Datensicher im mobilen Büro

Ob gezwungenermaßen durch die Corona-Pandemie oder ob es seit jeher zur Geschäftstätigkeit zählt. Das Arbeiten im Homeoffice hält viele rechtliche Herausforderungen parat. Allen voran die Tücken des Datenschutzes. Wie sich diese erkennen und beheben lassen.

Von ACHIM BARTH

Was andere Branchen seit den Corona-Lockdowns akut umtreibt, betrifft viele Unternehmen in der Finanzbranche schon seit Langem: Viele Vermittler, Makler, Berater und Co. arbeiten seit jeher flexibel im Büro, von zu Hause aus oder unterwegs in Zug und Hotel. Was sie mit den vielen frisch gebackenen Homeoffice-Anhängern gemein haben, ist jedoch die oft mangelnde Sorgfalt beim Thema Datenschutz. Da das mobile Office aus der Arbeitswelt nicht mehr wegzudenken ist, wirft dieser Trend auch für Finanzprofis neue Fragen und Sicherheitslücken auf. Denn natürlich müssen Unternehmer, Mitarbeiter und Chefs auch im Büro unter freiem Himmel zu jeder Zeit die DSGVO einhalten.

Ob groß oder klein – viele Betriebe kämpfen ja schon bei der statischen Büro-IT mit dem Thema Datenschutz. Diese Sicherheit auch für jeden mobilen Arbeitsplatz – für alle Laptops, Smartphones, Tablets – und jede technische Arbeitssituation zu gewährleisten, stellt Verantwortliche vor große Herausforderungen. Dabei steigt die Gefahr für Fehler und Cyberattacken im Homeoffice. Wird die Arbeit in eine vertraute Umgebung verlagert, schleicht sich schnell eine gewisse Sorglosigkeit ein. Die Fragen häufen sich: Worauf kommt es beim Datenschutz im mobilen Modus an? Was müssen Finanzvermittler unterwegs beachten? Weil Google selten klare Antworten ausspuckt, geben folgende Infos einen Überblick.

Schutz vor Hackern und neugierigen Blicken

Das A und O vorab: Wer im Homeoffice und unterwegs mit Kundendaten jongliert oder Mitarbeitern Remote Work ermöglicht, muss sicherstellen, dass kein Unberechtigter betriebliche und personenbezogene Informationen zu Gesicht bekommt. Was im Büro eine schlichte Einlasskontrolle garantiert, erweist sich in den heimischen vier Wänden oder in der Bahn als komplizierter. Zu Hause bewegen sich Familienmitglieder und Besucher, im Park unbekannte Dritte. Allen muss gleichermaßen der Zugriff zu jeder Zeit verwehrt werden.

Autor **Achim Barth** ist digitaler Aufklärer und kennt die Gefahren der Datenspinne, die Tricks der Datenräuber, aber auch zuverlässige Wege, wie jeder seine Privatsphäre im Netz schützen kann. Er ist einer der kompetentesten Ansprechpartner rund um den Schutz personenbezogener Daten. Zielgerichtet, sachkundig und immer up to date begleitet der mehrfach zertifizierte Datenschutzbeauftragte Privatleute und Unternehmen in die IT-Sicherheit. In Workshops, Seminaren und Vorträgen begeistert der Gründer von „Barth Datenschutz" mit praktikablen Lösungen. Sein Fachwissen vermittelt er eingängig und unterhaltsam – sodass sowohl Unerfahrene als auch Technikfans vom Mehrwert und Wettbewerbsvorteil seines Know-hows profitieren. http://www.barth-datenschutz.de/

FOTO: BARTH

Gleichzeitig sollten Finanzberater privat und beruflich mit unterschiedlicher Hardware arbeiten. Arbeitgeber stellen ihren Mitarbeitern eingerichtete Laptops, Smartphones und Co. zur Verfügung. Das verbessert die Kompatibilität und den hochwertigen Datenschutz. Natürlich gilt für alle bei Firmengeräten besondere Vorsicht vor Verlust. Um Diebstählen vorzubeugen, können Nutzer Notebooks und Dockingstations zum Beispiel mit Kabelschlössern sichern.

Gleichzeitig erweist es sich als schlechte Idee, Unternehmens-Notebooks an Freunde auszuleihen oder das geschäftliche Zoomkonto für private Surfeinheiten zu nutzen. Betriebliche Geräte sind fürs Business gedacht. Auch andersherum wird es kritisch: Wer mit dem Familienlaptop geschäftlich arbeiten will, braucht eine Sondergenehmigung von Chef oder IT-Abteilung. Nur in Ausnahmefällen – wie spontanen Quarantänephasen – und nach dem Go von oben dürfen Mitarbeiter für Firmenaktivitäten zu privater Hard- und Software wie Notebooks, USB-Sticks, Speicherkarten oder mobilen Laufwerken greifen. In diesem Fall brauchen Anwender klare Vorgaben, für welche betrieblichen Zwecke der eigene Laptop zum Einsatz kommen darf.

Verhalten auf Reisen

Auch unterwegs – im Zug oder beim Sicherheitscheck am Flughafen – dürfen Außendienstler Notebooks und sonstige Datenträger nicht ohne Aufsicht lassen. Die Geräte müssen ins Handgepäck. Im Auto ist Hardware nach Möglichkeit im Kofferraum mit einem Kabelschloss an der Karosserie befestigt. Im Hotel sollten Reisende mobile Geräte möglichst mitführen oder im Hoteltresor einschließen, Zimmertresore sind häufig zu unsicher. Bei Auslandsreisen erhöhen sich Risiken, Vorkehrungen und Auflagen noch.

Wer mobil aktiv ist, muss zudem aufpassen, dass Fremde vertrauliche Telefonate nicht mithören können – ob auf der Parkbank oder am Küchentisch. Diskretion bleibt oberstes Gebot. Wer tippt, wo andere von der Seite „mitgucken" können, den schützen Sichtschutzfolien vor neugierigen Blicken. In Bus, Tram und Bahn dürfen Aktive überhaupt keine personenbezogenen oder sonstigen sensiblen Daten verarbeiten. Auf Reisen erfasste Daten sichern Nutzer über geschützte Verbindungen auf den zentralen Systemen oder verschlüsselten Sicherungsdatenträgern – letztere sind getrennt vom Notebook aufzubewahren.

Drucken, speichern, schreddern

USB-Sticks und Co. stellen sowieso ein besonders Risiko dar. Durch leichtsinnigen Umgang besteht die Gefahr, dass Schad- oder Spionagesoftware eingeschleppt wird und „händisch" von einem Gerät zum nächsten wandert. Wechseldatenträger können extrem leicht ausspioniert werden. Um die Vertraulichkeit von Unternehmensdaten nicht zu gefährden, muss der sicherer Umgang mit ihnen daher klar geregelt sein.

Auch händische Unterlagen unterliegen der DSGVO. Ob im Homeoffice oder in der Bibliothek: Ausdrucke sollten nicht im Drucker liegen bleiben, damit weder Familienmitglieder, Freunde oder Fremde Zugriff haben. Enthalten die Papiere personenbezogene Daten, dürfen sie auch nicht einfach in den Hausmüll. Je nach Schutzgrad der Daten wird das schnell zum meldepflichtigen Vorfall. Auch in mobilen Büros müssen Berater heikle Unterlagen datenschutzkonform schreddern. Das gilt ebenso für handschriftliche Notizen. Ein Schredder gehört somit fest zur Homeoffice-Ausrüstung.

Digitale Türsteher

Dreh- und Angelpunkt beim Remote Office bleibt natürlich die technische Ausstattung. Nötig ist eine wasserdichte Verbindung von Firmenlaptop zu Büroserver. Um sich vor Angriffen zu schützen, geht nichts ohne VPN-Tunnel. Ein VPN-Client (Virtual Private Network) verschlüsselt die Datenvermittlung vom Server auf den Arbeitslaptop. Daten werden so nur geschützt übertragen, unabhängig von einer sicheren Internetverbindung. Durch die Verschlüsselung werden die Daten für Angriffe während der Übertragung nutzlos.

Zur sicheren IT gehören zudem Firewalls und Anti-Viren-Programme. Lokale Sicherheitssoftware schützt Geräte so auch von externen Standorten aus. Bei klassischen Büroarbeiten reichen die Windows-Angebote in der Regel aus. Trotzdem sollte ein IT-Profi die Software freigeben, installieren und pflegen. Systeme helfen nur, wenn sie richtig konfiguriert und aktuell sind. Nutzer sollten Updates und Patches zeitnah einspielen und alte Systeme zügig löschen.

DSGVO-konform sind Notebooks, Smartphones, Festplatten und einzelne Programme aber erst, wenn sie passwortgeschützt sind. Empfehlenswert sind Kombinationen aus acht bis zwölf Sonderzeichen („l5o4§p6!h9Mn") oder einem kurzen Satz über 20 Zeichen („MeinLiebstesEssenistPizza"). Ist das Passwort ausreichend lang und klebt nicht am Laptoprand, muss es auch nicht regelmäßig gewechselt werden. Auch bei Webmeetings und Videocalls kann Passwortschutz hilfreich sein.

Mitarbeiter sensibilisieren – Risiken aufzeigen

Auch wenn manchem erfahrenen Außendienstler diese Maßnahmen mühselig, übertrieben oder arbeitsintensiv erscheinen: Finanzberater sollten Datenschutz im mobilen Büro nicht als Schikane, sondern als Hilfsmittel betrachten. Schließlich geht es um Firmengeheimnisse, um die Privatsphäre des Unternehmers selbst und besonders um die Sicherheit sensibler Kundendaten. Wird etwas davon beschädigt, kann dieser Vertrauensverlust das Geschäft zerstören – neben möglichen Bußgeldern.

Unternehmer sollten die Sicherheit in ihren mobilen Büros gut unter die Lupe nehmen. Denn Verantwortlicher bleibt immer der Unternehmer. Daran ändert sich auch nichts, wenn Hotels schwache Internetverbindungen liefern oder beim Mitarbeiter die Kinder toben. Kommt es zu einer Datenpanne, ist es egal, wer Adressen transparent gemacht hat, warum unbeabsichtigt Vertragsdaten offengelegt oder wie Smartphones verloren wurden – verantwortlich bleibt der Inhaber, Geschäftsführer oder Vorstand.

Daher ist es unerlässlich, das ganze Team zu sensibilisieren, zu jeder Zeit achtsam mit Unternehmensdaten umzugehen. Wenn Verantwortliche diese Maßnahmen ernst nehmen, steht der Informations- und IT-Sicherheit eines mobilen Arbeitsplatzes nichts im Wege. Und nur wenn Daten im mobilen Büro gleichermaßen geschützt sind wie innerhalb des Firmengebäudes, ist Homeoffice ein sicheres Zukunftsmodell. **C.**