Bundesamt
für Sicherheit in der
Informationstechnik

Umsetzungshinweise zum Baustein SYS.4.5 Wechseldatenträger

1. Einleitung

Wechseldatenträger werden oft eingesetzt, um Daten zu transportieren, zu speichern oder um mobil auf sie zugreifen zu können. Zu Wechseldatenträgern gehören beispielsweise 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 bei ihrer Bauform. So gibt es auswechselbare Datenträger (z. B. verbaute Festplatten) oder externe Datenspeicher (z. B. USB-Sticks) .

2. Maßnahmen

Im Folgenden sind spezifische Maßnahmen für die Anforderungen des Bausteins SYS.4.5 *Wechseldatenträger* aufgeführt.

Alle Maßnahmen (gekennzeichnet mit M) sind aufsteigend nummeriert und korrespondieren mit den entsprechenden Anforderungen (gekennzeichnet mit A).

2.1. Maßnahmen zum Baustein SYS.4.5 Wechseldatenträger

SYS.4.5.M1 Sensibilisierung der Mitarbeiter zum sicheren Umgang mit Wechseldatenträgern (B)

In Institutionen werden die verschiedensten Arten von Wechseldatenträgern eingesetzt. Ebenso nimmt die Zahl von Geräten zu, die neben ihrer eigentlichen Funktion zusätzlich als Wechseldatenträgern einsetzbar

sind. Damit steigt sowohl die Zahl möglicher Verbreitungswege für Informationen als auch die Zahl möglicher Sicherheitslücken. Einige dieser Sicherheitsrisiken lassen sich zwar technisch minimieren. Dennoch ist es notwendig, die Mitarbeiter zum sicheren und sachgerechten Umgang mit Wechseldatenträgern zu schulen.

Alle Mitarbeiter müssen über die Arten und Einsatzmöglichkeiten von Wechseldatenträgern aufgeklärt werden. Dazu gehört auch, sie über die verschiedenen Bauformen und Varianten zu informieren, also dass beispielsweise auch ein Smartphone als Wechseldatenträger genutzt werden kann. Außerdem sollten die Mitarbeiter über potenzielle Risiken und Probleme bei der Nutzung informiert sowie über den Nutzen, aber auch die Grenzen der eingesetzten Sicherheitsmaßnahmen aufgeklärt werden. Die Mitarbeiter sind zudem regelmäßig über neue Gefahren und Aspekte von Wechseldatenträgern zu unterrichten, z. B. über entsprechende Artikel im Intranet oder in der Mitarbeiterzeitschrift.

Die Benutzer müssen darauf hingewiesen werden, wie sie sorgfältig mit den Wechseldatenträgern umgehen sollten, um einem Verlust oder Diebstahl vorzubeugen bzw. um eine lange Lebensdauer zu gewährleisten. Dabei sollten beispielsweise Fragen zur Aufbewahrung außerhalb von Büro- oder Wohnräumen sowie zur Empfindlichkeit gegenüber zu hohen oder zu niedrigen Temperaturen behandelt werden. Beschädigungen oder Verluste sind zeitnah zu melden.

Weitere Aspekte, auf die die Benutzer hingewiesen werden sollten, sind:

- 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 Daten auf Wechseldatenträgern sicher gelöscht werden können und wie Datenträger zu entsorgen sind.

SYS.4.5.M2 Verlust- bzw. Manipulationsmeldung (B)

Der Verlust oder Diebstahl eines Wechseldatenträgers muss umgehend gemeldet werden. Das gilt auch für private Datenträger, die ausnahmsweise dienstlich genutzt werden. Hierfür muss es in jeder Institution klare Meldewege und Ansprechpartner geben.

Ausfälle oder Defekte sollten ebenfalls gemeldet werden, auch bei geringpreisigen Wechseldatenträgern, damit erkannt werden kann, ob hiervon größere Lieferungen betroffen sind. Insbesondere bei Datenträgern, die für Datensicherungen und Archivierung eingesetzt werden, ist eine hohe Verlässlichkeit und eine lange Lebensdauer wichtig. Verliert ein Mitarbeiter einen Wechseldatenträger oder wird er gestohlen, muss wiederum schnell gehandelt werden, da es hier nicht nur darum geht, das Gerät wiederzubeschaffen, sondern auch darum, potenziellen Missbrauch der betroffenen Informationen zu verhindern.

Wenn verlorene Datenträger wieder auftauchen, wird dringend empfohlen, sie auf eventuelle Manipulationen zu untersuchen, z. B. ob Schrauben geöffnet oder Siegel entfernt wurden oder ob sich das Gewicht gegenüber dem Auslieferungszustand geändert hat. Besteht ein Verdacht, sollte das Gerät entweder gleich entsorgt oder von einem Spezialisten weiter untersucht werden. Um sicherzustellen, dass sich keine manipulierten Programme oder Schadsoftware auf den wiedererlangten Datenträgern befinden, sollte der Datenträger daraufhin untersucht werden. Im Zweifelsfall sollte der Datenträger nicht weiter verwendet werden.

Sollen Datenträger entsorgt werden, sollte vorher sichergestellt werden, dass die auf den Datenträgern abgespeicherten Restinformationen nicht in falsche Hände gelangen können. Hierzu sollte er sicher gelöscht werden.

SYS.4.5.M3 ENTFALLEN (B)

Die zugehörige Anforderung ist entfallen.

SYS.4.5.M4 Erstellung einer Richtlinie zum sicheren Umgang mit Wechseldatenträgern (S)

Über Wechseldatenträger können je nach technischer Auslegung eine große Menge an Daten bei hohen Durchsatzraten ausgetauscht werden. Die Varianten von Wechseldatenträgern sind mittlerweile vielfältig. Auch sind sie nicht immer auf den ersten Blick als solche zu erkennen. So gibt es beispielsweise Armbanduhren oder Schlüsselanhänger mit integriertem Datenspeicher. Die gängige Größe dieser Datenträger beginnt hier bei einigen hundert Megabyte und kann durchaus bis zu mehreren Terabyte reichen.

Daher sollten für den Umgang mit Wechseldatenträgern einige grundlegende Aspekte berücksichtigt und in einer Richtlinie festgehalten werden. Es ist zu klären,

- welche Wechseldatenträger in der Institution genutzt werden sollen wer diese einsetzt,
- welche Daten auf Wechseldatenträgern gespeichert werden dürfen und welche nicht,
- wie die auf diesen Wechseldatenträgern gespeicherten Daten vor unbefugtem Zugriff, Manipulation und Verlust geschützt werden,
- mit welchen externen Mitarbeitern oder Dienstleistern Wechseldatenträgern ausgetauscht werden dürfen und welche Sicherheitsregelungen dabei zu beachten sind,
- wie verhindert wird, dass Wechseldatenträgern dazu benutzt werden, unbefugt Informationen weiterzugeben,
- wie Wechseldatenträger zu versenden sind,
- wie Wechseldatenträger sicher zu löschen sind,
- wie gegen die Verbreitung von Schadsoftware über die Wechseldatenträger vorgebeugt wird.

Es sollte außerdem festgelegt werden, ob Mitarbeiter ihre privaten Wechseldatenträger innerhalb der Institution nutzen dürfen, und auch umgekehrt, ob Mitarbeiter private Daten auf dienstlichen Wechseldatenträgern speichern oder nutzen dürfen. Grundsätzlich sollte darauf verzichtet werden, dass Daten der Institution auf privaten Datenträgern gespeichert werden. Ebenso ist zu klären, ob die von Externen mitgebrachten Wechseldatenträger innerhalb der Institution eingesetzt werden dürfen, beispielsweise um Dateien auszutauschen.

Es sollte regelmäßig überprüft werden, ob die Sicherheitsvorgaben für den Umgang mit Wechseldatenträgern noch aktuell sind, angefangen damit, ob alle Varianten von derzeit gebräuchlichen Datenträgern noch erfasst sind.

SYS.4.5.M5 Regelung zur Mitnahme von Wechseldatenträgern (S)

Die IT-Komponenten, die innerhalb einer hauseigenen Liegenschaft eingesetzt werden, sind im Allgemeinen durch infrastrukturelle Sicherheitsmaßnahmen ausreichend vor Missbrauch und Diebstahl geschützt. Wechseldatenträgern werden jedoch oft außer Haus eingesetzt, z. B. bei Dienstreisen. Um diese ausreichend schützen zu können, muss die Mitnahme solcher Datenträger klar geregelt werden.

Dabei sollte festgelegt werden,

- welche Wechseldatenträger außer Haus mitgenommen werden dürfen,
- wer Wechseldatenträger außer Haus mitnehmen darf und
- welche grundlegenden Sicherheitsmaßnahmen dabei beachtet werden müssen (Virenschutz, Verschlüsselung schützenswerter Daten, Aufbewahrung etc.).

Die Art und der Umfang der anzuwendenden Sicherheitsmaßnahmen für extern eingesetzte Datenträger hängen einerseits vom Schutzbedarf der darauf gespeicherten IT-Anwendungen und Daten und andererseits von der Sicherheit der Einsatz- bzw. Aufbewahrungsorte ab.

Es sollten nur solche Wechseldatenträger extern eingesetzt werden, die explizit dafür vorgesehen sind. Insbesondere außerhalb der institutionseigenen Liegenschaften sollten die Benutzer für den Schutz der ihnen anvertrauten Datenträger sorgen. Darauf und auf die zu ergreifenden Vorsichtsmaßnahmen sind sie hinzuweisen. Dazu gehören folgende Regeln:

- Wechseldatenträger müssen stets sicher aufbewahrt werden.
- Wechseldatenträger, die schützenswerte Daten enthalten, sollten möglichst komplett verschlüsselt werden. Wenn solche Datenträger eine Verschlüsselungsfunktion ohne weitere Hilfsmittel ermöglichen, ist es empfehlenswert, diese Funktionen auch dann zu nutzen, wenn weniger schützenswerte Daten auf dem Datenträger enthalten sind.
- Die Verwaltung, Wartung und Weitergabe von extern eingesetzten Wechseldatenträgern sollte geregelt werden. Hierzu können beispielsweise Pools eingerichtet werden.
- Es sollte notiert werden, wann und von wem welche Datenträger außer Haus eingesetzt wurden.

SYS.4.5.M6 Datenträgerverwaltung (S)

Aufgabe der Datenträgerverwaltung als Teil der Betriebsmittelverwaltung ist es, den Zugriff auf Wechseldatenträger im erforderlichen Umfang und in angemessener Zeit gewährleisten zu können. Dies erfordert eine geregelte Verwaltung der Datenträger, die eine einheitliche Kennzeichnung sowie eine Führung von Bestandsverzeichnissen erforderlich macht. Weiterhin ist im Rahmen der Datenträgerverwaltung die sachgerechte Behandlung und Aufbewahrung der Datenträger, deren ordnungsgemäßer Einsatz und Transport und schließlich auch noch die Löschung bzw. Vernichtung der Datenträger zu gewährleisten.

Bestandsverzeichnisse ermöglichen einen schnellen und zielgerichteten Zugriff auf Wechseldatenträger. Sie geben beispielsweise Auskunft über Aufbewahrungsort, Aufbewahrungsdauer und berechtigte Empfänger.

Die äußerliche **Kennzeichnung** von Wechseldatenträgern ermöglicht deren schnelle Identifizierung. Die Kennzeichnung sollte jedoch für Unbefugte keinen Rückschluss auf den Inhalt erlauben (z. B. die Beschriftung eines USB-Sticks mit dem Stichwort "vertraulich"), um einen Missbrauch zu erschweren. Es sollte aber beachtet werden, dass flankierende Regelungen und Vorgaben, die für die Institution gelten, eine entsprechende Kennzeichnung fordern. In diesem Fall müssen in der Regel ergänzende Anforderungen aus diesen Regelungen und Vorgaben umgesetzt werden. Eine festgelegte Struktur von Kennzeichnungsmerkmalen (z. B. Datum, Ablagestruktur, lfd. Nummer) erleichtert die Zuordnung in Bestandsverzeichnissen.

Für eine **sachgerechte Behandlung** von Wechseldatenträgern sind die Herstellerangaben, die üblicherweise auf der Verpackung zu finden sind, heranzuziehen. Hinsichtlich der Aufbewahrung von Datenträgern sind einerseits Maßnahmen zur Lagerung (magnetfeld- und staubgeschützt, klimagerecht) und andererseits Maßnahmen zur Verhinderung des unbefugten Zugriffs (geeignete Behältnisse, Schränke, Räume) zu treffen.

Für die interne Weitergabe von Datenträger können Regelungen getroffen werden wie Quittungsverfahren, Abhol-/Mitnahmeberechtigungen sowie das Führen von Bestandsverzeichnissen über den Verbleib der Datenträger.

Für den Fall, dass **von Dritten erhaltene Datenträger** eingesetzt werden, sind Regelungen über deren Behandlung vor dem Einsatz zu treffen. Zum Beispiel sollten Dateien grundsätzlich auf Schadsoftware überprüft werden. Dies gilt entsprechend auch vor dem erstmaligen Einsatz neuer digitaler Datenträger. Es ist empfehlenswert, nicht nur beim Empfang, sondern auch vor dem Versenden von digitalen Datenträgern diese auf Schadprogramme zu überprüfen.

Eine geregelte Vorgehensweise für die Löschung oder Vernichtung von Datenträgern verhindert den Missbrauch der gespeicherten Daten. Bevor Wechseldatenträger wiederverwendet werden, sind die darauf gespeicherten Daten sicher zu löschen.

SYS.4.5.M7 Sicheres Löschen der Datenträger vor und nach der Verwendung (S)

Hinweise zum sicheren Löschen von Daten finden sich im Baustein CON.6 *Löschen und Vernichten*.

SYS.4.5.M8 ENTFALLEN (S)

Die zugehörige Anforderung ist entfallen.

SYS.4.5.M9 ENTFALLEN (H)

Die zugehörige Anforderung ist entfallen.

SYS.4.5.M10 Datenträgerverschlüsselung (B)

Vertrauliche Informationen können auf verschiedene Weise verschlüsselt und damit vor unbefugter Kenntnisnahme geschützt werden. So kann beispielsweise der komplette Datenträger, eine einzelne Partition oder nur eine einzelne Datei verschlüsselt werden. Aus Sicherheitssicht ist es besser, den kompletten Datenträger zu verschlüsseln, da dann weniger Benutzereingriffe erforderlich sind und alle Daten vor unbefugtem Zugriff geschützt sind. Werden nur einzelne Dateien oder Dateicontainer verschlüsselt, besteht die Gefahr, dass versehentlich schützenswerte Daten in unverschlüsselten Bereichen abgelegt werden. Zudem muss der Benutzer hierfür explizit ein Verschlüsselungsprogramm starten.

Datenträgerverschlüsselung lässt sich mit Software, aber auch mit Hardware-Unterstützung umsetzen. Software-Lösungen sind z. B. BitLocker von Microsoft oder das Open-Source-Programm VeraCrypt. Wechseldatenträger, wie USB-Sticks, sollten möglichst immer vollständig verschlüsselt werden, auch wenn sie nur gelegentlich für vertrauliche Informationen eingesetzt werden.

Die kryptographischen Schlüssel sollten sicher erzeugt und getrennt vom verschlüsselten Wechseldatenträger aufbewahrt werden (siehe CON.1 *Kryptokonzept*). Hierfür können beispielsweise Chipkarten oder USB-Token eingesetzt werden. Eine solche Trennung ist bei der Verschlüsselung von USB-Sticks in der Regel nicht möglich, was bei der Sicherheitsanalyse berücksichtigt werden sollte.

Um den Anforderungen der Vertraulichkeit der zu übertragenden Informationen zu entsprechen, sollten die IT-Systeme der Absender und der Empfänger den Zugriffsschutz auf das Verschlüsselungsprogramm ausreichend gewährleisten. Gegebenenfalls sollte dieses Programm auf einem auswechselbaren Datenträger gespeichert, verschlossen aufbewahrt und nur bei Bedarf eingespielt und genutzt werden.

Genutzte Passwörter sollten den Regelungen der Institution entsprechen. Weitere Hinweise dazu finden sich im Baustein ORP.4 *Identitäts- und Berechtigungsmanagement*.

SYS.4.5.M11 Integritätsschutz durch Checksummen oder digitale Signaturen (H)

Ist für den Datenaustausch lediglich die Integrität der zu übermittelnden Daten sicherzustellen, muss unterschieden werden, ob ein Schutz nur gegen zufällige Veränderungen, z. B. durch Übertragungsfehler, oder auch gegen Manipulationen geleistet werden soll. Sollen ausschließlich zufällige Veränderungen erkannt werden, können Checksummen-Verfahren (z. B. Cyclic Redundancy Checks, CRC) oder fehlerkorrigierende Codes eingesetzt werden. Schutz gegenüber Manipulationen bieten darüber hinaus Verfahren, die mithilfe eines symmetrischen Verschlüsselungsalgorithmus (z. B. AES) aus der zu übermittelnden Information einen so genannten Message Authentication Code (MAC) erzeugen. Andere Verfahren bedienen sich eines asymmetrischen Verschlüsselungsalgorithmus (z. B. RSA) in Kombination mit einer Hashfunktion und erzeugen eine "digitale Signatur". Die jeweiligen erzeugten "Fingerabdrücke" (Checksumme, fehlerkorrigierende Codes, MAC, digitale Signatur) werden über einen unabhängigen Transportweg an den Empfänger übertragen und können von diesem überprüft werden.

SYS.4.5.M12 Schutz vor Schadsoftware (B)

Es liegen keine Hinweise zur Umsetzung vor. Anregungen aus der Praxis werden gerne unter grundschutz@bsi.bund.de entgegengenommen.

SYS.4.5.M13 Angemessene Kennzeichnung der Datenträger beim Versand (S)

Es liegen keine Hinweise zur Umsetzung vor. Anregungen aus der Praxis werden gerne unter grundschutz@bsi.bund.de entgegengenommen.

SYS.4.5.M14 Sichere Versandart und Verpackung (H)

Der Versand oder Transport von Wechseldatenträgern muss so erfolgen, dass sie möglichst nicht beschädigt werden können (z. B. Magnetbandversandtasche, luftgepolsterte Umschläge). Die Verpackung des Datenträgers ist an seiner Schutzbedürftigkeit auszurichten (z. B. mittels verschließbaren Transportbehältnissen). Versand- oder Transportarten (z. B. Kuriertransport) müssen ebenso festgelegt werden wie das Nachweisverfahren über den Versand (z. B. Begleitzettel, Versandscheine) und den Eingang beim Empfänger (z. B. Empfangsbestätigung).

SYS.4.5.M15 Zertifizierte Produkte (H)

Es liegen keine Hinweise zur Umsetzung vor. Anregungen aus der Praxis werden gerne unter grundschutz@bsi.bund.de entgegengenommen.

SYS.4.5.M16 Nutzung dedizierter Systeme zur Datenprüfung (H)

Es liegen keine Hinweise zur Umsetzung vor. Anregungen aus der Praxis werden gerne unter grundschutz@bsi.bund.de entgegengenommen.

3. Weiterführende Informationen

3.1. Wissenswertes

Hier werden ergänzende Informationen aufgeführt, die im Rahmen der Maßnahmen keinen Platz finden, aber dennoch beachtenswert sind. Derzeit liegen für diesen Baustein keine entsprechenden Informationen vor. Sachdienliche Hinweise nimmt die IT-Grundschutz-Hotline gerne unter grundschutz@bsi.bund.de entgegen.

3.2. Quellenverweise

Für den Umsetzungshinweis SYS.4.5 *Wechseldatenträger* sind keine Quellenverweise vorhanden.