Niedersächsisches Ministerium
für Inneres und Sport

Wirtschaftsschutz - *Info*

Hannover im Februar 2012

„Konzernsicherheit ist nicht unbedingt der beliebteste Aspekt in einem Unternehmen. Sie hält auf und wird als Einschränkung der wertschöpfenden Arbeit betrachtet.“ So zitierte das Handelsblatt Ende 2011 den Leiter Cyber Forensic bei RWE, Andreas Rohr.
In derselben Ausgabe schreibt Sandro Gayken, Technik- und Sicherheitsforscher an der FU Berlin: *„Wirtschaftsspionage ist ein epochales Phänomen mit enormen Ausmaßen. Mit dem Investment von ein paar Millionen locken Milliardengewinne.“*

Wir wissen, dass eben aus diesem Grund Wirtschaftsspionage betrieben wird. Mit der Neuauflage der *Wirtschaftsschutz - Info* möchten wir dazu beitragen, durch aktuelle Informationen die Sicherheit Ihres Unternehmens zu erhöhen, bzw. eventuell vorhandene Schwachstellen zu erkennen.
Selbstverständlich stehen wir bei Rückfragen jederzeit gerne zur Verfügung und auch das Angebot des Wirtschaftsschutzes zu individuellen und vertraulichen Gesprächen bleibt davon unberührt.

Ihr Wirtschaftsschutz-Team

Niedersächsische Verfassungsschutzbehörde

Niedersächsisches Ministerium für Inneres und Sport
Referat 55 - Wirtschaftsschutz

Postfach 4420
30044 Hannover
Tel.: 0511 / 6709-247 oder -248
Email: wirtschaftsschutz@verfassungsschutz.niedersachsen.de

1. Geschäftsreisen und Gefahren im Ausland

Die Bandbreite krimineller Risiken im Ausland ist immens. In einem Atemzug mit Korruption wird als größte Gefahr auch Informationsabfluss/Industrie- und Wirtschaftsspionage genannt. Und auch die globale Finanz- und Wirtschaftskrise kann bei einer Verschlechterung der wirtschaftlichen Rahmenbedingungen den Nährboden für wirtschaftskriminelle Handlungen bilden.
Vor diesem Hintergrund ist es umso wichtiger, ein besonderes Augenmerk auf die jeweiligen Geschäftsabläufe zu legen und entsprechende Vorkehrungen zu treffen – im Hinblick auf den internationalen Geschäftspartner einerseits, aber auch zwecks der eigenen Sicherheit bei Geschäftsreisen andererseits.

<u>Folgende Fragen sollten Sie sich stellen:</u>

- Habe ich meine Geschäftspartner sorgfältig ausgewählt?
- Habe ich Hintergrundinformationen zum Unternehmen und zu den handelnden Personen eingeholt?
- Habe ich Referenzen überprüft?
- Habe ich Compliance-Richtlinien vertraglich fixiert?
- Habe ich mich mit der Sicherheitslage und aktuellen politischen Entwicklungen im Land beschäftigt?
- Habe ich mich mit den gesetzlichen Bestimmungen vertraut gemacht?
- Habe ich meine Mitarbeiter auf die Reise vorbereitet?
- Gibt es einen Notfallplan und Ansprechpartner für unvorhergesehene Ereignisse?
- Wird im Ausland separate und vom Firmennetz unabhängige Hardware genutzt und sind nicht benötigte Schnittstellen gesperrt?
- Habe ich nur die Daten dabei, die ich auch tatsächlich benötige?
- Ist eine Verschlüsselung der Daten möglich und zulässig?

Darüber hinaus sollten Sie davon ausgehen, dass…

- …Ihre Kommunikation ständig überwacht werden kann
- …zufällig erscheinende Begegnungen meistens alles andere als zufällig sind
- …ruhige Ecken für vertrauliche Gespräche gezielt ausgewählt und präpariert sein können
- …Hotelpersonal nicht immer Hotelpersonal ist und auch schon Restaurantpersonal im Vorfeld eines dort stattfindendem Geschäftsessens ausgetauscht worden ist

2. Aktuelles

In der Vergangenheit wurde uns eine Vielzahl von Fällen mitgeteilt, die in einem Zusammenhang mit dem Ausscheiden von Mitarbeitern stehen:
So hat sich ein Mitarbeiter eines Unternehmens kurz vor seiner Kündigung/Entlassung einen externen Zugang zu dem Firmennetzwerk eingerichtet. Dadurch verschaffte er sich die Möglichkeit, auch nach seinem Ausscheiden aus dem Unternehmen auf für ihn wertvolle Informationen zuzugreifen.
Was Sie in einem solchen Fall tun können (eine beispielhafte und nicht abschließende Aufzählung):

- Achten Sie darauf, dass mit jedem Ausscheiden von Mitarbeitern Zugriffsmöglichkeiten überprüft und Passwörter geändert werden
- Einrichten technischer Möglichkeiten, um ungewollten Datenverkehr zu erkennen und zu selektieren
- Verschwiegenheitsverpflichtungen vertraglich fixieren
- Schulung des Managements, bzw. der Mitarbeiter, um sog. *Red flags* (Auffälligkeiten, die auf kriminelle Machenschaften hindeuten) zu erkennen