Bundesamt
für Sicherheit in der
Informationstechnik

SYS.4.5 Wechseldatenträger

1. Beschreibung

1.1. Einleitung

Wechseldatenträger werden oft eingesetzt, um Daten zu transportieren, zu speichern oder um mobil auf sie zugreifen zu können. Zu Wechseldatenträgern gehören externe Festplatten, CD-ROMs, DVDs, Speicherkarten, Magnetbänder und USB-Sticks.

Wechseldatenträger sind danach klassifizierbar, ob sie nur lesbar, einmalig beschreibbar oder wiederbeschreibbar sind. Unterschiede gibt es auch bei der Art der Datenspeicherung (analog oder digital) oder ihrer Bauform. So gibt es auswechselbare Datenträger (z. B. verbaute Festplatten) oder externe Datenspeicher (z. B. USB-Sticks).

1.2. Zielsetzung

In diesem Baustein wird aufgezeigt, wie Wechseldatenträger sicher genutzt werden können. Außerdem wird beschrieben, wie verhindert werden kann, dass über Wechseldatenträger unbeabsichtigt Informationen weitergegeben werden.

1.3. Abgrenzung und Modellierung

Der Baustein SYS.4.5 *Wechseldatenträger* ist auf jeden Wechseldatenträger im Informationsverbund anzuwenden.

Dieser Baustein beschäftigt sich mit den Sicherheitseigenschaften von Wechseldatenträgern. Der Schutz der IT-Systeme, an denen die Wechseldatenträger angeschlossen werden können, wird in dem vorliegenden Baustein nicht berücksichtigt. Empfehlungen hierzu sind in den Bausteinen SYS.1.1 *Allgemeiner Server* und SYS.2.1 *Allgemeiner Client* sowie den betriebssystemspezifischen Bausteinen zu finden.

Wechseldatenträger speichern Daten elektronisch, magnetisch oder auf andere, nicht direkt wahrnehmbare Weise. Sie verarbeiten dabei selbst keine Daten. Die Anforderungen an solche Geräte, wie z. B. Smartphones und Tablets, werden im Baustein SYS.3.2.1 *Allgemeine Smartphones und Tablets* aufgeführt. Nicht zu den Wechseldatenträgern zählen auch Cloud-Speicher. Anforderungen an Cloud-Umgebungen sind im Baustein OPS.2.2 *Cloud-Nutzung* zu finden.

Wechseldatenträger können bei persönlichen Treffen oder auch per Versand ausgetauscht werden. Der sichere Austausch der eigentlichen Informationen wird in diesem Baustein nicht betrachtet. Dazu sind die Anforderungen des Bausteins CON.9 *Informationsaustausch* zu erfüllen.

2. Gefährdungslage

Da IT-Grundschutz-Bausteine nicht auf individuelle Informationsverbünde eingehen können, werden zur Darstellung der Gefährdungslage typische Szenarien zugrunde gelegt. Die folgenden spezifischen Bedrohungen und Schwachstellen sind für den Baustein SYS.4.5 *Wechseldatenträger* von besonderer Bedeutung.

2.1. Sorglosigkeit im Umgang mit Informationen

Häufig gibt es in Institutionen zwar organisatorische Regelungen und technische Sicherheitsverfahren für Wechseldatenträger, diese werden jedoch oft durch einen sorglosen Umgang mit den Wechseldatenträgern umgangen. So kommt es etwa vor, dass Wechseldatenträger während einer Pause unbeaufsichtigt im Besprechungsraum zurück- oder auch im Zugabteil liegen gelassen werden.

2.2. Unzureichende Kenntnis über Regelungen

Wenn die Regelungen für den korrekten Umgang mit Wechseldatenträgern nicht hinreichend bekannt sind, können sie sich auch nicht eingehalten werden. So können zahlreiche Gefährdungen hinsichtlich der Informationssicherheit eintreten, zum Beispiel, wenn nicht geprüfte USB-Sticks an die IT-Systeme der Institution angeschlossen werden.

2.3. Diebstahl oder Verlust von Wechseldatenträgern

Bei Wechseldatenträgern ist das Risiko von Datenverlusten höher als bei stationären IT-Systemen. Ursachen für Datenverluste sind etwa Diebstahl oder verlorengegangene Geräte. Die auf den Wechseldatenträgern abgelegten Informationen sind in diesen Fällen oft unwiederbringlich verloren. Außerdem können die Informationen Externen in die Hände fallen.

2.4. Defekte Datenträger

Wechseldatenträger sind aufgrund ihrer Größe und Anwendungsbereiche anfällig für Beschädigungen, Fehler oder Ausfälle. Ursache sind beispielsweise ständig wechselnde Einsatzumgebungen oder mechanische Einwirkungen.

2.5. Beeinträchtigung durch wechselnde Einsatzumgebung

Wechseldatenträger werden in sehr unterschiedlichen Umgebungen eingesetzt und sind dadurch vielen Gefährdungen ausgesetzt. Dazu gehören beispielsweise schädigende Umwelteinflüsse wie zu hohe oder zu niedrige Temperaturen und Staub oder Feuchtigkeit. Hinzu kommen beispielsweise Transportschäden. Ein weiterer wichtiger Aspekt ist, dass Wechseldatenträger oft in Bereichen mit unterschiedlichem Sicherheitsniveau benutzt werden.

2.6. Verbreitung von Schadsoftware

Wechseldatenträger werden oft benutzt, um Daten zwischen verschiedenen Geräten und dem Arbeitsplatzrechner auszutauschen. Schadsoftware könnte Daten auf den Wechseldatenträgern kompromittieren und sich so auf die Arbeitsplatzrechner übertragen.

3. Anforderungen

Im Folgenden sind die spezifischen Anforderungen des Bausteins SYS.4.5 *Wechseldatenträger* aufgeführt. Der oder die Informationssicherheitsbeauftragte (ISB) ist dafür zuständig, dass alle

Anforderungen gemäß dem festgelegten Sicherheitskonzept erfüllt und überprüft werden. Bei strategischen Entscheidungen ist der oder die ISB stets einzubeziehen.

Im IT-Grundschutz-Kompendium sind darüber hinaus weitere Rollen definiert. Sie sollten besetzt werden, insofern dies sinnvoll und angemessen ist.

Zuständigkeiten	Rollen
Grundsätzlich zuständig	IT-Betrieb
Weitere Zuständigkeiten	Fachverantwortliche, Benutzende

Genau eine Rolle sollte *Grundsätzlich zuständig* sein. Darüber hinaus kann es noch *Weitere Zuständigkeiten* geben. Falls eine dieser weiteren Rollen für die Erfüllung einer Anforderung vorrangig zuständig ist, dann wird diese Rolle hinter der Überschrift der Anforderung in eckigen Klammern aufgeführt. Die Verwendung des Singulars oder Plurals sagt nichts darüber aus, wie viele Personen diese Rollen ausfüllen sollen.

3.1. Basis-Anforderungen

Die folgenden Anforderungen MÜSSEN für diesen Baustein vorrangig erfüllt werden.

SYS.4.5.A1 Sensibilisierung zum sicheren Umgang mit Wechseldatenträgern (B)

Alle Benutzenden MÜSSEN für den sicheren Umgang mit Wechseldatenträgern sensibilisiert werden. Die Institution MUSS insbesondere darauf hinweisen, wie die Benutzenden mit Wechseldatenträgern umgehen sollten, um einem Verlust oder Diebstahl vorzubeugen und eine lange Lebensdauer zu gewährleisten.

Die Institution MUSS die Benutzenden darüber informieren, dass sie keine Wechseldatenträger, die aus unbekannten Quellen stammen, an ihre IT-Systeme anschließen dürfen.

SYS.4.5.A2 Verlust- und Manipulationsmeldung (B) [Benutzende]

Die Benutzenden MÜSSEN umgehend melden, wenn ein Wechseldatenträger gestohlen oder verloren wurde oder der Verdacht einer Manipulation besteht. Die Benutzenden MÜSSEN bei ihrer Meldung angeben, welche Informationen auf dem Wechseldatenträger gespeichert sind. Hierfür MUSS es in der Institution klare Meldewege und Zuständigkeiten geben.

Die Institution MUSS festlegen, wie Wechseldatenträger behandelt werden sollen, die nach einem Verlust wiedergefunden wurden. Wiedergefundene Wechseldatenträger DÜRFEN NICHT ohne vorherige Überprüfung auf Manipulation und Schadsoftware verwendet werden.

SYS.4.5.A3 ENTFALLEN (B)

Diese Anforderung ist entfallen.

SYS.4.5.A10 Datenträgerverschlüsselung (B)

Wenn Wechseldatenträger außerhalb eines sicheren Bereiches verwendet oder transportiert werden und dabei schutzbedürftige Daten enthalten, MÜSSEN die Daten mit einem sicheren Verfahren verschlüsselt werden.

SYS.4.5.A12 Schutz vor Schadsoftware (B) [Benutzende]

Die Institution MUSS sicherstellen, dass nur Daten auf Wechseldatenträger übertragen werden, die auf Schadsoftware überprüft wurden. Bevor Daten von Wechseldatenträgern verarbeitet werden, MÜSSEN sie auf Schadsoftware überprüft werden.

3.2. Standard-Anforderungen

Gemeinsam mit den Basis-Anforderungen entsprechen die folgenden Anforderungen dem Stand der Technik für diesen Baustein. Sie SOLLTEN grundsätzlich erfüllt werden.

SYS.4.5.A4 Erstellung einer Richtlinie zum sicheren Umgang mit Wechseldatenträgern (S)

Es SOLLTE eine Richtlinie für den richtigen Umgang mit Wechseldatenträgern erstellt werden. Folgende grundlegenden Aspekte SOLLTEN dabei berücksichtigt werden:

- welche Wechseldatenträger genutzt werden und wer diese einsetzen darf,
- welche Daten auf Wechseldatenträgern gespeichert werden dürfen und welche nicht,
- wie die auf Wechseldatenträgern gespeicherten Daten vor unbefugtem Zugriff, Manipulation und Verlust geschützt werden,
- wie die Daten auf den Wechseldatenträgern gelöscht werden sollen,
- mit welchen externen Institutionen Wechseldatenträger ausgetauscht werden dürfen und welche Sicherheitsregelungen dabei zu beachten sind,
- ob Wechseldatenträger an fremde IT-Systeme angeschlossen werden dürfen und was dabei zu beachten ist,
- wie Wechseldatenträger zu versenden sind sowie
- wie der Verbreitung von Schadsoftware über Wechseldatenträger vorgebeugt wird.

Die Institution SOLLTE in der Sicherheitsrichtlinie festlegen, unter welchen Bedingungen Wechseldatenträger gelagert werden sollen. Insbesondere SOLLTE die Institution vorgeben, dass nur berechtigte Benutzende Zugang zu beschriebenen Wechseldatenträgern haben. Die Institution SOLLTE festlegen, dass Angaben des herstellenden Unternehmens zum Umgang mit Datenträgern berücksichtigt werden müssen.

Die Institution SOLLTE die Verwendung von privaten Wechseldatenträgern untersagen.

Es SOLLTE regelmäßig überprüft werden, ob die Sicherheitsvorgaben für den Umgang mit Wechseldatenträgern aktuell sind.

SYS.4.5.A5 Regelung zur Mitnahme von Wechseldatenträgern (S)

Es SOLLTE klare schriftliche Regeln dazu geben, ob, wie und zu welchen Anlässen Wechseldatenträger mitgenommen werden dürfen. Insbesondere SOLLTE festgelegt sein, welche Wechseldatenträger von wem außer Haus transportiert werden dürfen und welche Sicherheitsmaßnahmen dabei zu beachten sind.

SYS.4.5.A6 Datenträgerverwaltung (S) [Fachverantwortliche]

Es SOLLTE eine Verwaltung für Wechseldatenträger geben. Die Wechseldatenträger SOLLTEN einheitlich gekennzeichnet werden. Die Verwaltung für Wechseldatenträger SOLLTE gewährleisten, dass Wechseldatenträger sachgerecht behandelt und aufbewahrt sowie ordnungsgemäß eingesetzt und transportiert werden.

SYS.4.5.A7 Sicheres Löschen der Wechseldatenträger vor und nach der Verwendung (S) [Fachverantwortliche]

Bevor Wechseldatenträger weitergegeben, wiederverwendet oder ausgesondert werden, SOLLTEN sie in geeigneter Weise sicher gelöscht werden.

SYS.4.5.A8 ENTFALLEN (S)

Diese Anforderung ist entfallen.

SYS.4.5.A13 Kennzeichnung der Wechseldatenträger beim Versand (S)

Wechseldatenträger, die versendet werden sollen, SOLLTEN so gekennzeichnet werden, dass die Absendenden und die Empfangenden sie sofort identifizieren können. Die Kennzeichnung der Wechseldatenträger oder deren Verpackung SOLLTE für die Empfangenden eindeutig sein. Die Kennzeichnung von Wechseldatenträgern mit schützenswerten Informationen SOLLTE für Außenstehende keine Rückschlüsse auf Art und Inhalte der Informationen zulassen.

SYS.4.5.A17 Gewährleistung der Integrität und Verfügbarkeit bei Langzeitspeichern (S)

Falls Wechseldatenträger verwendet werden, um Daten für lange Zeiträume zu speichern, SOLLTE die Institution sicherstellen, dass die verwendeten Wechseldatenträger geeignet sind, um die Integrität und Verfügbarkeit der Daten während des gesamten Nutzungszeitraums sicherzustellen. Die Integrität der Daten SOLLTE regelmäßig überprüft werden.

3.3. Anforderungen bei erhöhtem Schutzbedarf

Im Folgenden sind für diesen Baustein exemplarische Vorschläge für Anforderungen aufgeführt, die über dasjenige Schutzniveau hinausgehen, das dem Stand der Technik entspricht. Die Vorschläge SOLLTEN bei erhöhtem Schutzbedarf in Betracht gezogen werden. Die konkrete Festlegung erfolgt im Rahmen einer individuellen Risikoanalyse.

SYS.4.5.A9 ENTFALLEN (H)

Diese Anforderung ist entfallen.

SYS.4.5.A11 Integritätsschutz durch Checksummen oder digitale Signaturen (H)

Es SOLLTE ein Verfahren zum Schutz gegen zufällige oder vorsätzliche Veränderungen eingesetzt werden, mit dem die Integrität von vertraulichen Informationen sichergestellt wird. Die Verfahren zum Schutz vor Veränderungen SOLLTEN dem aktuellen Stand der Technik entsprechen.

SYS.4.5.A14 Sichere Versandart und Verpackung (H)

Die Institution SOLLTE überprüfen, wie vertrauliche Informationen bei einem Versand angemessen geschützt werden können. Es SOLLTE eine sichere Versandverpackung für Wechseldatenträger verwendet werden, bei der Manipulationen sofort zu erkennen sind. Die Institution SOLLTE alle Beteiligten auf notwendige Versand- und Verpackungsarten hinweisen.

SYS.4.5.A15 Verwendung zertifizierter Wechseldatenträger (H)

Die Institution SOLLTE nur Wechseldatenträger verwenden, die zertifiziert sind. Die Zertifizierung SOLLTE insbesondere eine integere Datenerhaltung sowie möglicherweise vorhandene Verschlüsselungsverfahren umfassen.

SYS.4.5.A16 Nutzung dedizierter IT-Systeme zur Datenprüfung (H)

Die Institution SOLLTE dedizierte IT-Systeme als Datenschleuse verwenden, bei denen Daten von einem Wechseldatenträger auf einen anderen übertragen werden und dabei auf Schadsoftware untersucht werden.

4. Weiterführende Informationen

4.1. Wissenswertes

Die International Organization for Standardization beschreibt in der Norm ISO/IEC 27001:2013 in Kapitel A.8.3 wie Wechseldatenträger sicher eingesetzt werden können.