

Mittelhessischer Außenwirtschaftstag 2007 China und Indien: Neues von Drachen und Tigern



Know-How-Klau:

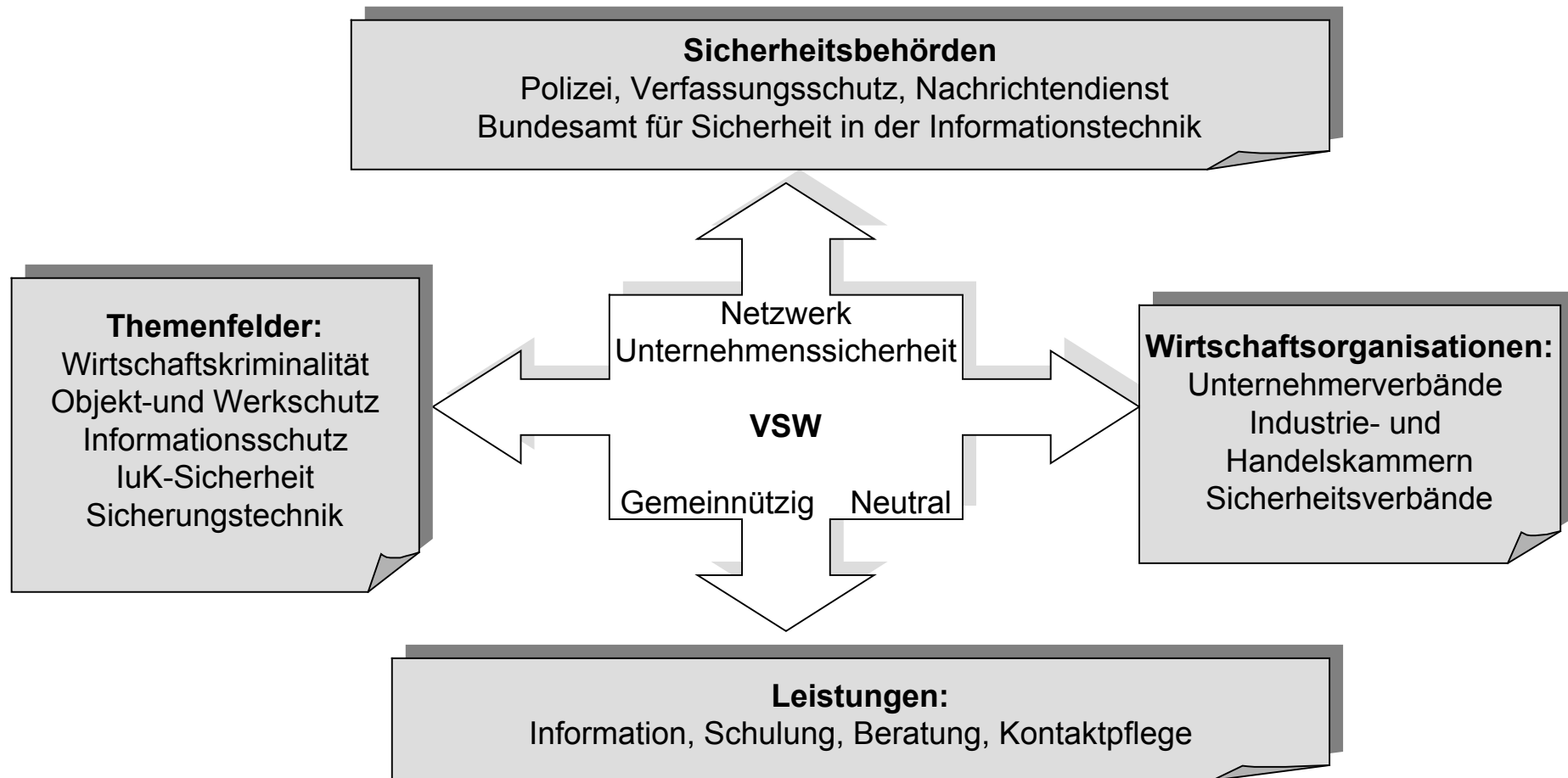
**Wie sollte sich Ihr Unternehmen im
Geschäft mit China und Indien schützen?**

08. Februar 2007, IHK Gießen

RA Ralf Schönfeld

Vereinigung für die Sicherheit der Wirtschaft e.V.

Wie funktioniert das Netzwerk der VSW?



Mögliche Unternehmens-Bedrohungen

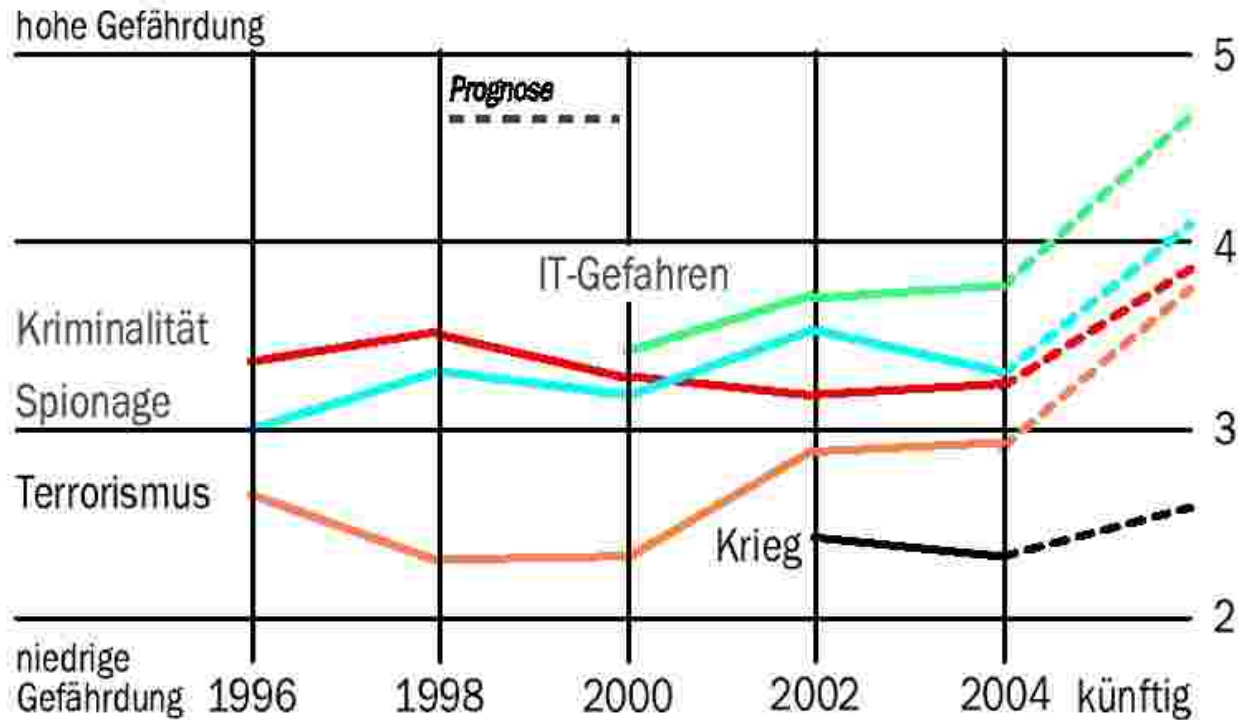
Einflussfaktoren der Unternehmenssicherheit:



WIK-Sicherheitsenquête 2005

IHK-Sicherheits *Enquête*® 2004/05

Entwicklung der Gefährdung



WIK-Sicherheitsenquête 2005

Womit wurden Sie im Rahmen Ihrer Tätigkeit in den letzten 24 Monaten häufig (= >5mal) konfrontiert?

- 36,8 % Massendelikte (Diebstahl, etc.)
- 32,2% Internetkriminalität (Hacking, DoS-Angriffe)
- 26,2% Mitarbeiterdelikte
- 12,7% Abhörversuche (Telefon, Computernetze)**
- 10,6% Konkurrenzspionage**
- ...
- 9,2% Korruption, Bestechung
- ...
- 3,0% Spionage durch fremde Nachrichtendienste**
- 2,5% Erpressungen
- 1,5% Terroranschläge

WIK-Sicherheitsenquête 2005

Welche Risiken werden zukünftig eher wachsen?

- 75,4% Hackerangriffe auf die betriebliche IT
- 71,0% Schadenssoftware aus dem Internet
- 66,7% Datendiebstahl (Laptops, Festplatten, etc.)
- 63,3% „Zeit-Diebstahl“ (Surfen im Web, PC-Spiele etc.)
- 57,5% Abhörversuche an Telefon und Fax**
- 53,1% Diebstahl durch Mitarbeiter
- 49,8% Betriebsspionage**
- ...
- 32,9% Ausfall der Sicherungstechnik (ZK, EMA, etc.)
- 20,3% Terroristische Angriffe auf das Unternehmen

Spionage-Worum geht es?

➔ WIRTSCHAFTSSPIONAGE

➔ KONKURRENZAUSSPÄHUNG

➔ PROLIFERATION

Informationsgewinnung

⇒ Open Sources (80%)

- Systematische Internet-Recherchen
- Auswertung von Messen und Kongressen
- Auswertung von (Fach-)Publikationen
- Fingierte Angebotsanforderungen
- Joint-Ventures und Übernahmen

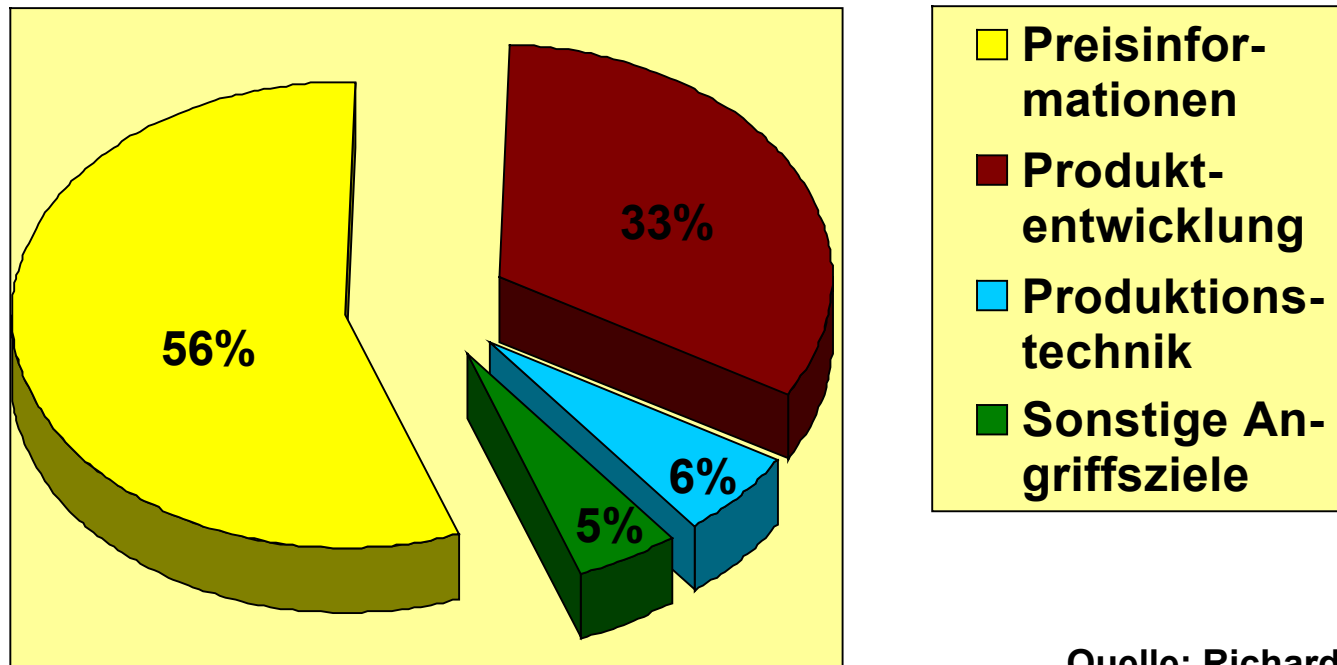
Informationsgewinnung

➔ Human Intelligence & Social Engineering

- **Gesprächsabschöpfung**
- **Einschleusung (langfristig ausgelegt)**
- **Anbahnung (sog. „Romeo-Masche“)**
- **Bestechung / Erpressung**
- **Observation / Diebstahl**

Ausspähungsziele

➔ Die wichtigsten Spionageziele



Quelle: Richard Heffernan, USA

Spionagerisiken im Geschäft mit China

Staatsziele:

- ➔ Bis spätestens 2020 führende Weltwirtschaftsmacht werden
- ➔ Schaffung einer Wissenschafts- und Technikarmee zum Aufbau Chinas (Technologieentwicklungspläne 863, 973, Falkenplan, Funkenplan - mit jeweils nachrichtendienstlicher Komponente
- ➔ Technologierückstand verringern
- ➔ (Technische) Bildung) wird als äußerst wichtig angesehen

Spionagerisiken im Geschäft mit China

Vorgehensweise chinesischer Nachrichtendienste:

- ➔ **Mitarbeiter chinesischer Nachrichtendienste** werden gezielt als Praktikanten/Diplomanden oder Doktoranden in deutsche Universitäten oder Unternehmen mit Hochtechnologie od. „gewünschter“ Technologie“ eingeschleust
- ➔ **Auffällig:** Studenten, die genauso lange wie Deutsche studieren und ein Praktikum nach dem anderen in „interessanten“ Firmen absolvieren

Spionagerisiken im Geschäft mit China

Vorgehensweise chinesischer Nachrichtendienste:

Besonders betroffene Branchen:

Kfz, Eisenbahn, Luftfahrt, Bio- & Gentechnologie,
Medizintechnik, chemische Industrie,
pharmazeutische Industrie, (Spezial)-Maschinenbau

- ➔ Überall dort, wo Deutschland noch „wertvolles Know-How“ besitzt
- ➔ Strategische Entwicklungsbranchen Chinas

Spionagerisiken im Geschäft mit China

Vorgehensweise chinesischer Nachrichtendienste:

- ➔ Ausspähen von Maschinen auf Messen
- ➔ Internetüberwachung
 - Ca. 50.000 Internetüberwachung von Chinas Regierung eingesetzt
 - Weitreichende Überprüfungs-, Sperrungs- und Lesemöglichkeiten vorhanden. Technik, Mails auf bestimmte Inhalte hin zu untersuchen und einzelne Empfänger oder Absender anzuvisieren

Methodik der Gefahrenanalyse

➔ Risikoanalyse

- Wie gefährdet ist mein Unternehmen?
- Wie gefährdet sind meine Mitarbeiter?

➔ Bedrohungsanalyse

- Wer und wie „potent“ ist mein Gegner?
- Spionage durch Nachrichtendienst oder Konkurrenzunternehmen?

Know-How-Verlust durch Fahrlässigkeit



Risikofaktor Mensch

➔ Ursachen für Informationsabflüsse

- **Unkenntnis / Blauäugigkeit / Naivität**
- **Anerkennungsbedürfnis („der/die versteht mich“)**
- **Geltungssucht / Machtstreben / Karrieredenken**
- **Materielle Gründe / Lebensstil („Gier frißt Hirn“)**
- **Ideelle Faktoren (Liebe, Haß, Weltanschauung)**

Risikofaktor Mensch

➔ Menschliche Begegnungen

- **Faustregel: Professionelle Informationsbeschaffer überlassen grundsätzlich nichts dem Zufall**
- **Vermeintlich „zufällige“ Begegnungen können gezielt lanciert sein (selbst in der Besenkammer)**
- **Bei zahlreichen Anlässen, wie z.B. großen Events, Fachkongressen oder an der Hotelbar können vermeintliche „Zufallsbegegnungen“ gezielt erfolgen**

Risikofaktor Mensch

➔ Menschliche Begegnungen

- **Verzicht auf die Annahme von Gast- und Werbe-
geschenken von Geschäftsfreunden (bzw. deren
ungeprüfte Plazierung in heimischen Räumen)**
- **Besondere Vorsicht bei werthaltigen Kunstge-
genständen und Sammlerstücken für das eige-
nen Büro**
- **Bekannte Sammelleidenschaften erhöhen das
Risiko der Unterschlebung von Lauschkitteln**

Schriftliche Dokumente

➔ Handhabung und Vorsichtsmaßnahmen

- **Wichtige Dokumente niemals in fremden Büros oder Hotelzimmern (auch nicht im Hoteltresor!) zurücklassen**
- **Vertrauliche Dokumente (z.B. Vertragsentwürfe, Angebote, Studien) immer mit sich führen**
- **Nicht mehr benötigte, vertrauliche Dokumente auch unterwegs stets nur persönlich im Aktenvernichter (mind. Stufe 4) entsorgen**

Digitale Datenträger

➔ Handhabung und Vorsichtsmaßnahmen

- Auf Laptops und sonstigen Datenträgern (CD, DVD, Disketten, USB-Stick usw.) vertrauliche Daten stets nur verschlüsselt speichern (möglichst hardwarebasierend, z.B. mittels PCMCIA-Verschlüsselungskarte)
- Laptops mit Boot-Passwortschutz und zusätzlichen Sicherheitsmechanismen (z.B. Fingerprint) versehen

Digitale Datenträger

➔ Handhabung und Vorsichtsmaßnahmen

- **Laptops und Datenträger niemals unbeaufsichtigt lassen - auch kurzzeitig nicht in Autos, Hotelzimmern oder fremden Büros**
- **Evtl. vorbereitete „Spieldaten“ deponieren, um tatsächliche Risiken besser einschätzen zu können und Gegner zu „beschäftigen“**
- **Löschen alter Daten nur durch mehrfaches Überschreiben mittels spezieller Programme**

Öffentliche Bereiche

⇒ Verkehrsmittel

- **Dokumente, Laptops und Datenträger bei Linienflügen nur im Handgepäck mitführen**
- **In der Business- und First Class keine Gespräche über vertrauliche Sachverhalte führen**
- **In der Öffentlichkeit keine Dokumente lesen oder Laptops benutzen, da das Mitlesen u.U. zur gezielten Informationsgewinnung eingesetzt wird**

Empfehlungen im China-Geschäft

➔ Praktische Know-How-Schutz-Maßnahmen

- Spezielle Vorbereitung der ins China-Projekt involvierten Delegationsmitglieder
- Vertrauliches Firmenmaterial auf Geschäftsreisen niemals im Hotelzimmer lassen
- „China-Laptop“ mitnehmen – so wenig Infos wie möglich (gilt auch für USB)
- Räume für vertrauliche Gespräche immer erst kurzfristig festlegen und regelmäßig wechseln (Abhörgefahr)
- Chinesische Praktikanten, Studenten, Diplomanden und Doktoranden grundsätzlich nicht in sensible Abteilungen

Zusammenfassung

➔ Maßnahmen zum Informationsschutz

- **Erstellung und Umsetzung individueller Richtlinien zum Informationsschutz auf Reisen**
- **Sensibilisierung der Mitarbeiter bezüglich Informationsschutz und spezielle Vorbereitung vor wichtigen Geschäftsreisen bzw. Veranstaltungen**
- **Gesprächsführung nach Geschäftsreisen und Auswertung sämtlicher Ereignisse**

Vielen Dank für Ihre Aufmerksamkeit!

Haben Sie noch Fragen?



Kontakt für weitere Informationen:

Vereinigung für die Sicherheit der Wirtschaft e.V.

RA Ralf Schönfeld
Jakob-Anstatt-Str.2
D-55130 Mainz

Telefon: 06131-891972

Telefax: 06131-984096

E-Mail: info@vsw-service.com

Internet: www.vsw-service.com