Arbeiten im Homeoffice

Empfehlungen für die Arbeitsplatzgestaltung

www.bitkom.org

bitkom

Herausgeber

Bitkom
Bundesverband Informationswirtschaft,
Telekommunikation und neue Medien e. V.
Albrechtstraße 10 | 10117 Berlin
T 030 27576-0
bitkom@bitkom.org
www.bitkom.org

Ansprechpartner

Marc Danneberg | Bitkom e. V.
T 030 27576-526 | m.danneberg@bitkom.org

Verantwortliches Bitkom-Gremium

FA Produktneutrale Ausschreibungen

Projektleitung

Marc Danneberg | Bitkom e. V.

Titelbild

© green-chameleon – unsplash.com

Inhaltsverzeichnis

Tabellenverzeichnis

Danksagung

Diese Veröffentlichung basiert auf Arbeitsergebnissen des Präventionsfeldes Büro der VBG. Der vorliegende Leitfaden entstammt einer intensiven Zusammenarbeit von Experten der öffentlichen Verwaltung und Vertretern von Mitgliedsunternehmen des Bitkom. Er verdankt seine Existenz der umfangreichen Zuarbeit der Projektgruppe »Produktneutrale Ausschreibung Homeoffice«. Besonderer Dank gilt hierbei:

- Andreas Frisch, DIN-Normenausschuss Bauwesen (NABau)
- Dr. Heiner Genzken, Intel Deutschland GmbH
- Stefan Gniza, VBG – Ihre gesetzliche Unfallversicherung
- Jürgen Graf, Fujitsu Technology Solutions GmbH
- Goran Hauser, Intel Deutschland GmbH
- Dr. Niklas Hellemann, SoSafe GmbH
- Dr. Heidi Koithan, Lexmark Deutschland GmbH
- Jürgen Meß, VBG – Ihre gesetzliche Unfallversicherung
- Florestan Peters, SoSafe GmbH
- Stephan Peters, Qualcomm CDMA Technologies GmbH
- Jens Polster, Konica Minolta Business Solutions Deutschland GmbH
- Christian Richter, VBG – Ihre gesetzliche Unfallversicherung
- Jörg Roskowetz, AMD Advanced Micro Devices GmbH
- Wolfgang Schestak, Fujitsu Client Computing Limited
- Daniel Schiwek, HP Deutschland GmbH
- Axel Simon, Hewlett-Packard GmbH
- Marco Sönksen, Polizei Berlin
- Andreas Stephan, VBG – Ihre gesetzliche Unfallversicherung
- Klaus-Peter Wegge, Siemens AG

1 Einleitung

Dezentrale und hybride Arbeitsformen gewinnen immer stärker an Bedeutung. In der Corona-Krise hat sich für viele Beschäftigte in kürzester Zeit die Arbeitsorganisation grundlegend verändert und flexible Arbeitsplatzmodelle werden auch nach der Pandemie die neue Normalität in der Arbeitswelt prägen. Dieser Leitfaden unterstützt Arbeitgeber und Beschäftigte bei der Ausgestaltung von Homeoffice-Arbeitsplätzen. Dabei werden ergonomische, technische und organisatorische Anforderungen in den Blick genommen.

Ziel des Dokumentes ist es, unterschiedliche Arbeitsplatzsituationen im heimischen Umfeld zu beleuchten und die Wahl der Arbeitsmittel mit Hinweisen und Erläuterungen zur Arbeitsplatzgestaltung zu unterstützen. Dabei werden auch Fragen zur IT-Sicherheit und zur Barrierefreiheit von Homeoffice-Arbeitsplätzen adressiert.

Verwiesen sei an dieser Stelle auch auf weitere Bitkom-Leitfäden für produktneutrale Ausschreibungen u. a. von **↗ Notebooks**, Desktops-PCs, **↗ Thin Clients**, **↗ Drucker und Multifunktionsgeräten** sowie **↗ Monitoren**. Diese Leitfäden geben öffentlichen Auftraggebern eine verlässliche und verständliche Hilfe an die Hand, damit sie ihre Ausschreibungen produktneutral, d. h. ohne Verwendung geschützter Markennamen oder Nennung bestimmter Hersteller und unter Berücksichtigung aktueller technischer Anforderungen formulieren können. Im vorliegenden Homeoffice-Leitfaden werden die unterschiedlichen Produktgruppen mit Blick auf den Einsatz im heimischen Umfeld kurz beschrieben. Finden sich in den Leitfäden für produktneutrale Ausschreibungen vertiefende Informationen zu den technischen Kriterien der einzelnen Produktgruppen, ist dies entsprechend vermerkt.

2 Differenzierung zwischen Telearbeit und mobilem Arbeiten

Mit Blick auf die Anforderungen an einen Arbeitsplatz im heimischen Umfeld ist zwischen Telearbeit und mobilem Arbeiten zu differenzieren.

Zumeist arbeiten Beschäftigte bei der Telearbeit alternierend an einem Bildschirmarbeitsplatz im Betrieb oder an einem Telearbeitsplatz im Privatbereich. Dies kann auch so ausgestaltet sein, dass die Beschäftigten weitestgehend im Homeoffice tätig sind und nur gelegentlich die Betriebsstätte aufsuchen. Bei einem Telearbeitsplatz handelt es sich um einen fest eingerichteten Bildschirmarbeitsplatz im privaten Umfeld des Beschäftigten, der den Regelungen der Arbeitsstättenverordnung unterliegt und für dessen Einrichtung der Arbeitgeber verantwortlich ist. Voraussetzung hierfür ist eine arbeitsvertragliche Regelung oder Vereinbarung zwischen Arbeitgeber und Beschäftigten. Ein Telearbeitsplatz ist idealerweise vergleichbar gestaltet und eingerichtet wie ein Bildschirmarbeitsplatz im Unternehmen.

Beim mobilen Arbeiten wird eine Bildschirmtätigkeit an einem Ort außerhalb der Betriebsstätte ausgeübt, zum Beispiel im Restaurant, im Zug oder im Hotel und kann gelegentlich auch im Privatbereich erfolgen. Grundsätzlich unterliegt mobile Arbeit den Regelungen des Arbeitsschutzgesetzes und des Arbeitszeitgesetzes, die Arbeitsstättenverordnung (ArbStättV) muss bei der Ausstattung des Arbeitsplatzes jedoch nicht berücksichtigt werden.

Homeoffice ist gemäß SARS-CoV-2-Arbeitsschutzregel eine besondere Form des mobilen Arbeitens, die es Beschäftigten ermöglicht, nach vorheriger Abstimmung mit dem Arbeitgeber zeitweilig im Privatbereich tätig zu sein.[1]

Im Sinne dieses Leitfadens umfasst der Begriff Homeoffice sowohl das mobile Arbeiten im Privatbereich als auch dauerhaft eingerichtete Telearbeitsplätze. Die nachfolgenden Empfehlungen gelten für mobiles Arbeiten (funktionale Ausstattung) und Telearbeitsplätze (optimale Ausstattung) im Homeoffice. Unter Beachtung von bestimmten Voraussetzungen können Arbeitsplätze mit funktionaler Ausstattung auch als Telearbeitsplätze genutzt werden (siehe Kapitel 3.1.1).

---

1 Die SARS-CoV-2-Arbeitsschutzregel konkretisiert für den gemäß § 5 Infektionsschutzgesetz festgestellten Zeitraum der epidemischen Lage von nationaler Tragweite die Anforderungen an den Arbeitsschutz in Hinblick auf SARS-CoV-2. Die SARS-CoV-2-Arbeitsschutzregel wird von den beratenden Arbeitsschutzausschüssen beim Bundesministerium für Arbeit und Soziales (BMAS) gemeinsam mit der Bundesanstalt für Arbeitsschutz und Arbeitsmedizin (BAuA) ermittelt bzw. angepasst und vom BMAS im Gemeinsamen Ministerialblatt bekannt gegeben. Weitere Informationen zu den Rechtsgrundlagen sind der Anlage dieser Handreichung zu entnehmen. [↗ **https://www.baua.de/DE/Angebote/Rechtstexte-und-Technische-Regeln/Regelwerk/AR-CoV-2/pdf/AR-CoV-2.pdf?__blob=publicationFile&v=6**] Für vertiefende Informationen zu den Rechtsgrundlagen von Telearbeit und mobilem Arbeiten s. Anlage dieser Handreichung.

3 Anforderungen an Bildschirmarbeitsplätze im heimischen Umfeld

Bei der Ausstattung und Gestaltung des Arbeitsplatzes im heimischen Umfeld sind funktionale und ergonomische Anforderungen zu berücksichtigen. Auch die Häufigkeit der Homeoffice-Nutzung und die konkreten Arbeitsinhalte sind in diesem Zusammenhang von Bedeutung: In der Regel kann bereits mit der Bereitstellung eines mobilen Endgeräts die Kommunikation aufrechterhalten werden. Dies mag ausreichend sein, um ein gelegentliches (auch mal arbeitstägliches) Arbeiten im Homeoffice zu ermöglichen, bei einer regelmäßigen Homeoffice-Nutzung ergeben sich jedoch weitreichendere Anforderungen an die Ausstattung und Gestaltung des Homeoffice-Arbeitsplatzes.

Die nachfolgenden Erläuterungen und Empfehlungen beziehen sich auf Arbeitssituationen, bei denen regelmäßig und für volle Arbeitstage im Homeoffice gearbeitet wird. Dabei wird zwischen einer funktionalen und einer optimalen Ausstattung bzw. Arbeitsplatzgestaltung unterschieden.[2]

	Funktional	Optimal	Typische Anwendungen
Häufigkeit der Homeoffice-Nutzung	bis zu 50 Prozent der Arbeitszeit	ab 50 Prozent der Arbeitszeit	Die hier vorgeschlagenen Anteile sind lediglich als grobe Richtwerte zu verstehen. Darüber hinaus sind die konkreten Arbeitsinhalte für die Ausstattung des Arbeitsplatzes ausschlaggebend. Bei der Entscheidung, ob die funktionale oder die optimale Kategorie als Orientierung für die Arbeitsplatzgestaltung heranzuziehen ist, sind deshalb verschiedene Kriterien und Anforderungen an den Arbeitsplatz in den Blick zu nehmen.
Tätigkeitsschwerpunkte	Mail- und Textbearbeitung, Anfertigung von Berichten und Präsentationen, Teilnahme an Videokonferenzen und Online-Workshops etc.	Mail-, Text- und Bildbearbeitung, Anfertigung von Berichten, Präsentationen und umfassenden Auswertungen, Teilnahme und Leitung von Videokonferenzen und Online-Workshops, regelmäßiger Kontakt mit Kunden und Partnern (z. B. Support, Beratung, Pressearbeit), häufiges Drucken und Scannen (z. B. Vertragsausgestaltung), häufige Nutzung von Fachverfahren und Spezialsoftware (z. B. ERP-Systeme, Dashboards, Grafikprogramme) etc.	Die hier skizzierten Tätigkeitsschwerpunkte sind als Anwendungsbeispiele zu verstehen. Die Aufgaben und deren Anforderungen an die Ausstattung des Homeoffice-Arbeitsplatzes variieren von Fall zu Fall.

2 Zwischen Arbeitgeber und Arbeitnehmer können Vereinbarungen getroffen werden, dass auch bereits bei gelegentlichen Arbeitseinsätzen aus dem heimischen Umfeld grundsätzlich die ArbStättV zu berücksichtigen ist. In diesem Fall gelten die Empfehlungen für Telearbeitsplätze (optimale Ausstattung) unabhängig von der Häufigkeit der Arbeit aus dem heimischen Umfeld.

	Funktional	Optimal	Typische Anwendungen
Telearbeit	Unter bestimmten Voraussetzungen für Telearbeit im Sinne der Arbeitsstättenverordnung geeignet.	Uneingeschränkt für Telearbeit im Sinne der Arbeitsstättenverordnung geeignet.	

Tabelle 1: Kategorien von Homeoffice-Arbeitsplätzen

3.1 Funktionale Ausstattung

Homeoffice-Arbeitsplätze der funktionalen Kategorie sind grundsätzlich als mobile Arbeitsplätze für ein mehrtägiges Arbeiten im heimischen Umfeld geeignet (Mail- und Textbearbeitung, Anfertigung von Berichten und Präsentationen, Teilnahme an Videokonferenzen und Online-Workshops etc.). Unter bestimmten Voraussetzungen (Verwendung nur eines Bildschirmgeräts, reduzierter Papieraufwand, Vorhandensein eines Bürodrehstuhls, freie Bewegungsfläche von mindestens 1,5 m² am Arbeitsplatz etc.) stellt diese Ausstattung auch einen geeigneten Arbeitsplatz für Telearbeit im Sinne der Arbeitsstättenverordnung dar.

3.2 Optimale Ausstattung

Die optimale Kategorie beschreibt einen eingerichteten Bildschirmarbeitsplatz, der uneingeschränkt für (alternierende) Telearbeit genutzt werden kann. Die Empfehlungen zur Ausstattung und Arbeitsplatzgestaltung eignen sich somit für Arbeitssituationen, bei denen Tätigkeiten sehr häufig oder ausschließlich im heimischen Umfeld ausgeführt werden.

4 Die Wahl der Arbeitsmittel

Die Arbeit aus dem Homeoffice kann neue Freiräume für Flexibilität, Kreativität und die Vereinbarkeit von Beruf, Familie und Freizeit schaffen. Dabei ist jedoch zu berücksichtigen, dass eine Homeoffice-Umgebung durch besondere Anforderungen gekennzeichnet ist, die bei der Wahl der Arbeitsmittel Berücksichtigung finden sollten, u. a. um gesundheitliche Probleme auszuschließen und IT-Sicherheitsrisiken zu minimieren. Eine Homeoffice-Arbeitsplatz kann sich je nach Wohn- und Lebenssituation durch die folgenden Aspekte auszeichnen:

- Berufliche und private Nutzung des Arbeitsplatzes und der Arbeitsmittel
- Eingeschränkte Platzverhältnisse
  (Arbeitsmittel werden regelmäßig auf- und abgebaut / verstaut)
- Umgebungsgeräusche
- Keine Support- und Unterstützungsfunktionen direkt vor Ort

Nachfolgend wird dargestellt, welche Funktionalitäten und Ausstattungsmerkmale bei der Wahl von Arbeitsmitteln für den Einsatz im Homeoffice bedacht werden sollten. Entscheidend ist dabei jedoch immer die konkrete Arbeits- und Lebenssituation.

Verwiesen sei an dieser Stelle auch auf weitere Bitkom-Leitfäden für produktneutrale Ausschreibungen von ↗ Notebooks, ↗ Desktop PCs, ↗ Thin Clients, ↗ Drucker und Multifunktionsgeräten sowie ↗ Monitoren. In diesen Leitfäden sind die verschiedenen Technologien und Anwendungspotenziale im Detail beschrieben. Zudem sind den Leitfäden Empfehlungen zu den technischen Mindestanforderungen und Bewertungskriterien zu entnehmen, die bei der Kaufentscheidung Berücksichtigung finden können.

4.1 Endgeräte

Die Entscheidung welches Endgerät bzw. welche Kombination aus Endgeräten im Homeoffice genutzt werden soll ist im hohen Maße vom Mobilitätsgrad abhängig (Wie häufig wird das Gerät bewegt? Wird das Gerät an verschiedenen Arbeitsplätzen genutzt?). Die Arbeitsorganisation ist somit entscheidend bei der Wahl der Arbeitsmittel.

BYOD-Konzepte stellen bei einer Verstetigung der Homeoffice-Nutzung schon aufgrund von IT-Sicherheitsanforderungen und der Verantwortung der Arbeitgeber gegenüber ihren Beschäftigten keinen Lösungsansatz dar.[3]

3 s. auch Glossar

4.1.1 Smartphone und Tablet

Bereits mit Smartphone oder Tablet kann die elektronische Kommunikation auf Reisen und im Homeoffice grundsätzlich aufrechterhalten werden. Das Schreiben längerer Texte, die ausführliche Beantwortung von E-Mails oder das Bewältigen komplexer Arbeitsaufgaben wird an solchen Geräten schnell mühsam.

Bei der Ausstattung des Homeoffice-Arbeitsplatzes ist ein Notebook bzw. Desktop-PC deshalb nicht zu ersetzen. Smartphones und Tablets können im Homeoffice als unterstützende Geräte zum Einsatz kommen (für Notizen, als zusätzliche Kameras oder Bildschirme, zur Nutzung App-basierter Produktivitätswerkzeuge etc.).

4.1.2 Notebook, 2-in-1-Gerät (Convertible) und Desktop-PC / Monitore

Das Notebook oder der Desktop-PC sind die zentralen Arbeitsmittel bei der Arbeit aus dem Homeoffice. Da Tastatur und Touchpad bei Notebooks fest integriert sind, lässt sich bei längerem Arbeiten der ideale Abstand zum Bildschirm nicht einhalten. Es ist deshalb der Einsatz einer separaten Maus, Tastatur und eines externen Monitors zu empfehlen (für die optimale ebenso wie die funktionale Ausstattung des Homeoffice-Arbeitsplatzes). Der empfohlene Abstand der Augen zum Bildschirm beträgt 50 bis 80 Zentimeter. Ein externer Monitor dient gleichzeitig der optimalen Sehhöhe, bei der sich die Oberkante nicht über der Augenhöhe befinden sollte.

Häufig wird der Notebookbildschirm als zweiter Monitor genutzt. Um die Höhe an den gekoppelten, externen Monitor anzugleichen, kann ein Laptopständer zum Einsatz kommen. Wird ein erhöhter Laptop nicht nur als zweiter Monitor, sondern auch zur Dateneingabe genutzt, dann sind externe Eingabemittel (Tastatur, Maus) aus ergonomischen Gründen besonders wichtig.

Im Homeoffice bietet sich zudem der Einsatz einer Docking-Station bzw. eines Port-Replikators an. Externe Monitore und Eingabemittel sowie sonstiges Zubehör (z. B. Kopfhörer, Headset, Webkamera etc.) müssen dann nicht jedes Mal neu an das Notebook angeschlossen werden. Eine Docking-Station kann herstellerabhängig sein und passt dann nur für die vorgesehenen Notebooks des Herstellers. Mittlerweile sind viele Docking-Stations mit einem USB Type-C Anschluss ausgestattet und können dadurch universell eingesetzt werden. Ein Port-Replikator wird als separates Gerät an einem freien USB-Port angeschlossen. Über ein einzelnes USB-Kabel wird das Signal mehrerer Anschlüsse übermittelt.

4.1.3 Thin Client

Da sich Homeoffice-Endgeräte häufig in sogenannten ungesicherten Netzen befinden, erhöht sich das Gefährdungspotenzial Cyberattacken ausgesetzt zu sein. Thin Clients bieten hier eine gute Lösung, denn durch ihr Betriebskonzept (schreibgeschütztes Betriebssystem und keinerlei lokale Speicherung von Benutzer- oder Applikationsdaten) bieten sie u. U. verbesserten Schutz gegen ungewollten Datenzugriff, verglichen mit klassischen PCs.

Egal ob mobiler Thin Client, d. h. ein Thin Client mit den Eigenschaften eines Notebooks, oder stationärer Thin Client: Für den Betrieb wird eine entsprechende Unternehmensinfrastruktur vorausgesetzt, die für den Zugriff von Thin Clients zwingend erforderlich ist. Näheres dazu findet sich im **↗ Bitkom-Leitfaden für die produktneutrale Ausschreibung von Thin Clients**.

4.2 Technisches Zubehör

Gerade beim Arbeiten im heimischen Umfeld können sich besondere Anforderungen an die Funktionalität und Ergonomie der technischen Geräte ergeben. Beispielsweise kann ein Heimarbeitsplatz dadurch gekennzeichnet sein, dass die Geräte recht häufig bewegt und verstaut werden, insbesondere dann, wenn der Arbeitsplatz in einen Wohnbereich integriert wurde oder abwechselnd von verschiedenen Haushaltsmitgliedern genutzt wird. Zudem ist zu berücksichtigen, dass je nach Wohnsituation Umgebungsgeräusche das konzentrierte Arbeiten stärker beeinträchtigen können als dies in einer Büroumgebung der Fall wäre. Diese Besonderheiten sind insbesondere bei der Ausstattung mit technischem Zubehör zu berücksichtigen.

4.2.1 Eingabegeräte

Wie bereits unter 4.1.2 zu den Notebooks beschrieben, ist grundsätzlich der Einsatz einer separaten Maus und Tastatur zu empfehlen. Diese sind entweder mit einem Anschlusskabel oder schnurlos mit dem Endgerät bzw. einer Docking-Station oder einem Port-Replikator verbunden (Empfänger am USB-Anschluss bzw. Bluetooth). Aufgrund eingeschränkter Platzverhältnisse und Mobilitätserfordernissen kann es empfehlenswert sein auf Kabel möglichst zu verzichten. Speziell bei Tastaturen sollte jedoch berücksichtigt werden, dass Luftschnittstellen ein erhöhtes Sicherheitsrisiko darstellen können, wenn es Dritten gelingt darüber unautorisierte Befehle an den Client zu senden. Dies ist bei der Ausstattungsplanung und im IT-Sicherheitskonzept entsprechend zu berücksichtigen (vgl. hierzu auch Kapitel 7 zur IT-Sicherheit).

4.2.2 Kopfhörer

Kopfhörer können mit dem Smartphone oder dem Computer verbunden werden (kabelgebunden oder schnurlos) und auf Reisen sowie im Homeoffice für Telefonate und Videokonferenzen genutzt werden. Dabei kann zwischen offenen und geschlossenen Systemen unterschieden werden: Offene Kopfhörer lassen Schallwellen in beide Richtungen passieren, d. h. Umgebungsgeräusche bleiben hörbar, der Nutzer fühlt sich nicht komplett von der Außenwelt abgeschottet. Dafür könnten sich Sitznachbarn (im Homeoffice, Büro, Zug etc.) von den nach außen dringenden Geräuschen gestört fühlen. Geschlossene Kopfhörer lassen kaum Geräusche nach außen dringen und dämmen Umgebungsgeräusche.

Unabhängig vom Bauprinzip werden klassische Bügelkopfhörer in ohraufliegende (On-Ear) und ohrumschließende (Over-Ear) Systeme unterschieden, was Auswirkungen auf den Tragekomfort hat, wobei dieser immer individuell zu bewerten ist. Die Polster eines ohraufliegenden Kopfhörers sind so geformt, dass sie direkt und relativ eng auf dem Ohr sitzen, während sich ohrum-

schließende Kopfhörer komplett um die Ohrmuscheln legen. In der Regel sind Over-Ear-Systeme größer und deshalb etwas schwieriger zu transportieren.

Um Umgebungsgeräusche nicht nur mechanisch zu dämpfen, sind Noise-Cancelling-Kopfhörer mit einer aktiven Geräuschunterdrückung ausgestattet. Hierfür lokalisieren Mikrofone den Umgebungsschall und geben ein entsprechendes negatives Signal (Gegenschall) ab. Treffen beide Schallimpulse aufeinander, wird der Außenschall dadurch gedämpft. Der aktiven Geräuschunterdrückung steht der Transparenzmodus gegenüber. Hier werden Außengeräusche effektiver aufgegriffen und an die Ohren weitergegeben. Wichtige Signale und Ansagen können so sehr deutlich wahrgenommen werden.

Übernehmen Beschäftigte häufiger aktive Aufgaben in Videokonferenzen, Onlineseminaren oder Kundengesprächen ist die Ausstattung mit einem Headset zu erwägen, bei dem der Kopfhörer um ein Mikrofon für die Sprachaufnahme erweitert wird. Die Aufnahmequalität kann dadurch in der Regel erheblich verbessert werden.

4.3 Drucker und Multifunktionsgeräte

Im Regelfall wird im Homeoffice ein Drucker oder ein Multifunktionsgerät, das Druckmedien bis DIN A4 verarbeiten kann, eingesetzt. Bei der funktionalen Ausstattung empfehlen wir den Einsatz eines Druckers, da weiterhin am Arbeitsplatz zeitnah die Möglichkeit besteht, notwendige Scan- und Kopiervorgänge zu erledigen. Verbringt der Mitarbeiter allerdings weit mehr als die Hälfte seiner wöchentlichen Arbeitszeit im Homeoffice empfiehlt es sich ein Multifunktionsgerät zur Verfügung zu stellen. Ob bei der funktionalen Ausstattung im Einzelfall dann doch schon auf ein Multifunktionsgerät zurückgegriffen wird, hängt von der Tätigkeit des jeweiligen Mitarbeiters ab. Wird im Homeoffice ein Drucker oder Multifunktionsgerät genutzt, muss dabei die Datensicherheit gewährleistet sein. Vor diesem Hintergrund kann es erforderlich sein, ergänzend einen Aktenvernichter und einen abschließbaren Schrank zu verwenden. Generell sollten zum Umgang mit Druckern, Multifunktionsgeräten und Dokumenten auch im Homeoffice der IT-Grundschutz-Baustein »SYS.4.1 Drucker, Kopierer und Multifunktionssysteme« beachtet und die notwendigen Schutzmaßnahmen ergriffen werden.

Des Weiteren ist bei Druckern und Multifunktionsgeräten zu beachten, dass Prozesse zur Bestellung bzw. Beschaffung von Verbrauchsmaterialien (z. B. Toner oder Tinte, Bildeinheit, Papier) etabliert werden müssen. Dabei ist auch wichtig zu beachten, ob der Drucker oder das Multifunktionsgerät in Lösungen für das gesamte Outputmanagement eingebunden werden soll.[4]
Dies hat große Auswirkungen auf die Systemauswahl. Viele Anbieter bieten Kundenportale an, womit der Mitarbeiter sein Gerät selbst managen kann und beispielsweise auch Verbrauchsmaterialien bestellen kann.

4 s. auch Glossar

Der Drucker oder das Multifunktionsgerät für das Home-Office sollte WLAN-fähig sein, um den Mitarbeitern einen flexiblen Aufstellungsort zu ermöglichen. Hier ist der BSI-Baustein NET.2.2 WLAN-Nutzung zu beachten.

4.4 LAN & WLAN-Infrastruktur für sicheres Arbeiten

Die Art und Weise, wie wir arbeiten, hat sich im letzten Jahrzehnt dramatisch verändert. Die Teams sind jetzt verteilt und gerade durch die Pandemie nicht mehr zwangsläufig am Arbeitsplatz im Büro. Die Möglichkeit, sich von zu Hause oder außerhalb des bisherigen Arbeitsplatzes zu verbinden, mit anderen Teammitgliedern zusammenzuarbeiten und auf die Werkzeuge und Daten zuzugreifen, die für ihre Arbeit erforderlich sind, ist für jede Organisation von entscheidender Bedeutung. Die Gewährleistung dieser Konnektivität und Zusammenarbeit auf sichere und konforme Weise ist ein zentrales Anliegen, da viele Unternehmen und öffentliche Organisationen eine zunehmend dezentralisierte und verteilte Belegschaft unterstützen müssen.

WICHTIGE ÜBERLEGUNGEN

Sichere Remote-Konnektivität – Geschwindigkeit, Einfachheit und Sicherheit sind für die Unterstützung einer ständig wachsenden Remote-Belegschaft, d. h. einer steigenden Anzahl von Beschäftigten, die aus dem Homeoffice arbeiten, von größter Bedeutung. Sicherheits- und Compliance-Überlegungen müssen maximalen Schutz und Risikominderung bieten, ohne die Erwartungen an Service Level und Verfügbarkeit zu beeinträchtigen. Da in diesen Fällen die Netzwerkzugänge in der Regel über den privaten oder einen öffentlichen Internetzugang erfolgen, ist der Zugang auf der Ebene des Netzwerkes nicht kontrollierbar. Um dennoch einen hohen Sicherheitsstandard auch aus der Ferne zu ermöglichen (analog zu den vor-Ort Netzen beim Arbeitgeber), ist es notwendig, die Verbindung zu verschlüsseln und den Netzwerkzugang, d. h. die individuellen Berechtigungen, mit der Rolle des Benutzers zu verknüpfen. Das heißt ganz konkret, dass die Netzwerkzugriffskontrolle und Segmentierung mindestens auf der Rolle des Benutzers und dem Verbindungsort basieren muss.

Bei einer wachsenden, dezentralen Belegschaft kann die Bereitstellung von Konnektivität eine Herausforderung sein. Um mit sich ständig ändernden externen Faktoren sowie Geschäftstreibern umgehen zu können, muss eine große Anzahl von Benutzern online geschaltet werden, ohne die Netzwerkinfrastruktur oder die Abläufe zu beeinträchtigen. Funktionen wie automatische Provisionierung bieten eine einfache Einrichtung, Konfiguration und Verwaltung des Netzwerks ohne IT-Unterstützung vor Ort, um das Onboarding neuer Remotebenutzer zu vereinfachen. Die VPN-Konnektivität kann auf Benutzer erweitert werden, die VPN-Clients oder Remote Access Points verwenden, die dann eine VPN Verbindung zu einem physikalischen Gateway oder virtuellen Gateway herstellen.

Nahtlose Benutzererfahrung – Remotebenutzer benötigen Zugriff auf alle Anwendungen, Daten und Ressourcen, an die sie sich gewöhnt haben bzw. für ihre Arbeit benötigen. Dies bedeutet, dass ihre Erfahrung aus der Ferne mit ihrer Erfahrung identisch sein sollte, wenn sie physisch im

Büro sind. Optimal dafür sind Remote Access Points (RAP) für den Einsatz am Telearbeitsplatz oder im Homeoffice geeignet. Eine fast ähnliche Funktion bieten VPN Clients auf dem Endgerät und erlauben damit auch eine Nutzung überall dort, wo ein ungeschützter Internetzugang besteht.

Zusammengefasst bedeutet dies, dass bei der Bereitstellung eines sicheren und leistungsstarken Internetzugangs weitere spezifische Lösungen zum Einsatz kommen (Remote Access Points, VPN Client, Controller und Gateways, Policy Manager, Policy Enforcement Firewall). Vertiefende Informationen und Erläuterungen zu diesen Technologien sind dem Glossar zu entnehmen.

5 Empfehlungen für die Ausstattung von Arbeitsplätzen im heimischen Umfeld

Nachfolgend werden Empfehlungen für die Arbeitsplatzgestaltung im Homeoffice skizziert. Dabei wird zwischen einer funktionalen und einer optimalen Ausstattung differenziert (vgl. Kapitel 3 »Anforderungen an Bildschirmarbeitsplätze im heimischen Umfeld«).

5.1 Arbeitsplatz

Ausstattung[5]	Funktional	Optimal	Bemerkungen / Erläuterungen
Arbeitsfläche des Schreibtisches	120 x 80 cm	160 x 80 cm	
	nicht höhenverstellbar Höhe 740 ± 20 mm	höhenverstellbar	Ausgehend vom eingestellten Stuhl (siehe unten), ist die Tischhöhe so einzustellen, dass bei Aufliegen der Unterarme auf der Tischplatte diese mit den Oberarmen einen rechten Winkel bilden. Kann der Arbeitstisch nicht in der Höhe eingestellt werden: Sitzposition für Oberkörper wie oben, dann prüfen ob Beinposition wie bei Stuhl passt, ggf. Fußstütze oder höherer Tisch.
Beinraumbreite	mindestens 85 cm	mindestens 85 cm empfohlen 120 cm	
Beinraumtiefe	mindestens 80 cm	mindestens 80 cm	
Arbeitsstuhl	Konferenz- oder Bürodrehstuhl	Bürodrehstuhl mit entsprechenden Rollen	Sitzhöhe ist möglichst anzupassen – Füße stehen am Boden, Ober- und Unterschenkel bilden einen Winkel von etwas mehr als 90°. Stehen die Füße nicht am Boden, hilft eine Fußstütze.
Freie Bewegungsfläche am mobilen Arbeitsplatz	120 x 80 cm	160 x 100 cm	Die Bewegungsfläche ist wichtig, damit am Arbeitsplatz unterschiedliche Körperhaltungen eingenommen werden können, Bewegung beim Sitzen möglich ist (dynamisches Sitzen) und auch mal zwischen Sitzen und Stehen gewechselt werden kann. Stolperfallen sind zu beseitigen.

Tabelle 2: Funktionale und optimale Ausstattung von Arbeitsplätzen

5 Zwischen Arbeitgeber und Arbeitnehmer können Vereinbarungen getroffen werden, dass auch bereits bei gelegentlichen Arbeitseinsätzen aus dem heimischen Umfeld grundsätzlich die ArbStättV zu berücksichtigen ist. In diesem Fall gelten die Empfehlungen für Telearbeitsplätze (optimale Ausstattung) unabhängig von der Häufigkeit der Arbeit aus dem heimischen Umfeld.

5.2 Technische Ausstattung

Bezüglich der Mindest- und Bewertungskriterien, die bei der Beschaffung von **↗ Notebooks**, **↗ Desktops-PCs**, **↗ Thin Clients**, **↗ Multifunktionsgeräten** und **↗ Monitoren** Berücksichtigung finden können sei an dieser Stelle auf die Bitkom-Leitfäden für produktneutrale Ausschreibungen verwiesen.[6] Bei den technischen Geräten ist in der Regel keine Unterscheidung zwischen funktionaler und optimaler Ausstattung erforderlich. Dort wo bei einer optimalen Ausstattung zusätzliche Merkmale in Erwägung gezogen werden können (z. B. Möglichkeit zum Anschluss eines zweiten, externen Monitors), ist dies nachfolgend dargestellt. Dies betrifft die Bereiche Notebooks sowie Drucker und Multifunktionsgeräte.

Ausstattung	Funktional	Optimal	Bemerkungen / Erläuterungen
Notebooks			
Displayauflösung	1.366 x 768 Pixel (HD)	1.920 x 1.080 Pixel (Full HD und höher)	Höhere Werte sind auf dem Markt verfügbar. In aller Regel verkleinern sich mit höheren Auflösungen die Bildschirmdarstellungen. Anpassungen der Schrift und Symbolgrößen sind ggf. im Betriebssystem möglich.
Bildschirmdiagonale	ab 12.5"	13" – 17"	Größe, Form und Gewicht müssen der Arbeitsaufgabe entsprechend angemessen sein. Wird nur ein Laptop genutzt sind mind. 15“ zu empfehlen. Wenn ergänzend mindestens ein externer Bildschirm genutzt wird, kann das Display des Laptops auch kleiner sein.
Entspiegelung	Reflexionsarm (non-glare)	Reflexionsarm (non-glare)	
Prozessortyp (CPU)	Multi-Core	Multi-Core	
Arbeitsspeicher (RAM)	Mindestens 8GB	Mindestens 8GB	
Massenspeicher	Mindestens 128GB SSD	Mindestens 200GB	
Ethernet	RJ45 Ethernet 10/100/1000 Mbit, mit Adapter erfüllbar	RJ45 Ethernet 10/100/1000 Mbit, mit Adapter erfüllbar	Insbesondere bei kleinen und flachen Notebooks ist oft bauartbedingt keine RJ-45 Schnittstelle vorhanden, entsprechende Adapter sind im Markt erhältlich.
WLAN	WLAN gemäß IEEE 802.11ac	WLAN gemäß IEEE 802.11ax (WiFi 6)	
	(WiFi 5) (Dual Band 2.4 und 5 GHz)	(Dual Band 2.4 und 5 GHz)	
Bluetooth	BT 5.0	BT 5.0	

6 **↗ Leitfäden | ITK-Beschaffung (itk-beschaffung.de)** oder **↗ https://www.itk-beschaffung.de/Leitfäden**

Ausstattung	Funktional	Optimal	Bemerkungen / Erläuterungen
WWAN	4G LTE (integriert), Datenübertragungsrate ≥100 Mbit/s für Download und ≥ 50 Mbit/s für Upload	4G LTE (integriert), Datenübertragungsrate ≥100 Mbit/s für Download und ≥ 50 Mbit/s für Upload	Höhere Datenübertragungsraten (z. B. 5G) sind auf dem Markt verfügbar.
USB	2 × USB 3.x (davon mind. 1 x Typ A oder Adapterlösung zur Bereitstellung von Typ A)	2 × USB 3.x (davon mind. 1 x Typ A oder Adapterlösung zur Bereitstellung von Typ A)	Wenn eine der USB Typ C Schnittstellen auch zum Laden des Notebooks verwendet wird, ist diese während des Ladevorgangs belegt und kann nicht zum Anschluss weiterer Peripherie genutzt werden. Adapter zur Erhöhung der Anzahl der USB-Anschlüsse sind im Markt erhältlich.
Displayausgang	1 Digitalanschluss für Bildschirme	1 Digitalanschluss für Bildschirme	Der genaue Typ sollte spezifiziert werden (z. B. HDMI, Mini HDMI, USB-C, DisplayPort, Mini DisplayPort)
Audio	Audio-In & Audio-Out	Audio-In & Audio-Out	Ein- und Ausgang werden bei vielen Geräten durch eine Kombi-Schnittstelle bereitgestellt
Tastatur	deutsches Tastatur Layout	deutsches Tastatur Layout, Tastatur mit Hintergrundbeleuchtung	Tragbare Bildschirmgeräte ohne Trennung zwischen Bildschirm und externem Eingabemittel (insbesondere Geräte ohne Tastatur) dürfen nur an Arbeitsplätzen betrieben werden, an denen die Geräte nur kurzzeitig verwendet werden oder an denen die Arbeitsaufgaben mit keinen anderen Bildschirmgeräten ausgeführt werden können. Tragbare Bildschirmgeräte mit alternativen Eingabemitteln sind den Arbeitsaufgaben angemessen und mit dem Ziel einer optimalen Entlastung der Beschäftigten zu betreiben.
Frontkamera	Auflösung HD 720p HD	Auflösung HD 720p und Hybrid Infrared (IR)	
Lautsprecher	Stereo	Stereo (front-facing)	
Mikrofon	Mono	Mono	
Touchpad	Zwei-Tasten-Funktion	Zwei-Tasten-Funktion	
Betriebssystem	z. B. Windows, ChromeOS, MacOS, Linux	z. B. Windows, ChromeOS, MacOS, Linux	
Grafikeinheit	Integriert in CPU DirectX 12-fähig	Integriert in CPU DirectX 12-fähig Support von zwei externen Displays	

Ausstattung	Funktional	Optimal	Bemerkungen / Erläuterungen
Drucker und Multifunktions-geräte	Drucker	Multifunktionsgerät	Ob ein Drucker oder ein Multifunktionsgerät nur in Schwarz/Weiß oder auch in Farbe drucken können muss, hängt von der Art der Tätigkeit und von der Häufigkeit und Vielfalt der Nutzung ab. Weitere Ausführungen zu den einzelnen Anforderungen und weitere Kriterien entnehmen Sie bitte den Leitfaden »Multifunktionsgeräte produktneutral ausschreiben«
Max. Format	DIN A4	DIN A4	
Arbeitsspeicher	256 MB	256 MB	
Papierausgabeka-pazität (Richtwerte)	100 Blatt	125 Blatt	
Scannen	-	600 x 600 dpi s/w Mind. 300 x 300 dpi Farbe	
Dokumen-tenechtheit	PTS-Zertifikat	PTS-Zertifikat	
USB für Client	Mind. USB 2.0	Mind. USB 2.0	
Netzwerkan-schluss	RJ 45 Ethernet 10/100	RJ 45 Ethernet 10/100	
Funkverbindung	WLAN-Infrastruk-tur (nach IEEE 802.11x)	WLAN-Infrastruktur (nach IEEE 802.11x)	
Druckgeschwin-digkeit	Mind. 20 ipm bei DIN A4 Gemäß ISO/IEC 24734	Mind. 20 ipm bei DIN A4 Gemäß ISO/IEC 24734	
Zertifizierungen	GS Zeichen Blauer Engel	GS Zeichen Blauer Engel	

Tabelle 3: Kriterien zur technischen Ausstattung

5.3 Externe Hardware für audiovisuelle Kommunikation

Ein essenzieller Faktor für die Kommunikation im Homoffice ist eine optimale Audio- und Videoqualität, diese kann durch den Einsatz externer Geräte unterstützt werden.

Ausstattung	Funktional	Optimal	Bemerkungen / Erläuterungen
Externes Headset			
Anschluss	kabelgebunden	Bluetooth	
Tragekomfort	Einfacher Tragekomfort	Individueller Tragekomfort	Individuelle Präferenzen: Stereo/ Mono, Kopfbefestigung (In-Ear, Over-Ear, Kopfbügel, Nackenbügel)
Lautstärkeregelung und mute	Per Software	Per Hardwareschalter am Headset	
Positionierung Mikrofon	Flexible Halterung	Zusätzlich Atem- und Spuckschutz	
Tonqualität	300-15000 hZ	Zusätzlich zuschaltbare Noise Cancellation	
Externes Mikrofon			
Tonqualität	300-15000 hZ Mono	Zusätzlich zuschaltbare Noise Cancellation Stereo	
Richtwirkung	Kugel	Niere	
Anschluss	kabelgebunden	Bluetooth	
Empfindlichkeit und mute	Per Software	Per Hardwareschalter am Headset	
Positionierung Mikrofon	Flexible Halterung	Zusätzlich Atem- und Spuckschutz	Entkopplung vom Körperschall, z. B. des PCs
Externe Freisprecheinrichtung			
Anschluss	kabelgebunden	Bluetooth	
Lautstärkeempfindlichkeit und mute	Per Software	Per Hardwareschalter am Gerät	Touch-Bedienung ist nicht barrierefrei
Audioqualität	Maximale Echoentkopplung	Zusätzlich Eliminierung von Störgeräuschen im eingehendem Audiosignal	
Mikrofonempfindlichkeit	Einzelnes Richtmikrofon	Mikrofonarray mit automatischer Sprechrichtungserkennung (bei mehreren Teilnehmern)	

Tabelle 4: Kriterien zur externen Hardware für audiovisuelle Kommunikation

6 Technische Unterstützung bei der Arbeit aus dem Homeoffice

Insbesondere dann, wenn technische Probleme im Homeoffice auftreten, ist es besonders wichtig, dass zuvor ein Support-Prozess definiert wurde und dieser den Mitarbeitern auch bekannt ist (z. B. Formalisierung in einem Benutzerhandbuch oder einer Support-Prozesslandkarte). Der Zugang zur technischen Unterstützung sollte dabei möglichst niedrigschwellig und transparent sein. Hierfür sind Ticketsysteme zu empfehlen, bei denen über verschiedene Kanäle Support-Prozesse angestoßen werden können (Webzugang, Mail, Hotline). Zudem sollte in der Organisation geregelt sein, wie im Schadensfall ein kurzfristiger Gerätetausch realisiert werden kann (z. B. Abholung).

Das Leistungsportfolio eines Anbieters muss nicht auf die Lieferung von Hardware und Software beschränkt sein, sondern kann auch weitere, mit dem Liefergegenstand in Zusammenhang stehende Leistungen umfassen, die auch aus dem Homeoffice abgerufen werden können.

Support / Helpdesk:

Denkbar wäre z. B. auf der Grundlage eines separaten Service-Vertrages oder über eine Garantieverlängerung die gelieferte Hardware und die ggf. mitgelieferte Software zu warten und auf aktuellem Stand zu halten. In diesem Zusammenhang ist zu klären, ob im Schadensfall die Zusendung der Geräte per Post erfolgen kann. Des Weiteren können zusätzliche Service-Dienstleistungen wie Störungsbeseitigung oder Hotline-Dienste bei allgemeinen technischen Fragen vereinbart werden.

Bei Notwendigkeit sollte der entsprechende Support mit der Spezifikation der Reaktionszeiten / Instandsetzungszeiten vereinbart werden.

Marktübliche Angebote unterscheiden sich nach:

- Dauer des Vertrages
- Reaktionszeiten (Zeit zwischen Störungsmeldung und erster Reaktion des Supports)
- Wiederherstellungszeit (Zeit zwischen Störungsmeldung und Wiederherstellung der Betriebsbereitschaft des Systems)
- Ersatzteillogistik
- Zusätzlich angebotenen technischen Dienstleistungen

Endgerätemanagement:

Bei der Inbetriebnahme neuer Geräte fallen in der Regel nicht zu unterschätzende Aufwände an. Ein Endgerätemanagementsystem (Device Management) kann hier unterstützen. Dabei ist zu klären, ob das Device Management durch die IT-Abteilung des Unternehmens oder durch einen externen Dienstleister zu betreiben ist.

7 IT-Sicherheit

Die IT-Sicherheit im Homeoffice hängt insbesondere von zwei Faktoren ab: Der Technik und dem Menschen. Dies trifft zwar auch auf die Arbeit in der Büroumgebung zu, aber im Homeoffice ist es aus Sicht vieler Organisationen wesentlich schwieriger, das regelkonforme Verhalten der Beschäftigten gewährleisten zu können. Durch den Umstieg auf mobile Arbeitsmodelle kommt den Beschäftigten also eine höhere Eigenverantwortung zu. Ein grober Überblick über einige potenzielle Cyber-Angriffstaktiken sowie typische Schwachstellen in IT-Sicherheitsinfrastrukturen, die beim mobilen Arbeiten besonders häufig zu beobachten sind:

- **Unzureichend geschützte Endpoints:** Viele Organisationen managen die Endgeräte im Homeoffice nicht aktiv, weil der direkte Zugriff auf die Geräte durch das Remote-Work-Setting erschwert ist. Organisationen verpassen es in diesen Fällen oftmals, regelmäßig Updates aufzuspielen oder Antiviren-Software flächendeckend zu kontrollieren. Ein solches fehlendes Mobile Device Management (MDM) und Patch Management führt zu Sicherheitslücken, die Cyberkriminelle gezielt für Angriffe ausnutzen.

- **IT-Infrastruktur:** Übertragen Beschäftigte arbeitsbezogene Daten vermehrt von heimischen oder öffentlichen Netzen über die geschützte Infrastruktur von Unternehmen, ergeben sich ganz besondere Herausforderungen. Private Zugangspunkte sind oft weniger gut abgesichert und übertragen die Daten teilweise ohne Verschlüsselung. Direkte Angriffe auf unzureichend gesicherte Router und WLAN-Netzwerke stellen für Hacker eine sehr einfache Möglichkeit dar, sensible Daten abzugreifen.

- **Organisatorische Risiken:** Die Mehrzahl der Cyberangriffe auf Organisationen nutzt Beschäftigte als Einfallstor. Hierzu gehören beispielsweise Phishing-Kampagnen, welche die Empfängerinnen und Empfänger manipulieren und zu gefährlichen Handlungen bewegen sollen. Während sich die Beschäftigten in den Räumlichkeiten ihres Arbeitgebers über mögliche Angriffe austauschen und auf diese Weise schützen können, sind sie im Homeoffice oftmals auf sich allein gestellt – was dazu führt, dass die Angriffe seltener erkannt und damit erfolgreicher werden.

- **Neue Tools und »Credential Theft«:** Im Homeoffice gewinnen digitale Kollaborationstools weiter an Bedeutung. Chat-Nachrichten, Telefonate und Videokonferenzen ersetzen die Meetings vor Ort und ermöglichen eine kontinuierliche Kommunikation, auch über Teams hinweg. Auf gerade diese Tools, die beim mobilen Arbeiten verstärkt in Einsatz kommen, fokussieren sich Cyberkriminelle bei sogenannten Credential-Theft-Angriffen, die das Abfischen von Anmeldedaten zum Ziel haben. Haben sich die Angreifenden erst einmal Zugang zu den Systemen verschafft, können sie nicht nur sensible Daten einsehen. Darüber hinaus haben sie es oftmals auf die Manipulation weiterer Beschäftigten abgesehen. Unter gestohlener Identität versenden sie Nachrichten unter falschem Namen und können vermeintliche Kolleginnen und Kollegen zu schadhaften Handlungen anstiften.

Um auf das Risiko zu reagieren, sollten Organisationen konkrete Maßnahmen bezogen auf die bereits genannten Faktoren »Technik« und »Mensch« umsetzen. Im Bereich der Technik geht es darum, die Übertragung, Verarbeitung und Speicherung von Daten und Informationen in ähn-

licher Weise abzusichern, wie dies im Kontext des Büros und der geschützten Unternehmensinfrastruktur der Fall ist (vgl. Kapitel 7.1 und 7.2).

Daneben sollten Arbeitgeber ihren Beschäftigten aber auch klare Richtlinien und Regeln zum Schutz von Daten und Geräten an die Hand geben. Der Umstieg auf mobile Arbeitsmodelle sollte daher durch entsprechende Schulungs- und Trainingsmaßnahmen begleitet werden, durch welche die Beschäftigten lernen, wie sie die beschriebenen Risiken minimieren können. Detaillierte Empfehlungen zur Stärkung der Cyber Security Awareness sowie zu weiteren Maßnahmen sind dem Kapitel »IT-Sicherheit im Homeoffice und bei mobiler Arbeit« des Bitkom Leitfadens **↗»Mobiles und hybrides Arbeiten. Arbeiten in und nach der Corona-Pandemie«** zu entnehmen.

7.1 Endgeräte Sicherheit

Mobile Endgeräte können Ziel von Cyberangriffen, Datenraub und Datenmissbrauch werden. Die Geräte sind v. a. dann einem erhöhten Gefährdungspotenzial ausgesetzt, wenn sie nicht nur im heimischen Umfeld, sondern auch mobil eingesetzt werden. Solche Angriffe gefährden die Vertraulichkeit, die Verfügbarkeit als auch die Integrität der mit den Geräten verarbeiteten und gespeicherten Daten genauso wie die Funktionsfähigkeit der Geräte selbst. Moderne Endgeräte können ab Werk mit integrierten Sicherheitsfunktionen ausgestattet werden, welche bei der Einhaltung der Sicherheitsvorgaben unterstützen können. Datenschutz und Datensicherheit lassen sich letztlich nur durch eine Kombination aus organisatorischen Maßnahmen, Sorgfaltspflichten des Gerätenutzers und geräteimmanenten Sicherheitsfunktionen herstellen.

Nr.	Kriterium	Anforderungen	Bemerkungen / Erläuterungen
1	**Mechanischer Diebstahlschutz**	▪ Vorrichtung zur Aufnahme einer mechanischen ▪ Diebstahlsicherung im inneren Notebook- Rahmen verankert	Passende Schlösser usw. müssen als Zubehör separat beschafft werden. Kann Einfluss auf die Bauform/Dicke/ Abmessungen des Geräts haben. Zusätzliche Verriegelungsmöglichkeiten siehe Docking-Funktionalität.
2	**Out-of-Band Management**	Sofern vorhanden, in Firmware deaktiviert ausgeliefert; nur mit Firmware Passwort aktivierbar	Fernwartungsfunktionen, die unabhängig vom Betriebssystem die Firmware und/ oder Daten verändern können, müssen, sofern vorhanden, deaktiviert ausgeliefert werden. Eine Aktivierung der Funktionen darf geschützt nur mit Firmware Passwort möglich sein. Im deaktivierten Zustand dürfen durch die Funktionen weder Netzwerkverbindungen aufgebaut noch angenommen werden.
3	**BIOS/UEFI/ coreboot Manipulationssicherheit**	Erkennen von und Schutz vor Manipulationen, zuverlässige Benachrichtigung des Eigentümers oder Nutzers.	Die Systeme müssen über Mechanismen verfügen, die Manipulationen der Firmware verhindern (z. B. durch Schreibschutz) oder Manipulationen erkennen (z. B. durch eine Signaturüberprüfung) und dem Fall den Eigentümer oder Nutzer zuverlässig benachrichtigen.
4	**Verschlüsselung**	Hardwarebasierte Laufwerksverschlüsselung	Integrierte Hard- und Firmware sorgen für eine automatisierte Verschlüsselung der Daten (z. B. OPAL). Es ist keine Unterstützung durch das Betriebssystem oder gesonderte Installation von Software erforderlich.
5	**Schnittstellenschutz**	Schnittstellen im BIOS/ UEFI/coreboot deaktivier- bar	z. B. Ethernet, USB, WLAN, WWAN, Bluetooth, Kamera, Mikrofon, Fingerprint Sensor usw.

Nr.	Kriterium	Anforderungen	Bemerkungen / Erläuterungen
6	**Authentifizierung des Nutzers**	Möglichkeiten der Multifaktor-Authentifizierung	z. B. Smartcard, Fingerprint, sonstige Biometrie-Merkmale, usw.
7	**Webcam-Abdeckung**	Integrierte oder nachträgliche physische Webcam-Abdeckung	
8	**Blickschutz**	Blickschutzfilter (integriert oder als Zubehörlösung)	Lösung Systemhersteller abhängig.

Tabelle 5: Kriterien und Anforderungen zur Sicherheit

7.2 Infrastruktursicherheit (Security und Datenschutz)

Nachfolgende Sicherheitsfunktionalitäten und Konfigurationsmöglichkeiten sollten je nach konkreter Ausgestaltung der Netzwerkanbindung des Homeoffice-Arbeitsplatzes bewertet werden.

VPN

Zur sicheren Anbindung über das Internet sollten die Geräte die VPN-Verschlüsselungstechnologie unterstützen. Die bei vielen Endgeräten und Gegenstellen verbreitete und hochsichere Technologie IPSec-VPN (nach dem aktuellen Standard IKEv2) ermöglicht die komfortable und flexible Anbindung externer Netzwerk-User oder ganzer Standorte und Dienstleister.

Anti Spam, Anti Virus

Anti Spam und Anti Virus Anwendungen unterstützen neben Security Awareness Maßnahmen die E-Mail Sicherheit. Dadurch wird sowohl die genutzte Infrastruktur langfristig geschützt, als auch die kurzfristige Arbeitsfähigkeit sichergestellt. Hierbei basieren moderne Lösungen auf einem zweistufigen Ansatz und prüfen möglicherweise gefährliche Dateien zunächst lokal (beispielsweise auf einer Firewall) und im zweiten Schritt via Sandboxing in der Cloud. Beim Sandboxing wird eine verdächtige Datei präventiv in einer abgeschotteten Umgebung ausgeführt, um mögliche Angriffe zu bewerten. Unter anderem durch Machine Learning wird die Aktualität der einzelnen Sicherheitsmechanismen gewährleistet.[7]

Zero Trust Security, Anti Malware, Intrusion Detection/Prevention, künstliche Intelligenz

Insbesondere durch die Vielfalt der Endgeräte und die steigende Zahl von Geräten des Internets der Dinge entstehen neue Angriffsvektoren. Das ist besonders kritisch, da derartige Endgeräte, sobald diese sicherheitskonform in eine Netzwerkinfrastruktur eingebunden und zugelassen

7 Weitere Erläuterungen im Glossar.

sind auf unterschiedliche Art und Weise kompromittiert werden können. Beispielsweise, um die vorhandenen Zugriffsprivilegien zu nutzen, um Daten auszulesen und an Angreifer zu übermitteln oder um Schäden oder Störungen zu erzeugen. Derart komplexere Cyberangriffe lassen sich durch die Verhaltensanalyseanalyse von Endgeräten erkennen, indem Abweichungen vom bisherigen Verhalten analysiert werden. In Form von typischen Angriffsmustern können mit einem Intrusion Detection und Prevention System bekannte Angriffe erkannt und vereitelt werden. Es ist jedoch wichtig, in der Lage zu sein, bisher unbekannte Angriffe zu erkennen, einzudämmen und zu verhindern. Derartige Systeme basieren auf künstlicher Intelligenz und helfen bei Verhaltensänderungen solche neuen Angriffe zu erkennen und abzuwehren, etwa wenn Daten an bisher nicht vorhandene Ziele übermittelt werden oder sich das Datenübertragungsmuster ändert. Diese Mechanismen sind mit der Plattform für eine rollenbasierte Netzzugangskontrolle zu kombinieren, um kompromittierte Geräte vom Netzzugang auszuschließen oder zumindest in Quarantäne zu schicken.

Rollenbasierter Netzzugang setzt einen Richtlinien-Manager voraus, um eine rollenbasierte Zugriffskontrolle und deren Durchsetzung für alle erkannten und profilierten Geräte anzuwenden. Dafür werden Echtzeitrichtlinien eingerichtet, die festlegen wie Benutzer und Geräte verbunden werden und worauf sie zugreifen können. Herkömmliche Firewalls, die IP-basierte VLANs zur Steuerung nutzen und erst aktiv werden, nachdem ein Benutzer oder ein Gerät in das Netzwerk aufgenommen wurde, bieten eine Möglichkeit für erweiterte Angriffe. Stattdessen deckt eine Benutzer- und Anwendungs-Firewall diese Sicherheitsanfälligkeit ab, indem Identität, Verkehrsattribute und andere Sicherheitskontexte verwendet werden, um die Zugriffsrechte zum Zeitpunkt der ersten Verbindung zentral zu steuern. Das Füllen dieser Lücke ist wichtig, denn in jeder Sekunde, in der ein Angreifer mit dem Netzwerk verbunden ist, können grundsätzlich tausende von Malware-Pakete freigesetzt werden.

Wireless Intrusion Detection System

Eine Netzwerkinfrastruktur kann auchhardwarebasierten Attacken ausgesetzt sein. Dies gilt insbesondere für WLAN-Netze, da sich Funksignale leicht auch über größere Distanzen verbreiten können und es im Gegensatz zum kabelgebundenen Netz keine klare Abgrenzung des Netzes zur Außenwelt gibt. Störquellen können daher das Funknetz beeinflussen. Störquellen können dabei schon ganz einfach andere Geräte wie Mikrowellen sein, die bei Betrieb Interferenzen auf den gleichen Funkfrequenzen wie WLAN erzeugen. Es kann sich aber auch um Angreifer handeln, die ein WLAN-Netzwerk gezielt lahmlegen oder ein WLAN-Netzwerk imitieren, um Daten der Endgeräte abzugreifen.

Daher ist es sinnvoll, bei der Auswahl einer WLAN-Lösung auch darauf zu achten, dass diese solche Störquellen erkennen, lokalisieren und bestenfalls meiden kann. Die Funktionen zur Erkennung böswilliger Angreifer fallen in den Bereich des Wireless Intrusion Detection and Prevention. Neben der Erkennung von Störquellen können die Access-Points damit typische Angriffsmuster erkennen, mit denen die Funkkommunikation gestört werden kann. Zusätzlich kann ein Spektrum-Monitoring und intelligente Kanalwahl helfen, allgemeine Interferenzen zu erkennen und zu meiden, um einen störungsfreien Betrieb sicherzustellen.

Neben einer Implementierung dieser essentiellen Sicherheitsfunktionalitäten im Netz sollte auch bei der Auswahl des Herstellers auf Sicherheitsaspekte geachtet werden. Folgende Dinge sollte der Hersteller implementiert haben:

DSGVO

Die Datenschutzgrundverordnung kommt in Netzwerken dann zum Tragen, wenn vom Netzwerk zu erbringende Dienste personenbezogene Daten verarbeiten (bspw. MAC-Adressen, IP-Adressen, Login-Informationen, Informationen über Dienste-Nutzung, E-Mail-Adressen o. ä.). Dies ist z. B. bei Content Filtern oder Netzwerkzugangskontrolle der Fall und beim Netzwerkmanagement über Cloud-Systeme. Es dürfen daher nur solche Lösungen zum Einsatz kommen, deren Hersteller die DSGVO-konforme Nutzung ermöglichen.

Common Criteria / BSI Zertifizierung

Die Common Criteria oder auch BSI Zertifizierung stellt sicher, dass die Netzwerkkomponenten den geprüften Sicherheitsstandard erfüllen und damit nachvollziehbar zur sicheren Infrastruktur beitragen. Die Common Criteria Zertifizierung sollte für möglichst viele Komponenten vorliegen und aktuellen Datums sein.[8]

Prozesse zur Erkennung und Behebung von Sicherheitslücken

Keine Software ist fehlerfrei, deswegen ist es umso wichtiger, dass jeder Hersteller organisatorische Prozesse implementiert hat, welche die jeweilige Lösung vor Veröffentlichung auf Schwachstellen überprüft und diese dann behebt. Wenn Schwachstellen nach Veröffentlichung von Dritten gefunden werden, gibt es die Möglichkeit diese an den Hersteller zu melden. Der Hersteller muss hierfür ein Critical oder Security Incident Response Team (CIRT oder SIRT) bereitstellen. Das IRT muss diese bearbeiten und entsprechend seiner eigenen Vorgaben beheben.

Support Organisation

Der Hersteller sollte über eine eigene Service & Support Organisation verfügen. Nur so kann sichergestellt werden, dass ein Austausch von Produkten im Hardware-Fehlerfalle erfolgt oder auch Software Updates zur Verfügung gestellt werden. Beides ist für einen möglichst langen, voll funktionalen Einsatz für Netzwerkprodukte wichtig.

Der Hersteller sollte unterschiedliche Servicelevel anbieten, die für den Bedarfsfall kurze Reaktionszeiten sicherstellen.[9]

---

8 Vertiefende Informationen zum Thema Common Criteria sowie weiterführende Links sind dem Glossar zu entnehmen.

9 Für vertiefende Informationen zur Infrastruktursicherheit s. auch Bitkom Leitfaden **↗ »Hardware produktneutral ausschreiben für den Schulbereich. Leitfaden für den öffentlichen IT-Einkauf«**.

8 Barrierefreiheit

Die Beschaffung barrierefreier Hard- und Software ist immer dann erforderlich, wenn Menschen mit Behinderung beschäftigt werden (dies gilt für öffentliche und private Arbeitgeber gleichermaßen). Die allgemeinen Anforderungen an die Barrierefreiheit sind in § 4 des Behindertengleichstellungsgesetzes (BGG, s: https://www.gesetze-im-internet.de/bgg/BJNR146800002.html) gesetzlich niedergelegt. Darüber hinaus gibt es weitere relevante Normen und Regelungen wie z. B. Teil 1 der Barrierefreie-Informationstechnik-Verordnung BITV 2.0 (↗ **https://www.gesetze-im-internet.de/bitv_2_0/BJNR184300011.html**). Zu den gesetzlichen Grundlagen und für weitere Informationen zur Barrierefreiheit vgl. Anhang B in diesem Leitfaden.

Die Beschaffung sollte auf diese oder äquivalente Anforderungen (vgl. Anhang B.2) Bezug nehmen. Der Anbieter legt eine Selbsterklärung vor, welche Barrierefreiheitsanforderungen vom angebotenen Produkt erfüllt werden und welche nicht erfüllt werden können. Dazu ist DIN EN 301549:2020-02 Barrierefreiheitsanforderungen für IKT-Produkte und -Dienstleistungen zu nutzen. Diese wird in § 3 Abs. 1 und 2 der Barrierefreie-Informationstechnik-Verordnung BITV 2.0 (↗ **https://www.gesetze-im-internet.de/bitv_2_0/BJNR184300011.html**) zum deutschen Behindertengleichstellungsgesetz (BGG) direkt referenziert. Dies ermöglicht nach Maßgabe des § 31 Abs. 2 Nr. 1 VgV in der Leistungsbeschreibung einen Verweis auf DIN EN 301549, um die Nutzerbedürfnisse von Menschen mit Behinderungen im Vergabeverfahren angemessen zu berücksichtigen. Vorlagen für die Selbsterklärung liefert Tabelle C.4 (Seite 56) des Technischen Berichts CEN/CLC/ETSI TR 101 552 (2014-03, https://www.etsi.org/deliver/etsi_tr/101500_101599/101552/01.00.00_60/tr_101552v010000p.pdf). Ebenso sollten gleichwertige Normen wie z. B. der US-amerikanische IKT-Barrierefreiheitsstandard US Section 508 akzeptiert werden (vgl. auch Anhang B.6: Internationale Selbsterklärung).

Weitere Informationen zur Barrierefreiheit von IKT-Produkten sind den Bitkom-Leitfäden für produktneutrale Ausschreibungen von ↗ **Notebooks** und ↗ **Thin Clients** zu entnehmen.

9 Beschaffungsmodelle

Grundsätzlich können zwei unterschiedliche Wege bei der Beschaffung der Bedarfe für das Homeoffice beschritten werden. Entweder es werden die Bedarfe im Rahmen der Beschaffung der jeweiligen Komponenten (z. B. mobile Endgeräte, Büromöbel) gedeckt oder die Lieferungen und Leistungen für das Homeoffice werden in einem eigenen Beschaffungsvorgang abgewickelt. Beide Vorgehensweisen haben Vor- und Nachteile.

	Beschaffung über die normalen Beschaffungszyklen der Bedarfe	Beschaffung des gesamten Homeoffice-Bedarfs in einem gesonderten Vorgang
Vorteile	Durch die Bündelung der Beschaffungsvorgänge können preisgünstigere Verträge abgeschlossen werden. Die Herstellervielfalt und der damit verbundene Administrationsaufwand kann reduziert werden. Unter Umständen kann den Mitarbeitern im Homeoffice mehr Leistungen angeboten werden.	Es kann genauer auf die Bedürfnisse im Homeoffice geachtet werden. Einheitlichere Ausstattungen im Bereich des Homeoffice Prozesse können genau auf den Bereich Homeoffice ausgerichtet werden. Die Bieter können diese Prozesse passgenauer umsetzen.
Nachteile	Bestell- und Serviceprozesse für das Homeoffice müssen in den Leistungsbeschreibungen mit bedacht werden. Bedarfe können teilweise nicht so zielgerichtet gedeckt werden.	Höherer Abwicklungs- und Administrationsaufwand, da zusätzliche Verträge abgeschlossen werden müssen. Unter Umständen wird die Beschaffung etwas teuer im Vergleich zu dem anderen Beschaffungsvorgang.

Tabelle 6: Beschaffungsmodelle

Eine Beschaffung von Hardware kann über Miete, Kauf oder Leasing erfolgen. Im Unterschied zur Miete erhält der Auftraggeber beim Leasing am Ende der vertraglichen Nutzungsdauer im Regelfall eine Kaufoption für den Leasinggegenstand. Welche Vorgehensweise der Beschaffer wählt, hängt nicht zuletzt davon ab, ob ihm ein einmaliges Budget oder ein Budget über mehrere Jahre zur Verfügung steht.

Die Entscheidung für eines der genannten Beschaffungsmodelle ist im Regelfall bereits im Vorfeld der Beschaffungsmaßnahme im Rahmen einer Wirtschaftlichkeitsbetrachtung zu treffen. Dabei ist auch zu entscheiden, ob Hardware und Betriebssystem aus einer Hand auf einheitlicher vertraglicher Grundlage (Bundling) oder von verschiedenen Anbietern bezogen werden sollen. Software-Hersteller bieten für Software, die in der öffentlichen Verwaltung eingesetzt werden soll, teilweise besondere Lizenzmodelle an.

Weiter ist zu bedenken, wie im Homeoffice Verbrauchsmaterialien insbesondere auch für die Drucker und Multifunktionsgeräte bestellt werden können und andere Serviceleistungen (z. B. Reparaturen) erbracht werden. Hier spielt auch eine große Rolle, in welchem Vertragsmodell diese Serviceleistungen eingekauft werden. An dieser Stelle verweisen wir auf die entsprechenden Leitfäden der Produkte. In diesen Leitfäden sind die möglichen Vertragsmodelle beschrieben, die bei den jeweiligen Produkten im Servicebereich üblich sind und welche Leistungen sie beinhalten. Daraus sind entsprechende Prozesse abzuleiten. Darüber hinaus sind Prozesse zu definieren, wie die Mitarbeiter im Homeoffice die benötigten Büromaterialien bestellen können und wohin sie geliefert werden. Da an dieser Stelle die organisatorischen Voraussetzungen ziemlich unterschiedlich sind, müssen hier für jeden Bedarfsträger individuelle Prozesse entwickelt werden.

Anlage A: Rechtsgrundlagen von Telearbeit und mobilem Arbeiten

Definition Telearbeitsplatz nach Arbeitsstättenverordnung (ArbStättV)

§ 2 Abs. 7

Telearbeitsplätze sind vom Arbeitgeber fest eingerichtete Bildschirmarbeitsplätze im Privatbereich der Beschäftigten, für die der Arbeitgeber eine mit den Beschäftigten vereinbarte wöchentliche Arbeitszeit und die Dauer der Einrichtung festgelegt hat.

Ein Telearbeitsplatz ist vom Arbeitgeber erst dann eingerichtet, wenn Arbeitgeber und Beschäftigte die Bedingungen der Telearbeit arbeitsvertraglich oder im Rahmen einer Vereinbarung festgelegt haben und die benötigte Ausstattung des Telearbeitsplatzes mit Mobiliar, Arbeitsmitteln einschließlich der Kommunikationseinrichtungen durch den Arbeitgeber oder eine von ihm beauftragte Person im Privatbereich des Beschäftigten bereitgestellt und installiert ist.

Anwendungsbereich der ArbStättV auf Telearbeitsplätze

§ 1 Abs. 3

Für Telearbeitsplätze gelten nur:

1. *§ 3 bei der erstmaligen Beurteilung der Arbeitsbedingungen und des Arbeitsplatzes,*
2. *§ 6 und der Anhang Nummer 6,*

soweit der Arbeitsplatz von dem im Betrieb abweicht. Die in Satz 1 genannten Vorschriften gelten, soweit Anforderungen unter Beachtung der Eigenart von Telearbeitsplätzen auf diese anwendbar sind.

Auszug aus der Begründung der Bundesrats-Drucksache 506/16 vom 23. September 2016. In Absatz 3 wird der Anwendungsbereich für Telearbeitsplätze festgelegt.

Die fehlenden Vorgaben und Maßstäbe für das Einrichten und Betreiben von Telearbeitsplätzen führten in den letzten Jahren in der Praxis zunehmend zu Konflikten zwischen Arbeitgebern und Beschäftigten. Für beide Gruppen stellt sich heute die Frage, welche Anforderungen konkret für Telearbeitsplätze gelten und wie diese Arbeitsplätze außerhalb des Betriebes zum Schutz der Beschäftigten zu gestalten sind. Eine Klarstellung in Bezug auf die Arbeitsplätze im Privatbereich wird umso drängender, da diese Art und Form der Arbeitsorganisation und Arbeitsgestaltung im Zuge der Vereinbarkeit von Familie und Beruf in Zukunft noch an Bedeutung gewinnen wird. […]

Telearbeitsplätze sind zumeist Arbeitsplätze von Beschäftigten, die alternierend im Betrieb oder im Privatbereich (Telearbeitsplätze) arbeiten. […]

»Mobiles Arbeiten« (gelegentliches Arbeiten von zuhause aus oder während der Reisetätigkeit, Abrufen von Emails nach Feierabend außerhalb des Unternehmens, Arbeit zuhause ohne eingerichteten Bildschirmarbeitsplatz usw.) unterliegt nicht der ArbStättV; es handelt sich dabei nicht um Telearbeit im Sinne der Verordnung. Mobiles Arbeiten ist vielmehr ein Arbeitsmodell, das den Beschäftigten neben der Tätigkeit im Büro noch Arbeiten außerhalb der regulären Arbeitszeit zuhause oder unterwegs ermöglicht (ständige Zugangsmöglichkeit über Kommunikationsmittel zum Unternehmen/Betrieb). […]

Auszug aus der »SARS-CoV-2-Arbeitsschutzregel« (Fassung 07.05.2021)

2.2 Homeoffice als Form mobiler Arbeit

(1) Mobiles Arbeiten ist eine Arbeitsform, die nicht in einer Arbeitsstätte gemäß § 2 Absatz 1 Arbeitsstättenverordnung (ArbStättV) oder an einem fest eingerichteten Telearbeitsplatz gemäß § 2 Absatz 7 ArbStättV im Privatbereich des Beschäftigten ausgeübt wird, sondern bei dem die Beschäftigten an beliebigen anderen Orten (zum Beispiel beim Kunden, in Verkehrsmitteln, in einer Wohnung) tätig werden.

(2) Für die Verrichtung mobiler Arbeit werden elektronische oder nichtelektronische Arbeitsmittel eingesetzt.

(3) Homeoffice ist eine Form des mobilen Arbeitens. Sie ermöglicht es Beschäftigten, nach vorheriger Abstimmung mit dem Arbeitgeber zeitweilig im Privatbereich, zum Beispiel unter Nutzung tragbarer IT-Systeme (zum Beispiel Notebooks) oder Datenträger, für den Arbeitgeber tätig zu sein.

(4) Regelungen zur Telearbeit bleiben unberührt.

Anlage B: Informationen zur Barrierefreiheit

B.1 Definition Barrierefreiheit

»Barrierefrei sind [...] Systeme der Informationsverarbeitung [...], wenn sie für Menschen mit Behinderungen

- in der allgemein üblichen Weise,
- ohne besondere Erschwernis und
- grundsätzlich ohne fremde Hilfe

auffindbar, zugänglich und nutzbar sind.

Hierbei ist die Nutzung behinderungsbedingt notwendiger Hilfsmittel zulässig.« (§ 4 BGG) Hilfsmittel sind z. B. Spezialtastaturen, alternative Zeigegeräte, Screen Reader oder Screen Magnifier.

B.2 Relevante Normen und Regulierung

Bei der Erstellung der Leistungsbeschreibung zur Beschaffung von Notebooks sind, außer in sachlich begründeten Ausnahmefällen, die Kriterien zur Barrierefreiheit zu berücksichtigen:

- Vergaberechtsmodernisierungs-Gesetz (VergRModG) (18.4.2016) (Umsetzung RL 2014/24/EU RL 2014/25/EU) § 121 Leistungsbeschreibung, Absatz 2
- Gesetz zur Gleichstellung von Menschen mit Behinderungen (Behindertengleichstellungsgesetz - BGG), (10.7.2018) § 12 Barrierefreie Informationstechnik, Absatz 2.

Hierbei ist besonders darauf zu achten, dass die Anforderungen sich an den Nutzerbedürfnissen ausrichten und zugleich technikneutral sowie innovationsoffen sind.

Um die Anforderungen an die Barrierefreiheit bei der Beschaffung von Produkten und Dienstleistungen der Informations- und Kommunikationstechnologie durch die öffentliche Hand in Europa zu harmonisieren, hatte die Europäische Kommission die europäischen Normungsorganisationen CEN, CENELEC und ETSI mit der Erstellung einer Norm beauftragt. Das Ergebnis des Auftrags ist die Europäische Norm EN 301549:2018-08 (↗ **https://www.etsi.org/deliver/etsi_en/301500_301599/301549/02.01.02_60/en_301549v020102p.pdf**), die im Amtsblatt der Europäischen Union unter der Richtlinie (EU) 2016/2102 *über den barrierefreien Zugang zu den Websites und mobilen Anwendungen öffentlicher Stellen* aufgeführt ist. Die Umsetzung dieser Europäischen Norm erfolgte mit DIN EN 301 549:2020-02 *Barrierefreiheitsanforderungen für IKT-Produkte und -Dienstleistungen*. Die Nachweisführung sollte über eine Eigenerklärung des Auftragneh-

mers erfolgen. Zertifikate können nicht als Nachweise gefordert werden, da eine entsprechende Zertifizierungsmöglichkeit zurzeit nicht besteht.

B.3 Normen zu Accessibility Features

Eine umfassende Übersicht über Accessibility Features, die auch von Desktop-PCs, Notebooks, Tablets und Smartphones erfüllt werden müssen, bietet ISO/IEC 20071-5 »Information technology - User interface component accessibility - Part 5: Accessible user interface for accessibility settings on information devices«. Diese Norm liegt bislang im Entwurf vor und wird voraussichtlich 2021 veröffentlicht werden. Der Anhang der Norm kann als Checkliste bei der Angebotserstellung dienen. Die Accessibility Features sind in Kapitel 4.2 der Norm gelistet.

B.4 Managementsystemnormen für Barrierefreiheit

DIN EN 17161 »Design für alle - Barrierefreiheit von Produkten, Waren und Dienstleistungen nach einem »Design für alle«-Ansatz - Erweitern des Benutzerkreises« ist eine Managementsystemnorm, die Organisationen hilft, Barrierefreiheit in ihren Prozessen sicherzustellen. Ihre Anwendung ist nicht verpflichtend, jedoch hilfreich bei der Selbsterklärung.

B.5 Ausblick

Eine Aktualisierung der Norm liegt als EN 301 549 (2021-03,-, **↗ https://www.etsi.org/deliver/etsi_en/301500_301599/301549/03.02.01_60/en_301549v030201p.pdf**) bereits vor. Ihre Veröffentlichung im Amtsblatt der EU sowie ihre Übersetzung als DIN EN 301549 wird Ende 2021 erwartet.

Die EU Richtlinie 2019/882/EU über die Barrierefreiheitsanforderungen für Produkte und Dienstleistungen (European Accessibility Act, EAA) (**↗ https://eur-lex.europa.eu/legal-content/DE/TXT/PDF/?uri=CELEX:32019L0882&from=EN**) fordert im Artikel 2 »Geltungsbereich« (1), »Produkte« u. a. die Barrierefreiheit von folgenden Produkten, die nach dem 28. Juni 2025 in Verkehr gebracht werden:

»a) Hardwaresysteme und für diese Hardwaresysteme bestimmte Betriebssysteme für Universalrechner für Verbraucher; [...]

c) Verbraucherendgeräte mit interaktivem Leistungsumfang, die für elektronische Kommunikationsdienste verwendet werden;

d) Verbraucherendgeräte mit interaktivem Leistungsumfang, die für den Zugang zu audiovisuellen Mediendiensten verwendet werden; [...]«

Darüber hinaus sind auch folgende Dienstleistungen im Artikel 2 (2) betroffen:

»a) elektronische Kommunikationsdienste mit Ausnahme von Übertragungsdiensten zur Bereitstellung von Diensten der Maschine-Maschine-Kommunikation;

b) Dienste, die den Zugang zu audiovisuellen Mediendiensten ermöglichen; [...]

f) Dienstleistungen im elektronischen Geschäftsverkehr [...]«

Das EAA sieht Barrierefreiheit als Teil der Selbsterklärung im Rahmen der CE-Kennzeichnung vor. Die Umsetzung des EAAs erfolgt im Wesentlichen eins zu eins in Deutschland durch das Barrierefreiheitsstärkungsgesetz (BFSG), das noch im Sommer 2021 verabschiedet werden soll. Für die zusätzlichen Barrierefreiheitsanforderungen im EAA ist eine Erweiterung des EN 301 549 als Normungsauftrag vorgesehen.

B.6 Internationale Selbsterklärung

Für die Selbsterklärung international tätiger IKT-Anbieter kann folgende Information hilfreich sein: Der »Information Technology Industry Council« (ITI) stellt ein kostenloses Berichterstattungswerkzeug zur Verfügung, das als Voluntary Product Accessibility Template (VPAT) bekannt ist, um festzustellen, ob Produkte und Dienstleistungen der Informations- und Kommunikationstechnologie die Anforderungen an die Barrierefreiheit, einschließlich der Regeln nach US Rehabilitation Act Section 508, erfüllen. Das ITI hat überarbeitete Ausgaben der VPAT (2.4) herausgegeben, die auf den überarbeiteten 508 Regeln des US Access Boards (VPAT 2.4 508) basieren. Zusätzlich werden auch Versionen für die WCAG 2.1 (VPAT 2.4 WCAG) und den EN 301 549 (VPAT 2.4 EU) sowie eine weitere Version, die auf allen drei basiert (VPAT 2.4 INT), angeboten.
↗ https://www.itic.org/policy/accessibility/vpat

Anlage C: Glossar

BYOD-Konzept	Konzept zur Integration privater mobiler Endgeräte wie Laptops, Tablets oder Smartphones in die Netzwerke von Unternehmen oder Schulen, Universitäten, Bibliotheken und anderen Einrichtungen (»Bring your own device«).
Common Criteria	Bei der Auswahl der informationstechnischen Komponenten, wie z. B. Netzwerk- und Securitylösungen ist auf eine Sicherheitszertifizierung zu achten. Die internationale Zertifizierung nach »Common Criteria« (CC), die auch das Bundesamt für Sicherheit in der Informationstechnik (BSI) vornimmt, stellt die größtmögliche Vielfalt an Lösungen bei gleichzeitiger Anwedungssicherheit sicher. Das BSI erkennt darüber hinaus bereits erstellte Zertifikate anderer Länder an, welche auf gemeinsamen Schutzprofilen (cPP) basieren. Das »Common Criteria Recognition Arrangement« Abkommen (CCRA) regelt die gegenseitige internationale Anerkennung, mit dem Ziel, mehrfache Zertifizierungen zu vermeiden. Es ist also darauf zu achten, dass die eingesetzten Komponenten über eine CC-Zertifizierung entweder vom BSI oder gleichwertig von einer Zertifizierungsstelle nach dem CCRA-Abkommen verfügen. Weiterführende Informationen: Seite des BSI: ↗ **https://www.bsi.bund.de/DE/Themen/ZertifizierungundAnerkennung/Produktzertifizierung/ZertifizierungnachCC/InternatAnerkennung/CCRA_Anerkennung.html** Suchmöglichkeit für CC-Zertifikate unterschiedlicher Hersteller: ↗ **https://www.niap-ccevs.org/** Common Criteria Portal: ↗ **https://www.commoncriteriaportal.org/**
Controller und Gateways	Controller und Gateways bieten Konnektivitäts- und Sicherheitsfunktionen, einschließlich VPN-Terminierung für Remote-Mitarbeiter für optimiertes Layer-3-Roaming, Skalierbarkeit und Redundanz für Campus-Netzwerke jeder Größe. Idealerweise haben Controller eine Firewall zur Durchsetzung von Zugriffsregeln, KI-basierte HF-Optimierung und die automatische Provisionierung von der sicheren Infrastruktur vor Ort bis hin zu den abgesetzten Elementen wie Remote Access Points oder VPN Clients.
Intrusion Detection und Prevention System	Ein Intrusion-Detection- oder Intrusion-Prevention-System (IDS / IPS) ist eine Security-Lösung, die ein Netzwerk oder eine Netzwerkkomponente wie einen Server oder einen Switch überwacht und versucht, Regelverletzungen und schädliche Vorfälle wie Hacker-Angriffe zu erkennen und diese dann teilweise automatisch abzuwehren.
Netzwerkmanagementsystem (NMS)	NMS ist eine allgemeine Bezeichnung für die Soft- und/oder Hardware, die das Netzwerkmanagement ausführt. Dazu gehören alle Funktionen und Komponenten zur Überwachung und Steuerung von Netzwerken
Policy Enforcement Firewall	Eine derartige Firewall ist die zugrunde liegende Technologie, die die automatische Provisionierung ermöglicht, um drahtgebundene und drahtlose Netzwerke zu vereinfachen und zu sichern. Diese Funktion erstreckt sich auf Remotebenutzer und bietet Administratoren wichtige Funktionen für Transparenz, Kontrolle und Durchsetzung der Sicherheit.
Policy Manager	Policy Management Plattformen enthalten Regelwerke, die die Zugriffsrechte für Nutzer und Endgeräte enthalten. Damit entsteht vollständige Transparenz und rollenbasierte Zugriffskontrolle für IoT, BYOD, Unternehmensgeräte sowie Mitarbeiter, Auftragnehmer und Gäste in allen kabelgebundenen, kabellosen und VPN-Infrastrukturen mehrerer Anbieter. Zugriffs-Richtlinien gelten auch für Remotebenutzer, die über VPN Clients oder Remote Access Points (RAPs) eine Verbindung herstellen.
Remote Access Points (RAPs)	Mit Remote Access Points (RAPs) wird eine sichere SSL / IPSec-VPN-Verbindung zu einem zentralen Controller über den privaten Internetzugang hergestellt, einschließlich Mobilfunk-, heimische DSL- und Kabelnetzwerke mit der Einfachheit von Plug-and-Play. RAPs sollten konstruktionsbedingt sicher sein und ein Werkszertifikat mit einem einen TPM-Chip für die Verbindung verwenden. Dadurch wird eine zertifikatbasierte Authentifizierung bereitgestellt, die an jeden einzelnen RAP gebunden ist. Zusätzlich wird der gesamte Datenverkehr verschlüsselt, um die Daten während der Übertragung zu sichern.
Sandboxing	Sandboxing ist ein Begriff aus dem Bereich der Computersicherheit, der sich darauf bezieht, dass ein Programm von anderen Programmen in einer getrennten Umgebung separiert wird, so dass im Falle von Fehlern oder Sicherheitsproblemen diese Probleme nicht auf andere Bereiche des Computers übergreifen.

VPN Client	Optimal sind hybride IPsec / SSL-VPN-Clients, die automatisch die beste und sicherste Verbindung zum Terminieren des unternehmensgebundenen Datenverkehrs scannt und auswählt. Im Gegensatz zu herkömmlichen VPNs, für die dedizierte Hardware erforderlich ist, integrieren VPN-Dienste direkt in die vorhandene sichere Infrastruktur im Büro, um Architektur und Verwaltung zu vereinfachen. In diesem Bereitstellungsmodell können mobile Geräte oder Desktop-Workstations sicher auf Netzwerke zugreifen, die kontrollierte, nicht klassifizierte, vertrauliche und klassifizierte Informationen verarbeiten.
Zero Trust Security	Dieser Begriff fasst die wichtigsten Elemente für die Implementierung von vollständiger Transparenz, was im Netzwerk unterwegs ist zusammen: Authentifizierung von Endgeräten und Nutzern, richtlinienbasierte Zugriffsautorisierung sowie Erkennung und Abwehr von Angriffen. Dabei wird davon ausgegangen nichts und niemandem zu vertrauen (Zero Trust) um eine kontinuierliche und dynamische Security herstellen zu können. Neben der Absicherung neuer Angriffsvektoren senkt ein Zero Trust Security die Komplexität im Betrieb, steigert die Benutzererfahrung, da die Überwachung im Hintergrund und automatisiert abläuft und ermöglicht es, die Konfiguration der Netzwerke durch Anwendung der Zugriffsregeln zu eliminieren, was wiederum zu völlig neuen Betriebsmodellen führen kann.

Bitkom vertritt mehr als 2.700 Unternehmen der digitalen Wirtschaft, davon gut 2.000 Direktmitglieder. Sie erzielen allein mit IT- und Telekommunikationsleistungen jährlich Umsätze von 190 Milliarden Euro, darunter Exporte in Höhe von 50 Milliarden Euro. Die Bitkom-Mitglieder beschäftigen in Deutschland mehr als 2 Millionen Mitarbeiterinnen und Mitarbeiter. Zu den Mitgliedern zählen mehr als 1.000 Mittelständler, über 500 Startups und nahezu alle Global Player. Sie bieten Software, IT-Services, Telekommunikations- oder Internetdienste an, stellen Geräte und Bauteile her, sind im Bereich der digitalen Medien tätig oder in anderer Weise Teil der digitalen Wirtschaft. 80 Prozent der Unternehmen haben ihren Hauptsitz in Deutschland, jeweils 8 Prozent kommen aus Europa und den USA, 4 Prozent aus anderen Regionen. Bitkom fördert und treibt die digitale Transformation der deutschen Wirtschaft und setzt sich für eine breite gesellschaftliche Teilhabe an den digitalen Entwicklungen ein. Ziel ist es, Deutschland zu einem weltweit führenden Digitalstandort zu machen.

Bundesverband Informationswirtschaft,
Telekommunikation und neue Medien e.V.

Albrechtstraße 10
10117 Berlin
T 030 27576-0
F 030 27576-400
bitkom@bitkom.org
www.bitkom.org

bitkom