BVT

WIS[sen] SCHUTZ DURCH WISSEN

WIRTSCHAFTS- UND INDUSTRIESPIONAGE

DAS BULLETIN

AUSGABE 1/2013

IN DIESER AUSGABE

Umgang mit sensiblen Daten im öffentlichen Raum

- Risiken auf Geschäftsreisen
- Sonderfall Messen
- Problematische Situationen im Alltag
- Informationen und Ausblick

BM.I REPUBLIK ÖSTERREICH BUNDESMINISTERIUM FÜR INNERES

Impressum:
Medieninhaber: Bundesministerium für Inneres, Generaldirektion für die öffentliche Sicherheit, 1014 Wien, Herrengasse 7, Telefon: +43 (0)1-53126-0, E-Mail: einlaufstelle@bmi.gv.at, www.bmi.gv.at
Inhaltlich verantwortlich: Bundesamt für Verfassungsschutz und Terrorismusbekämpfung (BVT), 1014 Wien, Postfach 100, Herrengasse 7, Telefon: +43 (0)1-53126-4100, E-Mail: wis@bvt.gv.at
Gestaltung: Bundesministerium für Inneres, Abteilung I/8 - Protokoll und Veranstaltungsmanagement

WKO WIRTSCHAFTSKAMMER ÖSTERREICH

FH CAMPUS WIEN UNIVERSITY OF APPLIED SCIENCES

WIRTSCHAFTS– UND INDUSTRIESPIONAGE

Der Wirtschaftsstandort Österreich ist geprägt durch eine Unternehmenslandschaft, in der sich insbesondere Klein- und Mittelbetriebe häufig auf Nischenprodukte spezialisiert haben oder in der Forschung und Entwicklung tätig sind und ein enormes ökonomisches Potenzial darstellen.

Aktuelle Studien zeigen deutlich, dass jedes Unternehmen – unabhängig von seiner Branchenzugehörigkeit – Opfer von Wirtschafts- und Industriespionage werden kann. Folglich bedarf es eines aktiven Wirtschaftsschutzes. Ergänzend zu dem im Jahr 2011 über Auftrag des BMI/BVT von der FH Campus Wien erstellten Handbuch „Wirtschafts- und Industriespionage – Handbuch Know-how-Schutz für die österreichische Wirtschaft“ liefert das vorliegende Bulletin Informationen zu ausgewählten Themen.

Das Bulletin erscheint zweimal jährlich jeweils im Jänner und September und bietet Themenschwerpunkte, die sich an aktuellen Entwicklungen orientieren, sowie eine Auswahl an relevanten Veranstaltungen und Informationen zu aktuellen Fällen von Wirtschafts- und Industriespionage.

Die vorliegende Ausgabe beschäftigt sich mit dem Umgang sensibler Daten im öffentlichen Raum.

Aufgabe des BVT im Bereich des Wirtschaftsschutzes ist es, neben der operativen Bearbeitung von Wirtschaftsspionage-Fällen im Sinne seiner strategischen Ausrichtung aktiv in der Prävention aufzutreten.

Der Schutz eines Unternehmens vor Wirtschafts- und Industriespionage beschränkt sich nicht ausschließlich auf den Gebäudeschutz, die IT-Sicherheit und die Schulung der Mitarbeiterinnen und Mitarbeiter über den Umgang mit Daten und Unterlagen. Da die Präsentation der Unternehmensprodukte auf internationaler Ebene an Bedeutung gewinnt, ist das Bewusstsein über den optimalen Know-how-Schutz im öffentlichen Raum von großer Bedeutung, sei es auf Reisen im In- und Ausland oder im Nahbereich des Unternehmens.

RISIKEN AUF GESCHÄFTSREISEN

Die Präsentation von Produkten auf Messen oder bei potenziellen Geschäftspartnern im In-, aber vor allem im Ausland ist ein wesentlicher Erfolgsfaktor für ein österreichisches Unternehmen. Dazu zählen persönliche Kontakte als Grundvoraussetzung für eine Vertrauensbasis und eine erfolgreiche Geschäftsbeziehung.

- Länderinformationen einholen.
- Daten auf speziellen Datenträgern sichern und stets mitführen.
- WLAN-Nutzung vermeiden.
- Keine sensiblen Gesprächsinhalte abseits der tatsächlichen Besprechung führen.
- Datenträger nie jemandem aushändigen oder mit fremden Geräten verbinden.

Gerade bei Geschäftsreisen im Ausland steigt das Risiko, Opfer von Wirtschafts- und Industriespionage zu werden. Neben Methoden wie Social Engineering an der Hotelbar erhöht sich die Gefahr des Diebstahls von sensiblen Daten, insbesondere von elektronischen Datenträgern.

Es empfiehlt sich neben Basisschutzmaßnahmen bereits vor Antritt der Reise bestimmte Maßnahmen zu ergreifen. Beispielsweise sollten nur die absolut unerlässlichen Daten mitgeführt werden.

Informationen über das Reiseland, über gesetzliche Bestimmungen, insbesondere Visabestimmungen, sowie über etwaige besondere Verhaltensregeln erhält man unter anderem über die Webseiten des Außenministeriums und der WKÖ.

Es empfiehlt sich, sensible Daten getrennt vom Laptop auf Datenträgern wie USB-Sticks oder SD-Karten (eventuell verschlüsselt) mitzuführen und diese sicher zu verwahren. Hier sollte im Vorfeld der Reise abgeklärt werden, ob eine Einreise bei Mitführen von verschlüsselten Daten gegebenenfalls verweigert werden kann (z. B. in China).

Gefahrenquellen sind im Wesentlichen alle vom Veranstalter zur Verfügung gestellten Kommunikationsmittel (z. B. WLAN, Bluetooth, Präsentations-PC), aber auch Hotelzimmer und Besprechungsräume. Bei Restaurant- und Hotelbarbesuchen sollte man Gespräche über Unternehmensgeheimnisse vermeiden, da andere Besucher mithören könnten.

SONDERFALL MESSEN

Messen werden nicht nur von Unternehmern, sondern auch von Angreifern genutzt. Zum einen bieten speziell für die Veranstaltung installierte IKT-Infrastrukturen und die in den Verkaufsständen verwendeten Datenträger (Laptops, Handys u. a.) gute Möglichkeiten für den Zugriff auf sensible Daten durch Unberechtigte. Zum anderen können Ausstellungsstücke oder Produktdarstellungen gefilmt oder fotografiert werden. Selten sind fertige Produkte Ziele einer Ausspähung, sondern es sind meist Forschungsinhalte und Details einzelner Komponenten von Produkten.

Einfache Gegenmaßnahmen sind die „Verfälschung“ von Skizzen, Konstruktionsplänen, Schauobjekten und Berechnungsbeispielen und die Überwachung des Standes während der Messe und der Auf- und Abbauarbeiten. Des Weiteren empfiehlt sich ein gesundes Misstrauen gegenüber „Give-aways“ wie USB-Sticks. Diese könnten unerwünschte Software enthalten.

PROBLEMATISCHE SITUATIONEN IM ALLTAG

In einer mobilen Welt wird beinahe jeder Bereich des täglichen Lebens zum Arbeitsplatz. Zu bedenken ist, dass geschäftliche Telefonate nur bedingt für fremde Zuhörer geeignet sind und dass insbesondere das Arbeiten auf dem Laptop, Tablet oder Smartphone eine erhöhtes Risiko des unerwünschten Informations-abflusses darstellt.

Wer öffentliche Verkehrsmitteln benützt, sollte bedenken, dass andere Passagiere am Display eines Endgerätes mitlesen könnten. Displayschutzfolien können den einsehbaren Bereich reduzieren. Sie bieten aber im Regelfall keinen Schutz bei direkten Blicken über die Schulter.

Funkbasierende Systeme wie WLAN, Bluetooth und NFC-Technologien (Near Field Communication) bergen vor allem im öffentlichen Raum das Risiko eines ungewollten Informationsabflusses. Deshalb wird bei der Nutzung von WLAN empfohlen, die Daten verschlüsselt abzuspeichern, ein von den schutzwürdigen Daten abgekoppeltes Benutzerprofil für die Internetnutzung anzulegen und sich nur in vertrauenswürdige Netze einzuloggen.

Bei Bluetooth-Geräten sollten die voreingestellten Konfigurationen überprüft und die Schnittstellen bei Nichtbenutzung deaktiviert werden. Die Kopplung an fremde Geräte sollte nur in einer geschützten Umgebung stattfinden und die Geräte müssen vertrauenswürdig sein.

Konkrete Schutzmaßnahmen bei NFC sind vorwiegend von den mit dieser Technologie verwendeten Anwendungen abhängig. Daher wird bei einer Verwendung im Geschäftsbereich eine Authentisierung und Verschlüsselung auf Anwendungsebene empfohlen.

Durch Meldungen von Verdachtsmomenten bzw. kritischer Situationen in Bezug auf Wirtschafts- und Industriespionage im Ausland oder bei Messen ist es dem BVT als kompetentem und vertrauenswürdigem Ansprechpartner möglich, Risikoprofile zu erstellen und dadurch aktuelle Trends aufzuzeigen.

INFORMATIONSQUELLEN FÜR GESCHÄFTSREISENDE

Die WKÖ bietet neben Länderinformationen auf ihrer Webseite (www.wko.at) eine Export-Service-App für iOS an, mit der kompakte Informationen zu Ländern und Branchen sowie Ansprechpartnerinnen und -partnern im In- und Ausland und Tipps für Geschäftsreisende abgerufen werden können.

Das Außenministerium bietet auf seiner Webseite (www.bmeia.gv.at) ebenfalls umfangreiche, nach Themen untergliederte Länder- und Reiseinformationen an.

AUSBLICK

Produkt- und Forschungsdaten im Bereich der erneuerbaren Energien stehen derzeit im Fokus von Wirtschafts- und Industriespionageangriffen. Deshalb wird dieses Thema in der **Ausgabe 1/2014** schwerpunktmäßig behandelt.

KONTAKT

Für weiterführende Informationen und vor allem im Anlassfall steht das BVT zur Verfügung:

Bundesamt für Verfassungsschutz und Terrorismusbekämpfung

E-Mail:	wis@bvt.gv.at
Telefon:	+43-(0)1-53126-4100
Postanschrift:	Herrengasse 7, Postfach 100, 1014 Wien

VERANSTALTUNGEN

- **Wirtschafts- und Industriespionage – So schützen Sie Ihr Unternehmen**
  19. September 2013 – WKNÖ
  Informationsveranstaltung mit Vorträgen von Vertretern des BVT, der ICC Austria und der FH Campus Wien über aktuelle Bedrohungen, NSA und Ausbildungsmöglichkeiten
- **Betriebs- und Wirtschaftsspionage**
  5./6. November 2013 – ICC Austria
  Seminar über aktuelle Bedrohungen im Bereich WIS
- **Datenschutz und IT-Sicherheit**
  5. November 2013 – ARGE Daten
  Tagesveranstaltung mit Informationen über IT-Sicherheit, Datenschutz sowie den Aufbau eines Information-Security-Management-Systems