- Beachten Sie die Länder- und Reiseinformationen des Auswärtigen Amtes (http://www.auswaertiges-amt.de/), hier können Sie sich über die allgemeine Gefährdungs- und Sicherheitslage des Reiselandes informieren.
- Machen Sie sich mit den Gebräuchen und Gesetzen des Landes vertraut und verstoßen Sie nicht gegen diese Gesetze.
- Beachten Sie aktuelle Ein- und Ausfuhrverbote oder -beschränkungen
- Machen Sie keine missverständlichen oder abweichenden Angaben zur Person bzw. zum Arbeitgeber in Ihrem Visumantrag
- Prüfen Sie die Geschäftsverbindung und beschaffen Sie sich möglichst viele Informationen zum Geschäftspartner aus öffentlich zugänglichen Quellen
- Schaffen Sie im Gastland auf keinen Fall Situationen, die Sie erpressbar machen („Honigfalle", „Schwarzgeld", Drogen …)!
- Wägen Sie Nutzen und Risiken einer Zusammenarbeit mit ausländischen Service- und Sicherheitsfirmen genau ab
- Seien Sie bei ungewöhnlichen und intensiven Fragestellungen misstrauisch
- Führen Sie niemals Gespräche mit Fremden über Reisezweck und Arbeitgeber
- Seien Sie bei privaten Kontakt- oder Begegnungsversuchen vorsichtig
- Verzichten Sie auf Stellungnahmen gegenüber Gesprächspartnern mit politischen oder berufsbezogenen Inhalten
- Meiden Sie Menschenmengen und Demonstrationen
- Lassen Sie sensible Firmenunterlagen nie unbeaufsichtigt im Hotelzimmer, Tagungs- oder Büroraum – auch Hotelsafes bieten keinen zuverlässigen Schutz!
- Lassen Sie Ihr Gepäck nie unbeaufsichtigt stehen
- Vernichten Sie nicht mehr benötigte Unterlagen vollständig – auch Abfall kann wertvolle Informationen enthalten!
- Vermeiden Sie den Gebrauch geschenkter USB-Sticks – es könnten sich Trojaner und Viren darauf verbergen
- Nutzen Sie nur gesicherte Kommunikationswege für sensible Informationsübermittlung – sämtliche unverschlüsselte Kommunikation (Fax, Telefon und E-Mail) ist gefährdet
- Zum Schutz von PC und Notebook: Setzen Sie Passwörter sowie Virenschutz- und Verschlüsselungsprogramme ein (hierbei sind spezifische Ländergegebenheiten zu beachten)
- Seien Sie bei der Nutzung von Mobiltelefonen vorsichtig: Es besteht Abhörgefahr! Lassen Sie Ihr Handy nie unbeaufsichtigt liegen – manipulierte Mobiltelefone können als Mikrofon dienen
- Speichern Sie geschäftliche Daten auf einem USB-Stick oder einer DVD und führen Sie den Datenträger am Körper mit; geben Sie ihn nie aus der Hand und bewahren Sie ihn nicht im Hotelsafe auf
- Spielen Sie auf Notebooks möglichst nur das Betriebssystem auf und nutzen Sie auf Reisen nur eine minimale Konfiguration

Die Verhaltensempfehlungen sollten nicht ausschließlich bei Geschäftsreisen Beachtung finden, sondern – natürlich mit Einschränkungen – auch auf Urlaubsreisen nicht völlig vernachlässigt werden.

Die Aktionen von ausländischen Nachrichtendiensten laufen in der Regel unauffällig, diskret und konspirativ ab. In Deutschland müssen sich fremde Nachrichtendienste z.B. auf nationale, territoriale und alle sonstigen Gegebenheiten des „Gastlandes" einstellen – sie agieren im Ausland. All diese Gegebenheiten werden zu Vorteilen für einen Nachrichtendienst, der im eigenen Land handelt. Hier kann er sich auf die uneingeschränkte Unterstützung in allen Bereichen, auch von staatlichen Institutionen und Behörde, einschließlich der Polizei verlassen – dies gilt insbesondere für Staaten, in denen nicht die vertrauten rechtsstaatlichen Garantien gelten, als in der Bundesrepublik. Bei konkreten

Verdachtsfällen stehen Ihnen im Ausland die diplomatischen oder konsularischen Vertretungen der Bundesrepublik Deutschland zur Verfügung.

Wie wichtig es ist, sich über die rechtlichen Bedingungen eines Reiselandes im Vorfeld zu informieren, mag das folgende Beispiel deutlich machen:

In der Volksrepublik China darf nur eine staatlich genehmigte Verschlüsselungssoftware genutzt werden. Der Gebrauch von Verschlüsselungstechniken oder Geräten, die Verschlüsselungstechniken verwenden, muss in der VR China bei der National Commission on Encryption Code Regulation (NCECR) angemeldet und genehmigt werden. Konkret enthält die Direktive Nr. 273 (Administration of Commercial Encryption Regulations – State Council Directive 273) folgende Kernaussagen:

- Ohne Erlaubnis der chinesischen Regierung/Behörden ist der Betrieb von Verschlüsselungslösungen und Technologien untersagt
- Die Erlaubnis zur Einführung und zum Betrieb, ist über die chinesischen Behörden unter Angabe der notwendigen Produktinformationen einzuholen
- Beim Einsatz von Hardwareverschlüsselungsgeräten müssen chinesische Geräte genutzt werden
- Bei der Einfuhr in die Volksrepublik China muss auf die Einhaltung der zollrechtlichen Bestimmungen geachtet werden

Wird gegen diese Maßgaben verstoßen, kann dies dazu führen, dass Computertechnik konfisziert wird. Vor diesem Hintergrund kann davon ausgegangen werden, dass nur Verfahren zugelassen sind, die von chinesischen Sicherheitsbehörden entschlüsselt werden können bzw. deren Schlüssel vom Verwender bei der NCECR hinterlegt wird.

Mit der Rückkehr nach Deutschland sollte eine unter Sicherheitsaspekten gut vorbereitete Auslandsreise nicht enden. Nehmen Sie sich, insbesondere nach Reisen in Länder mit erhöhten Sicherheitsrisiken, die Zeit für eine Nachbereitung. Lassen Sie Ihre Reise noch einmal unter Beachtung folgenden Punkten Revue passieren:

- Gab es Besonderheiten beim Grenzübertritt (z. B. sichtentzogene Kontrolle Ihres Gepäcks; „besondere“ Behandlung)?
- Bestand Interesse an Ihrer Person/beruflichen Tätigkeit über das normale Maß hinaus?
- Gab es Locksituationen oder Begebenheiten, die als solche ausgelegt werden könnten?
- Gab es Kontaktaufnahmen mit unklarer Zielstellung?
- Gab es Versuche, Sie für eine nachrichtendienstliche Tätigkeit zu werben oder zu verpflichten?
- Gab es sonstige Auffälligkeiten? - Auch Kleinigkeiten können große Wirkung haben!

Da es immer auf den Einzelfall ankommt, steht Ihnen die Verfassungsschutzbehörde des Landes Brandenburg für ergänzende Sensibilisierungs- und Beratungsgespräche gerne zur Verfügung. Ihre Hinweise, die mit Sicherheit vertraulich behandelt werden, können Ihr Unternehmen vor unbemerktem Know-how-Abfluss schützen, wichtige Informationen über die Arbeitsweisen fremder Nachrichtendienste enthalten und für die weitere Arbeit im Bereich der Spionageabwehr sehr wertvoll sein.