Bundesamt
für Sicherheit in der
Informationstechnik

INF: Infrastruktur

Umsetzungshinweise zum Baustein INF.9 Mobiler Arbeitsplatz

1 Beschreibung

1.1 Einleitung

Mithilfe von immer leistungsfähigeren IT-Geräten, wie Laptops, Smartphones oder Tablets, können Mitarbeiter nahezu an jedem Platz bzw. von überall arbeiten. Das bedeutet, dass dienstliche Aufgaben häufig nicht mehr nur in Räumen und Gebäuden der Institution erfüllt werden müssen, sondern an wechselnden Arbeitsplätzen in unterschiedlichen Umgebungen erledigt werden. Ob in Hotelzimmern, in Zügen oder bei Kunden, das mobile Arbeiten verändert die Dauer, Lage und Verteilung der Arbeitszeiten.

In mobilen Arbeitsplatz-Umgebungen kann die Sicherheit der Infrastruktur, wie sie in einer Büroumgebung anzutreffen ist, nicht vorausgesetzt werden. Daher sind Sicherheitsanforderungen erforderlich, die eine mit einem Büroraum vergleichbare Sicherheitssituation herbeiführen.

1.2 Lebenszyklus

Planung und Konzeption

Bevor ein Mitarbeiter einen mobilen Arbeitsplatz benutzt, muss entschieden werden, ob der Platz dafür überhaupt geeignet ist. Dafür benötigen die Mitarbeiter Auswahlkriterien, die von der Institution zu definieren sind (siehe INF.9.M1 *Geeignete Auswahl und Nutzung eines mobilen Arbeitsplatzes).*

Die Sicherheit mobiler Arbeitsplätze basiert größtenteils auf geeigneten organisatorischen Regelungen und personellen Maßnahmen. Daraus ergeben sich Anforderungen, die in den Maßnahmen INF.9.M2 *Regelungen für mobile Arbeitsplätze und* INF.9.M8 *Sicherheitsrichtlinie für mobile Arbeitsplätze* erläutert werden.

Umsetzung

Für alle Arbeiten von unterwegs ist zu regeln, welche Informationen außerhalb der Institution transportiert und bearbeitet werden dürfen und welche Schutzvorkehrungen dabei zu treffen sind (siehe INF.9.M2 *Regelungen für mobile Arbeitsplätze*). Dabei ist auch zu klären, unter welchen Rahmenbedingungen Mitarbeiter mit mobilen IT-Systemen auf interne Informationen ihrer Institution zugreifen dürfen.

Betrieb

Beim mobilen Arbeiten müssen nicht nur die mitgenommenen IT-Systeme (zum Beispiel Laptops, Smartphones oder Tablets), sondern auch die unterwegs bearbeiteten Informationen sorgfältig behandelt werden. So sollten die vom Arbeitgeber vorgesehenen Regelungen über die Arbeitsumgebung eingehalten sowie die Arbeitsmaterialien sicher aufbewahrt werden (siehe INF.9.M3 *Zutritts- und Zugriffsschutz* und INF.9.M4 *Arbeiten mit fremden IT-Systemen).*

Bei erhöhtem Schutzbedarf sind zusätzlich die Maßnahmen wie Diebstahlsicherungen (siehe INF.9.M10 *Einsatz von Diebstahlsicherungen)* oder gesicherte Kommunikationsverbindungen (siehe INF.9.M11 *Verbot der Nutzung unsicherer Umgebungen*) zu beachten.

Aussonderung

Gerade in fremden Infrastruktur-Umgebungen ist es wichtig, Datenträger und Ausdrucke sorgsam zu entsorgen und nicht einfach in den Müll zu werfen. Für eine sichere Aussonderung ist es daher erforderlich, neben den Anforderungen aus INF.9.M6 Entsorgung von vertraulichen Informationen auch die Anforderungen aus dem Baustein OPS.1.2.7 Verkauf/Aussonderung von IT zu berücksichtigen.

2 Maßnahmen

Im Folgenden sind spezifische Umsetzungshinweise im Bereich "Mobiler Arbeitsplatz" aufgeführt.

2.1 Basis-Maßnahmen

Die folgenden Maßnahmen sollten vorrangig umgesetzt werden:

INF.9.M1 Geeignete Auswahl und Nutzung eines mobilen Arbeitsplatzes (B)

Dank immer kleinerer und leistungsfähigerer IT-Systeme ist es heutzutage möglich, nahezu überall zu arbeiten. Dadurch kann jeder beliebige Ort oder Platz (weltweit) als mobiler Arbeitsplatz genutzt werden. Zum Beispiel ist es möglich in Hotelzimmern, in Bahnen, in Flugzeugen oder in Räumlichkeit beim Kunden zu arbeiten.

Solche mobilen Arbeitsplätze können vom Benutzer nur sehr beschränkt eingerichtet werden und müssen oft wie vorgefunden genutzt werden. Daher sollte jeder mobile Benutzer entscheiden können, ob eine Umgebung als mobiler Arbeitsplatz geeignet ist. Benutzer sollten deshalb für die Auswahl mit praktischen Handreichungen unterstützt werden.

Gründe, die gegen einen mobilen Arbeitsplatz sprechen, sind beispielsweise:

- Die zu bearbeitenden Informationen sind zu vertraulich, um außerhalb der geschützten Büroumgebung bearbeitet zu werden (siehe auch INF.9.M2 *Regelungen für mobile Arbeitsplätze*).
- Die Umgebung erlaubt es nicht, ohne Einsichtnahme Dritter zu arbeiten, zum Beispiel in engen Sitzplätzen in Bahnen oder Flugzeugen.
- Es ist weder eine Stromversorgung noch eine Netzanbindung vorhanden.
- Die Nutzung von mobilen IT-Geräten ist verboten, zum Beispiel im Flugzeug oder in fremden Büroräumen.
- Gründe, die für einen mobilen Arbeitsplatz sprechen, sind beispielsweise:
- Da viele mobile IT-Systeme durch Stürze zerstört werden, sollte ein stabiler Platz vorhanden sein, um diese abzustellen.
- Die Umgebung sollte nicht zu laut sein und ein angemessenes Arbeitsklima ermöglichen.
- Die Umgebung sollte ausreichend beleuchtet sein. Das Monitorlicht alleine reicht auf Dauer nicht. Störende Blendungen, Reflexionen oder Spiegelungen sollten vermieden werden.
- Der Monitor sollte so aufgestellt werden können, dass getätigte Eingaben für Dritte nicht einsehbar sind. Für Laptops gibt es Monitorfolien, die eine Einsichtnahme von der Seite verhindern.

- Die Umgebung sollte außerdem gewährleisten, dass die mobilen IT-Systeme nicht beeinträchtigt werden, sie sollte also nicht zu feucht, zu kalt oder zu warm sein. Der Mitarbeiter wird zwar solche Bedingungen auch um seines eigenen Wohlbefindens willen meiden, während er die Geräte benutzt. Damit die Geräte aber auch entsprechend geeignet aufbewahrt werden, sollten Regelungen festgelegt sein.
- Mobile Geräte sollten bei erhöhtem Schutzbedarf gegen Diebstahl geschützt werden (siehe auch INF.9.M10 *Einsatz von Diebstahlsicherungen*). Die Umgebung sollte hierfür die notwendigen Voraussetzungen bieten. Es muss zum Beispiel möglich sein, das Kabelschloss an einen festen Gegenstand anzuschließen, um den befestigen Laptop gegen eine einfache Wegnahme zu sichern. Wenn möglich, sollten Fenster und Türen des mobilen Arbeitsplatzes ge- und verschlossen werden, wenn der Mitarbeiter den Raum verlässt. Das ist beispielsweise bei Hotelzimmern oder Besprechungsräumen oft möglich.

In fremden Umgebungen wie Hotels ist es auch empfehlenswert, sich über das richtige Verhalten bei Bränden oder anderen Notfällen zu informieren, zum Beispiel über Warntöne und Fluchtwege.

INF.9.M2 Regelungen für mobile Arbeitsplätze (B)

Für alle Arbeiten unterwegs ist zu regeln, welche Informationen (Akten, Datenträger, IT-Systeme) außerhalb des Unternehmens bzw. der Behörde transportiert und bearbeitet werden dürfen und welche Schutzvorkehrungen dabei zu treffen sind.

IT-Systeme und Datenträger, die außerhalb der eigenen Institution eingesetzt werden, sind eher Risiken ausgesetzt, als solche, die sich innerhalb geschützter Räumlichkeiten befinden. Deswegen müssen folgende Punkte geregelt werden:

- Die Benutzer müssen darüber informiert sein, welche Informationen mit mobilen IT-Systemen unterwegs verarbeitet werden dürfen. Die Daten sollten dementsprechend klassifiziert sein, um den Benutzern Einschränkungen transparent zu machen. Dienstgeheimnisse dürfen nur dann auf mobilen IT-Systemen verarbeitet werden, wenn hierfür geeignete und freigegebene Sicherheitsmechanismen eingesetzt werden.
- IT-Systeme oder Datenträger, die vertrauliche Informationen enthalten, sollten möglichst komplett verschlüsselt werden. Wenn IT-Systeme eine Verschlüsselungsfunktion ohne weitere Hilfsmittel ermöglichen, ist es empfehlenswert, dass diese Funktionen immer genutzt werden. Dies gilt auch dann, wenn lediglich wenig vertrauliche Daten auf den IT-Systemen enthalten sind. Informationen, die ein hohes Maß an Sicherheit verlangen (zum Beispiel Angebote, Konstruktionsdaten, Wirtschaftsdaten der Institution) sollten stets verschlüsselt auf dem mobilen IT-System abgelegt werden.
- Beim Einsatz mobiler IT-Systeme ist zu klären, ob mobile Mitarbeiter von unterwegs auf interne Daten ihrer Institution zugreifen dürfen. Ist dies vorgesehen, muss der Zugriff angemessen geschützt werden.
- Es muss geklärt werden, ob mobile IT-Systeme auch für private Zwecke benutzt werden dürfen, beispielsweise für die private Kommunikation oder Computerspiele.
- Die Benutzer sollten darauf hingewiesen werden, wie sie sorgfältig mit den mobilen IT-Systemen und Datenträgern umgehen sollten, um einem Verlust oder Diebstahl vorzubeugen und eine lange Lebensdauer zu gewährleisten. Zu diesen Maßnahmen zählen die sorgsame Aufbewahrung außerhalb von Büro- oder Wohnräumen und das Beachten der Empfindlichkeiten gegenüber zu hohen oder zu niedrigen Temperaturen.
- Die Verwaltung, Wartung und Weitergabe von mobilen IT-Systemen und Datenträgern sollte geregelt werden.
- Wechseln die Benutzer, müssen alle benötigten Passwörter gesichert weitergegeben werden.
- IT-Systeme und Datenträger müssen stets sicher aufbewahrt werden. Bei Dienstreisen sollten sie nicht unbeaufsichtigt gelassen werden. Insbesondere sollten sie nicht in Fahrzeugen zurückgelassen werden.

- IT-Systeme wie Laptops, Tablets oder Smartphones und deren Anwendungen können im Allgemeinen durch PINs oder Passwörter abgesichert werden. Diese Mechanismen sollten prinzipiell genutzt werden.
- Es sollte protokolliert werden, wann und von wem, welche IT-Komponenten außer Haus eingesetzt wurden.
- Es sollte geregelt werden, wie mobile IT-Systeme oder Datenträger zu entsorgen sind (siehe INF.9.M6 *Entsorgung von vertraulichen Informationen*).

Zusätzlich sollte für die Benutzer ein kurzes und übersichtliches Merkblatt über die sichere Nutzung von mobilen IT-Systemen erstellt werden.

Mobile IT-Systeme sollten möglichst nicht unbeaufsichtigt bleiben. Falls ein mobiles IT-System in einem Kraftfahrzeug zurückgelassen werden muss, sollte es von außen nicht für Dritte sichtbar sein. Da ein sichtbares mobiles IT-System einen Wert darstellt, der potenzielle Diebe anlocken könnte, sollten diese generell abgedeckt oder im Kofferraum eingeschlossen werden.

Werden mobile IT-Systeme in fremden Büroräumen benutzt, sind auch die geltenden Sicherheitsregelungen der besuchten Institution zu beachten.

In Räumlichkeiten außerhalb der eigenen Institution, wie beispielsweise Hotelzimmern, sollten mobile IT-Systeme nicht ungeschützt liegen. Auch sollten alle Passwort-Schutzmechanismen aktiviert werden. Wenn möglich, sollten IT-Geräte in einem Schrank oder Rollcontainer eingeschlossen werden, um Gelegenheitsdiebe zu behindern.

Mitnahme mobiler IT

Weiterhin muss die Mitnahme von Datenträgern und IT-Komponenten klar geregelt werden. Dabei muss festgelegt werden,

- welche IT-Komponenten beziehungsweise Datenträger außer Haus mitgenommen werden dürfen,
- wer IT-Komponenten beziehungsweise Datenträger außer Haus mitnehmen darf,
- welche grundlegenden Sicherheitsmaßnahmen dabei beachtet werden müssen (beispielsweise Virenschutz, Verschlüsselung vertraulicher Daten, Aufbewahrung).

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

Grundsätzlich sollte für alle IT-Komponenten, die extern eingesetzt werden sollen, eine entsprechende Genehmigung eingeholt werden.

Es sollte möglichst stichprobenartig überprüft werden, ob die Regelungen für die Mitnahme von Datenträgern und IT-Komponenten eingehalten werden. Das bietet sich vor allem bei größeren Institutionen an, bei denen der Zutritt zu den Liegenschaften durch Pförtner beziehungsweise Sicherheitsdienste kontrolliert wird.

Sensibilisierung der Benutzer

Je kleiner und leichter IT-Systeme werden, desto leichtfertiger wird erfahrungsgemäß damit umgegangen. Daher sollten Mitarbeiter für den Wert mobiler IT-Systeme und den Wert der darauf gespeicherten Informationen sensibilisiert werden. Da es bei mobilen IT-Systemen eine große Bandbreite von Varianten und Kombinationsmöglichkeiten gibt, sollten sie vor allem über die spezifischen Gefährdungen und Maßnahmen der von ihnen benutzten Geräte aufgeklärt werden. Das kann sowohl Smartphones als auch Tablets oder Laptops mit ihren jeweils unterschiedlichen Schnittstellen betreffen.

Die Mitarbeiter sollten auch darüber aufgeklärt werden, dass sie vertrauliche Informationen unterwegs nicht mit jedem austauschen und unterwegs auch nicht in Hör- und Sichtweite von Externen darüber sprechen sollten. Insbesondere sollte die Identität jedes Kommunikationspartners vor detaillierten Auskünften hinterfragt werden. Die Sensibilisierung der Benutzer sollte im Rahmen der Bausteinanforderungen von *ORP.3 Sensibilisierung und Schulung zur Informationssicherheit* erfolgen.

INF.9.M3 Zutritts- und Zugriffsschutz (B)

Fenster und nach außen gehende Türen (zum Beispiel Balkone, Dachterrassen) müssen in Zeiten, in denen ein Raum nicht besetzt ist, geschlossen werden. Auch Außentüren sind abzuschließen. Im Keller- und Erdgeschoss und, je nach Fassadengestaltung, auch in den höheren Etagen, bieten offene Fenster und Türen Einbrechern ideale Einstiegsmöglichkeiten, die auch während der Betriebszeiten eines mobilen Arbeitsplatzes genutzt werden. Daher ist es notwendig Mitarbeiter darauf hinzuweisen, dass Fenster und Türen zu schließen sind, wenn die Räume verlassen werden.

Die Türen nicht besetzter Räume sollten abgeschlossen werden. Dadurch wird verhindert, dass Unbefugte auf darin befindliche Unterlagen und IT-Einrichtungen zugreifen können. Einzelne Büroräume abzuschließen, ist insbesondere dann wichtig, wenn sich diese in Bereichen mit Publikumsverkehr befinden oder der Zutritt nicht durch andere Maßnahmen kontrolliert wird. Türen müssen nicht abgeschlossen werden, wenn diese flurseitig über einen Blindknauf verfügen. Voraussetzung hierfür ist allerdings, dass die befugten Mitarbeiter ihren Schlüssel stets mit sich führen.

Wird während der normalen Arbeitszeiten sichergestellt, dass die Räume nur kurzzeitig leer stehen, kann von einer zwingenden Regelung für Büroräume sowie für Besprechungs-, Veranstaltungs- und Schulungsräumen unter Umständen abgesehen werden.

In Besprechungs-, Veranstaltungs- und Schulungsräumen gibt es meistens keine Möglichkeit, Unterlagen, IT-Systeme und Ähnliches gesondert einzuschließen. Daher sollte es möglich sein, solche Räume zumindest dann, wenn alle Teilnehmer einer Veranstaltung den Raum verlassen, abzuschließen oder ihn durch einen internen Mitarbeiter beaufsichtigen zu lassen.

In manchen Fällen, zum Beispiel in Großraumbüros, können die Türen nicht abgeschlossen werden. Dann sollte alternativ jeder Mitarbeiter vor seiner Abwesenheit seine Unterlagen (gemäß der Clean-Desk-Politik) und den persönlichen Arbeitsbereich verschließen. Dazu zählen beispielsweise der Schreibtisch, Schrank, Client, Laptop und das Telefon.

Türen müssen nicht abgeschlossen werden, wenn keine schutzbedürftigen Gegenstände wie Unterlagen oder Datenträger offen ausliegen und keine unbefugten Zugriffe auf die IT-Systeme im Raum (und die damit vernetzten IT-Systeme) möglich sind.

Bei laufendem Rechner müssen Türen nicht abgeschlossen werden, wenn Zugriffe nur nach erfolgreicher Authentisierung möglich sind, also zum Beispiel ein passwortunterstützter Sperrbildschirm aktiviert ist. Bei ausgeschaltetem Rechner kann darauf verzichtet werden, den Raum zu verschließen, wenn beim Booten des Rechners ein Passwort eingegeben werden muss. Die gleiche Funktion erfüllen Zugangsmechanismen, die auf Token oder Chipkarten basieren.

Der aufgeräumte Arbeitsplatz

Jeder Mitarbeiter sollte dazu angehalten werden, seinen Arbeitsplatz aufgeräumt zu hinterlassen. Die Benutzer müssen dafür sorgen, dass Unbefugte keinen Zugang zu Anwendungen oder Zugriff auf Daten erhalten. Alle mobilen Mitarbeiter müssen sicherstellen, dass keine vertraulichen Informationen frei zugänglich sind und die Verfügbarkeit, Vertraulichkeit oder Integrität von Daten nicht negativ beeinflusst werden kann. Es darf nicht möglich sein, dass Unbefugte auf Datenträger oder Unterlagen zugreifen können.

Für eine kurze Abwesenheit während der Arbeitszeit ist es ausreichend:

- den Raum, sofern möglich, zu verschließen.
- den Bildschirm so zu sperren, dass Zugriffe nur nach erfolgreicher Authentisierung möglich sind.

Bei geplanter Abwesenheit eines Mitarbeiters (zum Beispiel längere Besprechungen, Dienstreisen, Urlaub, Fortbildungsveranstaltungen) ist der Arbeitsplatz so aufzuräumen, dass keine schutzbedürftigen Datenträger oder Unterlagen unverschlossen am Arbeitsplatz zurückgelassen werden. Dafür benötigen die Mitarbeiter ausreichend dimensionierte und verschließbare Staumöglichkeiten, wie zum Beispiel stabile Schränke.

Auch Passwörter dürfen auf keinen Fall sichtbar aufbewahrt werden. Klebezettel am Monitor oder an einem leicht zu erratenden Ort wie zum Beispiel unter der Schreibtischauflage oder in der

unverschlossenen Schreibtischschublade sind ungeeignet. Ebenfalls sollten eindeutige Hinweise für das schnelle Erraten ausgeschlossen werden. Daher sollten die Passwörter keine Namen von Familienangehörigen enthalten. Trivialpasswörter wie aufeinanderfolgende Buchstaben und Zahlen sind ebenfalls zu vermeiden.

Die allgemeinen Arbeitsplatzanforderungen sind im Baustein INF.8 *Häuslicher Arbeitsplatz* beschrieben und sollten beachtet werden.

INF.9.M4 Arbeiten mit fremden IT-Systemen (B)

Häufig ist es erforderlich, unterwegs mithilfe fremder IT-Systeme auf digitale Informationen zugreifen zu können. Zum Beispiel ist das notwendig, um Terminkalender abzugleichen, E-Mails zu verschicken oder einzelne Dateien abzurufen. Hierfür ist es meist das einfachste, fremde IT-Systeme oder Kommunikationsanbindungen zu benutzen, also beispielsweise:

- aus einem Internet-Café,
- in einem Büro der besuchten Institution oder
- über einen WLAN-Hotspot im Hotel, im Zug oder am Flughafen.

Hierbei sollte sich aber jeder Benutzer darüber im Klaren sein, dass es sich um fremd-administrierte IT handelt und daher zusätzliche Sicherheitsmaßnahmen zu ergreifen sind. Daher sollte immer davon ausgegangen werden, dass das Sicherheitsniveau der fremden IT-Umgebung nicht bekannt ist und damit als niedrig eingeschätzt werden muss. Jeder Mitarbeiter sollte wissen, dass fremde Rechner und fremde IT-Umgebungen grundsätzliche höhere Sicherheitsrisiken darstellen. Selbst wenn das Sicherheitsniveau einen ausgezeichneten Eindruck macht, kann dies ein Trugschluss sein.

Daher sollten Benutzer folgende Empfehlungen beachten, bevor sie mit fremden IT-Systemen arbeiten oder Dienstleistungsangebote nutzen:

- Sie sollten sich über vorhandene Sicherheitsmaßnahmen informieren.
- Sie sollten sich genau überlegen, wie sie mit fremden IT-Systemen arbeiten. Sie sollten sich dabei an den Vorgaben und Regelungen für mobile Arbeitsplätze orientieren und fremde IT-Systeme oder Dienstleistungsangebote nicht für alle denkbaren Aktionen und Daten benutzen.
- Sobald die Arbeit beendet wurde, sollten bei einem fremden Rechner grundsätzlich alle währenddessen entstandenen temporären Daten gelöscht werden. Das ist allerdings meistens nicht einfach, da bei vielen Betriebssystemen temporäre Daten an vielen Stellen entstehen. Außerdem kann es bei fremden IT-Systemen auch vorkommen, dass die Zugriffsrechte es nicht zulassen, dass die entstandenen Daten gelöscht werden. Zumindest sollte der Zwischenspeicher (Cache) gelöscht werden.
- Auf keinen Fall sollten Browser-Funktionen zur Auto-Vervollständigung von Benutzernamen und Passwörtern genutzt werden, damit nachfolgende Benutzer sich nicht einfach unter diesem Benutzernamen irgendwo anmelden können.

2.2 Standard-Maßnahmen

Gemeinsam mit den Basis-Maßnahmen entsprechen die folgenden Maßnahmen dem Stand der Technik im Bereich "Mobiler Arbeitsplatz".

INF.9.M5 Zeitnahe Verlustmeldung (S)

Mitarbeiter müssen ihrer Institution umgehend melden, wenn Dokumente, IT-Systeme oder Datenträger verloren oder gestohlen wurden. Hierfür muss es klare Meldewege und Ansprechpartner innerhalb der Institution geben. Das gilt auch für private Geräte, die dienstlich genutzt werden.

Auf Laptops, Smartphones, Tablets, PDAs und ähnlichen Geräten, aber auch auf mobilen Datenträgern wie USB-Sticks können sich vertrauliche Daten befinden, nach deren Verlust umgehend gehandelt werden muss, beispielsweise:

- Zugangsdaten wie Passwörter: Alle Zugangsdaten der betroffenen IT-Systeme müssen umgehend geändert werden.
- Als vertraulich eingestufte Informationen (z. B. Patientenakten): Alle betroffenen Bereiche (z. B. Fachabteilung, Kunden etc.) müssen benachrichtigt werden, um entsprechende Maßnahmen ergreifen zu können.

Falls möglich, sollten, nachdem mobile Endgeräte verloren gegangen sind, auch Maßnahmen ergriffen werden, mit denen sich die Geräte sperren, löschen oder lokalisieren lassen. Die meisten Mobile-Device-Management-(MDM)-Lösungen (siehe SYS.3.2.2 *Mobile Device Management*) bieten diese Funktionen an. Dafür sind vorher klare Regeln zu definieren und entsprechende Maßnahmen in Absprache mit dem Benutzer, dessen Endgerät verloren ging, unverzüglich zu ergreifen.

Tauchen verlorene Geräte wieder auf, sollten sie auf eventuelle Manipulationen untersucht werden, z. B. ob Schrauben geöffnet, Siegel entfernt wurden oder 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 manipulierte Software auf den wiedererlangten Geräten befindet, müssen diese zumindest neu installiert werden.

INF.9.M6 Entsorgung von vertraulichen Informationen (S)

Betriebsmittel oder Sachmittel am häuslichen Arbeitsplatz (z. B. Druckerpapier, USB-Festplatten, DVDs, USB-Sticks, SD-Karten, aber auch spezielle Tonerkassetten) werden irgendwann nicht mehr benötigt oder müssen ausgesondert werden. Wenn sie schützenswerte Daten enthalten, müssen sie so entsorgt werden, dass keine Rückschlüsse auf vorher gespeicherte Daten möglich sind. Bei funktionstüchtigen Datenträgern sollten die Daten sicher gelöscht werden. Nicht funktionierende oder nur einmal beschreibbare Datenträger müssen mechanisch zerstört werden (siehe dazu auch CON.6 *Löschen und Vernichten*).

Die Art der Entsorgung schutzbedürftigen Materials sollte in einer speziellen Sicherheitsrichtlinie geregelt werden. In der Institution müssen die dafür benötigten Entsorgungseinrichtungen vorhanden sein.

Wird vertrauliches Material vor der Entsorgung gesammelt, so ist die Sammlung vor unberechtigtem Zugriff zu schützen.

Die ordnungsgemäße Entsorgung schützenswerter Betriebs- und Sachmittel muss den Anforderungen des Bausteins OPS.1.2.7 Verkauf/Aussonderung von IT entsprechen.

Entsorgung von Datenträgern und Dokumenten auf Reisen

Auch unterwegs gibt es häufig Material, das aus verschiedensten Gründen entsorgt werden sollte. Schon allein die notwendigen Entsorgungen, damit das Reisegepäck tragbar bleibt, müssen in diesem Kontext beachtet werden. Während in der eigenen Institution Entsorgungsverfahren für alte oder unbrauchbare Datenträger und Dokumente existieren, sind diese unterwegs nicht immer möglich. Daher ist vor jeder Entsorgung von ausgedienten Datenträgern und Dokumenten genau zu überlegen, ob diese schützenswerte Informationen enthalten könnten. Ist das der Fall, müssen die Datenträger und Dokumente im Zweifelsfall wieder mit zurücktransportiert werden. Das gilt auch, wenn die Datenträger defekt sind, da IT-Experten auch hieraus noch wertvolle Informationen zurückgewinnen können. Ebenso ist bei Einrichtungen zur Datenvernichtung in fremden Institutionen Vorsicht geboten, da hier nicht unbedingt ersichtlich ist, wer die Entsorgung durchführt beziehungsweise wie zuverlässig sie ist.

Die Anforderungen an die Entsorgung von Datenträgern und Dokumenten sind im Baustein OPS.1.2.7 *Verkauf/Aussonderung von IT* abgebildet. Sie sollten generell bei der Gestaltung der Sicherheitsrichtlinien und Regelungen zum Informationsschutz im Themenkomplex Entsorgung von Datenträgern und Dokumenten einbezogen werden.

INF.9.M7 Rechtliche Rahmenbedingungen für das mobile Arbeiten (S)

Institutionen müssen verschiedene arbeitsrechtliche und arbeitsschutzrechtliche Rahmenbedingungen für das mobile Arbeiten beachten und festlegen. Strittige Punkte sollten entweder durch Betriebsvereinbarungen oder durch zusätzlich zum Arbeitsvertrag getroffene individuelle Vereinbarungen zwischen dem mobilen Mitarbeiter und dem Arbeitgeber geklärt werden. In diesen Vereinbarungen sind beispielsweise folgende Punkte zu regeln:

- Freiwilligkeit der Teilnahme an der mobilen Arbeit
- Mehrarbeit und Zuschläge
- Aufwendungen für Fahrten zwischen Betrieb, häuslicher Wohnung, Kunden
- Aufwendungen zum Beispiel für Strom, Heizung, Miete
- Haftung (bei Diebstahl oder Beschädigung der IT, aber auch bei Arbeitsunfall oder Berufskrankheit)
- Beendigung der mobilen Arbeit

INF.9.M8 Sicherheitsrichtlinie für mobile Arbeitsplätze (S)

Die für die mobile Arbeit notwendigerweise umzusetzenden Sicherheitsmaßnahmen für den Umgang mit Informationen und mit der Informations- und Kommunikationstechnik, sind zusätzlich in einer Sicherheitsrichtlinie für das mobile Arbeiten zu dokumentieren.

Folgende Aspekte sollten darin beachtet werden:

Arbeitszeitregelung: Es sollte geregelt sein, wie die Arbeitszeiten auf Tätigkeiten innerhalb und außerhalb der Institution verteilt sind. Ebenso sollten feste Zeiten festgelegt werden, an denen der Mitarbeiter erreichbar ist (siehe INF.M7 *Rechtliche Rahmenbedingungen für das mobile Arbeiten*).

Reaktionszeiten: Es sollte geregelt sein, in welchen Abständen die mobilen Mitarbeiter aktuelle Informationen abrufen (zum Beispiel wie häufig E-Mails gelesen werden) und in welchem Zeitraum sie darauf zu reagieren haben.

Vertretungsregelung: Für jeden mobilen Mitarbeiter sollte ein Vertreter bestimmt werden, der über die laufenden Aktivitäten informiert sein muss, damit er auch kurzfristig die Vertretung übernehmen kann. Dazu müssen die Arbeitsergebnisse durch die mobilen Mitarbeiter immer sorgfältig dokumentiert werden. Eventuell sind sporadische oder regelmäßige Treffen zwischen dem mobilen Mitarbeiter und seinem Vertreter sinnvoll. Ergänzend muss geregelt werden, wie der Vertreter im unerwarteten Vertretungsfall auf die Daten auf den IT-Systemen und Anwendungen zugreifen kann oder die vorhandenen Unterlagen am mobilen Arbeitsplatz einsehen kann. Dieser Vertretungsfall sollte probeweise durchgespielt und ausgewertet werden. Die Auswertung sollte durch den mobilen Mitarbeiter und seine Vertretung erfolgen.

Umgang mit vertraulichen Informationen: Bei der mobilen Arbeit werden Informationen sowohl analog (zum Beispiel auf Papier) als auch digital (zum Beispiel auf Datenträgern) bearbeitet. Unabhängig davon, in welcher Form Informationen vorliegen, müssen sie vor unbefugtem Zugriff und anderen Sicherheitsrisiken geschützt werden. Daher ist der komplette Lebenszyklus schützenswerter Informationen angemessen abzusichern.

Meldeweg: Die mobilen Mitarbeiter sind zu verpflichten, sicherheitsrelevante Vorkommnisse unverzüglich an eine im Vorfeld zu bestimmende Stelle in der Institution zu melden.

Arbeitsmittel: Es sollte festgeschrieben werden, welche Arbeitsmittel die mobilen Arbeiter einsetzen können und welche nicht genutzt werden dürfen (zum Beispiel nicht freigegebene Software). So kann ein E-Mail-Anschluss zur Verfügung gestellt werden, aber die Nutzung von anderen Internet-Diensten untersagt werden. Weiterhin könnte die Nutzung von Datenträgern, wie beispielsweise DVDs oder USB-Sticks untersagt werden, wenn der mobile Arbeitsplatz es nicht erfordert.

Transport von Dokumenten und Datenträgern: Die Art und Absicherung des Transportes von Dokumenten und Datenträgern zwischen mobilen Arbeitsplätzen, Räumlichkeiten von Kunden und der Institution ist zu regeln. Vertrauliche Daten auf digitalen Datenträgern sollten nur verschlüsselt

transportiert werden (siehe INF.9.M2 *Regelungen für mobile Arbeitsplätze* und INF.9.M9 *Verschlüsselung tragbarer IT-Systeme und Datenträger*).

Datensicherung: Die mobilen Mitarbeiter sind zu verpflichten, regelmäßige Datensicherungen der lokal gespeicherten Daten durchzuführen. Darüber hinaus sollte vereinbart werden, dass jeweils eine Generation der Datensicherungen in der Institution hinterlegt wird, damit eine höhere Verfügbarkeit gewährleistet ist.

Synchronisation von Datenbeständen: Datenbestände, die sowohl in der Institution als auch an mobilen Arbeitsplätzen bearbeitet werden sollen, müssen geeignet synchronisiert werden. Das Vorgehen bei der Synchronisation muss genau geplant werden, damit es nicht zu Konflikten und damit zu einem Datenverlust kommen kann, wenn zwei Benutzer den gleichen Datensatz in gespiegelten Datenbeständen geändert oder gelöscht haben. Es empfiehlt sich, hierfür geeignete Software einzusetzen.

Datenschutz: Die mobilen Mitarbeiter sind darauf zu verpflichten, einschlägige Datenschutzvorschriften einzuhalten. Sie sind auf die notwendigen Maßnahmen bei der Bearbeitung von personenbezogenen Daten am mobilen Arbeitsplatz und bei Kunden hinzuweisen.

Datenkommunikation: Es sollte festgelegt sein, welche Daten auf welchem Weg übertragen werden sollen und welche Daten nicht oder nur verschlüsselt elektronisch zu übermitteln sind. Ebenso ist zu regeln, welche Dokumente zwischen Institution, mobilem Arbeitsplatz und den Kunden transportiert werden dürfen und wie diese dabei geschützt werden.

Entsorgung: Die Sicherheitsrichtlinie muss Regelungen enthalten, wie Mitarbeiter mit ausgedienten Datenträgern und Dokumenten umgehen sollen. (siehe INF.9.M6 *Entsorgung von vertraulichen Informationen* und *ORP.3 Sensibilisierung und Schulung zur Informationssicherheit*).

Sensibilisierung: Alle Mitarbeiter sollten regelmäßig für den ordnungsgemäßen Umgang mit mobiler IT sensibilisiert werden (siehe INF.9.M2 *Regelungen für mobile Arbeitsplätze*).

Die Regelungen sind jedem mobilen Mitarbeiter auszuhändigen. Entsprechende Merkblätter sind regelmäßig zu aktualisieren.

Informationsschutz auf Geschäfts- und Privatreisen

Mitarbeiter müssen mit vertraulichen Informationen auch auf Geschäfts- oder Privatreisen sorgfältig umgehen. Bei Auslandsreisen sollten daher die Anforderungen des Bausteins CON.6 *Informationssicherheit auf Auslandsreisen* berücksichtigt werden.

INF.9.M9 Verschlüsselung tragbarer IT-Systeme und Datenträger (S)

Um zu verhindern, dass schützenswerte Informationen durch unberechtigte Dritte eingesehen werden können, sollte sichergestellt werden, dass alle schützenswerten Informationen entsprechend den internen Richtlinien abgesichert sind.

Mobile Datenträger und IT-Systeme sollten nach unternehmensinternen Verfahren und Regelungen verschlüsselt werden, um schützenswerte Daten vor unbefugten Zugriff zu schützen. Dies gilt insbesondere für wiederbeschreibbare Datenträger. Es besteht die Möglichkeit, Datenträger nur partiell zu verschlüsseln. Im Rahmen der Benutzerfreundlichkeit empfiehlt es sich allerdings, den gesamten Datenträger zu verschlüsseln. Eine Verschlüsselung des Datenträgers erreicht man entweder mit Software, wie z. B. BitLocker von Microsoft oder FileVault von Apple, oder auch mit spezieller Hardware. Um die Daten zu entschlüsseln, ist ein kryptographischer Schlüssel notwendig, der in Form einer separaten Chipkarte oder eines USB-Tokens verwendet werden sollte. Hierbei sollte der Benutzer den kryptographischen Schlüssel und den verschlüsselten Datenträger bzw. Client getrennt voneinander aufbewahren.

Zudem ist es wichtig, Vorkehrungen gegen Datenverlust zu treffen, um Fehlfunktionen (z. B. Stromausfall, Abbruch der Verschlüsselung) systemseitig abzufangen. Darüber hinaus sind folgende Anforderungen sinnvoll:

- Der genutzte Verschlüsselungsalgorithmus sollte den Anforderungen der Institution entsprechen.
- Das Schlüsselmanagement muss mit den Funktionen des mobilen IT-Systems harmonisieren.

- Das mobile IT-System muss die sicherheitskritischen Parameter wie Schlüssel sicher verwalten. So dürfen Schlüssel (auch mittlerweile nicht mehr benutzte) nie ungeschützt, das heißt auslesbar oder unverschlüsselt, abgelegt werden. Sie müssen möglichst getrennt vom verschlüsselten Gerät aufbewahrt werden.

2.3 Maßnahmen für erhöhten Schutzbedarf

Im Folgenden sind Maßnahmenvorschläge aufgeführt, die über das dem Stand der Technik entsprechende Schutzniveau hinausgehen und bei erhöhtem Schutzbedarf in Betracht gezogen werden sollten. Die jeweils in Klammern angegebenen Buchstaben zeigen an, welche Grundwerte durch die Maßnahme vorrangig geschützt werden (C = Vertraulichkeit, I = Integrität, A = Verfügbarkeit).

INF.9.M10 Einsatz von Diebstahlsicherungen (H)

Diebstahlsicherungen sind überall dort einzusetzen, wo große Werte zu schützen sind beziehungsweise dort, wo andere Maßnahmen nicht umgesetzt werden können. Das trifft zum Beispiel bei Laptops im mobilen Einsatz zu. Diebstahlsicherungen sind außerdem dort sinnvoll, wo Publikumsverkehr herrscht oder die Fluktuation von Benutzern sehr hoch ist. Dabei sollte immer beachtet werden, dass die zu schützenden Werte nur zu einem kleinen Teil aus den Wiederbeschaffungskosten für das Gerät bestehen, sondern bei Laptops und ähnlichen IT-Systemen der Wert der darauf gespeicherten Daten berücksichtigt werden muss.

Arten von Diebstahlsicherungen

Auf dem Markt sind die unterschiedlichsten Diebstahl-Sicherungen erhältlich. Diese können zunächst in mechanische und elektronische Sicherungen unterteilt werden.

Zu den mechanischen Sicherungen gehören unter anderem Kabelsicherungen, Gehäusesicherungen (um das Gehäuse gegen Öffnung zu schützen), Sicherheitsplatten und Sicherheitsgehäuse. Es gibt hier zum einen Hardware-Sicherungen, die dem Diebstahl von IT-Geräten vorbeugen, z. B. indem das Gerät mit dem Schreibtisch verbunden wird. Es gibt zum anderen auch eine Reihe von Sicherungsmechanismen, die verhindern sollen, dass das Gehäuse geöffnet wird. Damit soll vorgebeugt werden, dass Angreifer Teile stehlen oder sicherheitsrelevante Einstellungen manipulieren, wie zum Beispiel Sicherheitskarten entfernen.

Bei der Beschaffung mechanischer Sicherungen ist die Wahl eines guten Schlosses wichtig, das über eine auf die jeweiligen Bedürfnisse abgestimmte Schließanlage verfügt. Je nach Produkt sind verschiedene Schließanlagen möglich:

- gleichschließend: Ein Schlüssel passt zum Beispiel auf alle Gerätesicherungen einer Institution oder Abteilung. Das hat den Vorteil, dass der Aufwand für die Schlüsselverwaltung geringer ist. Es bedeutet jedoch, dass sehr viele gleichartige Schlüssel im Umlauf sein können und dass im Schadensfall häufig keine Beweissicherung möglich ist.
- verschiedenschließend: Jede Gerätesicherung hat einen individuellen Schlüssel. Das hat den Nachteil, dass der Aufwand für die Schlüsselverwaltung höher ist. Es hat aber den Vorteil, dass es weniger Schlüsseldubletten gibt.
- Hauptschlüsselsystem: Jede Gerätesicherung hat einen individuellen Schlüssel, kann zusätzlich aber auch durch einen Hauptschlüssel geöffnet werden. Das hat den Vorteil, dass der Aufwand für die Schlüsselverwaltung geringer ist. Es hat aber den Nachteil, dass solche Systeme teurer in der Anschaffung sind.

Die meisten Notebooks oder einige andere Geräte haben einen kleinen Schlitz, der mit einem Ketten- oder Schloss-Symbol gekennzeichnet ist. Diese kleine Öffnung befindet sich seitlich oder hinten am Gerät. Es gibt eine breite Palette von Kabelsicherungen und anderen Produkten, die diese Öffnung für die Sicherung von Geräten nutzt.

Bei Kabelsicherungen muss dann nur eine Kabelschlinge um ein solides Objekt in der Nähe des Gerätes gelegt werden. Anschließend wird das zugehörige Schloss durch die entstandene Lasche gezogen und abgeschlossen. Für Geräte, die diese Öffnung nicht haben oder bei denen sie nicht widerstandsfähig

genug ist, gibt es Sicherungsprodukte, bei denen eine stabile Platte auf das Gerät geklebt wird. An dieser wird dann das Sicherungskabel befestigt.

Daneben gibt es elektronische Sicherungen, die beispielsweise einen akustischen Abschreckungs-Alarm am Gerät selber auslösen, der potenzielle Diebe dazu bringen soll, das Gerät liegenzulassen.

Bei Neuanschaffung von IT-Geräten sollte darauf geachtet werden, dass sie Ösen am Gehäuse besitzen, um sie an anderen Gegenständen befestigen zu können.

INF.9.M11 Verbot der Nutzung unsicherer Umgebungen (H)

Um die Gefährdungen und Sicherheitslücken bei erhöhtem Schutzbedarf zu minimieren, sollten Mindestkriterien für die Arbeitsumgebung festgelegt werden. Diese sollten vorwiegend die sichere mobile Verarbeitung von Informationen mit erhöhtem Schutzbedarf gewährleisten.

Die Mindestkriterien sollten dabei die folgenden Themenbereiche abdecken:

Einsicht und Zugriff durch Dritte: Es ist sicherzustellen, dass Bildschirminhalte und Ausdrucke möglichst nicht durch Dritte mitgelesen werden. Vor allem Zubehörteile wie Blickschutzfolien können es Dritten erschweren, Bildschirminhalte einzusehen. Da der Zugriff auf vertrauliche Informationen durch unbefugte Personen generell verhindert werden sollte, sind auch die Anforderungen der Maßnahme INF.9.M10 *Einsatz von Diebstahlsicherungen* zu berücksichtigen.

Geschlossene, abschließbare oder bewachte Räume: Je nach Schutzbedarf der Informationen sollten die Informationen entweder in geschlossenen, abschließbaren oder bewachten Räumen aufbewahrt werden. Falls mehrere Optionen zur Auswahl stehen, sollte bei erhöhtem Schutzbedarf immer die Option mit dem größtmöglichen Schutz ausgewählt werden.

Gesicherte Kommunikationsmöglichkeiten (IT / Telefon): Die Kommunikationsmöglichkeiten beim mobilen Arbeiten sollten immer entsprechend dem Schutzbedarf abgesichert werden. Sicherheitslösungen durch ein Virtual Private Network (VPN) oder Mobile Device Management (MDM) sollten daher angemessen auf das mobile Arbeiten bei erhöhtem Schutzbedarf abgestimmt sein. Ebenso sollte bei einer etablierten VPN-Lösung auch der Baustein NET.4.2 *VoIP* beachtet werden, um entsprechend den dort genannten Anforderungen sichere Vorgaben für mobile Endgeräte erstellen zu können. Die für das mobile Arbeiten prinzipiell notwendigen Kommunikationsbausteine befinden sich in den Schichten SYS.3 *Mobile Devices* und NET (*Netze und Kommunikation*). Sofern bestimmte Kommunikationsmöglichkeiten einem Outsourcing-Verhältnis unterliegen, sind auch die Anforderungen aus der Schicht OPS.2 *IT-Betrieb von Dritten* zu berücksichtigen.

Ausreichende Stromversorgung: Für die Arbeitsdauer mit mobilen Endgeräten ist immer die Stromversorgung zu gewährleisten. Daher sollten die Benutzer auch mit geeigneten Netzteilen für die Geräte ausgestattet sein. Gerade bei häufigen Reisen bieten sich zusätzliche Akkumulatoren an, die eine längere Stromversorgung garantieren. Für die Benutzung von Powerbanks sollte die Institution spezielle Regelungen festlegen, die dem jeweiligen Schutzbedarf entsprechen. Das ist notwendig, da Powerbanks die gleichen Sicherheitslücken aufweisen, wie normale USB-Sticks. Daher sollten möglichst nur geprüfte und abgesicherte Powerbanks der Institution durch die Benutzer verwendet werden.

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 Literaturverzeichnis

Weiterführende Informationen zu Gefährdungen und Sicherheitsmaßnahmen im Bereich "Umsetzungshinweise zum Baustein INF.9 *Mobiler Arbeitsplatz*" finden sich unter anderem in folgenden Veröffentlichungen:

[27001A6.2.1]	ISO/IEC 27001:2013: Information technology - Security techniques - Information security management systems - Requirements, insbesondere Annex A, A.6.2.1 Mobile device policy, International Organization for Standardization (Hrsg.), ISO/IEC JTC 1/SC 27, Oktober 2013
[ISFPA2]	Standard of Good Practice for Information Security: Area PA2 Mobile Computing, Information Security Forum (ISF), June 2018
[NIST80046]	Guide to Enterprise Telework, Remote Access and Bring Your Own Device (BYOD) Security: NIST Special Publication 800-46, Revision 2, Juli 2016, http://dx.doi.org/10.6028/NIST.SP.800-46r2, zuletzt abgerufen am 05.10.2018