



Leitfaden:

Sicher arbeiten im Homeoffice und von unterwegs

Arbeiten außerhalb des Büros gehört heute für viele zum Alltag. Damit das sicher funktioniert, kommt es nicht nur auf die Technik an – sondern auch auf das Verhalten jedes Einzelnen.

Dieser Leitfaden hilft Ihnen dabei, typische Risiken zu erkennen und einfache Schutzmaßnahmen im Alltag umzusetzen.

1. Warum ist dieses Thema wichtig

Arbeiten von zu Hause oder unterwegs gehört für viele inzwischen zum Alltag. Das bietet viel Flexibilität – bringt aber auch neue Herausforderungen mit sich.

Im Büro sorgt meist die IT-Abteilung für eine sichere Umgebung. Außerhalb des Büros ist das etwas anders: **Hier kommt es stärker auf das eigene Verhalten an.**

Die gute Nachricht:

Hinweis: Schon mit wenigen, einfachen Methoden und Maßnahmen können Sie einen großen Beitrag zur Sicherheit leisten.

»»» Dieser Leitfaden zeigt Ihnen, worauf es im Alltag ankommt – kurz, verständlich und direkt umsetzbar.

2. Die wichtigsten Grundregeln auf einen Blick

Wenn Sie sich nur ein paar Dinge merken möchten, dann diese:

- Nutzen Sie nur durch Ihr Unternehmen freigegebene Geräte und Programme
- Seien Sie **vorsichtig bei E-Mails und Nachrichten**. Klicken Sie bei verdächtigen E-Mails nicht auf Links und öffnen Sie keine Anhänge.
- Schützen Sie Ihr Gerät und Ihre Zugangsdaten
- Achten Sie darauf, wer **mitsehen und mithören kann**
- Im Zweifel gilt immer: **lieber nachfragen als riskieren**

3. Sicher verbunden – Internet und Zugriff

Wenn Sie außerhalb des Büros arbeiten, nutzen Sie oft andere Netzwerke als gewohnt. Diese sind nicht immer gleich gut geschützt.

Achten Sie deshalb auf ein paar einfache Dinge:

- Nutzen Sie **bekannte und vertrauenswürdige WLAN-Netzwerke** (z. B. zuhause)
- Öffentliche WLANs (z. B. im Café oder Hotel) sind oft weniger sicher
- **Deaktivieren** Sie die automatische Verbindung zu offenen WLANs
- Nutzen Sie – wenn möglich – ein **VPN**, um Ihre Verbindung zu schützen
- Alternativ können Sie Ihr Smartphone als **Hotspot** verwenden
- Achten Sie beim Surfen auf das **Schloss-Symbol** (https) im Browser
- Halten Sie Ihr Gerät durch **regelmäßige Updates aktuell**
- Prüfen Sie, dass Ihre **Firewall aktiviert** ist

Die Firewall des Routers aktivieren? Wie macht man das denn?

Einen einheitlichen Weg gibt es leider nicht. Online finden Sie Anleitungen für Ihren Router. Das Grundprinzip ist allerdings oft gleich.

1. **Router-Oberfläche öffnen** (z.B. in den Browser 192.168.0.1 eingeben)
2. **Anmelden** (Passwort steht meistens auf dem Gerät)
3. **Sicherheitsbereich** oder direkt **Firewall** suchen
4. **Firewall prüfen**

Gut zu wissen: In den meisten Fällen ist die Firewall automatisch aktiviert

4. Sicher kommunizieren & zusammenarbeiten

Ein großer Teil der Arbeit findet heute digital statt – in Meetings, Chats oder beim Austausch von Dateien. Gerade hier ist Aufmerksamkeit wichtig.

Achten Sie auf folgende Punkte:

- Treten Sie Meetings bewusst bei – **prüfen Sie, ob Ihre Umgebung geeignet ist**
- Teilen Sie Ihren Bildschirm nur gezielt und schließen Sie unnötige Fenster
- Achten Sie darauf, **was im Hintergrund sichtbar ist**
- Versenden Sie Dateien nur über **freigegebene Programme und Wege** (E-Mail, oder eine sichere Cloud)
- Prüfen Sie vor dem Versand, ob **die richtigen Empfänger ausgewählt sind**
- Teilen Sie nur die Informationen, die wirklich notwendig sind

Tipp: Fragen Sie sich kurz: "Wer kann das sehen – und ist das so gewollt?"

5. Geräte und Zugänge schützen

Ihr Arbeitsgerät ist ein wichtiger Zugang zu Unternehmensdaten. Entsprechend sorgfältig sollten Sie damit umgehen.

Sperrern Sie Ihr Gerät immer, wenn Sie es verlassen – auch für kurze Zeit. Lassen Sie es nicht unbeaufsichtigt in der Öffentlichkeit oder im Auto zurück.

Auch Ihre Zugangsdaten spielen eine wichtige Rolle: Verwenden Sie für **jeden Dienst ein eigenes, möglichst komplexes Passwort**. Wenn möglich, nutzen Sie einen Passwort-Manager.

Zusätzlich sollten Sie die **Multi-Faktor-Authentifizierung (MFA)** aktivieren. Dabei wird neben dem Passwort ein weiterer Code abgefragt – so bleibt Ihr Konto auch bei gestohlenen Passwörtern geschützt.

Hinweis: Ihr Gerät und Ihre Zugangsdaten sind Ihr Schlüssel zum Unternehmen – gehen Sie entsprechend sorgfältig damit um.

Wichtiger Schutz im Homeoffice: Multi-Faktor-Authentifizierung (MFA)

Wenn Sie außerhalb des Unternehmensnetzwerks arbeiten, fehlt oft ein Teil der gewohnten IT-Sicherheit. **MFA** sorgt dafür, dass Ihre Konten trotzdem gut geschützt bleiben.

Selbst wenn ein Passwort in falsche Hände gerät, kann sich niemand ohne den zweiten Faktor (z.B. Ihr Smartphone) anmelden.

Darauf sollten Sie achten:

- Bestätigen Sie nur Anmeldungen, die Sie selbst gestartet haben
- Geben Sie niemals Codes oder Freigaben weiter
- Schützen Sie Ihr Smartphone genauso wie Ihren Laptop

Hinweis: Wenn Sie unsicher sind, welche MFA-Methode im Unternehmen genutzt wird oder wie Sie diese einrichten, wenden Sie sich an Ihre IT-Abteilung. Die sicherste Lösung ist immer die, die im Unternehmen abgestimmt und freigegeben ist.

6. Sicher arbeiten im Alltag abseits des Büros

Ob im Café, im Zug oder auf dem Balkon: Beim Arbeiten außerhalb des Büros ist man oft nicht allein.

Ein kurzer Blick über die Schulter, ein mitgehörtes Telefonat oder ein offener Bildschirm – und schon können Informationen ungewollt nach außen gelangen.

Achten Sie deshalb auf Ihr Umfeld:

- **Vermeiden Sie vertrauliche** Gespräche in der Öffentlichkeit
- **Nutzen Sie Kopfhörer** bei Telefonaten und Meetings
- Achten Sie darauf, wer Ihren Bildschirm sehen kann
- **Sperren Sie Ihren Bildschirm**, wenn Sie Ihren Platz verlassen
- Nutzen Sie bei Bedarf eine **Sichtschutzfolie**

Tipp: Wenn Sie sich unsicher sind, ob eine Situation geeignet ist, warten Sie lieber oder wechseln Sie den Ort.

7. Private Geräte & Schatten-IT

Nicht jede praktische Lösung ist auch eine sichere.

Wenn Programme, Apps oder Geräte ohne Abstimmung mit der Unternehmens-IT genutzt werden, spricht man von „**Schatten-IT**“. Dabei entsteht quasi eine parallele IT-Struktur neben der eigentlichen IT-Abteilung – jedoch ohne deren Betreuung und Sicherheitsprüfung.

Das kann dazu führen, dass:

- Daten **unkontrolliert** weitergegeben werden
- Sicherheitslücken **unentdeckt** bleiben
- Datenschutzvorgaben **verletzt** werden

Deshalb gilt:

- Nutzen Sie möglichst nur **freigegebene Geräte und Programme**
- Verwenden Sie private Geräte nur mit ausdrücklicher **Genehmigung**
- Speichern Sie keine Firmendaten auf privaten Geräten
- Fragen Sie im Zweifel bei Ihrer IT nach

Hinweis: Praktisch ist nicht immer sicher – abgestimmte Lösungen sind der bessere Weg.

8. Warum ist eine Schatten-IT so gefährlich?

+ **Sicherheit** (geprüfte Tools, aktueller Schutz, sichere Datenverarbeitung)

+ **Datenschutz** (Einhaltung gesetzlicher Vorgaben)

+ **Support** (IT kann helfen)

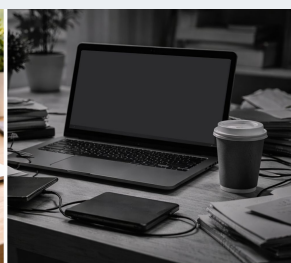
+ **Zusammenarbeit** (Alle arbeiten mit denselben Lösungen)

+ **Kostenkontrolle**

Unternehmens-IT



Schatten-IT



- **Sicherheitslücken** (Ungeprüfte Dienste, veraltete Systeme, unsichere Datenverarbeitung)

- **Datenunsicherheit** (Daten liegen in fremden Händen)

- **Kein Support** (IT kann nicht helfen)

- **Komplikationen & Mehraufwand** (Daten verstreut, nicht integrierbar)

- **Versteckte Kosten** (Doppelte Tools, unklare Lizenzen)

9. Phishing, Social Engineering & digitale Täuschung erkennen

Nicht alle Angriffe sind technisch – viele zielen darauf ab, Menschen zu täuschen.

Kriminelle versuchen z. B., sich als Kollegen oder Vorgesetzte auszugeben, um an Informationen oder Geld zu gelangen. Ein bekanntes Beispiel ist der sogenannte **CEO-Fraud**.

Dabei geben sich Angreifer als Führungskräfte aus und fordern zu dringenden Handlungen auf – etwa eine Überweisung oder die Weitergabe von Daten.

Typische Warnsignale

- Unerwartete oder dringende Anfragen
- **Nicht vertraute** Prozesse oder Kommunikationswege
- **Druck** („bitte sofort erledigen“)
- **Ungewöhnlicher** Schreibstil oder **unbekannte** Absender
- **Aufforderungen** zur Weitergabe von Daten oder Geld

So reagieren Sie richtig:

- Nehmen Sie sich einen Moment **Zeit** – nicht unter Druck handeln
- **Prüfen** Sie den Absender genau
- **Klicken** Sie **nicht** unüberlegt auf Links oder Anhänge
- **Bestätigen** Sie ungewöhnliche Anfragen über einen **zweiten Weg**
- **Informieren** Sie im Zweifel Ihre IT

Hinweis: Wenn etwas ungewöhnlich wirkt, lieber prüfen als sofort handeln.

10. Wenn etwas passiert: richtig reagieren

Trotz aller Vorsicht kann immer etwas passieren – zum Beispiel ein falscher Klick oder ein verlorenes Gerät.

Wichtig ist dann vor allem eines: Schnell reagieren.

- Melden Sie Vorfälle sofort an Ihre IT-Abteilung
- Versuchen Sie nicht, das Problem selbst zu lösen
- Haben Sie keine Sorge, etwas falsch gemacht zu haben

Hinweis: Schnelles Melden hilft, Schaden zu vermeiden.

11. Für IT- und Führungskräfte

Sicherheit funktioniert nur, wenn klare Regeln bestehen.

Mitarbeitende können sich nur dann sicher verhalten, wenn sie wissen, was erlaubt ist und worauf sie achten sollen. Unternehmen und Führungskräfte tragen daher die Verantwortung, klare Vorgaben zu schaffen.

Dazu gehören unter anderem:

- Regeln für Passwörter und MFA festlegen
- Updates und Sicherheitsmaßnahmen sicherstellen
- Freigegebene Tools und KI-Nutzung definieren
- Umgang mit privaten Geräten regeln
- Sichere Zugänge bereitstellen
- Klare Prozesse für Kommunikation und Freigaben schaffen
- Mitarbeitende regelmäßig informieren und sensibilisieren

Hinweis: Ziel ist es, Orientierung zu geben und sicheres Verhalten im Alltag zu ermöglichen.

12. KI im Unternehmen: Warum klare Regeln wichtig sind

KI-Tools bieten große Chancen für Effizienz und Produktivität. Gleichzeitig bringen sie neue Risiken mit sich – insbesondere beim Umgang mit sensiblen Daten.

Ohne klare Vorgaben entscheiden Mitarbeitende oft selbst, welche Tools sie nutzen und welche Informationen sie eingeben. **So entsteht schnell ein Kontrollverlust über Unternehmensdaten.**

Darauf kommt es an:

- Festlegen, welche KI-Tools genutzt werden dürfen
- Klare Regeln für den Umgang mit sensiblen und personenbezogenen Daten
- Transparenz schaffen: Was ist erlaubt – und was nicht?
- Mitarbeitende sensibilisieren und unterstützen

Hinweis: Nur mit klaren Richtlinien können Unternehmen die Vorteile von KI nutzen und gleichzeitig Risiken vermeiden. Zudem verpflichtet der AI Act Unternehmen dazu, Mitarbeitende im Umgang mit KI-Systemen angemessen zu schulen.

Impressum

Perseus Technologies GmbH
Hagelberger Straße 53-54
10965 Berlin

Telefon: +49 (30) 959998080
E-Mail: info@perseus.de

Geschäftsführer: Sören Brokamp

Handelsregister: Amtsgericht Charlottenburg HRB 180356 B
USt.-Ident-Nr.: DE308271739

Verantwortlicher gem. § 55 Abs. 2 RStV: Sören Brokamp

Besuchen Sie uns auf: www.perseus.de