



Hannover im Juli 2012

Sehr geehrten Damen und Herren,

aus gegebenem Anlass möchten wir Ihnen einen aktuellen Fall zum Themenfeld Auslandsreisen näher bringen, der dem niedersächsischen Wirtschaftsschutz gemeldet wurde.

Wiederholt hat der Wirtschaftsschutz Niedersachsen zu den Risiken bei Auslandsreisen, speziell nach China, sensibilisiert. In dem nachfolgenden Fall wurden wir in allen Facetten der Ausspähung durch Nutzung von Vertrauen und IT-Systemen bestätigt. Über die Identität der Angreifer, eventuell chinesischer Nachrichtendienst, kann nur spekuliert werden.

In diesem Zusammenhang möchten wir Ihnen nahelegen über die Nutzung eines Reiselaptops bei Auslandsreisen nachzudenken.

Selbstverständlich stehen wir bei Rückfragen jederzeit gerne zur Verfügung und auch das Angebot des Wirtschaftsschutzes zu individuellen und vertraulichen Gesprächen bleibt unberührt.

Ihr Wirtschaftsschutz-Team



Niedersächsische Verfassungsschutzbehörde

1. Falldarstellung

Ein Ingenieur, der im Bereich Qualitätssicherung der Luft- und Raumfahrtindustrie tätig ist, wird bei einem Arbeitsbesuch in China vom dortigen Auftraggeber ein USB-Stick mit angeblichen Arbeitsunterlagen überreicht, welchen er im Anschluss an seinem Netbook nutzt. Für den Internetzugang wird ein Netzwerkzugang der chinesischen Firma bereitgestellt, über den der Ingenieur sein eigenes Netbook anschließt. Für die Dauer des Aufenthaltes wird ein Gästehaus des Auftraggebers zur Verfügung gestellt. Wieder in Deutschland angekommen, stellt er fest, dass sein chinesischer Auftraggeber Kenntnis von seinen, über Skype-Telefonie, geführten Gesprächen mit anderen Zertifizierern bezüglich dieser chinesischen Firma hat. Weiterhin ist auffällig, dass einzelne, in China erstellte Dateien kurzfristig chinesische Schriftzeichen enthielten.

Es besteht der Verdacht, dass Schadsoftware über den USB-Stick oder das Firmennetzwerk auf dem Netbook installiert worden ist, welche die Internettelefonate mitschneidet und an die chinesische Firma sendet sowie dass Dateien von extern auf dem Netbook geöffnet worden sind.

Die genaue Art der Ausforschung ist zurzeit Gegenstand von Ermittlungen. Eine Zusammenarbeit mit Strafverfolgungsbehörden ist von dem Ingenieur nicht erwünscht.

Folgende Fragen sollten Sie sich stellen:

- Sind alle mitgeführten Daten für die Durchführung meines Aufenthaltes nötig?
- Sind diese Informationen für Unbefugte interessant?
- Sind meine Daten vor Ort ausreichend vor unberechtigtem Zugriff geschützt?
- Habe ich im Hotel eine sichere Aufbewahrungsmöglichkeit?
- Welche Datenverschlüsselung ist in dem Reiseland erlaubt?

Folgendes sollten Sie wissen:

Geübte Praxis von fremden Nachrichtendiensten ist:

- Die Manipulation von mobilen Endgeräten und Datenträgern.
- Die heimliche und zielgerichtete Hotelzimmer- sowie Gepäckdurchsuchung.
- Die Totalüberwachung des Internets und der Telekommunikation sowie der Postwege.

Wie Sie ihre Auslandsreise sicherer gestalten können (eine beispielhafte und nicht abschließende Aufzählung):

- Recherche zur Gefährdungs- und Sicherheitslage vor der Reise
- Kontaktadressen für Notfälle mitführen (Botschaften, Konsulate etc.)
- Beachtung gesetzlicher Vorgaben (Visa-, Ein- und Ausfuhrvorschriften)
- Skepsis bei auffälligen Kontaktversuchen (Flughäfen, Restaurants, Hotelbars...)
- Wachsamkeit gegenüber Dienstleistern (Dolmetscher, Reisebegleiter, Hotelmitarbeiter)
- Zurückhaltung bei politischen Themen
- Einsatz von „nackten“ Reiselaptops und Smartphones
- Sensible Informationen nicht aus der Hand geben, Hotelzimmer und -safe sind nicht sicher
- Nutzung – erlaubter – Verschlüsselungsprodukte
- Vertrauliche Kommunikation auf das notwendige Maß reduzieren
- Kontrolle der mobilen Informations- und Kommunikationstechnik auf Schadsoftware nach der Rückkehr
- Vorsicht bei Geschenken! Digitale Bilderrahmen, USB-Sticks, DVDs usw. nicht ungeprüft an Netzwerke anschließen
- Nachbereitung der Reise im Hinblick auf mögliche Auffälligkeiten
- Kontaktaufnahme zum Verfassungsschutz bei Vorfällen