittelten Schutzbedarf ausreichend, so muss nicht zwangsläufig eine separate Schnittstellenkontrolle eingesetzt werden. Grundsätzlich ist jede Lösung angemessen, die die aufgeführten Risiken (siehe Kapitel 3) absichert. In jedem Fall sind die Entscheidung für eine Variante oder eine Kombination sowie die umgesetzten organisatorischen Maßnahmen nachvollziehbar zu dokumentieren.

Dieser Mindeststandard gilt für alle Schutzbedarfsklassen und regelt im Detail Anforderungen für einen normalen Schutzbedarf. Ab Schutzbedarf „hoch“ oder über darüber hinausgehende Bedrohungen, sind weitere Anforderungen auf Basis einer Risikoanalyse sowie nach Einschätzung des Kunden zusätzlich erforderlichen Maßnahmen zu berücksichtigen.

1.3 Abgrenzung

Dieser Mindeststandard beschreibt Sicherheitsanforderungen für Konfiguration und Interaktion mit der Betriebssystemumgebung des IT-Systems, die eine softwaregestützte Schnittstellenkontrollen erfüllen muss. Weitere Schutzmaßnahmen, wie etwa physische Beschränkungen, werden 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]

Als Mindeststandard zielt dieser Standard auf ein Mindestmaß an Sicherheit ab und kann so vor Standardangriffen und unvorsichtigem Verhalten schützen. Einen vollständigen Schutz wie z. B. vor technisch versierten Angreifern oder Innentätern bietet der Mindeststandard nicht.

3 Definition von externen Schnittstellen siehe „Abkürzungsverzeichnis und Glossar“
4 Definition von IT-Systemen 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

2 Methode und Anwendung

Der Mindeststandard richtet sich primär an die Beschaffung und sekundär an den Betrieb einer Software zur Schnittstellenkontrolle und gliedert sich daher in folgenden Ablauf:

1. Analysieren typischer Bedrohungen (Kapitel 3), gegen die die Schnittstellenkontrolle bestehen muss.
2. Ableiten funktionaler Sicherheitsanforderungen (Kapitel 4.1.1). Diese muss die Schnittstellenkontrolle erfüllen, um gegen die Bedrohungen wirksam zu sein.
3. Sicherheitsanforderungen an Anbieter (Kapitel 4.1.2) und Betreiber (Kapitel 4.2) der Schnittstellenkontrolle, die die Sicherheitseigenschaften der Schnittstellenkontrolle stützen oder erweitern.

2.1 Zielgruppen

Dieser Mindeststandard richtet sich an IT-Verantwortliche, IT-Sicherheitsbeauftragte und IT-Fachkräfte sowie mit der Beschaffung beauftragte Stellen in der Bundesverwaltung.[6] Anbieter sowie weitere interessierte Personen, können diesen Mindeststandard zur Erhöhung der Informationssicherheit heranziehen.

2.2 Umsetzung

Zur Umsetzung des Mindeststandards ist zu prüfen, ob die umgesetzten Maßnahmen zur Schnittstellenkontrolle alle Sicherheitsanforderungen (siehe Kapitel 4) 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.

6 vgl. § 2 Absatz 3 BSIG

3 Bedrohungen

In diesem Kapitel werden typische Bedrohungen aufgeführt, die sich zum einem gegen die Integrität, Vertraulichkeit und Authentizität von Nutzerdaten und zum anderen gegen die Integrität von Konfigurationsdaten richten.

3.1 Integrität, Vertraulichkeit und Authentizität von Nutzdaten

Bedrohungen, die sich gegen die Integrität, Vertraulichkeit und Authentizität von Nutzerdaten richten, sind in Tabelle 1 dargestellt und näher beschrieben.

Bedrohung	Beschreibung
Fehlende Geräteidentifizierung	Der Zugriff auf zugelassene und nicht zugelassene Geräte[7] kann nicht kontrolliert werden.
Fehlende Geräteautorisierung	Ein Angreifer versucht, nicht zugelassene Geräte über eine offerierte externe Schnittstelle anzubinden, um z. B. schädlichen Code zu laden.
Fehlende Applikationsautorisierung	Applikationen nutzen unautorisiert externe Schnittstellen. Ein Angreifer versucht, einen Informationsfluss von Daten mittels nicht zugelassener Applikation zu erwirken.
Unbeschränkter Datenfluss	Die Datenflüsse einer zugelassenen Applikation können nicht kontrolliert werden. Ein Angreifer versucht, einen Informationsfluss von Daten mittels zugelassener Applikation zu erwirken.
Fehlende Protokollierung	Die mit (einem) Daten (-format) assoziierten Aktionen können nicht kontrolliert und protokolliert werden.
Administration	Eine fehlerhafte Administration der Schnittstellenkontrolle könnte zu einer unsicheren Konfiguration führen.

Tabelle 1: Bedrohungen gegen die Integrität, Vertraulichkeit und Authentizität von Nutzerdaten

3.2 Integrität von Konfigurationsdaten

Bedrohungen, die sich gegen die Integrität von Konfigurationsdaten richten, sind in Tabelle 2 dargestellt und näher beschrieben.

Bedrohung	Beschreibung
Fehlender Schutz des Konfigurationstransfers	Ein Angreifer versucht im Falle eines zentralen Managements von Konfigurationen, Veränderungen während der Übertragung vom Management zur Schnittstellenkontrolle vorzunehmen.
Fehlender Konfigurationsschutz	Ein Angreifer versucht Veränderungen an der zentralen oder

7 Zur Definition von Gerät siehe „Abkürzungsverzeichnis und Glossar“

Bedrohung	Beschreibung
	dezentralen Konfiguration der Schnittstellenkontrolle vorzunehmen.
Fehlender Konfigurationsabgleich	Regelabweichende Schnittstellenzugriffe oder Änderungen am Regelwerk werden nicht erkannt.
Darstellung	Die Schnittstellenkontrolle kann in einer Art und Weise benutzt werden, die unsicher ist, obwohl der Benutzer davon ausgeht, dass er die Schnittstellenkontrolle in einer sicheren Art und Weise nutzt. Ein Benutzer könnte unwissentlich z. B. mit einer nicht sicheren Konfiguration arbeiten.
Schwachstellen[8]	Ein Angreifer versucht, eine ihm bekannte Schwachstelle der Schnittstellenkontrolle oder einer von dieser vermittelten Ressource auszunutzen, um z. B. schädlichen Code auf den Rechner zu laden.
Korrumpiertes Update[9]	Ein Benutzer könnte unwissentlich eine nicht integre Aktualisierung der softwaregestützten Schnittstellenkontrolle nutzen.

Tabelle 2: Bedrohungen gegen die Integrität von Konfigurationsdaten

3.3 Spezifische Risikobetrachtung

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 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. Ein Beispiel dafür wäre etwa USB-ID-Spoofing. 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.

8 Ebenso eine Bedrohung für Nutzdaten und gesamten Programmablauf.
9 Ebenso eine Bedrohung für Nutzdaten und gesamten Programmablauf.

4 Sicherheitsanforderungen

Nachfolgend werden Sicherheitsanforderungen zunächst an das Produkt gestellt (Kapitel 4.1). Darauf folgen dann Sicherheitsanforderungen an den Betrieb (Kapitel 4.2).

4.1 Sicherheitsanforderungen an das Produkt

Sicherheitsanforderungen an das Produkt sind in funktionale und nicht-funktionale Sicherheitsanforderungen kategorisiert.

4.1.1 Funktionale Sicherheitsanforderungen

Kategorie	Bereich	Mindestanforderung
Vertrauenswürdige Kommunikation	Vertrauenswürdiger Kanal	Gesicherter Kanal: Die Schnittstellenkontrolle muss einen gesicherten Kanal zu Administrationszwecken bereitstellen.
		TLS-Support: Die Schnittstellenkontrolle unterstützt die aktuell gültige Version des Mindeststandards SSL/TLS[10] mit gegenseitiger zertifikatsbasierter Authentisierung oder Mechanismen mindestens gleicher Stärke zum Schutz der Integrität, Authentizität und Vertraulichkeit des Administrationskanals.
Identifikation und Authentisierung	Identifikation und Authentisierung der Benutzer	– Authentisierung: Die Schnittstellenkontrolle muss eine Benutzeridentifikation/-authentisierung durchführen. Diese kann auch mittels Single Sign-on, etwa über die Benutzeranmeldung am Betriebssystem umgesetzt werden.
		– Admin-Anpassungen: Nur nach erfolgreicher Benutzeridentifikation/-authentisierung des Admins dürfen Anpassungen an der Konfiguration der Schnittstellenkontrolle durch einen Administrator möglich sein.
	Identifikation der Geräte	Geräteidentifizierung: Die Schnittstellenkontrolle muss die eindeutige Identifizierung einzelner Geräte leisten; bei USB Devices etwa anhand Geräteklasse, Vendor-ID und Hardware-ID.
	Identifikation der Daten	Die Schnittstellenkontrolle muss Daten auf angeschlossenen Geräten anhand ihrer Metadaten (etwa Dateiendung, Dateisignatur/Magic Number) identifizieren können.
		Geschachtelte Daten identifizieren: Die Schnittstellenkontrolle muss die Identifizierung von geschachtelten bzw. eingebetteten (unverschlüsselten) Daten gewährleisten; zum Beispiel anhand von Dateisignatur und -endung.
		Individuelle Dateiformate: Die Schnittstellenkontrolle muss die Definition individueller Dateiformate zulassen; beispielsweise

10 Vgl. BSI (2015)

Kategorie	Bereich	Mindestanforderung
		um Dateien interner Fachanwendungen in die Schnittstellenkontrolle zu integrieren.
	Autonome Arbeitsweise	Offline-Konfiguration: Wenn die Schnittstellenkontrolle ihre Konfiguration von anderen IT-Systemen (Servern) bezieht, muss diese auch nach Trennung von jenen IT-Systemen funktionsfähig bleiben.
		Offline-Freigaben: Freigaben müssen auch im Offline-Betrieb geschützter Rechner einrichtbar sein, beispielsweise durch telefonische/schriftliche Challenge-Response-Verfahren.
Sichere Konfiguration	Schnittstellen	Aktuelle Schnittstellen: Die Schnittstellenkontrolle muss die Erkennung und Behandlung der nach dem Stand der Technik offerierten Schnittstellen ermöglichen. Alle anderen sollen gesperrt werden (Whitelisting).
	Applikationen	Die Schnittstellenkontrolle muss die Ausführung von Programmen und/oder Skripten, die sich auf den angeschlossenen Geräten befinden steuern, überwachen und protokollieren.
	Daten	Die Schnittstellenkontrolle muss den Zugriff auf Daten die sich auf einem Gerät befinden, steuern, überwachen und protokollieren.
	Management von Sicherheitsattributen	Sicherheitsattribute: 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 (hostseitige Lösung, ggf. auf VMM-ebene) ermöglichen.
Protokollierung	Generieren von Protokolldaten	Protokollierung: Die Schnittstellenkontrolle muss eine vollständige und unmittelbare Protokollierung der Informationsflüsse gewährleisten. Diese umfasst mindestens: – Zeitpunkt der Aktion – Aktion – Quelle des Informationsflusses – Übertragungsweg (betroffene Schnittstelle)

Kategorie	Bereich	Mindestanforderung
		– Ziel des Informationsflusses – Von dem Informationsfluss betroffene Applikationen – Die mit dem Informationsfluss verbundene Benutzeridentität sowie dessen Gruppenzugehörigkeit Die Protokollierung muss sich abschalten, pseudonymisieren und feingranular konfigurieren lassen. Die Schnittstellenkontrolle muss entweder die Protokollierungsfunktionen des Betriebssystems nutzen oder die Protokolle strukturiert an einen beliebigen Log-Server zur Auswertung übertragen können.
		Erweiterte Protokollierung: Eine darüber hinausgehende Protokollierung muss per Konfiguration festlegbar sein.
Zentrale Verwaltung	Zentrale Verwaltung	Import zentraler Konfigurationen: Die Schnittstellenkontrolle muss die Möglichkeit zum Import von zentral erstellten Konfigurationen bereitstellen.

Tabelle 3: Funktionale Sicherheitsanforderungen

4.1.2 Nicht-funktionale Sicherheitsanforderungen

Die in Tabelle 4: Nicht-Funktionale Sicherheitsanforderungen aufgeführten Sicherheitsanforderungen haben Anbieter von softwaregestützten Schnittstellenkontrollen zu gewährleisten.

Kategorie	Bereich	Mindestanforderung
Patch-Management	Patch-Management	Nach Bekanntwerden einer kritischen Schwachstelle soll durch den Anbieter innerhalb von 48 Tagen ein Software-Update zur Verfügung gestellt werden; im Falle der aktiven Ausnutzung (Proof of Concept) binnen 7 Tagen. Die Auslieferung der Updates muss integritätsgesichert erfolgen. Es sollen hierbei die Anforderungen der ISO/IEC 30111 berücksichtigt werden[11] Der Betreiber hat derartige Updates unverzüglich einzuspielen. Unabhängig von der Verfügbarkeit eines Updates muss der Betreiber nach spätestens 7 Tagen Maßnahmen zur Mitigation ergreifen.

Tabelle 4: Nicht-Funktionale Sicherheitsanforderungen

11 ISO/IEC (2013)

4.2 Sicherheitsanforderungen an den Betrieb

Die Wirksamkeit von Sicherheitsmechanismen einer softwaregestützten Schnittstellenkontrolle hängt auch vom jeweiligen Betrieb ab. Der Betreiber hat daher folgende Sicherheitsanforderungen umzusetzen.

Bereich	Mindestanforderung
Komplementäre Maßnahmen	Auf dem IT-System müssen folgende Maßnahmen umgesetzt werden: – Zeitnahes Einspielen sicherheitsrelevanter Patches und Updates (siehe Kapitel 4.1.2), – Erkennung und Behandlung von Schadprogrammen bei Datenträgeraustausch und -übertragung.[12]
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.
Fernadministration	Die Fernadministration der Schnittstellenkontrolle darf nur auf einem kryptographisch abgesicherten Kanal erfolgen (vertraulich, integer, authentisch). Die Vorgaben der technischen Richtlinie TR-02102-1 „Kryptographische Verfahren: Empfehlungen und Schlüssellängen“ sind zu beachten.[13]
Administration	Die Schnittstellenkontrolle ist nur von geschulten Administratoren oder Benutzern zu verwalten.
Einsatzumgebung	IT-Systeme und/oder ihre zugelassenen Schnittstellen sind in einer kontrollierten Ausführungsumgebung zu betreiben.
Protokolle	Protokolle sind und unter Berücksichtigung des Datenschutzes auszuwerten.[14]
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.
Auditdaten	Die Schnittstellenkontrolle muss beim Ausrollen datenschutzfreundlich konfiguriert sein – die Protokollierung ist lediglich im Bedarfsfall dokumentiert zu aktivieren.

Tabelle 5: Sicherheitsanforderungen an den Betrieb

12 Gem. BSI (2014)
13 BSI (2016a)
14 Bzgl. Protokolle siehe Kapitel 4.1.1 – Kategorie „Protokollierung“

Literaturverzeichnis

BSI (2014) Bundesamt für Sicherheit in der Informationstechnik: IT-Grundschutz-Kataloge, M 4.237 Sichere Grundkonfiguration eines IT-Systems, 14. Ergänzungslieferung, 2014

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

BSI (2016a) Bundesamt für Sicherheit in der Informationstechnik: TR-02102-1, Kryptographische Verfahren: Empfehlungen und Schlüssellängen, Version 2016-01, 2016

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
BYOD	Bring Your Own Device
COPE	Company Owned Privatly Enabled
Daten	Menschen- oder maschinenlesbare Zeichen
Dateisignatur	Dateiinterne Bytefolge zur Identifizierung von Dateitypen; Magic Number
DMA	Direct Memory Access
Externe Schnittstelle	Im Sinne des MST: Externe Schnittstellen nach Stand der Technik, insbesondere: USB, LAN, WLAN, Mobilfunk, Bluetooth, eSATA, PCMCIA, Firewire, Expresscard, Thunderbolt.
Geräte	Im Sinne des MST: Alle an externe Schnittstellen angeschlossene Geräte (etwa 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 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
TLS	Transport Layer Security