BEDROHUNGS-BIBLIOTHEK

JULITH GmbH
Awareness-as-a-Service

Remote-Arbeit & Reisen — wenn das Büro überall ist

Home-Office, Coworking, Flughafen-Lounge — jeder Ort hat eigene Risiken. Wir geben konkrete Routinen für Reisen, Public Wi-Fi, Konferenz-Räume und Heimnetzwerke.

min Lesezeit: 7 min **Aktualisiert:** 14. März 2026 **Risiko:** Mittleres Risiko
Quelle: awareness-as-a-service.com/de/resources/threats/remote-travel

Was bedeuten Remote-Arbeit & Reisen für die Sicherheit?

Die Verbreitung von Remote-Arbeit hat den Sicherheitsperimeter endgültig aufgelöst. Das Unternehmensnetzwerk endet nicht mehr am Patch-Panel im Serverraum, sondern reicht in jede Wohnung, jeden Coworking-Space und jeden Flughafen-Lounge-Sessel. Damit entstehen Angriffsflächen, die im klassischen Bürobetrieb nicht existierten.

Drei Probleme stehen im Vordergrund: **Unsichere Netzwerke** (öffentliches WLAN ohne Verschlüsselung oder mit gefälschtem Hotspot), **physische Exposition** (Shoulder Surfing, Geräteverlust) und **Heimnetz-Risiken** (private Router mit veralteter Firmware, Familienmitglieder auf demselben Netzwerksegment).

Besonders bei Reisen addieren sich diese Risiken: Zeitdruck, unbekannte Umgebungen und die Versuchung, verfügbare Infrastruktur (öffentliche USB-Ladestationen, Konferenz-WLAN) ohne Prüfung zu nutzen, senken die Aufmerksamkeit. Angreifer kennen diese Muster und setzen gezielt an Flughäfen, Hotels und Konferenzen an.

Auf einen Blick

01

VPN ist kein Luxus

Ein konsequent genutztes, unternehmensweites VPN verschlüsselt den Traffic auch in unsicheren Netzwerken und verhindert, dass Angreifer in einem WLAN Daten mitlesen können.

02

Juice Jacking ist real

USB-Ladekabel an öffentlichen Stationen können Daten übertragen oder Malware installieren. USB-Datenblocker (Charge-Only-Adapter) sind eine einfache Schutzmaßnahme.

03

Sichtbarkeit ist das grösste Heimrisiko

Schulter-Surfer im Zug oder Coworking sehen vertrauliche Inhalte oft nicht durch technische Kompromittierung — sondern einfach weil der Bildschirm von der Seite lesbar ist.

Woran erkennen Sie Risiken beim Remote-Arbeiten?

Nicht-zugewiesene WLAN-Hotspots
"FreeAirportWifi" oder "Hilton_Lobby" ohne Captive Portal, die kein Hotel/Flughafen offiziell ankündigt, können Evil-Twin-Hotspots sein.

Shoulder Surfing
Jemand in Ihrer Nähe ist dauerhaft in einem für Ihre Bildschirm günstigen Winkel positioniert — oder nimmt sein Handy in Richtung Ihres Bildschirms.

USB-Ladestationen ohne Stromadapter
Stationen, die nur USB-Kabel anbieten (kein Netzstecker), übertragen möglicherweise auch Daten. Im Zweifelsfall eigenes Netzteil oder Powerbank nutzen.

Konferenz-Räume mit "Bring Your Own Cable"
HDMI- oder USB-C-Kabel, die an Konferenzraum-Displays vorinstalliert sind, können Daten exfiltrieren (sogenannte O.MG-Kabel).

Hotel-WLAN ohne Captive Portal
Ein Hotel-WLAN, das sofort verbindet und keine Authentifizierung verlangt, ist möglicherweise kein legitimes Hotel-Netz.

Verloren geglaubte Geräte
Ein kurz "verlegtes" Notebook oder Smartphone im Hotel oder auf einer Konferenz kann in dieser Zeit kompromittiert worden sein — Evil Maid-Angriff.

So schützen Sie sich

Für Mitarbeitende

- **VPN immer aktiv** in öffentlichen oder unbekannten Netzwerken — auch für E-Mail, nicht nur für Dateiserver-Zugriffe.
- **Sichtschutzfolie (Privacy Screen)** am Notebook bei Reisen: Eine kleine Investition, die Shoulder Surfing im Zug, Flugzeug und Coworking verhindert.
- **Kein USB von unbekannten Quellen:** Weder laden an fremden USB-Ports ohne Datenblocker, noch fremde USB-Sticks an eigene Geräte anschließen.
- **Konferenz-Kabel misstrauen:** Eigenes HDMI/USB-C-Kabel mitbringen für Präsentationen.
- **Gerätverlust sofort melden** — nicht erst nach der Heimkehr. Jede Stunde zählt für Remote-Wipe und Zugangssperrung.

Für Administratoren

- **Unternehmensweites VPN mit Always-on-Konfiguration** ausrollen — Nutzer sollen nicht entscheiden müssen, wann sie es aktivieren.
- **Mobile Device Management (MDM)** mit Remote-Wipe-Funktion für alle mobilen Geräte, die Unternehmensdaten enthalten.
- **Endpoint-Verschlüsselung (BitLocker, FileVault)** auf allen Geräten — Pflichtanforderung, nicht Option.
- **Reise-Notebooks für Hochrisikoländer:** Für Reisen in Länder mit erhöhtem Spionagerisiko Clean-Devices ohne sensible Daten ausgeben.
- **Split-Tunneling-Risiken verstehen:** Split-Tunneling (nur Unternehmensverkehr über VPN) erhöht Performance, aber hinterlässt privatem Traffic ungeschützt.

Echte Beispiele

FALL 01 · BERATUNGSUNTERNEHMEN · DE · Q3/2025

Ein Berater arbeitete im Zug an einem Angebot. Ein Mitreisender fotografierte mit dem Smartphone diskret den Bildschirm und konnte Kalkulationsdetails und Kundennamen lesen. Das Material tauchte kurze Zeit später in einem Gespräch des Mitbewerbers auf.

Schaden: Wettbewerbsnachteil, Kundenverhältnis beschädigt · **Erkennung:** Kundenmeldung · **Lehre:** Privacy Screen kostet CHF 30. Kein Angebot oder Vertrag auf ungeschütztem Bildschirm in öffentlichen Verkehrsmitteln bearbeiten.

FALL 02 · TECHNOLOGIE-STARTUP · CH · Q4/2025

Ein Entwickler nutzte auf einer Konferenz das "Conference_Guest"-WLAN, das ein Angreifer als Evil-Twin-Hotspot betrieb. TLS-Verbindungen wurden mit einem gefälschten Zertifikat terminiert (MITM). Zugangsdaten für ein Code-Repository wurden abgefangen.

Schaden: Repository kompromittiert, sensibler Code abgeflossen · **Erkennung:** Anomalie-Login-Alert aus fremdem Land am nächsten Tag · **Lehre:** VPN hätte den Traffic verschlüsselt, bevor er den Hotspot erreichte.

Was tun, wenn es passiert ist?

DIE ERSTEN 15 MINUTEN

1. **Gerät vom Netzwerk trennen** (WLAN aus, Mobilfunk aus), wenn ein Angriff vermutet wird.
2. **IT sofort informieren** — besonders bei Gerätverlust oder Verdacht auf Datenkompromittierung.
3. **Remote-Wipe auslösen** lassen bei verlorenem oder gestohlenem Gerät — durch IT, nicht durch den Mitarbeitenden selbst.
4. **Zugangsdaten ändern**, die auf dem Gerät gespeichert oder in der Session genutzt wurden.
5. **Timeline dokumentieren:** Welche Netzwerke wurden genutzt, wann, was wurde gemacht?
6. **Gerät vor Weiternutzung forensisch prüfen** lassen, wenn ein Evil-Maid-Angriff nicht ausgeschlossen werden kann.

Häufige Fragen

Ist HTTPS nicht genug Schutz in öffentlichem WLAN?

Meistens schon — aber nicht immer. Certificate-Pinning-Lücken, selbstsignierte Zertifikate, die Nutzer weggeklickt akzeptieren, oder DNS-Hijacking sind reale Angriffsmethoden, gegen die HTTPS allein keinen vollständigen Schutz bietet. VPN ist eine zusätzliche Schicht.

Ist Hotspot vom Diensthandy sicherer?

Deutlich sicherer als öffentliches WLAN. Ein Mobilfunk-Hotspot über das Diensthandy ist die empfohlene Alternative zu unbekannten WLAN-Netzen auf Reisen.

Was ist Juice Jacking genau?

Der Angriff nutzt USB-Verbindungen, die gleichzeitig Strom und Daten übertragen. Eine kompromittierte Ladestation kann Daten lesen oder Malware installieren. USB-Datenblocker (passthrough nur für Strom) sind eine einfache und günstige Gegenmaßnahme.

Weitere Themen

Remote-Arbeit und BYOD sind eng verknüpft — private Geräte auf Unternehmens-Netzwerken schaffen ähnliche Risiken wie ungesicherte Netzwerke auf Reisen. Passwörter und MFA werden

kritischer, wenn der Zugriff nicht mehr aus einem kontrollierten Netz erfolgt.