Industrie- und Handelskammer Hannover

IT-Sicherheit auf Auslandsreisen

Ein Merkblatt der Industrie- und Handelskammer Hannover

Das Know-how der deutschen Wirtschaft weckt in anderen Ländern Begehrlichkeiten: Achten Sie insbesondere auf Geschäftreisen darauf, dass interne Informationen auch intern bleiben. Allein im Jahr 2005 zählte die Tourismusorganisation der Vereinten Nationen (UNWTO) knapp 150 Mio. Geschäftreisen für Deutschland. Davon führten etwa 30 Prozent ins Ausland.

Der Datenklau lauert überall – hier sind die wesentlichen Angriffsfelder zusammengestellt:

1. Verhalten auf Flughafen und Flug

Situation: Bereits der Flughafen und der Flug selbst sind ein ertragreiches Feld für Datensammler. Spionen können hier, ohne überhaupt strafbare Handlungen zu begehen, Sie und Ihre Daten ins Auge fassen. Sie hören Ihren Telefonaten – stationär oder mobil – zu, oder lesen aus guter Position mit, was Sie gerade auf dem Bildschirm Ihres Notebooks haben.

Schutz:

- Reden Sie nie über vertrauliche Informationen per Telefon oder Mobiltelefon in öffentlichen Bereichen oder wenn Sie sich nicht sicher sind, dass jemand Ihre Gespräche hören kann.
- Arbeiten Sie an öffentlichen Orten nicht mehr an Dateien und Schriftstücken, die vertraulich sind.
- Schließen Sie nach jedem Surfen auf jeden Fall die WLAN Funktion Ihres Notebooks.

2. Datenverlust durch Hardware-Klau

Situation: Notebook-Diebstahl ist nach Virusattacken das zweithäufigste Computer-Delikt. Schätzungsweise 10 Prozent aller Notebook-Computer werden jährlich gestohlen, davon ereignet sich jeder zehnte Diebstahl auf Flughäfen. Wenn neben dem Wert, den die Hardware und Software darstellt, auf dem Gerät Präsentationen oder andere relevante Daten für die Geschäftstermine aufgespielt waren, ist der Erfolg der Reise gefährdet bzw. die Reise hinfällig. IT-Sicherheitsexperten stellten zudem fest, dass

57 Prozent aller Probleme bei der Netzwerksicherheit auf den Diebstahl von mobilen Systemen zurückzuführen sind.

Die Gefährdung von Firmendaten durch Hardware-Klau wird sich mit steigendem Gebrauch von PDAs (Personal Digital Assistant) und Smartphones (zum Beispiel BlackBerry) nach Ansicht von Experten noch verschlimmern.
Schutz:

- Führen Sie Ihr Equipment bei der Reise im Handgepäck mit sich und behalten Sie es permanent unter Aufsicht.
- Lassen Sie Ihr Notebook im Zielland nie ungesichert liegen – weder am Arbeitsplatz noch in Hotels.
- Verstauen Sie Ihr Notebook im Auto so, dass es nie von außen sichtbar ist.
- Schließen Sie es in Schränken, Rollenbehälter oder Koffer innerhalb eines Gebäudes ein.
- Ist dies nicht möglich, sichern Sie Ihr Notebook mit einem Schloss oder Stahlseilsystem.
- Beispielsweise schreiben IT-Security-Policies bestimmter Konzerne vor, Notebooks in Risikoländern nur in den eigenen Standorten aufzubewahren.

Wenn Ihr Equipment schon gestohlen wurde, sollten Diebe bzw. Finder nicht an Ihre Informationen oder Dateien gelangen – ergreifen Sie folgende Maßnahmen:

- Nutzen Sie einen Bildschirmschoner für das Notebook mit einem Passwortschutz, der spätestens nach 15 Minuten aktiviert wird.
- Nutzen Sie die von den Systemen angebotenen Schutzmechanismen, z. B. eine Festplattenverschlüsselung und weitere Verschlüsselungstechniken.
- Ebenso sollte ein aktueller Virenschutz nicht fehlen.
- Wichtig sind auch sichere Passwörter: eine Kombination aus Buchstaben und Zahlen ist angebracht. Verwenden Sie nie gängige Begriffe wie Vornamen oder Geburtsdaten.
- Verschlüsseln Sie auch Datenträger wie USB-Sticks, CDs, DVDs oder auch PDAs.

3. Einreise

Situation: Weitere gezielte Angriffe auf Daten können im Reiseland auftreten. Allen voran sind hier Russland, die Gemeinschaft Unabhängiger Staaten (GUS) und China zu nennen.
Eine besondere Situation ergibt sich bei der Einreise in die USA. Dort haben der Zoll und die Sicherheitskräfte nach der aktuellen Gesetzeslage die Möglichkeit, Privat- und Geschäftsgeräte zu überprüfen und sogar zu konfiszieren – die Rückgabe kann sich jenseits von vier Wochen bewegen.

Schutz:

- Datenmedien sollten nie unbewacht sein.
- Geheime Daten können zumindest auf der Hinreise auf einer CD oder einem USB-Stick am Körper getragen werden und der Inhalt der Datenträger erst zur Präsentation auf das Notebook gespielt werden. Allerdings sind danach auch von dort gelöschte Daten von Profis rekonstruierbar.
- Geheime Konstruktionspläne sollten besser nur in Papierform am Körper getragen und nach Gebrauch vernichtet werden.

4. Kommunikation

Situation: Insbesondere in Russland, den GUS-Staaten und China findet eine umfassende Überwachung aller technischen Kommunikationskanäle statt. Telefonleitungen, Internetverbindungen oder optische und akustische Raumüberwachungsanlagen – hier laufen insbesondere Geschäftsreisende in die Gefahr der totalen Überwachung.

Schutz:

- Verschlüsseln Sie besser auch alle mobilen Datenträger, wie USB-Sticks, CD, DVD, PDA. Viele Smatphones und Handys können via Software verschlüsselt werden. Analoge ISDN-Telefone lassen sich mit kleinen Cryptoboxen erweitern.
- Das Notebook wird zu einem leichten Opfer, wenn Sie versehentlich die WLAN-Funktion durch Tastendruck aktivieren eine falsche Konfiguration haben oder vergessen, das Notebook nach dem Surfen abzuschalten. Der Angreifer täuscht dazu entweder einen Access Point unter falschem Namen vor, mit dem sich das Notebook automatisch verbinden kann, oder er verwendet die Funktionen zur direkten Rechnerkopplung über WLAN.

- Wenn Sie ein eigenes Firmennetz haben, ist ein VPN-Tunnel (Virtual Private Network) mit starker Verschlüsselung geeignet.
- Die Einwahl via Internet sollte nur über so genannte Einmalpasswörter erfolgen, die über einen Chip generiert werden.
- Auf dem BlackBerry lässt sich SIM-Karten unabhängig ein Kennwort einrichten, das nur eine zehnmalige Falscheingabe zulässt, wenn es vergessen wurde oder Ungefugte das Gerät knacken wollen, bevor der gesamte Inhalt gelöscht wird.
- Eine zusätzliche Verschlüsselungsmöglichkeit für den Datentransfer von Endgerät zu Endgerät bietet Zusatzsoftware von Drittherstellern wie PGP (Pretty Good Privacy) oder S/MIME. Allerdings erlauben Kanada und Großbritannien, in denen die BlackBerry-Server ihren Standort haben, den Sicherheitsbehörden den Zugriff auf die Daten.

Zusatz: Rechtliche Aspekte sind beim Verschlüsseln zu beachten: Russland, Weißrussland und Myanmar haben massive Beschränkungen und starke Kontrollen bei der persönlichen Nutzung von Kryptographie auf mobilen Endgeräten von Geschäftsreisenden.

5. Gebäude

1. Situation: Gebäude bieten ebenfalls Sicherheitsrisiken. Datendiebe können von der Straße aus systematisch Gebäude absuchen, in denen nicht geschützte WLAN-Verbindungen ein Ausspionieren ermöglichen – so genanntes Wardriving. Diese Gefahr besteht allerdings auch direkt vor der Haustür. WLAN-City-Maps mit offenen Verbindungen sind bereits für viele Städte erstellt worden.
Hinweis:

- Verwenden Sie größte Sorgfalt darauf, alle WLAN- Verbindungen zu verschlüsseln.

2. Situation: Wenn mobile Kleingeräte wie Handy, PDA, Smartphone mit Computern oder Peripheriegeräte (etwa einem Drucker) über eine drahtlose Funkvernetzung (Bluetooth) miteinander kommunizieren, sind diese ungesichert auch für Angreifer offen (Blueprinting).
Hinweis:

- Bluetooth sollte nur verdeckt betrieben werden. Alle Einstellungen sollten an den Geräten auf höchster Sicherheitsstufe konfiguriert und die kommunizierenden Geräte mit Kennwörtern geschützt werden.

3. Situation: Eine Reihe von Bluetooth-fähigen Geräten weisen eine Sicherheitslücke auf, die sich zum so genannten Bluebugging nutzen lässt. Dabei kann ein Angreifer über ein nicht geschütztes Mobiltelefon SMS-Nachrichten versenden, zum Beispiel an Adressaten aus dem Telefonbuch des "gekappten" Telefons. Für den Empfänger sieht es so aus, als käme die SMS von einem ihm bekannten Absender. Er kann somit an sensible Informationen kommen und nach dem Angriff sogar seine Spuren verwischen.
Hinweis:

- Achten Sie auch auf Ihre mobilen Endgeräte.

4. Situation: In Besprechungen und Verhandlungen möchten z. B. alle Teilnehmer die besprochenen Fakten vor Augen haben, weshalb oftmals vor Ort Unterlagen ausgedruckt oder kopiert werden.
Hinweis:

- Achten Sie darauf, dass Sie keine vertraulichen oder geheimen Informationen beim Kopierer liegen lassen.
- Faxen Sie auch keine vertraulichen Dokumente.

Weitere Informationen auch:

Niedersächsisches Ministerium für Inneres und Sport
Verfassungsschutz, Wirtschafts- und Geheimschutz
Tel. (0511) 6709-247
Fax: (0511) 6709-393
E-Mail: wirtschaftsschutz@verfassungsschutz.niedersachsen.de
www.verfassungsschutz.niedersachsen.de

Autor:
Sabine Hillmer
Abteilung Industrie und Verkehr
Tel. (0511) 3107-272
Fax (0511) 3107-430
E-Mail: hillmer@hannover.ihk.de
Industrie- und Handelskammer Hannover
Schiffgraben 49
30175 Hannover
www.hannover.ihk.de