



## Leitfaden - Risikofaktor Auslandsreise & Messen

INSIDERS  
**KNOWLEDGE**  
Security by Culture

# AGENDA



## 1 Risikofaktor Reise und Messe

Messen und Dienstreisen als Notwendigkeit  
Fremde Umgebung und Kontrollverlust

## 2 Aktuelle Themen und Beispiele

China als „Überwachungsmarkt“  
Zollkontrolle als Sicherheitsrisiko

## 3 Risiken und Konsequenzen für das Unternehmen

Verlust von sensiblen Daten auf Reisen und Messen

## 4 Abwehrmaßnahmen

Planung und gesonderte Infrastruktur für Reisen und Messen

## 5 Fazit & Ausblick

## 6 Kontaktinformationen

**INSIDERSKNOWLEDGE**

# RISIKOFAKTOR REISE UND MESSE

Mögliche Risiken durch Dienstreisen und Messebesuche



Für ein internationales Unternehmen sind Dienstreisen und Teilnahmen an Messen alltägliche Situationen. Manager treffen Businesspartner und Kunden, beaufsichtigen Fertigung und koordinieren Produktvertrieb und Netzwerke. Dabei tragen viele ihr SmartPhone, Laptop und andere technischen Datenträger mit sich, um die Reisezeit zum Lesen, Emails beantworten und Telefonieren zu nutzen. Dabei entstehen jedoch hohe Risiken:

Bei internationalen Kontrollen, Zollpassage und auch auf Messen werden diese Geräte und Datenträger zum Ziel von staatlichen Zugriffen, Industriespionage und Diebstahl.

Auch USB Sticks, die gerne als Werbegeschenke verteilt werden, können Schadsoftware enthalten und stellen so ein Sicherheitsrisiko da.

- Reisen und Messebesuche bergen viele Risiken für den unbefugten Zugriff auf Datenträger mit sensiblen Informationen.
- Messebesucher sind eine lohnendes Ziel für Industriespione. Mitgeführte Laptops und Datenträger sind das leichteste Ziel um schnell an relevante Informationen zu gelangen.
- In Ländern wie China nutzen auch Behörden gezielt Industriespionage um wirtschaftliche Vorteile zu schaffen.
- Werbegeschenke wie USB-Sticks auf Messen bieten sich als Schadsoftwareträger an
- Auf Reisen und Messen mitgeführte Datenträger sind ein leichtes Ziel und lohnenswerte Beute für Datendiebe. Messen mit spezifischen Themen sind besonders geeignet, hier ist der potentielle Wert entwendeter Daten besonders hoch.

# RISIKOFAKTOR REISE UND MESSE

Fremde Umgebung und Kontrollverlust



Internationale Reisen führen zu stressigen Situationen mit Zeitverschiebung, häufigem Kontakt zu fremden Menschen in ungewohnten Umgebungen unter fremden Gesetzen. Selbst vorsichtige Reisende, die Datenträger vor Verlust schützen, sind bei einer Behördenkontrolle oder dem Einbruch ins Hotelzimmer machtlos. Einmal im Besitz von Daten oder mobilen Geräten ist dem Angreifer keine Hürde mehr gesetzt, sich auch langfristig Zugang zu Daten zu sichern. Diese Angriffe werden häufig durch den Einsatz von Trojanern unterstützt. Damit ist langfristig der Zugriff auf das Unternehmensnetzwerk eröffnet.

- Kurzfristiger Kontrollverlust kann zu langfristigem, unbemerktem Zugang durch den Angreifer führen, der danach ungehindert auf firmeninterne Daten zugreifen kann.
  - Trojaner und Spionagesoftware stellen neben Datendiebstahl ein unkontrollierbares Risiko dar, denn selbst nicht mitgeführte Daten geraten in Gefahr.
  - Ein mobiles Gerät, auf das ein Angreifer zugegriffen haben kann, darf deshalb nicht ohne Überprüfung im Firmennetzwerk betrieben werden.
- Ein Zugang auf das Firmennetzwerk ist über einen Rechner möglich, der bei einer Messe oder Auslandsaufenthalt infiziert wurde. Auch Smartphones, USB Sticks und andere Datenträger bergen dieses Risiko.

# AGENDA



- 1 Risikofaktor Reise und Messe  
Messen und Dienstreisen als Notwendigkeit  
Fremde Umgebung und Kontrollverlust
- 2 **Aktuelle Themen und Beispiele**  
China als „Überwachungsmarkt“  
Zollkontrolle als Sicherheitsrisiko
- 3 Risiken und Konsequenzen für das Unternehmen  
Verlust von sensiblen Daten auf Reisen und Messen
- 4 Abwehrmaßnahmen  
Planung und gesonderte Infrastruktur für Reisen und Messen
- 5 Fazit & Ausblick
- 6 Kontaktinformationen  
**INSIDERSKNOWLEDGE**

# AKTUELLE THEMEN UND BEISPIELE

China als „Überwachungsmarkt“



„If a company has significant intellectual property that the Chinese and Russians are interested in, and you go over there with mobile devices, your devices will get penetrated,” said Joel F. Brenner, formerly the top counterintelligence official in the office of the director of national intelligence.”

- New York Times (10.02.2012)

"Wer in Forschung und Entwicklung tätig ist oder zu den Mitarbeitern zählt, bei denen Außenstehende weitreichende Zugriffsbefugnisse auf Firmendaten erwarten, sollte sich vor der Reise ins Ausland wappnen.“  
Denn die Gefahr sei hoch, Opfer eines Datendiebstahls zu werden.

- Toral Dirro (McAfee)

- Spiegel Online (14.02.2012)

- Beispielsweise New York Times und Spiegel Online berichten 2012 über das Verhalten von Geschäftsreisenden aus den USA nach Russland und China, die sich „leere“ Datenträger und Laptops leihen, und nach der Reise abgeben und löschen, um Datenverlust oder Infektion mit Trojanern zu verhindern.

# RISIKOFAKTOR REISE UND MESSE

Zollkontrolle als Sicherheitsrisiko



Die Installation von Trojanern und anderer Spionagesoftware bei der Ein- oder Ausreise ist bekannt und gilt vor allem für Russland und China. Die Sicherheits- oder Zollkontrolle von Behörden lassen sich vom Reisenden nicht verhindern, eine Rückverfolgung der veränderten, kopierten oder installierten Daten ist selten möglich, da sich moderne Schadsoftware sehr effizient verstecken kann oder sich nach einem Beutezug löscht, und beim Kopiervorgang die Originaldaten erhalten bleiben.

- Kurzfristiger Kontrollverlust kann zu langfristigem, unbemerktem Zugang für Angreifer führen, die sich dadurch auch im firmeninternen Netzwerk umschauen können.
- Trojaner und Spionagesoftware stellen neben Datendiebstahl ein erhebliches Risiko dar, denn selbst nicht mitgeführte Daten geraten in Gefahr.



- Behörden haben bei einem Grenzübertritt meist die Möglichkeit, sich im Rahmen einer Zoll- oder Sicherheitskontrolle Zugang zu einem Gerät zu verschaffen, und potentiell zu kompromittieren. Dies kann auch von dem vorsichtigsten Reisenden nicht verhindert werden, und muss bei der Risikobewertung einkalkuliert sein.

# AGENDA



- 1 Risikofaktor Reise und Messe
  - Messen und Dienstreisen als Notwendigkeit
  - Fremde Umgebung und Kontrollverlust
- 2 Aktuelle Themen und Beispiele
  - China als „Überwachungsmarkt“
  - Zollkontrolle als Sicherheitsrisiko
- 3 Risiken und Konsequenzen für das Unternehmen**
  - Verlust von sensiblen Daten auf Reisen und Messen
- 4 Abwehrmaßnahmen
  - Planung und gesonderte Infrastruktur für Reisen und Messen
- 5 Fazit & Ausblick
- 6 Kontaktinformationen
  - INSIDERSKNOWLEDGE**



# RISIKOFAKTOR REISE UND MESSE

## Datenverlust



Kommt es bei einer Reise oder Messe zu einem Datenverlust, sind diese Tatsache und die Folgen nicht sofort ersichtlich. Selbst der betroffene Mitarbeiter muss nicht zwangsläufig bemerkt haben, dass ihm durch Datenkopie oder geschickte Manipulation sensible Daten entlockt wurden. Auch mitgebrachte USB-Sticks und andere Datenträger erscheinen harmlos, können Angreifern jedoch Zugang zum Rechner, Netzwerk und somit auch zu sensiblen Daten ermöglichen.

- Angreifer beschaffen sich Zugang zu firmeninternen Daten, Netzwerken oder Personen durch den Zugang zu Datenträgern oder technischen Geräten und Einspeisung von Schadsoftware.
  - Unwissende Mitarbeiter geben einem geschickten Gesprächspartner ungewollt sensible Informationen preis, die später gegen diesen Mitarbeiter oder die Firma eingesetzt werden können.
  - Datenträger werden auf der Reise oder Messe verloren, eine Kontrolle über die Daten und ihren Verbleib ist nicht möglich, ein Missbrauch kann nicht ausgeschlossen werden.
- Reisen und Messen mit sensiblen Daten der Firma, oder mit Datenträgern mit späterem Zugang zum Firmennetzwerk bergen Risiken des Missbrauchs und der Infiltration. Auch unwissende Mitarbeiter können in fremder Umgebung manipuliert und zur Herausgabe sensibler Daten gebracht werden.

# AGENDA



- 1 Risikofaktor Reise und Messe
  - Messen und Dienstreisen als Notwendigkeit
  - Fremde Umgebung und Kontrollverlust
- 2 Aktuelle Themen und Beispiele
  - China als „Überwachungsmarkt“
  - Zollkontrolle als Sicherheitsrisiko
- 3 Risiken und Konsequenzen für das Unternehmen
  - Verlust von sensiblen Daten auf Reisen und Messen
- 4 Abwehrmaßnahmen**
  - Planung und gesonderte Infrastruktur für Reisen und Messen
- 5 Fazit & Ausblick
- 6 Kontaktinformationen
  - INSIDERSKNOWLEDGE**

# RISIKOFAKTOR REISE UND MESSE

## Abwehrmaßnahmen



Um dem Datenverlust und der Gefährdung der Sicherheit und Integrität des Firmennetzwerks vorzubeugen, sind zum Beispiel folgende Maßnahmen erforderlich:

- Trainings der Mitarbeiter in der Vorsicht bei Geschäftsreisen und auf Messen im Bezug auf die Risiken für die Datensicherheit, die Herausgabe von Informationen und der Einsatz technischer Abwehrmaßnahmen. Eine persönliche Sensibilisierung erhöht die Wachsamkeit und der Risikoeinschätzung.
- Implementierung eines strikten IT-Konzepts bei Reisen und Messen, wodurch nur bestimmte, vorher „gesäuberte“ technische Geräte verwendet und damit Zugriffe beschränkt werden. Diesen Geräten bleibt später der Einsatz im Firmennetzwerk versperrt.
- Installation von Fernwartung- und Fernlöschungssoftware auf allen mobilen Endgeräten, um Daten bei Verlust oder Diebstahl löschen zu können.
- Nur für die Veröffentlichung zugelassene Daten sollten auf Reisen mitgeführt werden.
- Die Vorbeugung eines Datenverlusts oder externen Zugriffs auf das Firmennetzwerk durch Angreifer auf Reisen oder Messen ist weder aufwändig noch kostenintensiv. Es ist lediglich ein Verständnis der Risiken und eine Einhaltung strikter Richtlinien im Umgang mit designierten „Reise-IT-Geräten“ notwendig. Trainierte Mitarbeiter minimieren das Risiko eines Datenverlusts.



# AGENDA



- 1 Risikofaktor Reise und Messe
  - Messen und Dienstreisen als Notwendigkeit
  - Fremde Umgebung und Kontrollverlust
- 2 Aktuelle Themen und Beispiele
  - China als „Überwachungsmarkt“
  - Zollkontrolle als Sicherheitsrisiko
- 3 Risiken und Konsequenzen für das Unternehmen
  - Verlust von sensiblen Daten auf Reisen und Messen
- 4 Abwehrmaßnahmen
  - Planung und gesonderte Infrastruktur für Reisen und Messen
- 5 Fazit & Ausblick**
- 6 Kontaktinformationen
  - INSIDERSKNOWLEDGE**

# RISIKOFAKTOR REISE UND MESSE

Fazit & Ausblick



Globalisierung und internationale Kooperation machen heutzutage Geschäftsreisen und die Teilnahme an Messen für die meisten Firmen absolut notwendig. Die Risiken eines Datenverlusts bei der Teilnahme sind real, aber nicht unvermeidlich. Durch einfache Maßnahmen und die Einhaltung bestimmter Richtlinien und Verhaltensweisen können Unternehmen die Risiken und Gefahren für Firmendaten und Mitarbeiter minimieren und sich schützen. Zudem sind Trainings der Mitarbeiter im Vorfeld für Geschäftsreisen und Messeteilnahmen auch für andere Geschäftsbereiche sinnvoll und können kombiniert werden. Aus technischer Sicht ist ein Etablierung von „Reise-IT-Geräten“ weder kosten- noch arbeitsintensiv und kann langfristig den Fremdzugang zum Firmennetzwerk verwehren.

Der Trend zu internationalen Wirtschaftsbeziehungen besteht weiter und wird sich verstärken, und internationale Konkurrenz macht Datendiebstahl und Sabotage weiterhin lukrativ. Unternehmen müssen sich dessen bewusst sein und sich gezielt vor Fremdzugriffen schützen. Trainierte Mitarbeiter minimieren langfristig dieses Risiko.



# AGENDA



- 1 Risikofaktor Reise und Messe
  - Messen und Dienstreisen als Notwendigkeit
  - Fremde Umgebung und Kontrollverlust
- 2 Aktuelle Themen und Beispiele
  - China als „Überwachungsmarkt“
  - Zollkontrolle als Sicherheitsrisiko
- 3 Risiken und Konsequenzen für das Unternehmen
  - Verlust von sensiblen Daten auf Reisen und Messen
- 4 Abwehrmaßnahmen
  - Planung und gesonderte Infrastruktur für Reisen und Messen
- 5 Fazit & Ausblick
- 6 **Kontaktinformationen**  
INSIDERSKNOWLEDGE

# INSIDERSKNOWLEDGE

Security by Culture



Wir unterstützen kleine und mittelständische Unternehmen bei der Entwicklung von Informations-Sicherheitsbewusstsein in der Unternehmenskultur. Die Mitarbeiter unserer Klienten sind die erste Verteidigungslinie zum Schutz von Geschäftsgeheimnissen und vertraulichen Daten.

Wir bieten umfassende Sicherheitskonzepte an, die wir individuell an Ihr Unternehmen anpassen. Wir unterstützen Sie gerne bei:

- Managementstrategien zur Stärkung des Sicherheitsbewusstseins im Unternehmen
- Mitarbeitertrainings zur Identifikation von Angriffen und Wirtschaftsspionage
- Trainings für Ihre IT-Mitarbeiter zur Identifikation und Abwehr aktueller Angriffsmethoden
- Analyse und Beratung zur Sicherung bestehender IT-Infrastruktur
- Und allen anderen Fragen zum Thema Informationssicherheit

Für eine kostenlose Vorstellung unserer Beratungsleistungen können uns gerne über [info@InsidersKnowledge.com](mailto:info@InsidersKnowledge.com) kontaktieren.