**INF: Infrastruktur**

# INF.9: Mobiler Arbeitsplatz

## 1 Beschreibung

### 1.1 Einleitung

Eine gute Netzabdeckung sowie leistungsfähige IT-Geräte, wie z. B. Laptops, Smartphones oder Tablets, ermöglichen es Mitarbeitern, nahezu an jedem Platz bzw. von überall zu arbeiten. Das bedeutet, dass dienstliche Aufgaben häufig nicht mehr nur in den Räumen und Gebäuden der Institution erfüllt werden, sondern an wechselnden Arbeitsplätzen in unterschiedlichen Umgebungen, z. B. in Hotelzimmern, in Zügen oder bei Kunden. Die dabei verarbeiteten Informationen müssen angemessen geschützt werden.

Das mobile Arbeiten verändert einerseits die Dauer, Lage und Verteilung der Arbeitszeiten. Andererseits erhöht es die Anforderungen an die Informationssicherheit, da in Umgebungen mit mobilen Arbeitsplätzen keine sichere IT-Infrastruktur vorausgesetzt werden kann, so wie sie in einer Büroumgebung anzutreffen ist.

### 1.2 Zielsetzung

Der Baustein beschreibt Sicherheitsanforderungen an mobile Arbeitsplätze. Ziel ist es, für solche Arbeitsplätze eine mit einem Büroraum vergleichbare Sicherheitssituation zu schaffen.

### 1.3 Abgrenzung und Modellierung

Der Baustein INF.9 *Mobiler Arbeitsplatz* ist für alle Räume anzuwenden, die häufig als mobiler Arbeitsplatz genutzt werden.

Der Baustein enthält grundsätzliche Anforderungen, die zu beachten und zu erfüllen sind, wenn Mitarbeiter nicht nur innerhalb der Institution arbeiten, sondern auch häufiger an wechselnden Arbeitsplätzen außerhalb.

Der Baustein bildet vor allem die organisatorischen, technischen und personellen Anforderungen an die vollständige oder teilweise mobile Arbeit ab. Um IT-Systeme, Datenträger oder Unterlagen, die beim mobilen Arbeiten genutzt werden, abzusichern, müssen alle relevanten Bausteine wie z. B. SYS.3.1 *Laptops*, SYS.3.2 *Allgemeine Smartphones und Tablets,* SYS.4.5 *Wechseldatenträger*, NET.3.3 *VPN* sowie SYS.2.1 *Allgemeiner Client* gesondert berücksichtigt werden.

Sicherheitsanforderungen an Bildschirmarbeitsplätze außerhalb von Gebäuden der Institution, die vom Arbeitgeber fest eingerichtet werden (Telearbeitsplätze), sind nicht Gegenstand des vorliegenden Bausteins. Diese werden im Baustein OPS.1.2.4 *Telearbeit* beschrieben. Ebenso wird nicht auf Sicherheitsanforderungen an die Infrastruktur des Telearbeitsplatzes eingegangen. Dieses Thema wird im Baustein INF.8 *Häuslicher Arbeitsplatz* behandelt.

# 2 Gefährdungslage

Folgende spezifische Bedrohungen und Schwachstellen sind für den Baustein INF.9 *Mobiler Arbeitsplatz* von besonderer Bedeutung:

## 2.1 Fehlende oder unzureichende Regelungen für mobile Arbeitsplätze

Ist das mobile Arbeiten nicht oder nur unzureichend geregelt, können der Institution unter anderem finanzielle Schäden entstehen. Ist beispielsweise nicht geregelt, welche Informationen außerhalb der Institution transportiert und bearbeitet werden dürfen und welche Schutzvorkehrungen dabei zu beachten sind, können vertrauliche Informationen in fremde Hände gelangen. Diese können dann von Unbefugten möglicherweise gegen die Institution verwendet werden.

## 2.2 Beeinträchtigung durch wechselnde Einsatzumgebung

Da mobile Datenträger und Endgeräte in sehr unterschiedlichen Umgebungen eingesetzt werden, sind sie vielen Gefährdungen ausgesetzt. Dazu gehören beispielsweise schädigende Umwelteinflüsse wie z. B. zu hohe oder zu niedrige Temperaturen, Staub oder Feuchtigkeit. Auch Transportschäden können auftreten.

Neben diesen Einflüssen ist auch die Einsatzumgebung mit ihrem unterschiedlichen Sicherheitsniveau zu berücksichtigten. Smartphones, Tablets, Laptops und ähnliche mobile Endgeräte sind nicht nur beweglich, sondern können auch mit anderen IT-Systemen kommunizieren. Dabei können beispielsweise Schadprogramme übertragen oder schützenswerte Informationen kopiert werden. Auch können eventuell Aufgaben nicht mehr erfüllt, Kundentermine nicht wahrgenommen oder IT-Systeme beschädigt werden.

## 2.3 Manipulation oder Zerstörung von IT-Systemen, Zubehör, Informationen und Software am mobilen Arbeitsplatz

IT-Systeme, Zubehör, Informationen und Software, die mobil genutzt werden, können unter Umständen einfacher manipuliert oder zerstört werden als in der Institution. Der mobile Arbeitsplatz ist oft für Dritte zugänglich. Auch sind hier die zentralen Schutzmaßnahmen der Institution nicht vorhanden, wie z. B. Pförtnerdienste. Werden IT-Systeme, Zubehör, Informationen oder Software manipuliert oder zerstört, ist der Mitarbeiter am mobilen Arbeitsplatz oft nur noch eingeschränkt arbeitsfähig. Des Weiteren müssen womöglich zerstörte IT-Komponenten oder Softwarelösungen ersetzt werden, was sowohl finanzielle als auch zeitliche Ressourcen erfordert.

## 2.4 Verzögerungen durch temporär eingeschränkte Erreichbarkeit

Meist hat ein Mitarbeiter am mobilen Arbeitsplatz keine festen Arbeitszeiten und ist unterwegs auch schwerer zu erreichen. Dadurch kann sich der Informationsfluss deutlich verzögern. Selbst wenn die Informationen per E-Mail übermittelt werden, verkürzt sich nicht zwingend die Reaktionszeit, da nicht sichergestellt werden kann, dass der mobile Mitarbeiter die E-Mail zeitnah liest. Die temporär eingeschränkte Erreichbarkeit wirkt sich dabei je nach Situation und Institution unterschiedlich aus, kann aber die Verfügbarkeit von Informationen stark einschränken.

## 2.5 Ungesicherter Akten- und Datenträgertransport

Wenn Dokumente, Datenträger oder Akten zwischen der Institution und den mobilen Arbeitsplätzen transportiert werden, können diese Informationen und Daten verlorengehen oder auch von Unbefugten entwendet, gelesen oder manipuliert werden. Dadurch können der Institution größere finanzielle Schäden entstehen. Der Akten- und Datenträgertransport kann auf verschiedene Arten unzureichend gesichert sein:

- Werden Unikate transportiert und fehlt eine entsprechende Datensicherung, können Ziele und Aufgaben nicht wie geplant erreicht werden, wenn das Unikat verloren geht.

- Fallen unverschlüsselte Datenträger in falsche Hände, kann dies zu einem schwerwiegenden Verlust der Vertraulichkeit führen.
- Ist unterwegs kein ausreichender Zugriffsschutz vorhanden, können Akten oder Datenträger unbemerkt kopiert oder manipuliert werden.

### 2.6 Ungeeignete Entsorgung der Datenträger und Dokumente

Ist es am mobilen Arbeitsplatz nicht möglich, Datenträger und Dokumente in geeigneter Weise zu entsorgen, wandern diese meist in den Hausmüll. Auch dort, wo unterwegs gearbeitet wird, werfen Mitarbeiter Entwürfe und andere vermeintlich unnütze Dokumente häufig direkt in den nächsten Papierkorb. Oder sie lassen sie einfach liegen, sei es im Hotel oder in der Bahn. Wenn jedoch Datenträger oder Dokumente nicht geeignet entsorgt werden, können Angreifer daraus wertvolle Informationen entnehmen, die sich gezielt für Erpressungsversuche oder zur Wirtschaftsspionage missbrauchen lassen. Die Folgen reichen vom Wissensverlust bis zur Existenzgefährdung der Institution, z. B. wenn dadurch wichtige Aufträge nicht zustande kommen oder Partnerschaften scheitern.

### 2.7 Vertraulichkeitsverlust schützenswerter Informationen

Am mobilen Arbeitsplatz können Angreifer einfacher auf vertrauliche Informationen zugreifen, die sich auf Festplatten, auf austauschbaren Speichermedien oder auf Papier befinden, besonders dann, wenn sie dabei professionell agieren. Auch können sie Kommunikationsverbindungen abhören. Werden Informationen unberechtigt gelesen oder preisgegeben, hat das jedoch schwerwiegende Folgen für die gesamte Institution. Unter anderem kann der Verlust der Vertraulichkeit dazu führen, dass die Institution gegen Gesetze verstößt oder dass Wettbewerbsnachteile und finanzielle Schäden entstehen.

### 2.8 Diebstahl oder Verlust von Datenträgern oder Dokumenten

Der mobile Arbeitsplatz ist nicht so gut abgesichert wie der Arbeitsplatz in einem Unternehmen oder in einer Behörde. Dienstliche IT-Systeme und Dokumente können daher z. B. während einer Bahnfahrt, aus einem Hotelzimmer oder aus externen Konferenzräumen leichter gestohlen werden.

Zudem können mobile IT-Systeme oder IT-Komponenten verloren gehen. Neben dem rein materiellen Schaden durch den unmittelbaren Verlust des mobilen IT-Systems kann zudem ein weiterer finanzieller Schaden entstehen, etwa wenn schützenswerte Daten wie z. B. E-Mails, Notizen von Besprechungen, Adressen oder sonstige Dokumente offengelegt werden. Auch könnte der Ruf der Institution geschädigt werden.

## 3 Anforderungen

Im Folgenden sind die spezifischen Anforderungen des Bausteins INF.9 *Mobiler Arbeitsplatz* aufgeführt. Grundsätzlich ist der Informationssicherheitsbeauftragte (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 Umsetzung von Anforderungen haben. Diese sind dann jeweils explizit in eckigen Klammern in der Überschrift der jeweiligen Anforderungen aufgeführt.

| **Zuständigkeiten** | **Rollen** |
|---|---|
| Grundsätzlich zuständig | Informationssicherheitsbeauftragter (ISB) |
| Weitere Zuständigkeiten | Mitarbeiter, IT-Betrieb, Zentrale Verwaltung, Personalabteilung |

## 3.1 Basis-Anforderungen

Die folgenden Anforderungen MÜSSEN für den Baustein INF.9 *Mobiler Arbeitsplatz* vorrangig erfüllt werden:

### INF.9.A1 Geeignete Auswahl und Nutzung eines mobilen Arbeitsplatzes [IT-Betrieb] (B)

Die Institution MUSS ihren Mitarbeitern vorschreiben, wie mobile Arbeitsplätze in geeigneter Weise ausgewählt und benutzt werden sollen. Es MÜSSEN Eigenschaften definiert werden, die für einen mobilen Arbeitsplatz wünschenswert sind. Es MÜSSEN aber auch Ausschlusskriterien definiert werden, die gegen einen mobilen Arbeitsplatz sprechen. Mindestens MUSS geregelt werden:

- unter welchen Arbeitsplatzbedingungen schützenswerte Informationen bearbeitet werden dürfen,
- wie sich Mitarbeiter am mobilen Arbeitsplatz vor ungewollter Einsichtnahme Dritter schützen,
- ob eine permanente Netz- und Stromversorgung gegeben sein muss sowie
- welche Arbeitsplatzumgebungen komplett verboten sind.

### INF.9.A2 Regelungen für mobile Arbeitsplätze [Personalabteilung] (B)

Für alle Arbeiten unterwegs MUSS geregelt werden, welche Informationen außerhalb der Institution transportiert und bearbeitet werden dürfen. Es MUSS zudem geregelt werden, welche Schutzvorkehrungen dabei zu treffen sind. Dabei MUSS auch geklärt werden, unter welchen Rahmenbedingungen Mitarbeiter mit mobilen IT-Systemen auf interne Informationen ihrer Institution zugreifen dürfen.

Die Mitnahme von IT-Komponenten und Datenträgern MUSS klar geregelt werden. So MUSS festgelegt werden, welche IT-Systeme und Datenträger mitgenommen werden dürfen, wer diese mitnehmen darf und welche grundlegenden Sicherheitsanforderungen dabei beachtet werden müssen. Es MUSS zudem protokolliert werden, wann und von wem welche mobilen Endgeräte außer Haus eingesetzt wurden.

Die Benutzer von mobilen Endgeräten MÜSSEN für den Wert mobiler IT-Systeme und den Wert der darauf gespeicherten Informationen sensibilisiert werden. Sie MÜSSEN über die spezifischen Gefährdungen und Maßnahmen der von ihnen benutzten IT-Systeme aufgeklärt werden. Außerdem MÜSSEN sie darüber informiert werden, welche Art von Informationen auf mobilen IT-Systemen verarbeitet werden darf. Alle Benutzer MÜSSEN auf die geltenden Regelungen hingewiesen werden, die von ihnen einzuhalten sind. Sie MÜSSEN entsprechend geschult werden

### INF.9.A3 Zutritts- und Zugriffsschutz [Zentrale Verwaltung, Mitarbeiter] (B)

Den Mitarbeitern MUSS bekannt gegeben werden, welche Regelungen und Maßnahmen zum Einbruch- und Zutrittsschutz am mobilen Arbeitsplatz zu beachten sind. Wenn der mobile Arbeitsplatz nicht besetzt ist, MÜSSEN Fenster und Türen abgeschlossen werden. Ist dies nicht möglich, z. B. im Zug, MÜSSEN die Mitarbeiter alle Unterlagen und IT-Systeme an sicherer Stelle verwahren oder mitführen, wenn sie abwesend sind. Es MUSS sichergestellt werden, dass Unbefugte zu keiner Zeit auf dienstliche IT und Unterlagen zugreifen können. Wird der Arbeitsplatz nur kurz verlassen, MÜSSEN die eingesetzten IT-Systeme gesperrt werden, sodass sie nur nach erfolgreicher Authentisierung wieder benutzt werden können.

### INF.9.A4 Arbeiten mit fremden IT-Systemen [IT-Betrieb, Mitarbeiter] (B)

Die Institution MUSS regeln, wie Mitarbeiter mit institutionsfremden IT-Systemen arbeiten dürfen. Jeder mobile Mitarbeiter muss über die Gefahren fremder IT-Systeme aufgeklärt werden. Die Regelungen MÜSSEN vorgeben, ob und wie schützenswerte Informationen an fremden IT-Systemen bearbeitet werden dürfen. Sie MÜSSEN zudem festlegen, wie verhindert wird, dass nicht autorisierte Personen die Informationen einsehen können. Wenn Mitarbeiter mit fremden IT-Systemen arbeiten, MUSS grundsätzlich sichergestellt sein, dass alle währenddessen entstandenen temporären Daten gelöscht werden.

## 3.2 Standard-Anforderungen

Gemeinsam mit den Basis-Anforderungen entsprechen die folgenden Anforderungen dem Stand der Technik für den Baustein INF.9 *Mobiler Arbeitsplatz*. Sie SOLLTEN grundsätzlich erfüllt werden.

### INF.9.A5 Zeitnahe Verlustmeldung [Mitarbeiter] (S)

Mitarbeiter SOLLTEN ihrer Institution umgehend melden, wenn Informationen, IT-Systeme oder Datenträger verlorengegangen sind oder gestohlen wurden. Dafür SOLLTE es klare Meldewege und Ansprechpartner innerhalb der Institution geben.

### INF.9.A6 Entsorgung von vertraulichen Informationen [Mitarbeiter] (S)

Vertrauliche Informationen SOLLTEN auch unterwegs sicher entsorgt werden. Bevor ausgediente oder defekte Datenträger und Dokumente vernichtet werden, MUSS überprüft werden, ob sie sensible Informationen enthalten. Ist dies der Fall, MÜSSEN die Datenträger und Dokumente wieder mit zurücktransportiert werden und auf institutseigenem Wege entsorgt oder vernichtet werden.

### INF.9.A7 Rechtliche Rahmenbedingungen für das mobile Arbeiten [Personalabteilung] (S)

Für das mobile Arbeiten SOLLTEN arbeitsrechtliche und arbeitsschutzrechtliche Rahmenbedingungen beachtet und geregelt werden. Alle relevanten Punkte SOLLTEN entweder durch Betriebsvereinbarungen oder durch zusätzlich zum Arbeitsvertrag getroffene individuelle Vereinbarungen zwischen dem mobilen Mitarbeiter und Arbeitgeber geregelt werden.

### INF.9.A8 Sicherheitsrichtlinie für mobile Arbeitsplätze [IT-Betrieb] (S)

Alle relevanten Sicherheitsanforderungen für mobile Arbeitsplätze SOLLTEN in einer für die mobilen Mitarbeiter verpflichtenden Sicherheitsrichtlinie dokumentiert werden. Sie SOLLTE zudem mit den bereits vorhandenen Sicherheitsrichtlinien der Institution sowie mit allen relevanten Fachabteilungen abgestimmt werden. Die Sicherheitsrichtlinie für mobile Arbeitsplätze SOLLTE regelmäßig aktualisiert werden. Die Mitarbeiter der Institution SOLLTEN hinsichtlich der aktuellen Sicherheitsrichtlinie sensibilisiert und geschult sein.

### INF.9.A9 Verschlüsselung tragbarer IT-Systeme und Datenträger [IT-Betrieb] (S)

Bei tragbaren IT-Systemen und Datenträgern SOLLTE sichergestellt werden, dass diese entsprechend den internen Richtlinien abgesichert sind. Mobile IT-Systeme und Datenträger SOLLTEN dabei verschlüsselt werden. Die kryptografischen Schlüssel SOLLTEN getrennt vom verschlüsselten Gerät aufbewahrt werden.

### INF.9.A12Nutzung eines Bildschirmschutzes [Mitarbeiter] (S)

Wenn IT-Systeme an mobilen Arbeitsplätzen genutzt werden, SOLLTEN die Mitarbeiter einen Sichtschutz für die Bildschirme der IT-Systeme verwenden.

## 3.3 Anforderungen bei erhöhtem Schutzbedarf

Im Folgenden sind für den Baustein INF.9 *Mobiler Arbeitsplatz* 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.

### INF.9.A10Einsatz von Diebstahlsicherungen [Mitarbeiter] (H)

Bietet das verwendete IT-System eine Diebstahlsicherung, SOLLTE sie benutzt werden. Die Diebstahlsicherungen SOLLTEN stets dort eingesetzt werden, wo ein erhöhter Publikumsverkehr herrscht oder die Fluktuation von Benutzern sehr hoch ist. Dabei SOLLTEN die Mitarbeiter immer beachten, dass der Schutz der auf den IT-Systemen gespeicherten Informationen meist einen höheren Wert besitzt als die Wiederanschaffungskosten des IT-Systems betragen. Die Beschaffungs- und Einsatzkriterien für Diebstahlsicherungen SOLLTEN an die Prozesse der Institution angepasst und dokumentiert werden.

**INF.9.A11Verbot der Nutzung unsicherer Umgebungen [IT-Betrieb] (H)**
Es SOLLTEN Kriterien für die Arbeitsumgebung festgelegt werden, die mindestens erfüllt sein müssen, damit Informationen mit erhöhtem Schutzbedarf mobil bearbeitet werden dürfen. Die Kriterien SOLLTEN mindestens folgende Themenbereiche abdecken:

- Einsicht und Zugriff durch Dritte,
- geschlossene und, falls nötig, abschließbare oder bewachte Räume,
- gesicherte Kommunikationsmöglichkeiten sowie
- eine ausreichende Stromversorgung.

# 4 Weiterführende Informationen

## 4.1 Wissenswertes

Die International Organization for Standardization (ISO) gibt in der Norm ISO/IEC 27001:2013 im Annex A.11.2 Vorgaben zur Ausrüstung bzw. Ausstattung von mobilen Arbeitsplätzen.

Die International Organization for Standardization (ISO) gibt in der Norm ISO/IEC 27001:2013 im Annex A.6.2.1. Vorgaben zur Erarbeitung einer Richtlinie für mobile Geräte.

Das Information Security Forum (ISF) macht in seinem Standard „The Standard of Good Practice for Information Security“ im Kapitel PA2 Vorgaben zum Umgang mit mobilen Endgeräten.

Das National Institute of Standards and Technology (NIST) hat im Rahmen seiner Special Publications die NIST Special Publication 800-46 zu „Remote Access and Bring Your Own Device (BYOD)“ veröffentlicht und macht Vorgaben zum Fernzugriff auf Handware.

# 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 INF.9 *Mobiler Arbeitsplatz* von Bedeutung.

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 0.18 Fehlplanung oder fehlende Anpassung

G 0.19 Offenlegung schützenswerter Informationen

G 0.21 Manipulation von Hard- oder Software

G 0.22 Manipulation von Informationen

G 0.23 Unbefugtes Eindringen in IT-Systeme

G 0.24 Zerstörung von Geräten oder Datenträgern

G 0.25 Ausfall von Geräten oder Systemen

G 0.29 Verstoß gegen Gesetze oder Regelungen

G 0.30 Unberechtigte Nutzung oder Administration von Geräten und Systemen

G 0.31 Fehlerhafte Nutzung oder Administration von Geräten und Systemen

G 0.44 Unbefugtes Eindringen in Räumlichkeiten

G 0.45 Datenverlust

G 0.46 Integritätsverlust schützenswerter Informationen