



OPS.1.2.4 Telearbeit

1. Beschreibung

1.1. Einleitung

Unter Telearbeit wird jede auf die Informations- und Kommunikationstechnik gestützte Tätigkeit verstanden, die ganz oder teilweise außerhalb der Geschäftsräume und Gebäude der Institution verrichtet wird. Bei der heimbasierten Telearbeit arbeiten die Mitarbeitenden regelmäßig tages- oder stundenweise abwechselnd an ihrem Arbeitsplatz in den Räumlichkeiten der Institution und am häuslichen Arbeitsplatz.

1.2. Zielsetzung

Das Ziel des Bausteins ist der Schutz von Informationen, die während der Telearbeit gespeichert, verarbeitet und übertragen werden. Dazu werden typische Gefährdungen aufgezeigt und spezielle Anforderungen an die sichere Telearbeit definiert.

1.3. Abgrenzung und Modellierung

Der Baustein OPS.1.2.4 *Telearbeit* ist für jeden Telearbeitsplatz anzuwenden.

Dieser Baustein konzentriert sich auf die Form der Telearbeit, die im häuslichen Umfeld durchgeführt wird (heimbasierte Telearbeit). Es wird davon ausgegangen, dass zwischen dem Telearbeitsplatz und der Institution eine sichere Telekommunikationsverbindung besteht, die es ermöglicht, geeignet Informationen auszutauschen und auf Daten auf dem Server der Institution zuzugreifen. Die Anforderungen dieses Bausteins umfassen die folgenden drei Bereiche:

- die Organisation der Telearbeit,
- den Arbeitsplatz-PCs der Mitarbeitenden und
- die Kommunikationsverbindung zwischen Telearbeitsrechnern und Institution.

Sicherheitsanforderungen an die Infrastruktur des Telearbeitsplatzes werden im vorliegenden Baustein nicht berücksichtigt, sondern sind im Baustein INF.8 *Häuslicher Arbeitsplatz* beschrieben. Anforderungen an einen nicht dauerhaft eingerichteten Arbeitsplatz sind im Baustein INF.9 *Mobiler Arbeitsplatz* zu finden.

Detaillierte Empfehlungen, wie die IT-Systeme konfiguriert und abgesichert werden können, werden nicht im Rahmen dieses Bausteins behandelt. Sie sind in SYS.2.1 *Allgemeiner Client* sowie in den betriebssystemspezifischen System-Bausteinen zu finden. Weitere für die Telearbeit relevante

Sicherheitsaspekte, wie z. B. für WLAN, werden in den Bausteinen der Teilschichten NET.2 *Funknetze* oder NET.4 *Telekommunikation* betrachtet.

Sofern Daten, die bei der Telearbeit verändert wurden, nicht unmittelbar auf IT-Systemen der Institution gespeichert werden, muss geregelt werden, wie eine Datensicherung durchgeführt wird. Anforderungen dazu sind im Baustein CON.3 *Datensicherungskonzept* zu finden.

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 OPS.1.2.4 *Telearbeit* von besonderer Bedeutung.

2.1. Fehlende oder unzureichende Regelungen für den Telearbeitsplatz

Die Nutzung eines Telearbeitsplatzes erfordert ergänzende organisatorische Absprachen zwischen den Mitarbeitenden und den Führungskräften. Zudem brauchen sie Handlungsanweisungen für den Fall, dass sicherheitsrelevante Vorkommnisse am Telearbeitsplatz eintreten. Gelangen beispielsweise vertrauliche Informationen in die Hände Dritter, können schwerwiegende Schäden für die Institution entstehen.

2.2. Unerlaubte private Nutzung des dienstlichen Telearbeitsrechners

Im häuslichen Bereich kann leichter nicht geprüfte und nicht freigegebene Hard- oder Software eingesetzt werden und so durch unbedachtes Handeln beispielsweise Schadsoftware auf den Telearbeitsrechner gelangen. Dadurch könnten vertrauliche Informationen kompromittiert werden.

2.3. Verzögerungen durch temporär eingeschränkte Erreichbarkeit der Mitarbeitenden

Haben die Mitarbeitenden keine festen Arbeitszeiten am Telearbeitsplatz und werden keine festen Zeiten vereinbart, an denen sie erreichbar sein müssen, kann aufgrund dessen der Arbeitsablauf verzögert werden.

2.4. Mangelhafte Einbindung der Mitarbeitenden in den Informationsfluss

Da die Mitarbeitenden nicht täglich in der Institution sind, haben sie weniger Gelegenheit, am direkten Informationsaustausch mit den Führungskräften sowie den Kollegen und Kolleginnen teilzuhaben. Es ist daher möglich, dass Telearbeitende insbesondere mündlich weitergegebene Informationen nicht oder erst verzögert erhalten. Hierdurch können Arbeitsabläufe und betriebliche Prozesse gestört und die Produktivität des oder der Mitarbeitenden eingeschränkt werden.

2.5. Nichtbeachtung von Sicherheitsmaßnahmen

Am Telearbeitsplatz können beispielsweise fehlende Kontrollmöglichkeiten dazu führen, dass Mitarbeitende empfohlene oder angeordnete Sicherheitsmaßnahmen nicht oder nicht in vollem Umfang umsetzen. So können z. B. vertrauliche Informationen in die Hände Dritter geraten.

3. Anforderungen

Im Folgenden sind die spezifischen Anforderungen des Bausteins OPS.1.2.4 *Telearbeit* 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	Informationssicherheitsbeauftragte (ISB)
Weitere Zuständigkeiten	Mitarbeitende, IT-Betrieb, Vorgesetzte, Personalabteilung

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.

OPS.1.2.4.A1 Regelungen für Telearbeit (B) [Vorgesetzte, Personalabteilung]

Alle relevanten Aspekte der Telearbeit MÜSSEN geregelt werden. Zu Informationszwecken MÜSSEN den Telearbeitenden die geltenden Regelungen oder ein dafür vorgesehenes Merkblatt ausgehändigt werden, das die zu beachtenden Sicherheitsmaßnahmen erläutert. Alle strittigen Punkte MÜSSEN entweder durch Betriebsvereinbarungen oder durch zusätzlich zum Arbeitsvertrag getroffene individuelle Vereinbarungen zwischen dem Mitarbeitenden und der Institution geregelt werden. Die Regelungen MÜSSEN regelmäßig aktualisiert werden.

OPS.1.2.4.A2 Sicherheitstechnische Anforderungen an den Telearbeitsrechner (B)

Es MÜSSEN sicherheitstechnische Anforderungen festgelegt werden, die ein IT-System für die Telearbeit erfüllen muss.

Es MUSS sichergestellt werden, dass nur autorisierte Personen Zugang zu den Telearbeitsrechnern haben. Darüber hinaus MUSS der Telearbeitsrechner so abgesichert werden, dass er nur für autorisierte Zwecke benutzt werden kann.

OPS.1.2.4.A3 ENTFALLEN (B)

Diese Anforderung ist entfallen.

OPS.1.2.4.A4 ENTFALLEN (B)

Diese Anforderung ist entfallen.

OPS.1.2.4.A5 Sensibilisierung und Schulung der Mitarbeitenden (B)

Anhand eines Leitfadens MÜSSEN die Mitarbeitenden für die Gefahren sensibilisiert werden, die mit der Telearbeit verbunden sind. Außerdem MÜSSEN sie in die entsprechenden Sicherheitsmaßnahmen der Institution eingewiesen und im Umgang mit diesen geschult werden. Die Schulungs- und Sensibilisierungsmaßnahmen für Mitarbeitenden SOLLTEN regelmäßig wiederholt 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.

OPS.1.2.4.A6 Erstellen eines Sicherheitskonzeptes für Telearbeit (S)

Es SOLLTE ein Sicherheitskonzept für die Telearbeit erstellt werden, das Sicherheitsziele, Schutzbedarf, Sicherheitsanforderungen sowie Risiken beschreibt. Das Konzept SOLLTE regelmäßig aktualisiert und überarbeitet werden. Das Sicherheitskonzept zur Telearbeit SOLLTE auf das übergreifende Sicherheitskonzept der Institution abgestimmt werden.

OPS.1.2.4.A7 Regelung der Nutzung von Kommunikationsmöglichkeiten bei Telearbeit (S) [IT-Betrieb, Mitarbeitende]

Es SOLLTE klar geregelt werden, welche Kommunikationsmöglichkeiten bei der Telearbeit unter welchen Rahmenbedingungen genutzt werden dürfen. Die dienstliche und private Nutzung von Internetdiensten bei der Telearbeit SOLLTE geregelt werden. Dabei SOLLTE auch geklärt werden, ob eine private Nutzung generell erlaubt oder unterbunden wird.

OPS.1.2.4.A8 Informationsfluss zwischen Mitarbeitenden und Institution (S) [Vorgesetzte, Mitarbeitende]

Ein regelmäßiger innerbetrieblicher Informationsaustausch zwischen den Mitarbeitenden und der Institution SOLLTE gewährleistet sein. Alle Mitarbeitenden SOLLTEN zeitnah über geänderte Sicherheitsanforderungen und andere sicherheitsrelevante Aspekte informiert werden. Allen Kollegen und Kolleginnen der jeweiligen Mitarbeitenden SOLLTE bekannt sein, wann und wo diese erreicht werden können. Technische und organisatorische Telearbeitsregelungen zur Aufgabenbewältigung, zu Sicherheitsvorfällen und sonstigen Problemen SOLLTEN geregelt und an die Mitarbeitenden kommuniziert werden.

OPS.1.2.4.A9 Betreuungs- und Wartungskonzept für Telearbeitsplätze (S) [IT-Betrieb, Mitarbeitende]

Für Telearbeitsplätze SOLLTE ein spezielles Betreuungs- und Wartungskonzept erstellt werden. Darin SOLLTEN folgende Aspekte geregelt werden: Kontaktperson des IT-Betriebs, Wartungstermine, Fernwartung, Transport der IT-Geräte und Einführung von Standard-Telearbeitsrechnern. Damit die Mitarbeitenden einsatzfähig bleiben, SOLLTEN für sie Kontaktpersonen für Hard- und Softwareprobleme benannt werden.

OPS.1.2.4.A10 Durchführung einer Anforderungsanalyse für den Telearbeitsplatz (S) [IT-Betrieb]

Bevor ein Telearbeitsplatz eingerichtet wird, SOLLTE eine Anforderungsanalyse durchgeführt werden. Daraus SOLLTE z. B. hervorgehen, welche Hard- und Software-Komponenten für den Telearbeitsplatz benötigt werden. Die Anforderungen an den jeweiligen Telearbeitsplatz SOLLTEN mit den IT-Verantwortlichen abgestimmt werden. Es SOLLTE immer festgestellt und dokumentiert werden, welchen Schutzbedarf die am Telearbeitsplatz verarbeiteten Informationen haben.

3.3. Anforderungen bei erhöhtem Schutzbedarf

Für diesen Baustein sind keine Anforderungen für einen erhöhten Schutzbedarf definiert.

4. Weiterführende Informationen

4.1. Wissenswertes

Die International Organization for Standardization (ISO) gibt in der Norm ISO/IEC 27001:2013, insbesondere in Annex A, A.6.2.1 „Mobile device policy“ und A.11.2.6 „Security of equipment and assets off-premises“, Informationen zum Umgang mit Telearbeit.

Das Information Security Forum (ISF) macht in seinem Standard „The Standard of Good Practice for Information Security“, insbesondere in Area PA2 Mobile Computing, ebenfalls Vorgaben zur Telearbeit.

Das National Institute of Standards and Technology (NIST) hat im Rahmen seiner Special Publications die NIST Special Publication 800-46 als „Guide to Enterprise Telework, Remote Access and Bring Your Own Device (BYOD) Security“ veröffentlicht.