ViCoTec
IT-SICHERHEIT & DATENSCHUTZ

FAQ zum Datenschutz in mobiler Arbeit

Was ist eine Remote-Desktop-Verknüpfung?
Eine Remote-Desktop-Verknüpfung stellt eine direkte Verbindung zwischen 2 Computern her. Hierbei werden die Programme von dem Computer im Unternehmen ausgeführt, während mit dem PC von zu Hause aus auf diesen zugegriffen wird. Es wird von zu Hause aus virtuell auf dem Computer im Betrieb gearbeitet.

Was ist VoIP-Telefonie oder Cloud-Telefonie?
Bei der VoIP-Telefonie (Voice-Over-IP Telefonie) oder auch Internettelefonie ist die Sprachkommunikation über das Internet statt der gewöhnlichen ISDN-Telefonie gemeint. Dies kann sich z. B. durch ein einfaches Headset in Kombination mit einer Telefon-Software realisieren lassen. Hierdurch bietet sich somit eine einfache Möglichkeit, kostengünstig die Telefonie mit dem eigenen privaten Anschluss zu vermeiden.

Was ist ein starkes Passwort?
Sichere Passwörter bestehen in der Regel aus mindestens 10 Zeichen.
Diese sollten möglichst aus Groß- und Kleinbuchstaben, Zahlen und Sonderzeichen (z. B. $, §, !, ?, *) bestehen.
Hierbei sollte vermieden werden, dass sich nebeneinanderstehende Zeichen oder Abfolgen dieser in dem Passwort wieder finden (z. B. „qwertz“). Auch sollten Sie keine Worte aus dem Duden verwenden.
Die Nutzung eines Passwortes sollte für jede unterschiedliche Login-Kennung neu gewählt werden.
Ein Beispiel für ein sicheres Passwort wäre z. B. „O02ä’s1_Xc-t“

Was ist eine VPN-Verbindung?
Ein VPN ist ein **V**irtuelles **P**rivates **N**etzwerk, dass den Zugriff auf ein bestehendes Netzwerk (z. B. das des Unternehmens) ermöglicht. Durch dieses wird eine verschlüsselte Verbindung zwischen dem Notebook und dem Firmen-Server hergestellt, hier für bildet er eine Art „sicheren Tunnel“ zwischen dem Notebook und dem Server, sodass Daten von außen nicht abgreifbar sind.

Was ist Blurring?

Als Blurring wird das unkenntlich machen des Hintergrundes bei der Videotelefonie bezeichnet. Somit lässt sich im Videochat nur der jeweilige Mitarbeiter ohne Details im Hintergrund erkennen. Dies dient unter anderem dazu, Rückschlüsse auf Persönlichkeitsmerkmale anhand von Einrichtungsgegenständen zu erschweren.

Wie richte ich eine Desktopsperre ein?

Windows 10:

Zunächst muss die Einstellung aktiviert werden. Dies ist möglich, in dem Sie die „Windows-Taste“ drücken, anschließend wählen Sie „Einstellungen“ aus. Nun wählen Sie den Menüpunkt „Personalisierung“ und klicken „Einstellungen für den Bildschirmschoner“ an. In dem sich öffnenden Fenster aktivieren Sie „Anmeldeseite bei Reaktivierung“ und übernehmen dies.

Ab jetzt wird nach der von Ihnen angegebenen Zeit der Desktop ohne Tätigkeit automatisch gesperrt.

Was ist eine sichere Videokonferenzplattform?

Um die Verbindung während eines digitalen Meetings sicher zu gestalten, sollte die Videokonferenzplattform auf der Anmeldeseite das HTTPS-Protokoll verwenden und während der Konferenz „Ende-zu-Ende“ verschlüsselt zu sein (dies erkennen Sie an dem kleinen Schloss neben der URL). Weiterhin muss die Plattform eine Form der Indikation bei Nutzung der Kamera und des Mikrofons bieten, um das Ausspähen von Personen zu verhindern.

Zusätzlich muss eine Möglichkeit gegeben sein, sich jederzeit eine Liste aller Teilnehmenden anzeigen zu lassen sowie die Möglichkeit auf einen Hinweis bei Eintreten eines neuen Nutzers. Falls eine Funktion zur Aufnahme besteht, muss dies bei Aktivität allen Teilnehmenden angezeigt werden. Abschließend muss beim Teilen von Bildschirminhalten (Screensharing) die Möglichkeit zum Treffen einer Auswahl der zu teilenden Inhalte vorhanden sein (z. B. die Auswahl nur bestimmter Fenster).

Weiterführende Informationen finden Sie auf der Website des BSI (Bundesamt für Sicherheit in der Informationstechnik).

Was ist 2-Faktor-Authentifizierung?

Als 2-Faktor-Authentifikation bezeichnet man einen Login-Vorgang, bei dem eine 2. Form der Authentifikation abgefragt wird. Geschehen kann dies z. B. durch ein Einmal-Passwort oder einen immer neu generierten TAN. Bekannt sein dürfte Ihnen das Verfahren aus ihrem Online-Banking, wo Sie sich mit einer Kombination aus Passwort und generiertem TAN einloggen.
Die Sicherheit in diesem Login-Verfahren liegt darin, dass es nahezu unmöglich für den Angreifer ist, beide Authentifikationen zu besitzen.

Wie finde ich einen sicheren Cloud-Anbieter?

Einen konkreten Cloud-Anbieter können wir hier leider nicht nennen, jedoch einige Hinweise geben, anhand derer ein ausreichend sicherer Cloud-Anbieter identifiziert werden kann.
Handelt es sich um einen Cloud-Anbieter mit guter Reputation?
Bietet der Cloud-Anbieter eine Ende-zu-Ende-Verschlüsselung?
Bietet der Cloud-Anbieter die Möglichkeit zur 2-Faktor-Authentifikation?
Ist der Serverstandort innerhalb der EU oder sogar in Deutschland?
Ist der Cloud-Anbieter gewillt, einen Auftragsverarbeitungsvertrag abzuschließen?
Besteht ein Lösch- und Backup-Konzept durch den Cloud-Anbieter?
Weitere Informationen erhalten Sie auf der Website des BSI (Bundesamt für Sicherheit in der Informationstechnik).

Wie sichere ich mein WLAN?

Um das hauseigene WLAN entsprechend dem aktuellen Stand der Technik zu sichern, reicht es aus für das Funknetz den Verschlüsselungsstandard „WPA2“ (Wi-Fi-Protected-Access 2) zu nutzen. Alternativ ist das Arbeitsnotebook direkt mit einem LAN-Kabel mit dem Router zu verbinden.
Wie genau Sie Ihren persönlichen Router vor Ort konfigurieren, entnehmen Sie am besten dem beigelegten Handbuch.

Wie vernichte ich Daten datenschutzkonform?

Die einfachste Methode ist, dienstliche Dokumente in Papierform über den Betrieb zu entsorgen, da dieser einen dafür vorgesehenen Aktenvernichter nach DIN 66399 Standard im Betrieb hat. Alternativ können Sie auch zu Hause, nach Absprache mit dem DSB sowie der Geschäftsführung, einen entsprechenden Aktenvernichter zu Hause in Betrieb nehmen.