SYS.4: Sonstige Systeme

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.

Datenträger sind danach klassifizierbar, ob sie nur lesbar, einmalig beschreibbar oder wiederbeschreibbar sind. Unterschiede gibt es auch bei der Art der Datenspeicherung (analog oder digital), wie sie bearbeitet werden können oder nach 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* muss auf alle Wechseldatenträger im Informationsverbund angewendet werden.

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* oder 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 von digitalen und analogen Datenträgern, um Informationen zwischen verschiedenen Kommunikationspartnern und IT-Systemen zu übertragen, wird in diesem Baustein nicht betrachtet. Dazu sind die Anforderungen des Bausteins CON.9 *Informationsaustausch* zu erfüllen.

2 Gefährdungslage

Folgende spezifische 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 den sorglosen Umgang der Mitarbeiter umgangen. So kommt es etwa vor, dass Wechseldatenträger während einer Pause unbeaufsichtigt im Besprechungsraum zurück- oder auch im Zugabteil liegengelassen werden.

2.2 Unzureichende Kenntnis über Regelungen

Wenn Mitarbeitern die Regelungen für den korrekten Umgang mit Wechseldatenträgern nicht hinreichend bekannt sind, können sie sich auch nicht daran halten. 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 Systemen. Ursachen für Datenverluste sind etwa Diebstahl oder verlorengegangene Geräte. Die auf den Datenträgern abgelegten Informationen sind in diesen Fällen oft unwiederbringlich verloren. Außerdem können die Informationen fremden Personen 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, ebenso Staub oder Feuchtigkeit. Hinzu kommen beispielsweise Transportschäden. Ein weiterer wichtiger Aspekt ist, dass Datenträger oft in Bereichen mit unterschiedlichem Sicherheitsniveau benutzt werden.

2.6 Verbreitung von Schadprogrammen

Wechseldatenträger werden oft benutzt, um Daten zwischen verschiedenen Geräten und dem Arbeitsplatz auszutauschen. Schadprogramme könnten Daten auf dem Wechseldatenträgern kompromittieren und sich so auf die Arbeitsplatz-Systeme übertragen.

3 Anforderungen

Im Folgenden sind die spezifischen Anforderungen des Bausteins SYS.4.5 *Wechseldatenträger* aufgeführt. Grundsätzlich ist der IT-Betrieb für die Erfüllung der Anforderungen zuständig. Der Informationssicherheitsbeauftragte (ISB) ist bei strategischen Entscheidungen stets einzubeziehen. Außerdem ist der ISB dafür zuständig, dass alle Anforderungen gemäß dem festgelegten Sicherheitskonzept erfüllt und überprüft werden. Zusätzlich kann es noch andere Rollen geben, die weitere Zuständigkeiten bei der Erfüllung von Anforderungen haben. Diese sind dann jeweils explizit in eckigen Klammern in der Überschrift der jeweiligen Anforderungen aufgeführt.

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

3.1 Basis-Anforderungen

Die folgenden Anforderungen MÜSSEN für den Baustein SYS.4.5 *Wechseldatenträger* vorrangig erfüllt werden:

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

Alle Mitarbeiter MÜSSEN für den sicheren Umgang mit Wechseldatenträgern sensibilisiert werden. Die Mitarbeiter MÜSSEN insbesondere darauf hingewiesen werden, wie sie mit den Wechseldatenträgern umgehen sollten, um einem Verlust oder Diebstahl vorzubeugen und eine lange Lebensdauer zu gewährleisten.

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

SYS.4.5.A2 Verlust- bzw. Manipulationsmeldung [Benutzer] (B)

Benutzer MÜSSEN umgehend melden, wenn ein Wechseldatenträger gestohlen wird oder der Verdacht einer Manipulation besteht. Der Benutzer MUSS bei seiner Meldung angeben, welche Informationen auf dem Wechseldatenträger gespeichert sind. Hierfür MUSS es in jeder Institution klare Meldewege und Ansprechpartner geben.

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 vertrauliche Daten enthalten, MÜSSEN sie mit einem sicheren Verfahren verschlüsselt werden.

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

Nur auf Schadsoftware überprüfte Daten DÜRFEN auf Wechseldatenträger übertragen werden. 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 den Baustein SYS.4.5 *Wechseldatenträger*. 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,
- ob und wie private Datenträger genutzt werden dürfen,

- mit welchen externen Mitarbeitern oder Dienstleistern Datenträger ausgetauscht werden dürfen und welche Sicherheitsregelungen dabei zu beachten sind,
- wie Datenträger zu versenden sind sowie
- wie der Verbreitung von Schadsoftware über Wechseldatenträger vorgebeugt wird.

Die Institution SOLLTE in der Sicherheitsrichtlinie festlegen, unter welchen Bedingungen Datenträger gelagert werden sollen. Insbesondere SOLLTE sie vorgeben, dass nur berechtigte Benutzer Zugang zu beschriebenen Datenträgern haben. Sie SOLLTE festlegen, dass Herstellerangaben zum Umgang mit Datenträgern berücksichtigt werden sollen.

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. Darin SOLLTE festgelegt sein, welche Datenträger von wem außer Haus transportiert werden dürfen und welche Sicherheitsmaßnahmen dabei zu beachten sind.

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

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

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

Bevor wiederbeschreibbare Datenträger weitergegeben, wiederverwendet oder ausgesondert werden, SOLLTEN sie in geeigneter Weise gelöscht werden.

SYS.4.5.A8 ENTFALLEN (S)

Diese Anforderung ist entfallen.

SYS.4.5.A13 Angemessene Kennzeichnung der Datenträger beim Versand [Benutzer] (S)

Benutzer SOLLTEN Datenträger, die versendet werden sollen, so kennzeichnen, dass Absender und Empfänger sie sofort identifizieren können. Die Kennzeichnung der Datenträger bzw. deren Verpackung SOLLTE für den Empfänger eindeutig sein. Die Kennzeichnung von Datenträgern mit schützenswerten Informationen SOLLTE für Außenstehende keine Rückschlüsse auf Art und Inhalte der Informationen zulassen.

3.3 Anforderungen bei erhöhtem Schutzbedarf

Im Folgenden sind für den Baustein SYS.4.5 *Wechseldatenträger* exemplarische Vorschläge für Anforderungen aufgeführt, die über das dem Stand der Technik entsprechende Schutzniveau hinausgehen und BEI ERHÖHTEM SCHUTZBEDARF in Betracht gezogen werden SOLLTEN. Die konkrete Festlegung erfolgt im Rahmen einer 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. Die Benutzer SOLLTEN eine sichere Versandverpackung für Datenträger

verwenden, bei der Manipulationen sofort zu erkennen sind. Der Versender SOLLTE alle beteiligten Mitarbeiter auf notwendige Versand- und Verpackungsarten hinweisen.

SYS.4.5.A15 Zertifizierte Produkte (H)

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

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

Die Institution SOLLTE dedizierte 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.

5 Anlage: Kreuzreferenztabelle zu elementaren Gefährdungen

Die Kreuzreferenztabelle enthält die Zuordnung von elementaren Gefährdungen zu den Anforderungen. Anhand dieser Tabelle lässt sich ermitteln, welche elementaren Gefährdungen durch welche Anforderungen abgedeckt sind. Durch die Umsetzung der aus den Anforderungen abgeleiteten Sicherheitsmaßnahmen wird den entsprechenden elementaren Gefährdungen entgegengewirkt. Die Buchstaben in der zweiten Spalte (C = Vertraulichkeit, I = Integrität, A = Verfügbarkeit) zeigen an, welche Grundwerte der Informationssicherheit durch die Anforderung vorrangig geschützt werden. Die folgenden elementaren Gefährdungen sind für den Baustein SYS.4.5 *Wechseldatenträger* von Bedeutung.

G 0.2 Ungünstige klimatische Bedingungen

G 0.4 Verschmutzung, Staub, Korrosion

G 0.14 Ausspähen von Informationen (Spionage)

G 0.16 Diebstahl von Geräten, Datenträgern oder Dokumenten

G 0.17 Verlust von Geräten, Datenträgern oder Dokumenten

G 0.19 Offenlegung schützenswerter Informationen

G 0.20 Informationen oder Produkte aus unzuverlässiger Quelle

G 0.21 Manipulation von Hard- oder Software

G 0.22 Manipulation von Informationen

G 0.23 Unbefugtes Eindringen in IT-Systeme

G 0.29 Verstoß gegen Gesetze oder Regelungen

G 0.39 Schadprogramme

G 0.46 Integritätsverlust schützenswerter Informationen