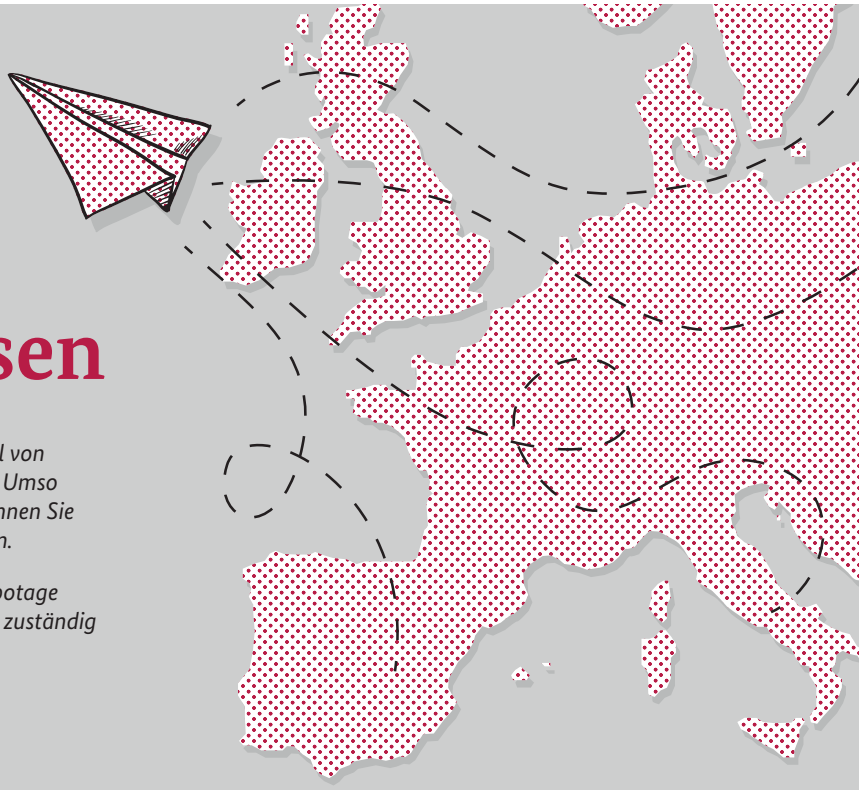
Bundesamt für Verfassungsschutz

Info Blatt

**Informationsblätter zum Wirtschaftsschutz**

# Sicherheit auf Geschäftsreisen



*Auf Geschäftsreisen ins Ausland besteht die Gefahr, dass Sie Ziel von Spionageaktivitäten ausländischer Nachrichtendienste werden. Umso wichtiger ist eine systematische Vor- und Nachbereitung. So können Sie mögliche Gefährdungen frühzeitig identifizieren und minimieren.*

*Der Verfassungsschutz ist für die Abwehr von Spionage und Sabotage durch ausländische Nachrichtendienste sowie von Extremismus zuständig und steht als vertraulicher Ansprechpartner zur Verfügung.*

## Checkliste

### VOR DER REISE

- Informieren Sie sich über die **Gefährdungs-, Sicherheits- und Gesetzeslage im Zielland**, v. a. bei Reisen in Staaten mit besonderen Sicherheitsrisiken i. S. v. § 13 Abs. 1 Nr. 17 SÜG. Nutzen Sie z. B. die Reise- und Sicherheitshinweise des Auswärtigen Amts.
- Fragen Sie nach **Erfahrungen von anderen Reisenden und Tipps von Sicherheitsverantwortlichen** und nutzen Sie **Schulungsangebote**.
- Stellen Sie **Kontaktadressen für Notfälle** zusammen (Unternehmenssicherheit, Botschaften/Konsulate, medizinische Versorgung usw.). Tragen Sie sich in die **Krisenvorsorgeliste des Auswärtigen Amts** (ELEFAND) ein.
- **Vorsicht bei IT**: Nehmen Sie keine Privatgeräte mit. Nutzen Sie einen **speziellen (unverschlüsselten) Laptop** ohne Zugriff auf das Firmennetzwerk bzw. ein **spezielles (unverschlüsseltes) Mobiltelefon**, auf dem nur die wichtigsten Nummern/Daten gespeichert sind.
- **Vorsicht bei Dokumenten**: Nehmen Sie nur mit, was für die Reise unbedingt gebraucht wird. Fertigen Sie Sicherheitskopien für den Verbleib zu Hause/im Büro an.
- Achten Sie auf **Datensparsamkeit** (z. B. bei Standort- und Bewegungsdaten). Machen Sie in Einreise- und Anmeldeformularen wahrheitsgemäße, aber möglichst allgemein gehaltene Angaben (z. B. zu Beschäftigungsverhältnissen).

### UNTERWEGS

- Seien Sie skeptisch bei der **Kontaktaufnahme durch Ihnen unbekannte Personen und bei Geschenken**, um kompromittierende Situationen zu vermeiden. Reisen Sie, wenn möglich, in Begleitung.
- Planen Sie **Transportmittel und -routen** vorab.
- Halten Sie sich von potentiell **gefährlichen Situationen** (z. B. Protesten) fern.
- Beschränken Sie **Gespräche über vertrauliche Inhalte** auf ein Minimum.
- Sollten Sie **sensible Daten aus der Hand geben** müssen, nutzen Sie eine **Sicherheitstasche** mit manipulationssicherem Selbstklebeverschluss und eindeutiger Barcode-Kennzeichnung.
- Verwenden Sie nur **eigene Ladegeräte** – fremde Ladegeräte könnten manipuliert sein.
- Meiden Sie offene **WLAN- und Bluetooth-Verbindungen**.
- Lassen Sie Vorsicht gegenüber **Dienstleistern/Servicepersonal** walten.

### NACH DER RÜCKKEHR

- Besprechen Sie Ihre Reise mit **Mitreisenden und Sicherheitsverantwortlichen** nach.
- Lassen Sie Ihre **mitgenommenen Geräte** auf Schadsoftware prüfen und ändern Sie unterwegs genutzte **Zugangsdaten**.
- Notieren Sie **auffällige Beobachtungen, Ereignisse und Unregelmäßigkeiten** und melden Sie diese an die zuständigen Stellen (Unternehmenssicherheit, Sicherheitsbehörden).

# Sichere Mobiltelefonie im Ausland

- Bei Reisen außerhalb Europas befinden Sie sich in einem von unseren Gegebenheiten stark abweichenden Rechtsraum.
- Sicherheitsbehörden im Ausland haben teilweise weitreichende Befugnisse, dies gilt insbesondere in politischen Systemen mit totalitären Tendenzen.
- Auch Personen, die sich aufgrund ihrer Tätigkeit als uninteressant für die nachrichtendienstliche Aufklärung sehen, können zum Ziel werden.
- Ausländische Nachrichtendienste (AND) sammeln massenhaft Daten und infiltrieren IT, um aus diesem Vorrat langfristig schöpfen zu können.
- AND können Zugriff auf den Internet- und Mobilfunkverkehr haben, Daten abfangen und kontrollieren.
- Auch können staatliche Cyberakteure Mobiltelefone aus der Ferne kompromittieren und auslesen.
- Soweit möglich, sollten Sie mittels einer manuellen Einstellung internationale Internetserviceprovider und Mobilfunkanbieter auswählen. Sofern sich eine Nutzung nationaler Provider nicht vermeiden lässt, sollten VPN-Clients auf den Endgeräten genutzt werden.

SCAN ME

***WEITERE INFORMATIONEN***

*Ausführliche Informationen zur IT-Sicherheit auf Reisen finden Sie im IT-Grundschutz-Kompendium des BSI „CON.7 Informationssicherheit auf Auslandsreisen“ auf* ***www.BSI.Bund.de***

# Angriffsvektoren

Die Technische Aufklärung gehört aufgrund ihrer effizienten und ressourcenschonenden Einsetzbarkeit zum wahrscheinlichsten Angriffsszenario während Geschäftsreisen. Nachrichtendienste schöpfen jedoch alle Möglichkeiten der Informationsgewinnung aus – konkret drohen:

- Totalüberwachung von Internet, Telekommunikation, Post
- Sperrung bestimmter Internetangebote
- Heimliche Durchsuchungen von Hotelzimmern und Gepäck
- Abhörmaßnahmen
- Observation
- Manipulation mobiler Endgeräte und Datenträger
- Willkürliche staatliche Repression
- Inszenierung von kompromittierenden Situationen
- Nachrichtendienstliche Kontaktaufnahme beim (Online-) Dating, sog. „Honey Trapping“
- Verhinderung der Ausreise z. B. durch fingierte Verkehrsunfälle

# Reise-Check-up/Notizen

**HABEN SIE NEUE KONTAKTE GEKNÜPFT?**

**HABEN SIE GESCHENKE ERHALTEN?**

**WURDEN SIE UNTER DRUCK GESETZT?**

**HABEN SIE IHRE MITGENOMMENEN GERÄTE PRÜFEN LASSEN?**

**IST IHNEN ANSONSTEN ETWAS UNGEWÖHNLICHES AUFGEFALLEN?**

Wirtschaft & Wissenschaft.
Zukunftssicher.
Verfassungsschutzverbund des Bundes und der Länder

*Das Bundesamt für Verfassungsschutz und die 16 Landesbehörden für Verfassungsschutz bilden gemeinsam den Verfassungsschutzverbund. Auch im Bereich des präventiven Wirtschaftsschutzes arbeitet dieser eng zusammen. Auf diese Weise entsteht ein starkes Netzwerk bis zu Ihnen vor Ort. Eine Übersicht über die Ansprechbarkeiten in den Landesbehörden finden Sie unter* ***www.verfassungsschutz.de****.*

initiative wirtschaftsschutz
Gemeinsam. Werte. Schützen.

*Die Initiative Wirtschaftsschutz ist ein Zusammenschluss von BfV, BKA, BND und BSI. Auf der Informationsplattform* ***www.wirtschaftsschutz.info*** *stellen sie zusammen mit verschiedenen Partnerverbänden ihre Expertise im Bereich Wirtschaftsschutz zur Verfügung. Dazu gehört das Thema Cyberkriminalität genauso wie Wirtschafts- und Wissenschaftsspionage oder das Thema IT-Sicherheit.*

## Ihr direkter Kontakt zum Wirtschaftsschutz

SCAN ME

**Bundesamt für Verfassungsschutz**
Bereich Prävention (Wirtschafts- und Wissenschaftsschutz)
**030 18792-3322**
**wirtschaftsschutz@bfv.bund.de**