



Bild1: Bei Unaufmerksamkeit lässt sich ein USB-Stick schnell entwenden. Bilder: Innenministerium NRW

Wenn einer eine Reise tut ...

Sensible Daten auch unterwegs sichern

Geschäftsreisen im Inland wie auch in das benachbarte oder weiter entfernte Ausland gehören heute zum beruflichen Alltag. Die vielen Stolpersteine, die unterwegs zu Know-how-Verlust führen können, sind aber den Wenigsten bekannt oder bewusst. Viele schrecken auch vor dem Thema zurück, weil sie alltagsuntaugliche und kostenintensive Maßnahmen auf sich zukommen sehen. Dennoch ist es möglich, den vielfältigen Angriffen und Risiken mit relativ wenig Aufwand zu begegnen.

Wie bei jeder Reise, ist auch hier der erste Schritt der wichtigste, und der beginnt bereits vor dem Antritt der Reise mit einer mentalen Vorbereitung. Aus zahlreichen Gesprächen mit Unternehmensvertretern weiß die Spionageabwehr NRW: Es kommt immer wieder zu Know-how-Abfluss, weil den betreffenden Informationsträgern nicht in aller Schärfe bewusst ist, welche Firmendaten offen sind und welche auf keinen Fall weitergegeben werden dürfen.

Das Grundprinzip bei jeglichem Know-how-Schutz ist dabei zuerst die Definition und Geheimhaltung der fünf bis maximal 15 Prozent an vertraulichen Daten, die nicht offen bei Vertragsverhandlungen, Messen oder in Werbemate-

rialen und ähnlichem präsentiert werden. Dies hört sich lapidar an. Aber jeder, der schon einmal in einem ICE-Abteil gesessen hat, in dem ein geltungsbedürftiger Geschäftsreisender seiner Assistentin komplette Berichte über pharmakologische Forschungen in das Handy diktierte, oder in einem Flugzeug die Powerpoint-Präsentation seines Sitznachbarn bewundern durfte, weiß, wovon hier die Rede ist. Es sind die kleinen menschlichen Schwächen, die immer wieder dazu verleiten, mehr preiszugeben, als man eigentlich bei distanzierter Betrachtung preisgeben wollte.

Vergegenwärtigt man sich diese Gefahr aber vor Antritt der Reise und führt sich noch einmal die absolut

vertraulich zu behandelnde Datenmenge vor Augen, reduziert sich die Wahrscheinlichkeit, dass man unabsichtlich Know-how verrät, bedeutend.

Risiken mobiler Kommunikationsmittel

Heutzutage ist eine Geschäftsreise ohne Datenträger und Kommunikationsmittel wie Notebook, PDA, USB-Stick und Handy nicht mehr vorstellbar. Diese Hilfsmittel erleichtern die Arbeit zwar sehr, lassen aber häufig vergessen, dass sie in ihrer Kompaktheit Datenmengen in einem Umfang vorrätig halten, der vor einigen Jahren noch einen leistungsfähigen PC erfordert hätte.

Deswegen gilt auch hier die Maxime, nach Möglichkeit datentechnisch

→ AUTOR

Heike Vehling ist Referentin für Spionageabwehr im Innenministerium NRW, Düsseldorf
Tel.: 0211 871 2821
E-Mail: abteilung-vi@im.nrw.de
www.im.nrw.de



mit „leichtem Gepäck“ zu reisen. Es sollten nur die Daten mitgenommen werden, die unbedingt vor Ort benötigt werden. Denn alles, was man gar nicht erst mitnimmt, kann unterwegs auch nicht verloren werden. Der Verlust tritt möglicherweise schneller ein, als man sich das vorstellt. Mobile Datenträger werden aufgrund ihrer Kompaktheit leicht entwendet, was zwar eine primitive, aber nichtsdestotrotz sehr wirksame Maßnahme darstellt, um an fremdes Wissen heranzukommen (Bild 1).

Der Diebstahl eines Notebooks und ähnlichem Gerät aus Hotelzimmern, etwa in Moskau, berichteten Geschäftsreisende der Spionageabwehr NRW schon häufiger. Daher ist es absolut notwendig, auf solche Datenträger sorgsam zu achten und sie zu schützen. Wenn man sie nicht ständig bei sich tragen kann, sollte man sie also zumindest gut verschließen. Ein weiteres Risiko - von vielen schnell abgetan - liegt in dem schlichten „Vergessen“ solcher Geräte. Wie Studien aus der jüngsten Zeit belegen, stellt dies weltweit eine der häufigsten Ursachen für Datenverlust dar. Angesichts dieser Fakten sollte der Appell zur Achtsamkeit jedenfalls keine Heiterkeit mehr hervorrufen.

Schutz sensibler Daten

Aber selbst, wenn einmal ein Datenträger verloren geht, bedeutet dies keine Katastrophe, wenn vorher darauf geachtet wurde, dass der Zugang zu den gespeicherten Daten effektiv geschützt ist. Auch dies klingt banal, aber wie die Erfahrungen zeigen, sind es immer wieder die einfachen Sicherungsmaßnahmen, die im Eifer des Gefechts oder aus Bequemlichkeit missachtet werden. Jeder User weiß, dass er den Zugang zu seinem Notebook mit Passwort sichern sollte und dass er hochsensible Informationen mit einer Verschlüsselung schützen muss. Im Einzelfall können aber Umstände wie eine gezielte Überrumpelungstaktik dazu führen, dass diese Sicherheitsmaßnahmen nicht durchgeführt werden (Bild 2).

In einem Fall, den Firmenvertreter nach einer China-Reise der Spionageabwehr NRW berichteten, wurden die gut vorbereiteten und sensibilisierten deutschen Geschäftsreisenden zunächst in ihren Verhandlungsgesprächen unterbrochen. Anschließend bat man sie in höchst dringlicher und aufgeregter Form, sofort den Verhandlungstisch

zu verlassen, um einen hochrangigen Politiker kurz zu begrüßen, der gerade vor Ort weilte. Sie wurden damit unter Druck gesetzt, dass ein anderes Verhalten als Beleidigung verstanden worden wäre, so dass sie diesen dringenden Bitten nachkamen, sicherten aber in der Hektik ihre Notebooks nicht. Als sie schließlich nach mehreren Stunden wieder in den Besprechungsraum zurückkehrten, stellten sie Manipulationen an ihren Geräten fest.

Jeder, der sich jetzt selbstsicher zurücklehnt und meint, dass könne ihm nicht passieren, sollte sich einmal eine ehrliche Antwort darauf geben, ob er wirklich dem immensen Druck in einem fremden Land in einer ungewohnten Situation ruhig begegnen könnte, zumal dann, wenn er keine bösen Absichten unterstellt.

„Feind hört mit“

Es weiß auch jeder im Prinzip, dass E-Mails wie Postkarten sind, für den erfahrenen Internetnutzer offen lesbar. Aber wer denkt daran, wenn man unterwegs, im Hotelzimmer oder wenn es schnell gehen muss auf fremde Hot Spots zugreift? Auch von möglichen Sicherheitslücken beim Einsatz von Blackberrys, die aktuell Gegenstand einer Untersuchung des Bundesamts für Sicherheit in der Informationstechnik sind, haben Geschäftsreisende immer wieder gehört. Das mögliche Risikoszenario, dass die in England und USA stationierten Mailserver von den dortigen Nachrichtendiensten angezapft werden, hat die französischen Sicherheitsbehörden veranlasst, ihrer Regierung die Nutzung zu untersagen.

Grundsätzlich sollte man auf Reisen den Einsatz von Verschlüsselungssoftware erwägen, denn es gibt Länder, in denen die Nachrichtendienste jederzeit unkontrollierten Zugriff auf Internetverbindungen haben, also jede Kommunikation und jeden Schritt im Internet mitbekommen.

Häufig geht allerdings mit diesen Überwachungsmethoden ein Verbot des Einsatzes von Kryptotools Hand in Hand, so dass in jedem Einzelfall recherchiert werden muss, ob es sich um ein legales Mittel handelt. Zu den Ländern, die jede Internetkommunikation überwachen können, gehört zum Beispiel Russland, das mit dem Gesetzesakt SORM2



Bild 2: Profis können von Unterlagen nahezu perfekte Kopien anfertigen.

geregelt hat, dass private Internetprovider nur dann eine Lizenz erhalten, wenn sie eine ständige Schnittstelle für die staatlichen Stellen einrichten. Vergleichbar, nur noch etwas komfortabler für den Staat, ist die Situation in China, das ausschließlich staatliche Internetprovider kennt und somit jederzeit einen ungehinderten Zugriff auf Internetverbindungen hat.

Schwächen ausnutzen

Zum Schluss muss wieder einmal das Klischee bemüht werden: Geschäftsreisende sollten sich dessen bewusst sein, dass auch die „altmodischen“ Methoden immer noch eingesetzt werden. Situationen, in denen menschliche Schwächen wie Drogen-, Spielsucht, Alkoholprobleme, Prostituiertenkontakte oder ähnliches dokumentiert werden, um sie zur Zusammenarbeit und zum Verrat von Know-how zu veranlassen, finden immer wieder ihre Entsprechung in der Realität. Dass zu diesem Zweck Hotelzimmer mit Überwachungselektronik ausgestattet werden, überrascht nicht. Solche Berichte gibt es vor allem aus Russland und China. Die einfachste Methode, solchen Gefahren aus dem Weg zu gehen, liegt auch hier darin, sich diese Risiken bewusst zu machen und ein gesundes Misstrauen zu kultivieren. □