Bildquelle: AdobeStock_347366618

FAQ Homeoffice für Endanwender

1. Hardware und Infrastruktur

Ist jeder Raum in meiner Wohnung zum Arbeiten geeignet - worauf muss ich achten?

Grundsätzlich unterscheiden sich die Anforderungen an den Arbeitsplatz im Homeoffice nicht von den Anforderungen an einen Büroarbeitsplatz. Die Arbeitsstättenverordnung kommt dann nicht zum Tragen, wenn es sich bei der Tätigkeit im Homeoffice um gelegentliche Tätigkeiten von zu Hause handelt.

Welche Infrastrukturkomponenten benötige ich im Homeoffice?

Die Faustregel lautet: die gleichen Komponenten wie im Büro, wenn das Tätigkeitsspektrum gleich bleibt, d.h. wenn beispielsweise Drucken oder Scannen möglich sein soll, werden auch die entsprechenden Geräte benötigt. Natürlich kann im Homeoffice z.B. mit einem Notebook oder einem Tablet gearbeitet werden statt mit PC oder ThinClient im Büro. Die Interaktion mit unterschiedlichen Endgeräten ist dann naturgemäß eine andere.

Wer stellt die Infrastruktur zur Verfügung?

Diese Frage wird von Arbeitgeber zu Arbeitgeber unterschiedlich beantwortet. Grundsätzlich kann auch mit privaten Geräten auf die Infrastruktur des Arbeitgebers zugegriffen werden, wenn die technischen Voraussetzungen (z.B. Zugriff über TerminalServer/VDI) erfüllt sind.

Sind beim Notebook ein separater Monitor, zusätzliche Maus oder externe Tastatur sinnvoll?

Das ist eine Frage der Vorlieben und der Zeit, die man im Homeoffice mit dem Arbeiten an diesen Geräten verbringt; außerdem auch eine Frage der zur Verfügung stehenden Arbeitsfläche.

Was muss ich beim Monitor beachten?

Empfehlenswert sind zwischen 21 und 27 Zoll Bildschirmdiagonale. Achten Sie ebenfalls darauf, die Bildschirmhelligkeit nicht auf 100 Prozent zu stellen. 90 Prozent reichen häufig vollkommen aus und beugen der Augenermüdung vor.

Was ist eine Docking Station?

Als Docking Station bezeichnet man eine Hardware-Erweiterung von Notebooks (oder auch Tablets), an die man in der Regel Anschlüsse, wie z.B. Strom, Monitor, Maus, Tastatur und USB-Geräte, dauerhaft anschließen kann.

Darf ich meinen privaten Rechner (oder Tablet bzw. Handy) im Homeoffice für Firmenapplikationen benutzen?

Das ist abhängig vom Arbeitgeber. Grundsätzlich kann auch mit privaten Geräten auf die Infrastruktur des Arbeitgebers zugegriffen werden, wenn die technischen Voraussetzungen erfüllt sind (z.B. Zugriff über TerminalServer/VDI).
Voraussetzungen: Die Geräte sind entsprechend konfiguriert und rechtliche Vorkehrungen (z.B. in Form verbindlicher schriftlicher Vereinbarungen) wurden getroffen.

Kann ich meinen privaten Drucker aus dem Firmennetzwerk ansteuern?

Ja, insofern der Zugriff auf die Firmeninfrastruktur über TerminalServer/VDI erfolgt und diese TerminalServer/VDI-Infrastruktur das entsprechend zulässt.

Ich habe zu Hause keinen Drucker und muss gelegentlich einen Druck ins Büro schicken - geht das?

Ja, insofern der Zugriff auf die Firmeninfrastruktur über TerminalServer/VDI erfolgt, dann haben Sie von extern die gleichen Zugriffe auf Ressourcen wie vom Büro aus.

Software und Applikationen

Benötige ich alle Programme, die ich auf meinem Bürorechner habe auch im Homeoffice - muss ich die alle installieren?

Nein, sofern der Zugriff auf die Firmeninfrastruktur über TerminalServer/VDI erfolgt. Dann haben Sie zu Hause die gleichen Programme zur Verfügung wie im Büro.

Im Büro arbeiten wir normalerweise mit Windows, ich habe aber einen Apple Computer - funktioniert das?

Ja, sofern der Zugriff auf die Firmeninfrastruktur über TerminalServer/VDI erfolgt und der entsprechende TerminalServer/VDI-Client (RDP/Citrix/Horizon/etc.) auf dem Apple Computer installiert ist.

Wie funktioniert das mit den Updates?

Sofern der Zugriff auf die Firmeninfrastruktur über TerminalServer/VDI erfolgt, kümmert sich der Arbeitgeber um die Updates dieser Infrastruktur. Für die Updates des lokalen Betriebssystems und Programme des PCs/Notebooks/Tablets ist bei privat genutzten Geräten der Arbeitnehmer zuständig, sonst der Arbeitgeber. Aber auch im letzten Fall kann es sein, dass der Benutzer zu einer Interaktion aufgefordert wird. Grundsätzlich sollte man wissen, dass Updates auch dazu führen können, dass anschließend die Kommunikation und/oder das Arbeiten mit der Infrastruktur des Arbeitgebers nicht mehr reibungslos funktionieren. Das sollte man in Hinterkopf behalten und Updates beispielsweise nicht in einer kritischen Arbeitsphase durchführen. Gegebenenfalls ist es sinnvoll, vorher Rücksprache mit dem IT-Support des Arbeitgebers zu halten.

Wie funktioniert das mit dem Backup?

Sofern der Zugriff auf die Firmeninfrastruktur über TerminalServer/VDI erfolgt und kein lokales Bearbeiten von Firmendaten stattfindet, sorgt der Arbeitgeber für das Backup dieser Infrastruktur.

Bildquelle: AdobeStock_330681088

3. Internet und Bandbreite

Was ist besser - Verbindung per Kabel oder WLAN?

Technisch gesehen ist eine Verbindung per Kabel vorzuziehen: Sie ist normalerweise sicherer, stabiler und schneller. Außerdem gibt es die Möglichkeit, kabelgebundene Verbindungen über das Stromnetz zu realisieren (PowerLine-Adapter). Damit können gewisse Einschränkungen und Nachteile eines WLAN ohne großen Aufwand umgangen werden, die Verbindungsqualität ist jedoch nicht mit einer "normalen", dedizierten IT-Verkabelung vergleichbar.

In meinem Homeoffice ist die WLAN-Verbindung schlecht - was kann ich tun?

Versuchen Sie alternativ, mit einem PowerLine-Adapter zu arbeiten oder mit der Kombination von PowerLine und WLAN.

Ich habe nicht in jedem Raum meiner Wohnung die gleiche Verbindungsqualität - was kann ich tun?

Versuchen Sie alternativ, mit einem PowerLine-Adapter zu arbeiten oder mit der Kombination von PowerLine und WLAN.

Wen kontaktiere ich, wenn mein WLAN nicht funktioniert?

Dafür ist leider in der Regel weder Ihr Internet-Provider, noch die IT Ihres Arbeitgebers zuständig. Falls Sie den Fehler nicht selbst beheben können, wenden Sie sich bitte an den Dienstleister, der Ihnen ursprünglich das WLAN eingerichtet hat oder an einen anderen lokalen Dienstleister Ihrer Wahl.

Ich nutze gelegentlich ein freies WLAN - ist das bedenklich?

Ja und nein. Alle öffentlichen WLAN-Hotspots sind, wie der Name schon sagt, uneingeschränkt durch die Öffentlichkeit nutzbar. Dazu können auch Angreifer gehören, die es z.B. auf Ihre Passwörter und Zugangsdaten abgesehen haben, indem sie Ihnen gefakte WLAN-Login-Portale präsentieren, sogenannte „Man-in-the Middle-Attacken“ starten oder auch Ihren Rechner angreifen, ohne dass sie das merken. Sofern der Zugriff auf die Firmeninfrastruktur über TerminalServer/VDI mit zusätzlicher Absicherung über eine Zwei-Faktor-Authentifizierung erfolgt, ist eine Nutzung von öffentlichen WLAN-Hotspots aus Sicht des Arbeitgebers unbedenklich.

Meine Kinder nutzen mein WLAN und Internet auch - ist das ein Problem?
Das kann aus mehreren Gründen zu einem Problem werden: Die Kinder belegen Ihre Bandbreite und Angreifer können die Rechner der Kinder nutzen, um auch Ihren Rechner anzugreifen. Sofern der Zugriff auf die Firmeninfrastruktur über TerminalServer/VDI erfolgt und zusätzlich eine Absicherung über eine Zwei-Faktor-Authentifizierung erfolgt, bleibt nur das Problem der Bandbreite, und Sie wundern sich, warum Sie immer wieder in einer Webkonferenz schlecht verstanden werden ;-)

Welche Bandbreite braucht mein Internetanschluss mindestens?

Die Antwort ist: das verfügbare Maximum. Sofern der Zugriff auf die Firmeninfrastruktur über TerminalServer/VDI erfolgt, werden Sie auch mit einem 16.000-Anschluss gut arbeiten können. Wenn Ihr Arbeitgeber aber zusätzlich weitere Cloud-Infrastrukturen, wie z.B. Videokonferenzen, nutzt oder Internet-Telefonie ermöglicht, reicht diese Einstiegs-Bandbreite nicht mehr aus.

Wie kann ich feststellen, wieviel Bandbreite mein Anschluss hat?

Es gibt einige sogenannte "Speedtest-Seiten" im Internet, z.B. https://speedtest.chip.de oder https://speedtest.computerbild.de.

Wie kann ich meine Bandbreite erhöhen?

Dazu müssen Sie eine entsprechende Anfrage bei Ihrem derzeitigen Internet-Provider stellen.

Ich habe nur einen Mobilfunkvertrag mit ausreichend Datenvolumen - reicht das aus?

Unter Umständen ja. Mit der großräumigen Verfügbarkeit von LTE und dem kommenden 5G-Standard sind die Bandbreiten, die über Mobilfunk erzielbar sind, ausreichend - sofern der Zugriff auf die Firmeninfrastruktur über TerminalServer/VDI erfolgt.

Mein Zugriff auf das Firmennetzwerk dauert sehr lange - woran kann das liegen?

Leider ist diese Frage nicht immer einfach zu beantworten. Gründe dafür können sein:

- Das Heim-Netzwerk im Homeoffice (WLAN, PowerLine): Reichweite (Bandbreite) zu gering, zu viele Nutzer, parallele Nutzung z.B. von Streamingdiensten oder defekte Komponenten.
- Der Internet-Anschluss im Homeoffice: Bandbreite zu gering, zu viele Nutzer im Haushalt, aber auch in der Nachbarschaft, parallele Nutzung z.B. von Streamingdiensten.
- Der Internet-Anschluss des Arbeitgebers.
- Die IT-Infrastruktur des Arbeitgebers.

4. Firmennetzwerk und Anbindung

Mein Arbeitgeber hat mir für das Homeoffice einen „ThinClient“ zur Verfügung gestellt - was ist das eigentlich?

Ein ThinClient ist ein Rechner, der ausschließlich für die Nutzung mit TerminalServer/VDI - Infrastrukturen vorgesehen ist. Der Vorteil von ThinClients ist, dass sie ein geschlossenes und aus der Ferne sehr gut administrierbares System darstellen, und dadurch im Betrieb weniger Kosten verursachen. Darüber hinaus bieten sie Angreifern deutlich weniger Angriffsfläche und benötigen weniger Strom.

Was ist eigentlich ein VPN?

Ein VPN (Virtual Private Network) stellt eine durch Verschlüsselung gesicherte Verbindung zwischen zwei digitalen Kommunikationspartnern her. Oft wird dieser Begriff für das sogenannte "Einwählen" in das Firmennetz über das Internet verwendet - meist ohne zusätzliche Hilfen, wie z.B. TerminalServer/VDI. Ohne die lokale Absicherung des Gerätes kann diese Art der Anbindung an das Firmennetz Schadsoftware erlauben, das Firmennetzwerk zu kompromittieren und ist daher nur bedingt geeignet. Darüber hinaus wirken sich Bandbreitenprobleme oder -schwankungen ungefiltert auf die Zugriffszeiten aus.

Warum ist es so wichtig, wie zwischen den Geräten im Heimnetzwerk und im Firmennetzwerk eine Verbindung aufgebaut wird?

Die Verbindung darf einem Schädling oder Angreifer nicht erlauben, das Firmennetzwerk zu kompromittieren und/oder Daten aus dem Firmennetzwerk abfließen lassen.

Was bedeutet Remote Access?

In der Regel wird damit der Zugriff auf IT-Infrastrukturen (z.B. die des Arbeitgebers) von außerhalb bezeichnet.

Was ist eine Multi-Faktor-Authentifizierung?

Eine Multi-Faktor-Authentifizierung (z.B. Zwei-Faktor-Authentifizierung) bezeichnet eine mehrfache Überprüfung, ob eine Person berechtigt ist, sich an einer Anwendung oder einem sonstigen Dienst anzumelden. Das bekannteste Ein-Faktor-Authentifizierungs-Verfahren ist Username/Passwort. Ein weiterer, zweiter Faktor kann z.B. das Versenden eines Codes per SMS an eine bestimmte Mobilnummer, der Empfang eines Codes auf einer App am Mobiltelefon oder das Ablesen eines Codes auf einem Schlüsselanhänger sein.

Was ist eine VDI?

Als VDI (Virtual Desktop Infrastructure) wird in der Regel eine IT-Infrastruktur bezeichnet, bei der die Arbeitsrechner der Anwender nicht physisch am Arbeitsplatz des Anwenders vorhanden sind, sondern aus sogenannten virtuellen Rechnern bestehen, die in einem Rechenzentrum zentral vorgehalten und für die Anwender bereitgestellt werden.

Wie sieht der sicherste Remote-Zugriff auf das Firmennetzwerk eines Unternehmens aus?

Der sicherste Zugriff mit einer klaren Trennung von Heim- und Firmennetzwerk ist und bleibt derzeit eine TerminalServer- oder VDI-Verbindung mit einem dedizierten und abgesicherten Gateway. Diese kann durchaus auch mit privaten Geräten genutzt werden und wird idealerweise um eine Zwei-Faktor-Authentifizierung ergänzt.

Wie erhalte ich im Homeoffice Zugriff auf meine Dokumente/Dateien im Firmennetzwerk?

Sofern der Zugriff auf die Firmeninfrastruktur über TerminalServer/VDI erfolgt, haben Sie vom Homeoffice aus den gleichen Zugang zu Ihrer Dokumentenablage wie im Büro.

Bildquelle: AdobeStock_226008623

5. Sicherheit und Datenschutz

Braucht mein Tablet einen Virenschutz?

Sofern es sich um ein Apple-iPad handelt, ist das nicht unbedingt notwendig; bei anderen Betriebssystemen wie z.B. Android oder Windows ist ein Virenschutz empfehlenswert.

Wie überprüfe ich die Sicherheit meines Routers?

Leider kann diese Frage nicht einfach beantwortet werden. Das hängt von Ihrem technischen Vorwissen und dem jeweiligen Router ab. Es ist grundsätzlich darauf zu achten, dass der Router immer auf dem neusten Stand der Firmware ist, dass das Administrator-Passwort, mit dem der Router ausgeliefert worden ist, geändert wurde, und dass der administrative Zugang von außerhalb (über das Internet) nicht möglich bzw. deaktiviert ist.

Wie erstelle ich ein sicheres Passwort für meinen PC?

Dazu gibt es klare Empfehlungen des BSI.

Ich arbeite über eine TerminalServer-Verbindung - muss ich dann noch auf Virenschutz auf meinem PC achten?

Ja, sofern der Zugriff auf die Firmeninfrastruktur über TerminalServer/VDI erfolgt, ist diese durch einen ungeschützten PC zwar nicht automatisch gefährdet; trotzdem ist der PC an sich, also Ihre Daten und Zugänge, gefährdet.

Können Sie mir eine Antivirus-Software für meinen privaten PC empfehlen?

Der Markt ist hier ständig in Bewegung, insofern kann eine Empfehlung von heute sehr schnell schon wieder überholt sein. Grundsätzlich ist der von Microsoft mit dem Windows10-Betriebssystem ausgelieferte Virusschutz "Defender" empfehlenswert; Sie müssen aber darauf achten, dass er aktiviert und immer auf dem neuesten Stand ist.

Brauche ich zu Hause eine Firewall?

Ja, vor allem wenn auch andere Geräte, wie z.B. Drucker, Scanner oder NAS das Netzwerk zu Hause nutzen. In der Regel bieten die meisten Provider mit dem gelieferten Abschluss-Router Firewall-Funktionalitäten an. Empfehlenswert ist es hier - sofern man die Wahl hat - auf Produkte der Firma AVM (FritzBox) zurück zu greifen.

Ich arbeite auch mal im Zug, wie kann ich mich vor fremden Einblicken schützen?

Das können Sie beispielsweise mit einer Blickschutzfolie.

Wie ist das eigentlich mit der Datensicherung auf meinem privaten Laptop?

Sofern der Zugriff auf die Firmeninfrastruktur über TerminalServer/VDI erfolgt und ein lokales Bearbeiten von Firmendaten nicht stattfindet, sorgt der Arbeitgeber für das Backup dieser Infrastruktur. Eine Datensicherung der eigenen Daten muss natürlich regelmäßig erfolgen - am einfachsten mit einer Backup-Software und mindestens zwei im Wechsel eingesetzten externen Festplatten.

Ist es sicher, Dateien zwischen dem Heim- und Unternehmensnetz per E-Mail hin- und herzuschicken?

Sofern der Zugriff auf die Firmeninfrastruktur über TerminalServer/VDI erfolgt, ist diese Arbeitsweise nicht notwendig. Ein Versenden von Firmendaten vom Firmen-E-Mail-Account auf den privaten E-Mail-Account ist nicht zulässig

Wie sieht es mit dem Datenschutz aus?

Unabhängig davon, ob man mobil arbeitet, gelegentlich im Homeoffice tätig ist, oder ob es sich um einen voll ausgestatteten Tele-Arbeitsplatz handelt: Die Vorgaben der Datenschutzgrundverordnung (DSGVO) müssen immer und überall erfüllt werden. Dabei liegt die datenschutzrechtliche Verantwortung immer beim Arbeitgeber bzw. beim Dienstherren.

Wie muss die Arbeitsumgebung gestaltet sein?

Die Homeoffice-Arbeitsumgebung sollte immer so ausgestaltet sein, dass die Vertraulichkeit und Verfügbarkeit der Daten sichergestellt sind:

- Der Arbeitsplatz ist so zu wählen, dass weder Familienmitglieder noch Besucher Einblick auf elektronische- und/oder Papierunterlagen erhalten.
- Papierunterlagen mit personenbezogenen Daten sind in Mappen oder Schränken zu verschließen, bzw. mit einem Aktenvernichter zu entsorgen.
- Auch im Homeoffice sollte der PC beim Verlassen des Arbeitsplatzes immer gesperrt werden, falls der Zugriff Dritter – egal ob gewollt oder ungewollt – nicht ausgeschlossen werden kann.
- Es ist darauf zu achten, dass Telefongespräche nicht von unbefugten Personen mitgehört werden können, sei es z. B. durch eine offene Tür, ein offenes Fenster oder bei einer Videokonferenz.
- Bei Verlassen des Arbeitsplatzes bzw. am Ende des Arbeitstages dürfen keine Dokumente zurückgelassen werden (Clean-Desk-Richtlinie).

6. Support und Wartung

Kann die IT-Abteilung meines Arbeitgebers auch mein privates Equipment mit einem Remote-System fernwarten und mir helfen?

Grundsätzlich ja - abhängig von Bedarf, auf Anforderung und entsprechenden Regelungen, und solange es um die Einrichtung des Remote-Zugangs geht. Beispielsweise bei der Ersteinrichtung des entsprechenden TerminalServer/VDI-Client (RDP/Citrix/Horizon/etc.). Weitere Hilfen, wie z.B. Troubleshooting im Bereich WLAN/Internetzugang/private Drucker/Scanner sind ausgeschlossen, dafür bitten wir um Verständnis.

Wen kann ich anrufen, wenn ich im Homeoffice mit meinem PC Probleme habe?

Die IT-Hotline Ihres Arbeitgebers, sofern es sich eindeutig um Probleme in Zusammenhang mit dem Zugriff auf die Firmen-Infrastruktur handelt.

Bildquelle: AdobeStock_347366618

netcos GmbH – Ihr Managed Services IT-Dienstleister München

Als IT-Dienstleister sorgen wir dafür, dass unsere Kunden ihre IT störungsfrei und sicher nutzen können. Damit stellen wir sicher, dass sie sich darauf konzentrieren können, ihr Kerngeschäft erfolgreich zu betreiben und weiterzuentwickeln.

Dazu bieten wir professionelle IT-Beratung, zuverlässigen IT-Betrieb und schnellen Anwender-Support. Als Full-Service-Anbieter übernehmen wir auch die Betriebsverantwortung für komplette IT-Infrastrukturen im Managed Service.

Seit 2002 unterstützen wir mit einem 20-köpfigen Team branchenübergreifend sowohl lokale mittelständische Unternehmen als auch multinationale Konzerne in der Digitalen Transformation.