Bundesamt
für Sicherheit in der
Informationstechnik

Umsetzungshinweise zum Baustein OPS.1.2.4 Telearbeit

1. Einleitung

Unter Telearbeit wird jede auf die Informations- und Kommunikationstechnik gestützte Tätigkeit verstanden, die ausschließlich oder zeitweise außerhalb der Geschäftsräume und Gebäude des Arbeitgebers verrichtet wird.

Es gibt verschiedene Formen der Telearbeit. Sie kann beispielsweise als heimbasierte Telearbeit in der Wohnung des Mitarbeiters oder auch als mobile Telearbeit von unterwegs erbracht werden. Es ist ebenfalls möglich, dass die Mitarbeiter im Rahmen der On-Site-Telearbeit bei Kunden oder Lieferanten eingesetzt werden und dort mit der Ausstattung des eigenen Arbeitgebers arbeiten. Eine weitere Möglichkeit ist die Telearbeit in sogenannten Telecentern oder auch Satelliten- oder Nachbarschaftsbüros.

Bei der heimbasierten Telearbeit wird zwischen der ausschließlich zu Hause erbrachten Arbeit und der alternierenden Telearbeit unterschieden. Bei der alternierenden Telearbeit arbeiten die Arbeitnehmer wechselweise an ihrem Arbeitsplatz beim Arbeitgeber und am häuslichen Arbeitsplatz.

2. Maßnahmen

Im Folgenden sind spezifische Maßnahmen für die Anforderungen des Bausteins OPS.1.2.4 *Telearbeit* aufgeführt.

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

2.1 Maßnahmen zum Baustein OPS.1.2.4 Telearbeit

OPS.1.2.4.M1 Regelungen für Telearbeit (B)

Institutionen müssen Regelungen für die Telearbeit festlegen. Die für die Telearbeit im Umgang mit Informationen und der Informations- und Kommunikationstechnik notwendigerweise umzusetzenden

Sicherheitsmaßnahmen sollten zusätzlich in einer Sicherheitsrichtlinie zur Telearbeit dokumentiert werden. Alternativ können die Inhalte in bereits bestehende Richtlinien der Institution integriert werden.

Folgende Aspekte sollten beispielsweise in den Regelungen für Telearbeit beachtet werden:

- **Unterweisung**: Bevor Mitarbeiter erstmalig in Telearbeit gehen, müssen sie entsprechend den geltenden Richtlinien unterwiesen werden. Als Grundlage für die Unterweisung eignet sich z. B. die Richtlinie zum Incident Management.
- **Meldeweg:** Die Mitarbeiter müssen verpflichtet werden, sicherheitsrelevante Vorkommnisse unverzüglich an eine Stelle in der Institution zu melden. Diese Stelle muss bestimmt werden, bevor die Telearbeit ermöglicht wird.
- **Arbeitszeitregelung:** Es sollte geregelt sein, wie die Arbeitszeiten auf Tätigkeiten zwischen der Institution und dem Telearbeitslatz verteilt sind. Auch müssen feste Zeiten festgelegt werden, an denen der Mitarbeiter am Telearbeitsplatz erreichbar ist.
- **Reaktionszeiten:** Es sollte geregelt werden, in welchen Abständen die Mitarbeiter aktuelle Informationen abrufen sollen (z. B. wie häufig E-Mails gelesen werden) und in welchem Zeitraum sie darauf zu reagieren haben.
- **Umgang mit vertraulichen Informationen:** Bei der Telearbeit werden vertrauliche Informationen sowohl analog (z. B. auf Papier) als auch digital bearbeitet. Unabhängig davon, in welcher Form Informationen vorliegen, müssen sie vor unbefugtem Zugriff und anderen Sicherheitsrisiken geschützt werden. Daher ist der komplette Lebensweg vertraulicher Informationen angemessen abzusichern.
- **Arbeitsmittel:** Es sollte festgeschrieben werden, welche Arbeitsmittel die Mitarbeiter einsetzen dürfen und welche nicht benutzt werden dürfen (z. B. nicht freigegebene Software).
- **Datensicherung:** Die Mitarbeiter müssen verpflichtet werden, lokal gespeicherte Daten regelmäßig zu sichern. Zusätzlich sollte vereinbart werden, dass jeweils eine Generation der Datensicherungen in der Institution hinterlegt wird. Falls die Datensicherung über den Fernzugriff zur Institution bereits ausreichend sichergestellt ist und kein erhöhter Schutzbedarf vorliegt, kann von einer lokalen Datensicherung abgesehen werden.
- **Synchronisation von Datenbeständen:** Datenbestände, die sowohl in der Institution als auch an Telearbeitsplätzen bearbeitet werden, müssen geeignet synchronisiert werden. Synchronisationskonflikte können z. B. dann auftreten, wenn zwei Benutzer den gleichen Datensatz in gespiegelten Datenbeständen ändern. Das Vorgehen bei der Synchronisation muss so geplant werden, dass solche Konflikte vermieden werden und es zu keinem Datenverlust kommt. Es empfiehlt sich, die Datenbestände mithilfe einer geeigneten Software zu synchronisieren.
- **Datenschutz:** Die Mitarbeiter sind darauf zu verpflichten, einschlägige Datenschutzvorschriften einzuhalten.
- **Datenkommunikation:** Es muss festgelegt werden, welche Daten auf welchem Weg übertragen werden dürfen. Insbesondere muss geregelt werden, welche Daten entweder nur verschlüsselt oder gar nicht elektronisch übermittelt werden dürfen.
- **Transport von Dokumenten:** Es muss festgelegt werden, welche Dokumente zwischen Institution und Telearbeitsplatz transportiert werden dürfen. Insbesondere muss geregelt werden, wie welche Papierdokumente dabei zu schützen sind.
- **Transport von Datenträgern:** Es muss festgelegt werden, welche Datenträger zwischen dem Telearbeitsplatz und der Institution transportiert werden dürfen. Vertrauliche Daten auf digitalen Datenträgern sollten grundsätzlich nur verschlüsselt transportiert werden.
- **Zutrittsrecht Telearbeitsplatz:** Es sollte ein Zutrittsrecht zum Telearbeitsplatz vereinbart werden, gegebenenfalls nach vorheriger Anmeldung. Dies ist insbesondere dann von Bedeutung, wenn der Vertretungsfall eintritt und ein stellverstretender Mitarbeiter Akten und Daten vom Telearbeitsplatz benötigt.

Die Regelungen für die Telearbeit sind jedem Mitarbeiter auszuhändigen. Entsprechende Merkblätter sind regelmäßig zu aktualisieren.

OPS.1.2.4.M2 Sicherheitstechnische Anforderungen an den Telearbeitsrechner (B)

Die sicherheitstechnischen Anforderungen an die Telearbeitsrechner richten sich nach dem Schutzbedarf der zu bearbeitenden Daten am Telearbeitsplatz und der Daten, auf die die Mitarbeiter über den Kommunikationsrechner der Institution zugreifen können. Je höher der Schutzbedarf, desto mehr Maßnahmen müssen ergriffen werden, um diesen Schutz zu gewährleisten.

Allgemeine Sicherheitsziele für den Telearbeitsrechner

- Telearbeitsrechner dürfen **nur von autorisierten Personen** benutzt werden. Damit wird sichergestellt, dass nur autorisierte Personen auf Daten und Programme zugreifen können, die auf einem Telearbeitsrechner gespeichert sind. Gleiches gilt für Informationen und Daten, die über den Telearbeitsrechner erreichbar wären (z. B. mittels VPN). Autorisierte Personen sind der Administrator des Telearbeitsrechners, der Mitarbeiter selbst sowie sein Stellvertreter.
- Telearbeitsrechner dürfen **nur für autorisierte Zwecke** benutzt werden. So wird Schäden vorgebeugt, die durch Fehlbedienung und Missbrauch entstehen könnten. Z. B. sollte der Benutzer keine ungenehmigten Programme installieren dürfen.
- Schäden aufgrund eines Diebstahls oder Defektes eines Telearbeitsrechners müssen tolerabel sein. Telearbeitsrechner werden üblicherweise in einer wenig gesicherten Umgebung eingesetzt. Dort ist ein Diebstahl oder Defekt wahrscheinlicher als in der geschützten Betriebsumgebung einer Institution. Im Schadensfall können sowohl die Verfügbarkeit als auch die Vertraulichkeit der gespeicherten Daten leiden. Um die **Schäden bei Diebstählen** gering zu halten, sollten die Daten z. B. nur verschlüsselt gespeichert werden. Um Schäden durch Defekte zu begrenzen, eignen sich zum Beispiel regelmäßig durchgeführte Datensicherungen.
- Mitarbeiter sollten so unterwiesen werden, dass sie **Manipulationen** und Manipulationsversuche am Telearbeitsrechner erkennen können. Dies erhöht die Wahrscheinlichkeit, dass der Telearbeitsrechner in einem integren Zustand verbleibt. Versteckte Manipulationsversuche können jedoch insbesondere am Telearbeitsplatz nicht ausgeschlossen werden.

Sicherheitsrelevante Funktionalitäten für den Telearbeitsrechner

Aus dem Schutzbedarf derjenigen Daten, die am Telearbeitsplatz bearbeitet werden, leiten sich bestimmte Sicherheitsziele ab. Aus diesen Sicherheitszielen ergeben sich die sicherheitstechnischen Anforderungen an einen Telearbeitsrechner. Es muss dokumentiert werden, welche der nachfolgend beschriebenen sicherheitsrelevanten Funktionalitäten ein Telearbeitsrechner aufweisen muss und wie diese umgesetzt werden.

Der Telearbeitsrechner muss über einen **Identifizierungs- und Authentisierungsmechanismus** verfügen. Insbesondere sind dabei folgende Punkte sicherzustellen:

- Sicherheitskritische Parameter, wie Passwörter oder Benutzerkennung müssen sicher verwaltet werden. Passwörter dürfen nie unverschlüsselt auf dem Telearbeitsrechner gespeichert werden.
- Das Zugangsverfahren muss definiert auf Fehleingaben reagieren. Erfolgt zum Beispiel dreimal hintereinander eine fehlerhafte Authentisierung, ist der Zugang zum Telearbeitsrechner zu sperren oder es sind die zeitlichen Abstände sukzessiv zu vergrößern, nach denen ein weiterer Zugangsversuch erlaubt wird.
- Es muss möglich sein, Minimalvorgaben für die sicherheitskritischen Parameter vorzugeben.
- Nach zeitweiser Inaktivität der Tastatur oder Maus, muss automatisch eine Bildschirmsperre aktiviert werden, die erst nach erneuter Identifikation und Authentisierung deaktiviert wird.

Der Telearbeitsrechner muss über eine **Zugriffskontrolle** verfügen. Insbesondere sind folgende Anforderungen umzusetzen:

- Der Telearbeitsrechner muss verschiedene Benutzer unterscheiden können. Es muss möglich sein, mindestens zwei getrennte Rollen auf dem Telearbeitsrechner einzurichten, nämlich Administrator und Mitarbeiter.
- Mittels einer differenzierten Rechtestruktur (zum Beispiel lesen, schreiben, ausführen) muss der Zugriff auf Dateien und Programme regelbar sein. Bei mobilen Endgeräten ist eine differenzierte Rechtestruktur nicht immer möglich. Gerade Smartphones und Tablets verfügen häufig über keine derartige Differenzierung. Es sollte daher geprüft werden, ob sich die Geräte für den vorliegenden Schutzbedarf eignen.

Telearbeitsrechner sollten über eine **Protokollierung** verfügen. Es ist sinnvoll, folgende Anforderungen umzusetzen:

- Der Mindestumfang, den der Telearbeitsrechner protokollieren soll, sollte parametrierbar sein. Beispielsweise sollten folgende Aktionen inklusive der aufgetretenen Fehlerfälle protokollierbar sein:
- bei Authentisierung: z. B. Benutzerkennung, Datum und Uhrzeit, Ergebnis des Anmeldeversuchs bei der Zugriffskontrolle
- Art des Zugriffs: Was wurde wie geändert, gelesen, geschrieben?
- Durchführung von Administrator-Tätigkeiten
- Auftreten von funktionalen Fehlern
- für Unberechtigte darf keine Möglichkeit bestehen, die Protokollierung zu deaktivieren. Die Protokolle selbst dürfen für Unberechtigte weder lesbar noch modifizierbar sein.
- Die Protokollierung muss übersichtlich, vollständig und korrekt sein.

Falls der Telearbeitsrechner über eine **Protokollauswertung** verfügen soll, dann können folgende Anforderungen sinnvoll sein:

- Eine Auswertefunktion muss nach den protokollierten Datenarten unterscheiden können (z. B. Filtern aller unberechtigten Zugriffe auf alle Ressourcen in einem vorgegebenen Zeitraum).
- Die Auswertefunktion muss auswertbare, d. h. lesbare Berichte erzeugen, sodass keine sicherheitskritischen Aktivitäten übersehen werden.

Telearbeitsrechner sollten über Funktionen zur **Datensicherung** verfügen. Diese sollten unter anderem folgende Anforderungen erfüllen:

- Die Datensicherung für die Telearbeit sollte den Rahmenbedingungen zur Datensicherung der Institution entsprechen und diese einhalten
- Das Datensicherungsprogramm muss benutzerfreundlich und schnell arbeiten. Es sollte automatisierbar sein.
- Es muss konfigurierbar sein, welche Daten wann gesichert werden.
- Es muss eine Option existieren, um beliebige Datensicherungen wieder einzuspielen.
- Die Funktion muss ermöglichen, mehrere Generationen zu sichern.
- Datensicherungen von Zwischenergebnissen aus der laufenden Anwendung sollen möglich sein.

Telearbeitsrechner sollten über eine **Verschlüsselungskomponente** verfügen. Hierfür ist zunächst zu überlegen, welche Funktionalität benötigt wird:

- die Verschlüsselung ausgewählter Daten (offline) oder
- automatisch der gesamten Festplatte (online).

Grundsätzlich sollte die automatische Verschlüsselung aller Datenträger vorgezogen werden, da dies benutzerfreundlicher und effizienter ist. Das setzt voraus, dass ein geeignetes Verschlüsselungsprodukt

eingesetzt wird und dass ein Datenverlust bei Fehlfunktion (Stromausfall, Abbruch der Verschlüsselung) systemseitig abgefangen wird. Darüber hinaus sind folgende Anforderungen sinnvoll:

- Der implementierte Verschlüsselungsalgorithmus sollte den Anforderungen der Institution entsprechen.
- Das Schlüsselmanagement muss mit der Funktionalität des Telearbeitsrechners harmonieren. Dabei sind insbesondere grundsätzliche Unterschiede der Algorithmen zu berücksichtigen: Symmetrische Verfahren benutzen einen geheim zu haltenden Schlüssel für die Ver- und Entschlüsselung, asymmetrische Verfahren benutzen einen öffentlichen Schlüssel für die Verschlüsselung und einen privaten (geheim zu haltenden) für die Entschlüsselung.
- Der Telearbeitsrechner muss die sicherheitskritischen Parameter wie Schlüssel sicher verwalten. So dürfen Schlüssel (auch mittlerweile nicht mehr benutzte) nie ungeschützt, das heißt, auslesbar auf dem Telearbeitsrechner abgelegt werden.

Falls der Telearbeitsrechner über Mechanismen zur **Integritätsprüfung** verfügen soll, sind folgende Anforderungen sinnvoll:

- Es sollten Verfahren zur Integritätsprüfung eingesetzt werden, die absichtliche Manipulationen am Telearbeitsrechner bzw. an den Daten zuverlässig aufdecken können.
- Bei der Datenübertragung müssen Mechanismen eingesetzt werden, mit denen absichtliche Manipulationen an den Adressfeldern und den Benutzerdaten erkannt werden können. Daneben darf die bloße Kenntnis der eingesetzten Algorithmen ohne spezielle Zusatzkenntnisse nicht ausreichen, um unerkannte Manipulationen an den oben genannten Daten vornehmen zu können.

Der Telearbeitsrechner sollte über einen **Boot-Schutz** verfügen, um zu verhindern, dass unbefugt von Wechseldatenträgern gebootet werden kann.

Es sollte möglich sein, die **Benutzerumgebung** des Telearbeitsrechners **einzuschränken**. Damit soll der Administrator festlegen können, welche Programme der Mitarbeiter ausführen kann, welche Peripheriegeräte nutzbar sind und welche Änderungen der Mitarbeiter am System vornehmen darf. Darüber hinaus sollte der Mitarbeiter Einstellungen, die für den sicheren Betrieb notwendig sind, nicht unautorisiert ändern und nicht unerlaubt Fremdsoftware aufspielen können.

In Abhängigkeit des installierten Betriebssystems und anderer vorhandener Schutzmechanismen des Telearbeitsrechners muss geprüft werden, ob **Viren-Schutzprogramme** eingesetzt werden sollen. Ist dies der Fall, muss vor dem Einspielen von Daten von auswechselbaren Datenträgern, vor der Weitergabe von Datenträgern beziehungsweise beim Senden und Empfangen von Daten ein Virencheck durchgeführt werden.

Wenn der Telearbeitsrechner über **Fernwartung (Remote Administration)** administriert werden sollte, ist sicherzustellen, dass die Fernadministration nur autorisiert durchgeführt werden kann. Bei der Fernwartung müssen eine Authentisierung des Fernwartungspersonals, die Verschlüsselung der übertragenen Daten und eine Protokollierung der Administrationsvorgänge gewährleistet sein.

Auswahl geeigneter Funktionialitäten

Aus den obigen Funktionalitäten sind diejenigen auszuwählen, die aufgrund der Sicherheitsanforderungen an die Telearbeitsrechner benötigt werden und entsprechend dem Schutzbedarf möglich sind. Anhand dieser Funktionalitäten muss dann ein geeignetes Betriebssystem als Plattform ausgewählt werden. Wenn dieses nicht alle benötigten Funktionalitäten unterstützt, müssen dazu Zusatzprodukte eingesetzt werden. Dabei sollten möglichst alle Telearbeitsrechner einer Institution gleich ausgestattet sein, um die Betreuung und Wartung zu erleichtern und gleichartige Systeme als Client-Gruppen zusammenführen zu können. Das Gesamtsystem ist durch die Administratoren so zu konfigurieren, dass maximale Sicherheit erreicht werden kann.

Weitere Anforderungen zu den einzelnen Client-Systemen werden in der Bausteinschicht SYS.2 *Desktop-Systeme* aufgeführt. Diese sollten entsprechend der eingesetzten Client-Lösung für den Telearbeitsrechner umgesetzt werden.

OPS.1.2.4.M3 Entfallen (B)

Die zugehörige Anforderung ist entfallen.

OPS.1.2.4.M4 Entfallen (B)

Die zugehörige Anforderung ist entfallen.

OPS.1.2.4.M5 Sensibilisierung und Schulung der Mitarbeiter (B)

Anhand eines Leitfadens für Telearbeit müssen die Mitarbeiter eine Einweisung in die entsprechenden Sicherheitsmaßnahmen der Institution erhalten. Dabei sind insbesondere folgende Punkte zu berücksichtigen:

- Dienstliche Unterlagen müssen am Telearbeitsplatz sicher aufbewahrt werden, also zum Beispiel in Schränke weggeschlossen werden.
- Fenster und nach außen gehende Türen (Balkone, Terrassen) sind abzuschließen, wenn der Telearbeitsplatz verlassen wird.
- Strukturelle und sicherheitsrelevante Änderungen an der Telearbeitsplatz-IT dürfen nur durch die Administratoren der Institution vorgenommen werden.
- Der Telearbeitsrechner darf nur über den dafür vorgesehenen Anschluss an öffentliche Kommunikationsnetze angebunden sein (z. B. nur über eine VPN-Verbindung).
- Beim Datenaustausch mittels Datenträgern zwischen IT-Systemen der Institution und dem Arbeitsplatz-PC am Telearbeitsplatz dürfen nur die von der Institution beschafften Datenträger benutzt werden. Datenträger sollten nur verschlüsselt transportiert werden. Dienstliche und private IT-Systeme oder Datenträger sollten sorgfältig getrennt bleiben.
- Falls Datensicherungen am Telearbeitsplatz durchgeführt werden, müssen Backup-Datenträger dort verschlossen aufbewahrt werden. Es ist sicherzustellen, dass nur der Mitarbeiter und sein Vertreter darauf zugreifen können.
- Der unbefugte Zugriff auf die IT der Mitarbeiter ist durch Zugriffssperren zu verhindern, zum Beispiel Boot- und Bildschirm-Sperren. Passwörter sind generell geheim zu halten.

Darüber hinaus sind die Mitarbeiter soweit im Umgang mit den Telearbeitsrechnern zu schulen, dass sie einfache Fehlerkorrekturen (zum Beispiel Druckerpatrone wechseln) vornehmen beziehungsweise einfache Probleme selbstständig beheben können.

Für das geordnete und strukturierte Vorgehen bei sicherheitstechnischen Einweisungen der Mitarbeiter sollten auch die Anforderungen des Bausteins ORP.3 *Sensibilisierung und Schulung zur Informationssicherheit* beachtet werden.

OPS.1.2.4.M6 Erstellen eines Sicherheitskonzeptes für Telearbeit (S)

Es sollte ein Sicherheitskonzept für Telearbeit erstellt werden, in dem die Sicherheitsziele, der Schutzbedarf der bei der Telearbeit zu bearbeitenden Informationen sowie die Risiken und Sicherheitsmaßnahmen aufgezeigt werden.

Bei der Telearbeit werden Informationen meist außerhalb der geschützten Betriebsumgebung verarbeitet. Daher ist im Vorfeld eine Schutzbedarfsfeststellung der betroffenen Informationen, Geschäftsprozesse, Anwendungen, IT-Systeme, Kommunikationsverbindungen und Räume (vor allem der Telearbeitsplätze) bezüglich Vertraulichkeit, Integrität und Verfügbarkeit durchzuführen. Aus dem Schutzbedarf der zu bearbeitenden Daten am Telearbeitsplatz leiten sich die Sicherheitsziele und damit die sicherheitstechnischen Anforderungen an die Mitarbeiter, die Telearbeitsrechner und die Telearbeitsplätze ab.

Neben einem Überblick über die Gefährdungslage und den organisatorischen, infrastrukturellen und personellen Sicherheitsmaßnahmen können Maßnahmen aus folgenden Bereichen sinnvoll sein:

- Umgang mit Daten und schützenswerten Betriebsmitteln wie Dokumenten und Speichermedien (insbesondere Regelungen zum Anfertigen von Kopien und zum Löschen beziehungsweise Vernichten von Datenträgern)
- Absicherung der Kommunikation zwischen Institution und Telearbeitsplatz (z. B. durch E-Mail-Verschlüsselung, elektronische Signatur)
- Authentisierungsmechanismen
- Regelungen für weitere Netzanbindungen
- Regelungen für den Datenaustausch (z. B. nur über VPN-Verbindung, siehe NET.3.3 *VPN*)
- Datensicherung (Insbesondere wenn die Daten des Telearbeitsplatzes nur zentral in der Institution gespeichert werden, muss die Übertragungskapazität für das Volumen der zu sichernden Daten ausreichend sein, siehe CON.3 *Datensicherungskonzept.*)

Zur Ausgestaltung der Telearbeit sind zusätzlich diverse Gesetze und Vorschriften zu beachten (siehe OPS.1.2.4.M1 *Regelungen für Telearbeit*).

Die Anforderungen, Ziele und die zu ergreifenden Maßnahmen zur Sicherheit bei Telearbeit sind zu dokumentieren. Das Sicherheitskonzept zur Telearbeit ist mit dem übergreifenden Sicherheitskonzept der Institution abzustimmen und zu harmonisieren. Außerdem muss es regelmäßig aktualisiert werden und ist an Änderungen in der Institution oder der Technik anzupassen.

Die von den Mitarbeitern umzusetzenden Sicherheitsmaßnahmen sind in einer Sicherheitsrichtlinie zur Telearbeit zielgruppengerecht zusammenzufassen.

OPS.1.2.4.M7 Regelung der Nutzung von Kommunikationsmöglichkeiten bei Telearbeit (S)

Für die Telearbeit werden typischerweise verschiedene Kommunikationsmöglichkeiten, wie Telefon-, Fax- und Internet-Anbindung, aber auch Postaustausch sowie Akten- und Datenträgertransport benötigt.

Es muss geregelt werden, auf welche Weise die vorhandenen Kommunikationsmöglichkeiten genutzt werden dürfen. Auch der Postaustausch sowie der Akten- und Datenträger-Transport zwischen Institution und Telearbeitsplatz müssen dabei betrachtet werden. Ebenso sollte die private Benutzung der Kommunikationsmöglichkeiten klar geregelt werden, z. B. des Internetanschlusses. Alle Regelungen sind schriftlich zu fixieren (siehe *OPS.1.2.4.*M1 *Regelungen für Telearbeit*) und den Mitarbeitern auszuhändigen.

Zu klären sind dabei zumindest folgende Punkte:

Datenflusskontrolle

Der Austausch von Informationen zwischen dem Telearbeitsplatz und der Institution muss so geregelt sein, dass die Sicherheit der Informationen gewährleistet ist.

- Welche Dienste dürfen zum Informationsaustausch und zur Datenübertragung genutzt werden?
- Welche Informationen dürfen dabei an wen weitergegeben werden?
- Welche Dienste dürfen explizit nicht genutzt werden?
- Welcher Schriftverkehr darf über E-Mail abgewickelt werden? Ist eine Unterschriftenregelung für die Kommunikation vorgesehen?
- Welche Authentisierungsverfahren werden für den Schriftverkehr und für den Datenaustausch genutzt?
- Werden digitale Signaturen eingesetzt?

Zugriffsberechtigungen

Muss der Mitarbeiter auf die IT der Institution (zum Beispiel auf einen Server) zugreifen können, sollte zuvor festgelegt werden, welche Objekte (zum Beispiel Daten oder IT) er tatsächlich für seine Aufgaben benötigt. Die benötigten Zugangs- und Zugriffsrechte sollten nach den festgelegten Vorgaben der Institution vergeben werden.

Sicherheitsmaßnahmen beim Informationsaustausch

Der Informationsaustausch bei der Telearbeit muss angemessen abgesichert werden. Vertrauliche Informationen müssen sicher transportiert werden. Dazu sind mindestens folgende Fragen zu beantworten:

- Für welche Datenträger soll welche Versandart eingesetzt werden (zum Beispiel Kurierdienst)? Welche Art der Transportsicherung ist angemessen (zum Beispiel Umschläge mit Sicherheitsetiketten)?
- Für welche Daten sollen welche Verschlüsselungsverfahren eingesetzt werden? Daten sollten bei der Datenübertragung und auf Datenträgern möglichst immer verschlüsselt werden, damit Transportverluste höchstens deren Verfügbarkeit und nicht deren Vertraulichkeit gefährden.
- Werden von zu übertragenden Daten, die nur zum Zweck der Datenübertragung erstellt beziehungsweise zusammengestellt worden sind, Sicherungskopien vorgehalten?
- Für welche Daten ist eine Löschung nach erfolgreicher Übertragung notwendig? Das kann beispielsweise für personenbezogene Daten gelten.
- Von welchen Daten soll trotz der erfolgreichen Übertragung eine Kopie der Daten auf dem Telearbeitsrechner verbleiben?
- Wird vor Versand und nach Erhalt von Daten ein Malware-Check der Daten durchgeführt?
- Für welche Datenübertragungen sollte eine Protokollierung erfolgen? Falls eine automatische Protokollierung von Datenübertragungen nicht möglich sein sollte, ist festzulegen, ob und in welchem Umfang eine handschriftliche Protokollierung vorzusehen ist.

Internet-Nutzung

Es ist zu regeln, ob über den Telearbeitsrechner Internet-Dienste genutzt werden dürfen. Dabei ist auch zu klären, ob eine private Nutzung erlaubt wird. Dabei zu klärende Fragen:

- Wird die Nutzung von Internet-Diensten generell verboten?
- Welche Internet-Dienste dürfen genutzt werden?
- Dürfen Daten aus dem Internet geladen werden? Bei Daten von fremden Servern besteht die Gefahr, dass sie Schadsoftware enthalten.
- Welche Rahmenbedingungen und technischen Sicherheitsmaßnahmen müssen bei der Internet-Nutzung beachtet werden? Welche Sicherheitsmechanismen sollen beispielsweise im Browser aktiviert werden?
- Dürfen sich Mitarbeiter am Informationsaustausch über Internet-Plattformen, Newsgruppen, Blogs oder Ähnlichem beteiligen? Ist hierfür ein Pseudonym erforderlich?

OPS.1.2.4.M8 Informationsfluss zwischen Mitarbeiter und Institution (S)

Damit Mitarbeiter nicht vom betrieblichen Geschehen ausgeschlossen werden, muss ein regelmäßiger Informationsaustausch zwischen den Mitarbeitern und den Arbeitskollegen der Institution erfolgen. Hierfür sind sowohl die Vorgesetzten, als auch die Mitarbeiter selber verantwortlich. Die jeweiligen Vorgesetzten müssen sicherstellen, dass die Mitarbeiter alle notwendigen Informationen für ihre Arbeitsbereiche erhalten. Die Mitarbeiter müssen jedoch auch selbstständig nach Informationen und Neuigkeiten fragen. Der regelmäßige Informationsaustausch ist wichtig, damit die Mitarbeiter über Planungen und Zielsetzungen in ihrem Arbeitsbereich informiert sind.

Die Mitarbeiter sollten an den Umlaufverfahren für Hausmitteilungen, einschlägige Informationen und Zeitschriften beteiligt werden. Dies stellt ein Problem dar, wenn Mitarbeiter ausschließlich zu Hause arbeiten. Eine Lösungsmöglichkeit ist, wichtige Schriftstücke einzuscannen, um sie den Mitarbeitern per E-Mail zuzustellen. Die Mitarbeiter müssen auf jeden Fall zeitnah über geänderte Sicherheitsmaßnahmen und andere sicherheitsrelevante Aspekte unterrichtet werden.

Die Arbeitskollegen in der Institution müssen über die Anwesenheits- und Erreichbarkeitszeiten der Mitarbeiter in Kenntnis gesetzt werden. Die entsprechenden E-Mail-Adressen und Telefonnummern sollten

allen Kollegen bekannt sein. Außerdem sollte eine Anrufweiterleitung vom Telefonanschluss des Mitarbeiters in der Institution zum Telefon am Telearbeitsplatz eingerichtet werden.

Folgende Punkte müssen darüber hinaus bei der Telearbeit geklärt werden:

- Wer ist Ansprechpartner bei technischen und/oder organisatorischen Problemen bei der Telearbeit?
- Wem müssen Sicherheitsvorkommnisse mitgeteilt werden?
- Wie erfolgt die Aufgabenzuteilung?
- Wie erfolgt die Übergabe der Arbeitsergebnisse?

Treten technisch-organisatorische Probleme auf, müssen diese vom Mitarbeiter unverzüglich der Institution gemeldet werden.

OPS.1.2.4.M9 Betreuungs- und Wartungskonzept für Telearbeitsplätze (S)

Für Telearbeitsplätze sollte ein spezielles Betreuungs- und Wartungskonzept erstellt werden, das folgende Punkte vorsieht:

- **Benennen von Ansprechpartnern für den Benutzerservice:** An diese Stelle können sich Mitarbeiter bei Software- und Hardware-Problemen wenden. Der Benutzerservice versucht (auch telefonisch) kurzfristig Hilfe zu leisten beziehungsweise leitet Wartungs- und Reparaturarbeiten ein. Dazu sollte dem Benutzerservice die Konfiguration der Telearbeitsrechner bekannt sein.
- **Wartungstermine:** Die Termine für Wartungsarbeiten an den Telearbeitsgeräten sollten frühzeitig bekannt gegeben werden, damit die Mitarbeiter zu diesen Zeiten den Wartungstechnikern Zutritt zum Telearbeitsplatz oder den Zugriff auf Telearbeitsrechner gewähren oder zu wartende IT-Geräte in die Institution bringen können.
- **Einführung von Standard-Telearbeitsrechnern:** Die IT-Ausstattung aller Mitarbeiter einer Institution sollte standardisiert sein, damit der Benutzerservice schnell bei Problemen helfen kann. Auch wird dadurch der konzeptionelle und administrative Aufwand für den Aufbau eines sicheren Telearbeitsrechners vermindert.
- **Fernwartung:** Falls der Telearbeitsrechner über Fernwartung administriert und gewartet werden kann, sind die notwendigen Sicherheitsmaßnahmen zu klären. Außerdem ist mit den betroffenen Mitarbeitern der Zeitpunkt für einen Online-Zugriff zur Wartung zu vereinbaren. Damit der Fernwartungszugang nicht missbraucht werden kann, müssen angemessene Sicherungsverfahren festgelegt werden.
- **Transport der IT:** Es sollte aus Gründen der Haftung festgelegt werden, wer autorisiert ist, IT-Geräte und andere Ausstattung für die Telearbeitsplätze zwischen der Institution und den Telearbeitsplätzen zu transportieren. Dabei muss auch der Schutz der Geräte beachtet werden. Ein Laptop kann beispielsweise vom Mitarbeiter persönlich transportiert werden, sollte aber mit einer Diebstahlsicherung versehen sein. Die Informationen sollten verschlüsselt sein.

OPS.1.2.4.M10 Durchführung einer Anforderungsanalyse für den Telearbeitsplatz (S)

Bevor ein Telearbeitsplatz eingerichtet wird, sollte eine Anforderungsanalyse durchgeführt werden. Sinn dieser Anforderungsanalyse ist es, alle infrage kommenden Einsatzszenarien zu bestimmen, um daraus die benötigten Hard- und Software-Komponenten abzuleiten. Die Ergebnisse einer solchen Anforderungsanalyse müssen dokumentiert und mit den IT-Verantwortlichen abgestimmt werden.

Im Rahmen dieser Anforderungsanalyse sind unter anderem folgende Fragen zu klären:

- Bis zu welchem Vertraulichkeitsanspruch dürfen Daten am Telearbeitsplatz bearbeitet werden?
- Zu welchem Zweck wird der Zugang zur Institution genutzt (Abfragen von Informationen, Einstellen von Informationen, Programmnutzung)?
- Wie hoch ist der Datenverkehr zwischen dem Telearbeitsplatz und der Institution?

- Muss der Mitarbeiter auf das Intranet der Institution zugreifen? Wenn ja, muss er auf das gesamte Intranet, das heißt auf alle dort verfügbaren Daten und Dienste oder nur auf Teilbereiche des Intranets zugreifen können?
- Ist für die Mitarbeiter die Nutzung des Internets vorgesehen? Wenn ja, bekommt der Mitarbeiter einen eigenen Internet-Zugang oder wird dieser Zugang über das Intranet der Institution realisiert?

Je nach Vertraulichkeit der Daten kann es erforderlich sein, bestimmte Übertragungswege von der Institution zum Telearbeitsplatz festzulegen. Dabei kann es sinnvoll sein, einzelne Übertragungswege auszuschließen oder Mindestanforderungen dafür festzulegen. Beispielsweise könnte es vorgeschrieben sein, Papierdokumente mit vertraulichen Informationen nur auf direktem Weg von der Institution zum Telearbeitsplatz in verschlossenen Transportbehältern zu transportieren. Ebenso könnten für verschiedene Vertraulichkeitsgrade unterschiedliche Verschlüsselungsverfahren für die Datenübertragung vorgesehen sein.

Ähnliche Überlegungen sollten angestellt werden, wenn die im Rahmen der Telearbeit zu verarbeitenden Informationen besonders vor Manipulation geschützt werden müssen.

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 OPS.1.2.4 *Telearbeit* sind keine Quellenverweise vorhanden.