Eine Frage des Überlebens

Informationsschutz als Grundvoraussetzung

Ansgar Alfred Huth ist International anerkannter Sachverständiger für Datenschutz und Lauschabwehr

In einer Zeit, in der Unternehmen nach schwarzer Zahlenluft schnappen, wird mit harten Bandagen ums Überleben gekämpft. Die angespannte Wirtschaftslage lässt viele Protagonisten von der Bildfläche verschwinden. Aber nicht nur die schleppende Konjunktur ist ein Unternehmenskiller. Immer mehr Firmen fallen der Industriespionage zum Opfer.

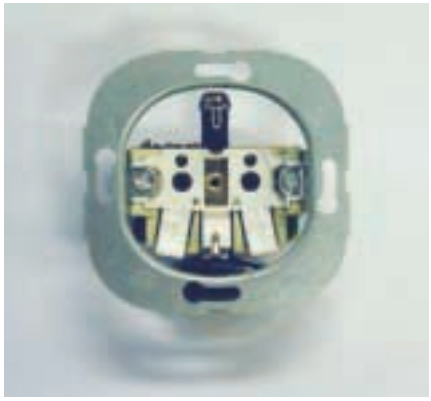

Bild 1: Einbaufertige, verwanzte Unterputzsteckdose: Die Wanze geht nur auf Sendung, wenn gesprochen wird.

Die reduzierte Luft am internationalen Umsatzhimmel veranlasst so manchen Geschäftsmann, über den Einsatz illegaler Informationsbeschaffer nachzudenken. Mit so gewonnenen Interna eines lästigen Mitanbieters lässt sich auf elegante Art und Weise ein Unternehmen aushöhlen und sicher zu Konkursmasse verwandeln. Die Bereitschaft, solche verbotenen Informationsbringer einzusetzen, ist in den vergangenen Jahren immens gestiegen, da minimaler Kostenaufwand für die Lauschmittel maximalen Vorteil verspricht (**Bild 1**). Hinzu kommt, dass das Risiko des Lauschers, bei einer Abhöraktion ertappt zu werden, gegen null tendiert (**Bild 2**). Denn wer verfügt schon über eine schützende Lauschabwehreinrichtung?

Die nicht selten zu beobachtende Arroganz, mit der – meist junge – Manager und deren Sicherheitsbeauftragte die potenzielle Gefahr von Industriespionage und Informationsdiebstahl abhandeln, ist definitiv ein verantwortungsloses Unternehmensmanagement „à la Kamikaze“. Dabei gibt es für ein im harten Konkurrenzkampf stehendes Unternehmen nichts Gefährlicheres als das Abhandenkommen vertraulicher Informationen.

Unbequemes Thema

Hat sich ein Unternehmen einmal mit dem unbequemen Thema Industriespionage und Informationsdiebstahl auseinandergesetzt, dann glauben Verantwortliche oft, mit einem einzigen Lauschabwehreinsatz der Vorsorgepflicht Genüge getan zu haben. Wird bei diesem Lauschabwehreinsatz kein direkter Angriff detektiert, so hören Sachverständige für Datenschutz und Lauschabwehr hin und wieder hellseherische Sätze wie „das habe ich mir schon so gedacht, dass da nichts ist.“ Sollte ein Sachverständiger während eines Einsatzes aber einen Lauschangriff detektieren oder diesen im Nachhinein nachweisen können, bricht in diesem Moment die geordnete planerische Welt der Geschäftsführung in sich zusammen. Plötzlich erscheinen bisher nicht erklärliche Vorgänge aus der Vergangenheit in einem ganz anderen Licht.

Meist braucht es einige Tage, um zu realisieren, was dieser unbemerkte Informationsabfluss bei einem Unternehmen wirklich bedeutet. Ob Vertriebsstrategien, Kaufabsichten oder bevorstehende Übernahmen: Dies alles sind für den Informationsdieb Gewinn bringende Ereignisse und für das Unternehmen unkalkulierbare Risiken. In dieser Situation stellen sich der Geschäftsführung sorgenvolle Fragen: Wie lange hören die uns schon ab? Was und wie viel können die von unserer Planung und unserer wirtschaftlichen Gegenwart wissen? Wer verfügt jetzt über unsere Informationen? Welche Informationen haben wir verloren? Wer hier nicht durch sinnvolle Maßnahmen Vorsorge geleistet und z. B. in überschaubaren Abständen den Dienst eines Lauschabwehr-Sachverständigen geordert hat, für den gibt es in dieser Stunde keine Antwort.

Die Warnungen und Aufklärungsbroschüren der Behörden und Bundesämter in Sachen Industriespionage sind ernst zu nehmen. Der Erkenntnis, dass Informationsbeschaffung, intelligente Auswertung der Informationen und deren gezielter Einsatz Grundlage des Erfolgs sind, kann sich niemand verschließen.

Zu begreifen, wie einfach es ist, sein Gegenüber durch Informationsmissbrauch zu vernichten, ist der Schlüssel zum Schutz der eigenen Informationen. Es gibt hier allerdings, so zeigt die Praxis, einen erheblichen Nachholbedarf. Das Thema Wirtschaftsspionage behandeln heute dementsprechend zunehmend große Zeitungen und verantwortungsvolle Fachzeitschriften Europas. Wirtschaftsspionage kristallisiert sich in immer mehr aufgedeckten Fällen als Kern des Unternehmensübels heraus. Große und kleine Unternehmen werden zunehmend unbemerkt von Know-how-Dieben heimgesucht und sterben immer öfter einen unerklärbaren, langsamen Tod. Meist suchen Verantwortliche dann an allen möglichen Stellen nach Ursachen und drehen das Personalkarussell, ohne dass die Verantwortlichen auf den Gedanken kämen, dass es ein „Informationsloch“ gibt.

Schwachstelle Handy

Geschäftsführer müssen permanent zu erreichen sein. Zum Glück gibt es ja Handys

Bild 2: Empfänger, der belauschte Gespräche an einem sicheren Ort empfängt und aufzeichnet: Mit einem ISDN-Anschluss oder GSM-Handy kombiniert, kann der Lauscher weltweit mithören und aufzeichnen. (Fotos: Huth)

in allen Varianten und Formen. Jedoch gibt es auch Applikationen dieser kleinen Informationsbringer, die eigenmächtig und vom Nutzer unbemerkt auf Sendung gehen. Die im Umkreis des Handy-Besitzers geführten Gespräche, vertraulich oder nicht, werden dann direkt an eine vorprogrammierte Telefonnummer weltweit versendet. Ein „Spy-Handy“ kann z. B. über eine intelligente Sprachsteuerung verfügen, die eigenständig entscheidet, wann es am sinnvollsten auf Sendung geht und den Lauscher mit den Gesprächen des abgehörten Geschäftsmannes versorgt, und wann es sich besser wieder in den Energie sparenden Bereitschaftsmodus begibt.

Nutzt beispielsweise ein Handelsvertreter ein Spy-Handy, kann dieses eigenmächtig seine Fahrtroute und den aktuellen Aufenthaltsort aufzeichnen und unbemerkt per SMS oder E-Mail an den wissensbegierigen Mitbewerber versenden. Überwacht der Mitbewerber dieses Handy mit einem Laptop oder per Internet, so kann er nicht nur das Bewegungsprofil dieses Vertreters aufzeichnen, sondern er kann, je nach übermitteltem Aufenthaltsort dieses Handy-Besitzers, eigene Programmabläufe starten und z. B. Sonderangebotsfaxe auslösen. Es ist erschreckend, wie sehr ein Mitbewerber mit solch einem System einem überwachten Vertreter oder Manager das Geschäftsleben schwer machen kann.

Der Geschäftsmann von heute muss über eine sinnvolle Informationsschutzausbildung verfügen und nicht nur seinen eigenen Bewegungsradius im Griff haben. Auch der Informationsradius seiner Mitarbeiter ist für ihn von großer Bedeutung. Dazu gehört, dass er neben seinen eigenen Kommunikationsmitteln auch die seiner Gesprächspartner im Griff hat und jederzeit z. B. einen Handy-Spionageangriff ohne großen Aufwand abwehren kann. Wenn während einer Besprechung ein Anwesender einen Anruf erhält, dann ist dies nichts Besonderes, solange sich das Handy auch wie gewohnt bemerkbar macht. Sollte sich jedoch eines der Handys selbstständig machen und getarnt auf Sendung gehen, dann muss der Geschäftsmann diesen Angriff, ohne großartig abgelenkt zu werden, sicher detektieren können und seinen Gesprächspartner auf das aktive Handy aufmerksam machen.

Solche und andere Informationen erhält man in Seminaren, die z. B. das Aufspüren und Überwachen von GSM-Handys, das gezielte Modifizieren eines Handys zu einem wertvollen Informationsbringer oder die Möglichkeiten der Verwendung eines handlichen GPS-Systems zur Informationsbeschaffung zum Thema haben. Allgemeine Seminare zu Informationsschutz und Abhörsicherheit geben einen Überblick zum Thema Angriffs- und Abwehrtechniken der illegalen Informationsbeschaffung, eine realistische Einschätzung der bestehenden Gefahr und einen Querschnitt über die Möglichkeiten der effektiven Vorbeugung.

Das Thema in Kürze

Thema: Spionage und Informationsdiebstahl im Unternehmen
Problemstellung: Der Diebstahl vertraulicher Informationen kann Unternehmen in den Ruin treiben.
Lösung: Eine sinnvolle Ausbildung in Informationsschutz und der tatsächlichen Bedrohung entsprechende Einrichtungen zur Lauschabwehr können helfen, die Gefahr durch Wirtschaftsspionage zu begrenzen.

Ansgar Alfred Huth,
Hanauer Str. 58, 63755 Alzenau,
Tel.: 06023-918700, Fax: -918701,
huth@spionage.info, www.spionage.info