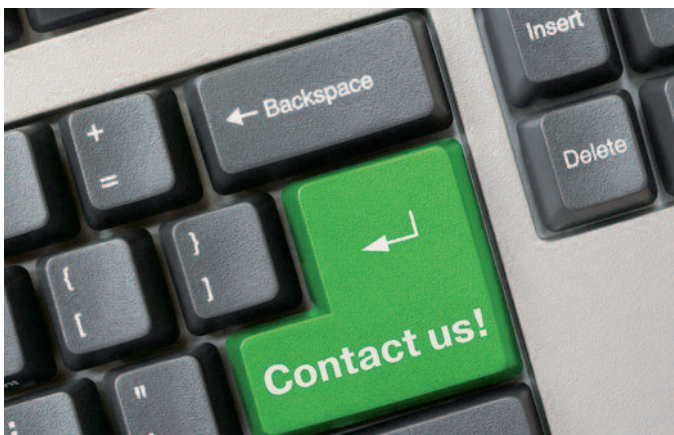


# Empfehlungen

## Nach der Reise:

- Kontrolle der Reiselaptops sowie Smartphones auf Schadsoftware
- Nachbereitung der Reise im Hinblick auf mögliche Auffälligkeiten
- Erfahrungen mit anderen teilen
- Kontaktaufnahme zum Verfassungsschutz bei sicherheitsrelevanten Vorfällen

**Sprechen Sie uns an und vereinbaren Sie einen Termin für ein vertrauliches Sensibilisierungsgespräch**



## Ihre Ansprechpartner im Wirtschaftsschutz



Dort finden Sie weitere Informationen sowie die Kontaktdaten Ihrer örtlichen Ansprechpartner.



[www.wirtschaftsschutz.info](http://www.wirtschaftsschutz.info)

## Verfassungsschutz



**Bund  
Länder**

**Wirtschaftsschutz**

**Schützen Sie Ihr Know-how unterwegs**

Impressum: Bundesamt für Verfassungsschutz für die Verfassungsschutzbehörden in Bund und Ländern  
Bilder: © Parris Cope - Fotolia.com  
© Nikolai Sorokin - Fotolia.com  
Gestaltung: Bundesamt für Verfassungsschutz  
Druck: Bundesamt für Verfassungsschutz  
Stand: März 2016

## Andere Länder – Andere Sitten

Der Schritt, neue Märkte in anderen Ländern zu erschließen, eröffnet Unternehmen eine Vielfalt an wirtschaftlichen Chancen. Doch mit diesen neuen Möglichkeiten entsteht eine Vielzahl an Sicherheitsrisiken.



## Bedenken Sie auf Geschäftsreisen

Die tatsächliche Rechtssituation im Gastland kann sich erheblich von der deutschen Rechtslage unterscheiden. Dürfen Sie z.B. einen kryptierten USB-Stick ins Zielland importieren oder überall bedenkenlos fotografieren?

Fremde Nachrichtendienste besitzen auf Ihrem Hoheitsgebiet „Heimvorteil“. Sie handeln häufig mit umfassenden Exekutivbefugnissen.

## Beispiele

- Totalüberwachung des Internets, der Telekommunikation sowie der Postwege
- Sperrung bestimmter Internetangebote
- Heimliche und zielgerichtete Hotelzimmer- sowie Gepäckdurchsuchungen
- Manipulation mobiler Endgeräte und Datenträger
- Schaffung kompromittierender Situationen
- Willkürliche staatliche Repressionen
- Verhinderung der Ausreise durch fingierte Verkehrsunfälle
- Erpressbarkeit durch Kontakt zu Oppositionellen
- Infizierung mobiler Endgeräte durch Trojaner auf fremden USB-Sticks



## Empfehlungen

### Vor der Reise:

- Recherche zur Gefährdungs- und Sicherheitslage im Zielland
- Einholen von Kontaktadressen für Notfälle
- Über gesetzliche Vorgaben informieren
- Grundsatz der Datensparsamkeit und Einsatz von Reiselaptops/Smartphones ohne sensible Firmendaten

### Während der Reise:

- Skepsis bei Kontaktversuchen und Geschenken
- Wachsamkeit gegenüber Dienstleistern
- Zurückhaltung bei politischen Themen
- Sensible Informationen nicht aus der Hand geben – Hotelzimmer und -safe sind nicht sicher
- Nutzung erlaubter Verschlüsselungsprodukte
- Vertrauliche Kommunikation auf das notwendige Maß reduzieren
- Bei Verdacht auf Datenverlust und ungewöhnlichen Vorkommnissen sofort Ihr Unternehmen in der Heimat informieren