Datenschutz beim mobilen Arbeiten und im Home Office

Unna, 23. März 2020

Auf Grund der aktuellen Rahmenbedingungen arbeiten zur Zeit sehr viel mehr Menschen mobil oder im Home Office als normalerweise. Im Folgenden finden Sie wichtige Tipps, wie Sie personenbezogene und andere vertrauliche Unternehmensdaten vor fremdem Zugriff sichern können, wenn Sie außerhalb des normalen Büros arbeiten. Weitere Informationen zum Thema „Home Office“ finden Sie auch auf der Website von K&K Networks, u.a. den umfassenden „Home-Office-Guide“ des Fachmagazins t3n.

1. Geräte

- Achten Sie darauf, dass mobile Geräte wie Smartphones, Tablets, Notebooks, USB-Sticks oder mobile Festplatten nicht verloren gehen
- Stellen Sie sicher, dass alle Geräte mit den neuesten Updates ausgestattet sind. Dies gilt für das Betriebssystem (z.B. Windows, MacOS, iOS oder Android) ebenso wie für Anwendungs- und Antiviren-Software. Vor allem auch, wenn Sie private Geräte für die Datenverarbeitung nutzen müssen.
- Sollten Sie private Geräte zur Verarbeitung personenbezogener Daten oder anderer vertraulicher Daten Ihres Unternehmens nutzen müssen, achten Sie bitte darauf, dass diese Daten vor unautorisiertem Zugriff durch andere Personen in Ihrem Haushalt geschützt sind. Verwenden Sie für Ihren Zugang zwingend einen persönlichen Login mit einem Passwort, das nur Ihnen bekannt ist. Das gilt auch für Ihr Smartphone, wenn Sie dort z.B. dienstliche E-Mails empfangen.
- Behalten Sie Ihre mobilen Geräte und Speichereinheiten stets im Auge. Achten Sie darauf, dass niemand anderes Ihren Bildschirm einsehen kann, insbesondere wenn Sie personenbezogene oder andere vertrauliche Unternehmensdaten bearbeiten.
- Sperren Sie Ihr Gerät, wenn Sie es unbeaufsichtigt lassen müssen, z.B. in Pausenzeiten.
- Stellen Sie sicher, dass Ihre Geräte ausgeschaltet, gesperrt und/oder sorgfältig gespeichert sind, wenn Sie sie gerade nicht nutzen.
- Nutzen Sie wirksame Zugriffskontrollen wie z.B. sichere Kennwörter oder Zwei-Faktor-Authentifizierung
- Nutzen Sie - soweit verfügbar – Verschlüsselungsmöglichkeiten, um den Zugriff auf Ihre Geräte einzuschränken und die Risiken bei Verlust oder Diebstahl der Geräte deutlich zu verringern. Viele einfache Verschlüsselungstools sind kostenlos verfügbar.
- Wenn ein Gerät verloren gegangen ist oder gestohlen wurde, sollten Sie sofort versuchen, eine Löschung der Geräte „aus der Ferne“ anzustoßen, soweit dies möglich ist.

2. E-Mails

- Beachten Sie alle geltenden Richtlinien in Ihrem Unternehmen zur Verwendung von E-Mails.
- Verwenden Sie für dienstliche E-Mails mit personenbezogenen oder anderen vertraulichen Unternehmensdaten soweit möglich ausschließlich Ihre dienstliche E-Mail-Adresse. Bitten Sie Ihre IT-Administration bei Bedarf, Ihnen einen mobilen Zugriff auf Ihr E-Mail-Konto einzurichten.
- Wenn Sie dennoch Ihre persönliche E-Mail-Adresse für dienstliche Belange verwenden müssen, versenden Sie vertrauliche Inhalte und Anhänge bitte nur verschlüsselt und vermeiden Sie die Verwendung persönlicher oder vertraulicher Daten in Betreffzeilen. Fragen Sie bei Bedarf bei Ihrer IT-Administration nach, welche einfachen Verschlüsselungsmöglichkeiten Sie nutzen können (z.B. verschlüsselte ZIP-Archive oder PDF-Dateien).
- Stellen Sie vor dem Versand einer E-Mail sicher, dass Sie diese auch wirklich an die richtigen Empfänger senden, insbesondere bei E-Mails mit großen Mengen personenbezogener oder anderer vertraulicher Daten.

3. Cloud- und Netzwerkzugriff

- Verwenden Sie nach Möglichkeit nur die offiziellen Netzwerkzugänge (per VPN) und/oder offizielle Cloud-Dienste Ihres Unternehmens und halten Sie die organisatorischen Regeln in Bezug auf Cloud- oder Netzwerkzugriff, Anmeldung und gemeinsame Nutzung von Daten ein.
- Wenn Sie ohne Cloud- oder Netzwerkzugriff arbeiten, stellen Sie sicher, dass lokal gespeicherte Daten ausreichend gesichert sind. Sorgen Sie in diesem Falle auch für tägliche Sicherungskopien, damit die Ergebnisse Ihrer Arbeit nicht verlorengehen.

4. Unterlagen in Papierform

- Bitte denken Sie daran, dass Datenschutz und Datensicherheit nicht nur für elektronisch gespeicherte oder verarbeitete Daten gelten, sondern auch für personenbezogene oder andere vertrauliche Daten in Papierform.
- Wenn Sie unterwegs oder im Home-Office mit Papierunterlagen arbeiten, gewährleisten Sie bitte die Sicherheit und Vertraulichkeit dieser Unterlagen. Bewahren Sie die Unterlagen in einem abgeschlossenen Aktenschrank oder einer abgeschlossenen Schublade auf, wenn Sie diese nicht verwenden. Lassen Sie vertrauliche Unterlagen nirgendwo offen herumliegen. So vermeiden Sie, Einsichtnahme in diese Unterlagen oder gar deren Diebstahl. Sorgen Sie für eine sichere Entsorgung/ Vernichtung von vertraulichen Papierunterlagen, wenn Sie diese nicht mehr benötigen (z.B. durch Verwendung eines Aktenvernichters).
- Wenn Sie Unterlagen unterwegs oder im Home-Office bearbeiten, die „besondere Kategorien personenbezogener Daten“ gemäß DS-GVO Art. 9 (z.B. Gesundheitsdaten) enthalten, achten Sie bitte ganz besonders darauf, deren Vertraulichkeit zu gewährleisten. Nehmen Sie diese nur mit ins Home-Office, wenn dies unbedingt erforderlich ist.
- Notieren Sie sich sicherheitshalber, welche Aufzeichnungen Sie mit nach Hause genommen haben, um diesbezüglich einen guten Überblick zu bewahren.

5. Wenn doch einmal etwas schiefgeht: Umgang mit Datenpannen

- Sollte trotz aller Vorsichtsmaßnahmen doch einmal etwas schiefgegangen sein und sind personenbezogene oder andere vertrauliche Daten des Unternehmens offengelegt oder verlorengegangen, informieren Sie bitte ***umgehend*** Ihre Geschäftsführung und/oder Ihre IT-Administration und/oder Ihren Datenschutzbeauftragten! Diese werden dann mit Ihnen gemeinsam die erforderlichen Schritte einleiten.