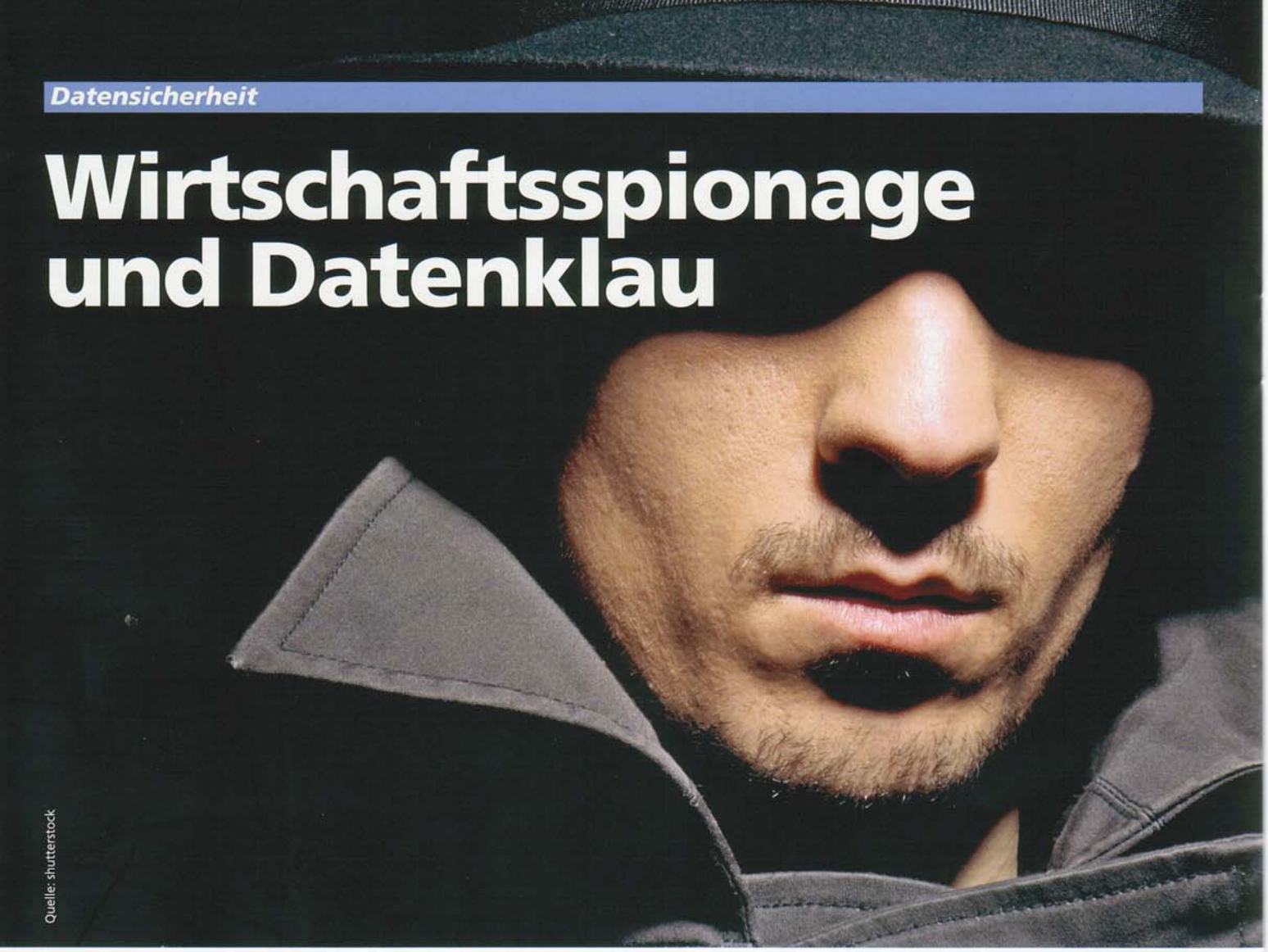
Wirtschaftsspionage und Datenklau



Quelle: shutterstock

Einerseits haben die letzten Monate gezeigt, dass es selbst bei grossen Firmen wie Amazon, Apple oder Sony zu schlimmen Pannen mit Kundendaten kommt. Andererseits stellen sich neue Anforderungen in Bezug auf den technologischen Fortschritt und unseren zunehmend selbstverständlicheren Umgang mit neuen Kommunikationsmitteln. Aktuelle Zeugen dieser Tendenzen sind die schnelle Verbreitung mobiler Geräte mit immer mehr Funktionen und der Einbezug von Social-Media-Plattformen in kommerzielle Prozesse. Die Bedrohungslage hat sich insoweit geändert, dass die Mittel dazu moderner werden, die Bevölkerung immer vernetzter ist und dass ein zu geringes oder gar kein Sicherheitsbewusstsein vorhanden ist.

VON WOLFGANG SIDLER

Ein Grossteil der Daten, welche in einem Unternehmen ausgetauscht werden, ist schützenswert, was sich auch in gesetzlichen Bestimmungen widerspiegelt. Verfehlungen im Umgang mit Daten gehen in den meisten Fällen mit der Verletzung vertraglicher Pflichten einher. Daten natürlicher und juristischer Personen unterstehen zusätzlich dem Datenschutzgesetz. Zusätzlich wird es für Unternehmen schwieriger, welche grenzüberschreitend oder global Daten austauschen und so eine Vielzahl von landesspezifischen Bestimmungen beachten müssen.

Der Hype um die Clouds verschärft das Thema. Der Nutzer weiss in der Public Cloud (z.B. Amazon) nicht, auf welchen Systemen, in welchem Rechenzentrum und in welchem Land der Provider seine Daten speichert. Seit Juni 2011 ist bekannt, dass die US-Behörden auf europäische Cloud-Daten zugreifen dürfen. Das gilt insbesondere für den Patriot Act, der US-Strafverfolgern weitreichende Zugriffsrechte auf Daten gibt. In den entsprechenden Service Level Agreements (SLA) kann zum Beispiel der folgende Passus stehen «Unter bestimmten Umständen kann (Name des Providers) Daten ohne Ihre vorherige Zustimmung weitergeben. Dazu gehört die Befolgung rechtlicher Anforderungen». Für ein rechtlich abgesichertes Cloud-Szenario sind dedizierte Anforderungen an den Cloud Provider sowie wasserdichte Verträge ein Muss.

Kürzlich wurde in der Presse ein interessanter Angriff auf ein Unternehmen mit einer manipulierten Computer-Maus beschrieben. Die Maus wurde einem Mitarbeitenden des Unternehmens als Werbegeschenk getarnt zugeschickt. In das Gehäuse der Maus wurde ein zusätzlicher Mikrocontroller mit USB-Unterstützung

eingebaut, welcher eine Tastatur simulierte und das Ganze um einen USB-Speicher ergänzte. Alle Tastatureingaben werden auf der Computer-Maus gespeichert und ein spezielles Programm wird vom Speicher der Maus gestartet. Das Programm sucht dann den von McAfee stammenden Virenscanner und deaktiviert diesen. Auch manipulierte Android-Handys können sich beim Anschluss an den Computer als Keyboard zu erkennen geben und so die Kontrolle übernehmen.

Die Cyber-Bedrohung entwickelt sich hauptsächlich im Zusammenhang mit den technologischen Fortschritten im Bereich der Informatik. Ein neue Bedrohung sind die mobilen Geräte. Die Vielzahl von Schnittstellen und Sensoren in den modernen mobilen Geräten und die Tatsache, dass diese überall mit dem Besitzer mitgehen, bieten unzählige Möglichkeiten, um ihn und sein Umfeld auszuspionieren (Datendiebstahl, Ortung, Abhören der Gespräche, Ton- und Bildaufnahmen ohne Wissen des Besitzers usw.). Auch Plattformen, deren Architektur öffentlich weniger bekannt sind, wie z.B. Blackberry, dürften durch die Reverse-Engineering-Anstrengungen aus der Profi-Hacker-Community gegenüber Cyber-Angriffen zunehmend verwundbarer werden.

Wirtschaftsspionage

Unter Wirtschaftsspionage versteht man die Gesamtheit von Handlungen zugunsten eines Staates, einer Firma oder einer Person, zwecks Beschaffung von geschützten oder geheimen Informationen aus den Bereichen Militär, Politik, Wirtschaft, Wissenschaft und Technologie, die zum Nachteil eines Landes oder einer Firma führen. KMU und wissenschaftliche Institute stellen wegen ihrer innovativen Forschungs- und Entwicklungsarbeiten und ihres Know-hows häufig interessante Ausspähungsziele dar. Besonders beliebt sind auch Messen wie beispielsweise die CeBIT in Hannover. Hier sind Spione gezielt am Werk und greifen offen auf Informationen zu, die nicht selten in Joint Ventures münden.

Der USB-Stick als beliebtes Give-away kann unerwünschte Schadprogramme enthalten.
Quelle: shutterstock

Es gilt, die folgenden externen Bedrohungen zu unterscheiden:

a) Delikte durch Einzelpersonen an der Firma: Einbruch, Drohung, Nötigung, Betrug, Erpressung durch Kunden als «Verhandlungsstrategie»

b) Wirtschaftsspionage: Konkurrenzausspähung, abhören, kopieren, fotografieren an Messen etc.

c) Cybercrime: Diebstahl geistigen Eigentums von Produktions- und Marketingplänen, Geschäftsstrategien, Rezepten, Patenten durch spezielle Trojaner und Spyware, welche durch E-Mails (Spam) unbemerkt auf den Firmencomputern installiert werden.

Firmen im Visier

Folgende Methoden sind üblich im Bereich der Wirtschaftsspionage:

► Unternehmensbesuche von ausländischen Delegationen mit oder ohne Begleitung durch einen Botschaftsvertreter.

► Angebote von Dienstleistungen an Forschungsunternehmen, Universitäten und Rüstungsbetriebe.

► Teilnahme an gemeinsamen Unternehmen (Joint Ventures) und Forschungsprojekten.

► Erwerb von Technologien und Unternehmen zwecks Platzierung neuer Mitarbeiter in sensiblen Bereichen.

► Abschöpfung ehemaliger Mitarbeiter, die Zugang zu sensiblen Informationen hatten.

Beispiele einiger Spionagefälle:

a) 2005: Grossunternehmen in Israel horchten sich gegenseitig mit individualisierten trojanischen Pferden aus (Mobilfunkprovider, Satelliten-TV-Anbieter, Auto-Importeure).

b) 2007: Angriff auf interne E-Mails der PNOS-Parteileitung.

c) 2005: Valéo, ein französischer Automobilteile-Hersteller entdeckte, dass eine chinesische Praktikantin namens Li Li

Potenzielle zukünftige Mitarbeiter für sensible Bereiche sollten vor der Anstellung überprüft werden. Quelle: shutterstock

Whuang in ihr Computersystem eingedrungen war und dort Daten über neue Konzepte kopiert hatte. Whuang war seit drei Jahren in Frankreich, galt als brillant und hatte Universitätsdiplome in Mathematik und Physik. Die Polizei fand bei ihr zu Hause mehrere Computer und Festplatten mit enormen Speicherkapazitäten, die sie angeblich nur für ihre Arbeit bei Valéo benutzte.

d) 2007: Eine Delegation liess sich in einem deutschen Unternehmen eine neue Anlage vorführen. Die Steuerung des Verfahrens erfolgte über ein älteres Notebook. Dies bewahrte der zuständige Ingenieur in seinem Büro im Schreibtisch auf. Die Täter drangen wenige Tage nach der Präsentation in das Gebäude ein und entwendeten das ältere Notebook aus dem Schreibtisch. Hierbei liessen sie ein neues Notebook samt Netzgerät ausser Acht, das auf dem Schreibtisch stand.

Es ist also zu erwarten, dass sich heute Spione (z.B. Studenten) aus China und anderen Staaten unter dem Denkmantel «Praktikant oder Trainee» von Firmen anstellen lassen, damit sie an die vertraulichen Daten gelangen. In vielen Fällen wurde zunächst nur wegen Einbruchs oder Einbruchdiebstahls ermittelt und erst nach einer Sensibilisierung durch die Sicherheitsspezialisten die tatsächliche Zielrichtung – der Angriff auf das Firmen-Know-how – erkannt. Die Beteiligung fremder Nachrichtendienste an solchen Sachverhalten ist zwar oft schwierig zu belegen, vor allem dann, wenn bereits einige Zeit seit der Tat vergangen ist. Aber gerade deshalb ist es wichtig, einen Sicherheitsspezialisten so früh wie möglich beizuziehen. Denn häufig sind an diesen Straftaten auch sogenannte Innentäter beteiligt, sodass weitere Verluste von sensiblem Firmen-Know-how zu befürchten sind.

Wie wird heute spioniert?

Fremde Staaten können E-Mails, Faxe oder Telefone durch Satelliten abhören und Wanzen installieren, oder sie können durch Angriffe via Trojaner in ein IT-System eindringen und dort meistens unbemerkt Informationen sammeln und weiterleiten (z.B. unbemerktes Weiterleiten aller E-Mails).

Wer kennt es nicht? Sie besuchen eine Messe und bekommen auf den Unternehmensständen nach Abschluss eines Gesprächs kleine Werbegeschenke angeboten. Darunter ist auch ein USB-Speicherstick mit einer Kapazität von einigen Gigabytes. Obwohl gerade ein USB-Speicherstick ein hochwertiges Give-away ist, ist bei solchen Geschenken Vorsicht geboten! USB-Speichermedien dieser Art gelten nur sekundär als Werbegeschenke. Primär verfolgen die Absender das Ausspionieren der Adressaten. In einigen Fällen ist ein solches Speichermedium mit einem Trojaner infiziert, der den Datenverkehr ausspioniert und diesen kontinuierlich an den Verursacher leitet.

Wie können Sie feststellen, ob Ihr Unternehmen ausgehorcht wird? Erhalten Sie zum Beispiel auf Ihre Offerten über Monate hinweg keine Aufträge mehr – sondern Ihr Mitbewerber gewinnt die Aufträge – könnte es sein, dass Ihre E-Mails mit den Offerten unbemerkt an Ihren Mitbewerber gesendet werden.

Wie können Sie sich schützen?

In Anbetracht der weltweit verschärften Konkurrenzsituation und einer steigenden Abhängigkeit von modernen Informations- und Kommunikationssystemen wird es immer wichtiger, sich gegen illegale Nutzung des eigenen Wissens zu schützen. Mit zunehmender Vernetzung kommt der Sicherheit der IT-Infrastruktur Priorität zu. Informationssicherheit darf nicht an Firmen- oder Landesgrenzen haltmachen. International tätige Firmen müssen sich bewusst sein, dass Informationsverluste bei ausländischen Niederlassungen, Konzerngesellschaften oder Geschäftspartnern möglich sind. Einen vollständigen Schutz gegen Informationsabfluss gibt es nicht, doch geeignete Massnahmen können wirkungsvollen und finanziell tragbaren Schutz bieten.

Folgende präventiven Massnahmen können unter anderem ergriffen werden:

Personensicherheit: Vor jeder Neuanstellung, speziell für sensible Bereiche, empfiehlt es sich, die Identität und Referenzen des Bewerbers zu überprüfen. Achten Sie aber auch darauf, wenn Sie Hilfskräfte (z.B. Reinigungspersonal) einstellen.

In einem Unternehmen sollten alle Mitarbeiter inkl. Management sichtbar einen Ausweis (Badge) tragen. Nur so können die Mitarbeiter in einem grösseren Unternehmen interne von externen Mitarbeitern unterscheiden. Externe Mitarbeiter (Handwerker, temporäre Mitarbeiter) müssen einen speziell markierten Ausweis sichtbar tragen. Begleiten Sie Handwerker in die Räumlichkeiten. Verfügt Ihr Unternehmen über eine Entwicklungsabteilung, verbieten Sie digitale Kameras oder andere Mobilgeräte mit einer eingebauten Kamera während einer Führung durch diese Räumlichkeiten.

Verschlüsselung: Schützen Sie Ihr Firmen-Know-how durch eine geeignete Verschlüsselung der Notebook-Festplatte. Wenn Sie vertrauliche Dokumente via E-Mail versenden, verschlüsseln Sie das

Infos

Am 7. März 2012 findet der 7. Nationale Tag der Computer-Sicherheit, der SwissSecurityDay statt, welcher durch den Verein InfoSurance zur Sensibilisierung der Schweizer Bevölkerung im Umgang mit dem Computer und Internet durchgeführt wird. Werden Sie Partner! www.InfoSurance.ch

E-Mail und dessen Inhalt. Nur mit einer angemessenen Verschlüsselung können Sie die Vertraulichkeit wahren.

Passwörter: Verwenden Sie jeweils starke Passwörter und geben Sie Ihr Passwort nie bekannt. Keine Passwortliste unverschlüsselt speichern oder ausdrucken.

USB-Sticks: Schliessen Sie keine USB-Sticks mit unbekannter Herkunft an Ihr Notebook an. Überprüfen Sie Ihnen vertraute USB-Sticks und CDs nach Viren, bevor Sie diese verwenden. Speichern Sie vertrauliche Firmendaten nur verschlüsselt auf einem USB-Stick. Schliessen Sie Ihren USB-Stick an keinen unbekannten PC oder Notebook an, denn die Daten auf dem USB-Stick können schnell, unbemerkt und ohne Spuren zu hinterlassen auf den PC kopiert werden.

Handy und PDA: Vorsicht im Umgang mit PDAs (iPhone, Blackberry etc.). Nehmen Sie solche elektronischen Geräte bei wichtigen und vertraulichen Verhandlungen nicht ins Sitzungszimmer. Auch ein angeblich ausgeschaltetes Handy kann mit einem speziellen Handy-Trojaner alles im Raum aufnehmen oder das Gespräch live übertragen.

Öffentlichkeit: Behandeln Sie geschäftliche Themen und Informationen in der Öffentlichkeit vertraulich, etwa während einer Bahn- oder Flugreise oder im Restaurant. Lassen Sie andere nicht mithören und lassen Sie sich nicht aushorchen.

Büro: Schliessen Sie vertrauliche Unterlagen weg. Verlassen Sie Ihren Arbeitsplatz jeweils aufgeräumt (Clear Desk). Werfen Sie keine Datenträger (CDs) und Dokumente mit sensiblem Inhalt ungeschreddert in den Papierkorb. Wenn Sie Ihren Arbeitsplatz auch nur für kurze Zeit verlassen, aktivieren Sie Ihren Bildschirmschoner.

E-Mail: Versenden Sie vertrauliche E-Mails nur verschlüsselt und überprüfen Sie den oder die Empfänger vor dem Senden genau. Senden Sie – wenn möglich – keine Word-Dokumente (DOC) in einem E-Mail. Senden Sie nur PDF-Dokumente als Anhang in einem E-Mail. Denn Word-Dokumente beinhalten viele Informationen (Meta-Daten), welche Sie in kompromittierende Situationen bringen könnten.

Software: Installieren Sie keine unbekannte Software. Vorsicht bei Freeware-Software. Stellen Sie sicher, dass die Quelle vertrauenswürdig ist. Es gab Fälle, wo Spyware in den Gratisprogrammen eingebaut war. Halten Sie Ihren Virenschutz und Ihre Programme inkl. Betriebssystem auf dem aktuellsten Stand.

Informatik: Vor der Entsorgung von Computern ist die Festplatte «sicher zu löschen». Dasselbe gilt vor dem Verschenken oder Verkaufen von Computern. Löschen oder deaktivieren Sie alle Benutzer-IDs von Mitarbeitern, welche Ihr Unternehmen verlassen haben.

Recht: Bestehen Sie darauf, dass Ihre Mitarbeiter bei der Anstellung eine Vertraulichkeitsvereinbarung (Geheimhaltungs-, Sorgfaltspflicht und Treuepflicht) unterschreiben, welche auch nach dem Austritt Gültigkeit hat.

Weisungen: Stellen Sie sicher, dass alle Mitarbeiter die internen Firmen-Weisungen in Bezug auf die Nutzung der Informatik-Mittel kennen. Es empfiehlt sich, eine Sicherheitspolitik erstellen zu lassen, welche die generellen Ziele der Informationssicherheit und die Informationssicherheits-Organisation definiert.

Sensibilisierung: Sensibilisieren Sie Ihre Mitarbeiter mit einfachen, aber wirkungsvollen Präsentationen und Publikationen. Besonders Mitarbeiter im Verkauf, Marketing, in der Entwicklung und Filialleiter im In- und Ausland.

Zutritt: Schützen Sie Ihre Büroräumlichkeiten und Computerräume vor unbefugtem Zutritt.

Risiko-Analyse: Führen Sie mit Hilfe eines Sicherheitsspezialisten eine Risiko-Analyse in Ihrem Unternehmen durch. Dabei geht es darum, die Unternehmenswerte zu identifizieren, damit die Risiken und Gefahren explizit richtig eingeschätzt werden können. Ermitteln Sie die möglichen Szenarien mit den entsprechenden Gegenmassnahmen.

Geschäftsführung: Erstellung eines Informationssicherheitskonzepts und Ernennung einer dafür verantwortlichen Person, die mit Unterstützung der Geschäftsleitung Kontrollen durchführt und die Sicherheit durchsetzt.

Fazit

Wirtschaftsspionage und Datenabfluss sind eine Realität! Durch die wachsende Komplexität und Vernetzung der IT-Systeme und die Globalisierung ergeben sich neue Herausforderungen an den Schutz der Daten und Informationen. Schützen Sie Ihr Firmen-Know-how mit Ihren Möglichkeiten und lassen Sie sich wenn nötig von einem Sicherheitsspezialisten beraten. Befolgen Sie die hier beschrieben Tipps und Empfehlungen, die dazu beitragen werden, Ihr Firmen-Know-how angemessen zu schützen. ■

Der Autor: Wolfgang Sidler ist Präsident des Vereins InfoSurance und Inhaber der SIDLER Information Security GmbH, Master of Advanced Studies in Information Security, Certified ISO 27001 Lead Auditor und Mitautor des «IT-Sicherheitshandbuches für die Praxis».

Verhaltenstipps bei Geschäftsreisen

► Vor Reiseantritt möglichst genaues Bild vom Gastland erarbeiten, allgemeine Gefährdungs- und Sicherheitslage eruieren und mit den Gebräuchen und Gesetzen des Landes vertraut machen.

► Lassen Sie Ihr Notebook, Handy, PDA und sensible Firmenunterlagen nie unbeaufsichtigt liegen. Dies gilt insbesondere auch für die Aufbewahrung in Fahrzeugen, Seminarräumen und Hotelzimmern.

► Vermeiden Sie es, Ihr mobiles Gerät auf irgendeine Weise mit Ihrer Firma in Verbindung zu bringen und verzichten Sie auf das Anbringen von Logos, Klebern etc. sowie auf die Aktivierung entsprechender, eindeutiger Bildschirmschoner.

► Tragen Sie Ihr Notebook und andere Mobilgeräte bei Flugreisen ausschliesslich im Handgepäck. Dies gilt auch für wichtige Unterlagen. Verstauen Sie alle Geräte für Sie gut einsehbar unter dem vorderen Sitz.

► Setzen Sie Passwörter, Virenschutz- und Verschlüsselungsprogramme zum Schutz Ihres PCs und Notebooks ein.

► Seien Sie besonders aufmerksam, wenn Sie Ihr Notebook am Flughafen durchleuchten lassen müssen. Legen Sie es erst auf das Förderband, wenn Sie selbst durch den Metalldetektor gehen. Sollten Sie durch Anstehen aufgehalten werden, dann behalten Sie Ihr Notebook im Auge und achten Sie dabei auf verdächtige Personen, die es in der Zwischenzeit vom Band nehmen können.

► Nutzen Sie für sensible Kommunikation nur gesicherte Wege (Vorsicht insbesondere bei Fax-, E-Mail- und Telefonverkehr von unterwegs).

► Berücksichtigen Sie bei Telefongesprächen vom Mobiltelefon, dass diese ohne grossen technischen Aufwand abzuhören sind.

► Vernichten Sie nicht mehr benötigte Unterlagen. Ihr Abfall kann für andere wertvolle Informationen enthalten.

► Seien Sie misstrauisch, wenn Sie sich ungewöhnlich stark ausgefragt fühlen. Nicht jeder Gesprächspartner hat das gemeinsame Geschäft im Sinn. Niemals Gespräche mit Fremden über Reisezweck und Arbeitgeber führen.

► Analysieren Sie in der Gesprächsvorbereitung, welche Informationen Ihre Gesprächspartner zu Ihrem Nachteil verwenden könnten.

► Sitzen Sie in der Bahn oder in einem Flugzeug, verwenden Sie für Ihr Notebook einen speziellen Sichtschutzfilter. So kann der Nachbar nicht mitlesen.

► Seien Sie vorsichtig beim Eröffnen von Filialen und Produktionsstätten in allen Ländern, die den Patent- und Markenschutz nicht respektieren oder nicht durchsetzen.

► Wenn Sie Ihre neuen Produkte auf internationalen Ausstellungen präsentieren, achten Sie darauf, dass während der Ausstellung kein Firmen-Know-how gestohlen wird.