Tipps fürs Arbeiten im Homeoffice

Stand: 02.09.2020

Technik

1. Firmen sollten mobile Geräte mit einem modernen Standard anschaffen, die für ein effektives Arbeiten im Homeoffice geeignet sind und auch bei hypriden Arbeitsformen in der IT-Landschaft des Unternehmens genutzt werden können. Wichtige Ausstattungsmerkmale sind dabei

    a. Aktuelles Betriebssystem
    b. Großer Arbeitsspeicher und große Festplatte
    c. Kamera mit hoher Auflösung
    d. Headset
    e. Lautsprecher
    f. Displaygröße ab 15 Zoll

    Tipp: Wer auch Software für die Einrichtung der Homeoffice Arbeitsplätze im größeren Stil wie z.B. Lizenzen für eine Videokonferenzlösung, Teamsoftware, Betriebssystem, Office Anwendungen und anderes benötigt, sollte statt alles zu kaufen und in Zukunft pflegen und warten zu müssen, über eine „Workplace as a Service“-Lösung nachdenken. Also darüber, die erforderliche Hard- und Software inklusiver entsprechender Services, zum Beispiel Beratung, Installation, Versicherung etc., zu mieten. Vorteil, Sie haben im Schadensfall meistens einen schnellen Ersatz und können die Geräte regelmäßig erneuern und durch modernere ersetzen.

2. Internetanbindung an das Unternehmen über VPN („Virtual Private Network“); gute Internetverfügbarkeit am Wohnort des Mitarbeiters sicherstellen.
3. Fortlaufende IT-Sicherheit des Gerätes und der Internetverbindung! (siehe IT-Sicherheit)

    Tipp: Firmen sollten unbedingt die Hinweise des Bundesamtes für Informationssicherheit zum sicheren Arbeiten im Homeoffice beherzigen (Siehe auch Abschnitt- IT-Sicherheit): https://www.bsi.bund.de/DE/Presse/Kurzmeldungen/Meldungen/Empfehlungen_mobiles_Arbeiten_180320.html

4. Unternehmen sollten die Telefonanlage auf die Diensthandys der Beschäftigten umstellen und entsprechende Zeiten der Erreichbarkeit programmieren, die dann auch an Kunden kommuniziert werden können.
5. Einsatz eines Monitoring Tools, um das Geschehen im eigenen Firmennetzwerk im Blick zu behalten. Sollten Sie einen IT-Dienstleister für die Pflege und Administration Ihres Netzwerkes haben, sollte dies von diesem Dienstleister gewährleistet werden können.

Organisation

1. Welche Arbeitszeitmodelle will das Unternehmen für welche Mitarbeiter einführen? (z.B. 100 % Homeoffice, Hybrides Arbeitsmodell mit Präsenztagen im Unternehmen u.s.w.)
2. Ausstattung der Homeoffice Arbeitsplätze und räumliche Verhältnisse im heimischen Umfeld des Mitarbeiters, gegebenenfalls durch einen vor Ort Termin, klären! (Eigens Arbeitszimmer vorhanden, Schreibtisch und guter Bürostuhl)
3. Welche Unternehmensprozesse sind ausreichend digitalisiert und welche sollen und müssen noch digitalisiert werden, die das Arbeitsfeld des Mitarbeiters betreffen? *(Häufige Schwachstelle: Digitalisierung der Eingangspost)*
4. Was sind die konkreten Aufgabenpakete/Projekte des Beschäftigten im Homeoffice und welche Erwartungen an die Arbeitsleistung hat die Geschäftsführung?
5. Was ist in Bezug auf Datenschutz durch dezentrale Arbeit zu beachten?
6. Klare Regelungen zur Zeiterfassung, telefonischer Erreichbarkeit und Pausen treffen.

   ***Tipp**:* Denken Sie an dieser Stelle über eine flexible Zeiterfassung über verschiedene Endgeräte mit einer Zuordnung zu Projekten, Tätigkeitsfeldern und Kostenstellen nach! Ebenso kann es Sinn machen, eine flexible Platzierung der Kernarbeitszeit durch den Mitarbeiter zu erlauben, um die Vorteile des Homeoffice in Bezug auf die Vereinbarkeit von Familie und Beruf zu nutzen. Hinweise zu Möglichkeit von „bewegten" Pausen tragen zur Fitness des Mitarbeiters bei und sind Teil eines betrieblichen Gesundheitsmanagements.

7. Personalvertretung einbinden
8. Klare Vorgaben zum Auftreten und Verhalten in Video-/Telefonkonferenzen intern sowie mit Kunden/Geschäftspartnern. (Siehe auch Knigge für Videokonferenzen)
9. Regelmäßige interne Video-/Telefonkonferenzen, etwa auf Abteilungs- oder Teamebene, für Absprachen und die Beantwortung von Fragen
10. Arbeitsergebnisse und Projektfortschritte regelmäßig kontrollieren
11. Fairness gegenüber allen Mitarbeitenden
12. Loyalität zum Unternehmen sicherstellen

    Tipp: Homeoffice schafft Distanz. Sorgen Sie deshalb gerade jetzt weiterhin und vermehrt für Teamgeist und eine Verbundenheit zum Unternehmen! Verzichten Sie also nicht auf Kommunikationsformate (Präsenz oder Online) mit Ihren Mitarbeitern und seien Sie auch im Rahmen der aktuellen Corona Herausforderungen hierbei kreativ. Die Inhalte solcher Treffen sollten nicht immer einen fachlichen Bezug haben.

IT-Sicherheit

1. Das mitgebrachte Gerät Ihres Arbeitgebers bzw. den privaten Computer nie unbeaufsichtigt lassen.
2. Den Einsatz von privaten Geräten für Firmenzwecke, aufgrund der möglicherweise vertraulichen Daten die verarbeitet werden, vermeiden.
3. Lassen Sie keine weiteren Personen am Homeoffice Rechner arbeiten, um die Vertraulichkeit der Daten zu gewährleisten. Wechseln Sie regelmäßig die Zugangsdaten.
4. Führen Sie für eine sichere Einwahl ins Firmennetzwerk eine Zwei Faktor Authentifizierung ein. (Zugangsdaten + Einmalpasswort)

5. Sperren Sie den Rechner, sobald Sie den Arbeitsplatz verlassen oder fahren ihn komplett herunter. Die Tastenkombination Windows+L sperrt Ihren Rechner schnell. Bei privaten Computern darauf achten, dass
    a. das Betriebssystem aktuell ist (z.B. Windows-Updates automatisch installieren lassen)
    b. vor der Arbeit eine routinemäßige Kontrolle auf anstehende Updates erfolgt und
    c. eine Sicherheitssoftware (Antivirus, Firewall) installiert und diese aktuell ist (Updates).
6. Vorsicht beim Einsatz von externen Datenträgern (USB-Stick, ext. Festplatte): Vor der Nutzung prüfen, woher diese kommen bzw. wo/bei wem diese bisher im Einsatz waren. Empfehlung: Nutzen Sie für den „Datenaustausch“ ins Büro z.B. DGVO konforme Clouddienste oder versenden Sie Dokumente per E-Mail/Outlook (Dateigrößen beachten).
7. Geräte des Arbeitsgebers vor Anschluss und Synchronisation mit dem Firmennetzwerk auf den neusten Stand bringen/bringen lassen und alle aktuellen Updates und Patches für die verwendete Software ausführen.

8. **Tipps für sicheres WLAN**:
    a. Konfigurieren (bzw. kontrollieren) Sie den Router, bevor Sie diesen in Betrieb nehmen (insbesondere bei WLAN-Nutzung). Wie die Konfiguration gelingt, können Sie in der Betriebsanleitung des Gerätes nachlesen.
    b. Schalten sie die Möglichkeit, den Router über eine WLAN-Verbindung zu konfigurieren ab
    c. die Konfiguration sollte nach Möglichkeit nur über eine kabelgebundene Verbindung erfolgen.
    d. Konfigurieren Sie die Verschlüsselung und wählen dabei den sogenannten WPA2- Standard (wird in der Regel von allen modernen Geräten, auch Tablets und Smartphones, unterstützt).
    e. Deaktivieren Sie die Möglichkeit der Wartung via Fernzugriff in den Einstellungen Ihres Routers (falls vorhanden
    f. Ändern Sie immer so schnell wie möglich das Administrations-Passwort des Routers. Auch dies können Sie in der Betriebsanleitung des Gerätes nachlesen.
    g. Wählen Sie ein sicheres Passwort aus. Sichere Passwörter bestehen gerade für den WLAN-Zugang aus einer möglichst langen zufälligen Zeichenkette (32 Zeichen und mehr), gemischt aus Groß- und Kleinschreibung, Ziffern und Sonderzeichen.
    h. Halten Sie auch die Firmware Ihres Routers immer auf dem aktuellen Stand. Aktivieren Sie (falls vorhanden) die Möglichkeit von automatischen Updates (FirmwareUpdates des Herstellers).
    i. Schalten Sie das WLAN grundsätzlich aus, wenn es nicht gebraucht wird. Einige Router bieten die Möglichkeit, entsprechende Zeiträume zu definieren, in denen das WLAN automatisch an- beziehungsweise ausgeschaltet wird. Generelle

Empfehlung: Schalten Sie alles aus, was Sie nicht brauchen. Aktivieren Sie Funktion nach Bedarf – also temporär. Das BSI (Bundesamt für Sicherheit in der Informationstechnik) gibt weiterführende Sicherheitstipps zum privaten LAN-Einsatz sowie Sicherheitstipps zum privaten WLAN-Einsatz.