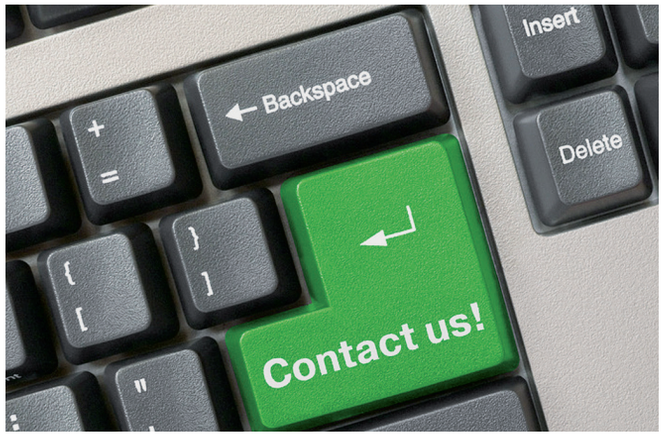
Empfehlungen

Nach der Reise:

- Kontrolle der Reiselaptops, sowie Smartphones und Speichermedien auf Schadsoftware
- Nachbereitung der Reise im Hinblick auf mögliche Auffälligkeiten
- Erfahrungsaustausch mit anderen
- Kontaktaufnahme zum Verfassungsschutz bei sicherheitsrelevanten Sachverhalten

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



Ihre Ansprechpartner im Wirtschaftsschutz

Wirtschaftsschutz
Niedersächsisches Ministerium für Inneres und Sport - Verfassungsschutz -
Postfach 44 20
30044 Hannover
Telefon (0511) 6709 - 0
Telefax (0511) 6709 - 393
E-Mail wirtschaftsschutz@verfassungsschutz.niedersachsen.de

initiative wirtschaftsschutz

Gemeinsam. Werte. Schützen.

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

www.wirtschaftsschutz.info

Impressum

Herausgeber: Bundesamt für Verfassungsschutz für den Verfassungsschutzverbund

Bilder: © Parris Cope - Fotolia.com
© Westend61 - Fotolia.com
© Nikolai Sorokin - Fotolia.com

Stand: März 2016

Verfassungsschutz

Bund Länder

Wirtschaftsschutz

Sicherheit bei Auslandsreisen

Geschäftsreisen

Prävention durch Dialog und Information

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 rechtliche Situation im Gastland kann sich erheblich von der in Deutschland 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
- Erpressung auf Grund des Kontaktes 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
- Informationen über gesetzliche Vorgaben
- 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