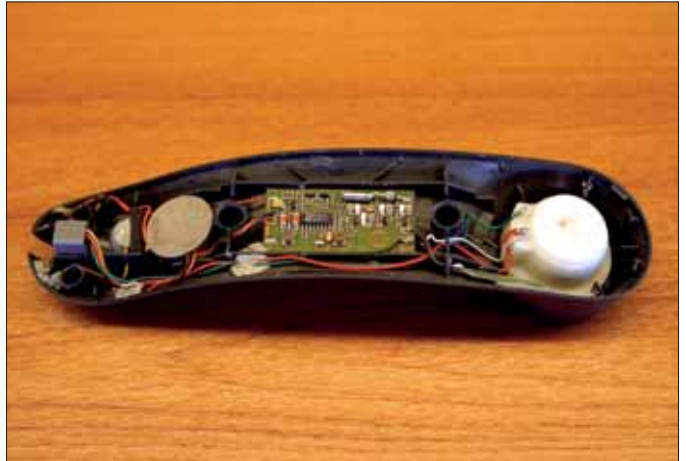




Späh- und Lauscheinrichtungen werden oft in „unverdächtigen“ Gegenständen installiert wie Telefonverteiler.



Angezapfter Telefonhörer: Gespräche können leicht mitgehört werden.

# Lauscher und Späher

Bei einem Forum der Simedia GmbH zum Thema „Wirtschafts- und Konkurrenzspionage“ am 16. und 17. Mai in Bonn erläuterten Experten, wie sich Unternehmer vor dem Abfluss von Informationen schützen können.

**W**irtschaftsspionage geht von staatlichen Stellen aus. Einige Nachrichtendienste haben den Auftrag, Wirtschaftsdaten zu erheben. Konkurrenzspionage hingegen betrifft den Wettbewerb von Unternehmen untereinander. Die Methoden der Informationsabschöpfung sind fast gleich. Nach dem Ergebnis einer WIK-Sicherheitsenquete haben sich im Jahr 2004 14 Prozent der Unternehmen durch Wirtschaftsspionage, 45 Prozent durch Konkurrenzspionage und 49 Prozent durch Abhörversuche bedroht gesehen.

**Spionagemethoden.** „Etwa 80 Prozent der Information stammen aus offenen Quellen, und können etwa durch Marktbeobachtung und systematische Internet-Recherchen bezogen werden – oder durch bloßes Lesen und Auswerten von Zeitungen“, berichtete Manfred Fink, Lauschabwehrspezialist aus Coburg, Bayern. Unternehmen müssen einerseits aus rechtlichen Gründen einiges über sich bekannt geben; sie versenden auch Werbematerial, Produktbeschreibungen, Kundenzeitschriften und Pressemitteilungen. Dazu kommt die Auswertung von Fachpublikationen und wissenschaftlichen Arbeiten, von Messen und Kongressen. Angebote, die besonders lukrativ erscheinen, können lediglich zu dem Zweck eingeholt werden, um Informationen über den

Anbieter zu erhalten und Problemlösungen in Erfahrung zu bringen. „Eine gängige Methode“, betonte Fink. Jointventures und Übernahmen können lediglich in der Absicht erfolgen, Information abzusaugen. Zur Auswertung von offenen Quellen (*Open Source Intelligence – OSINT*) kommt der Mitarbeiter, dessen Wissen abgeschöpft wird (*Human Intelligence – HUMINT*) oder dessen Fehlleistungen ausgenutzt werden. „Professionelle Informationsbeschaffer überlassen grundsätzlich nichts dem Zufall“, sagte Fink. „Vermutlich zufällige Begegnungen können lanciert sein, wie etwa bei Fachkongressen oder an der Hotelbar.“

Durch gezielte Gesprächsführung merkt das Opfer nicht, dass es abgeschöpft wird. Froh, jemanden gefunden zu haben, der geduldig zuhört, wird drauf los geplaudert, es werden die eigenen Leistungen hervorgekehrt (Anerkennungsbedürfnis) oder der Betreffende redet sich seinen Frust von der Seele. Wenn Raucher aus dem Gebäude in den Hinterhof verbannt werden, sieht ein aufmerksamer Beobachter nicht nur, über welche verschwiegenen Zugänge sie wieder in das Haus gelangen, sondern es bietet sich auch die Möglichkeit mitzuhören, was da in Arbeitspausen so gesprochen wird. Dr. Christian Reiser, Experte für Informationssicherheit aus Wien, tritt deshalb für

Raucherzimmer in den Gebäuden ein. Zu diesen Fällen des unabsichtlichen Geheimnisverrats kommen auch Mitarbeiterinnen und Mitarbeiter, die aus materiellen Motiven heraus handeln, der „Romeo-Masche“ erlegen sind, eingeschleust wurden oder erpresst werden.

Im Bereich der Informationstechnologie ist das *Social Engineering* gebräuchlich, dass also beispielsweise Passwörter in Erfahrung gebracht werden, indem sich der Anrufer als Vertreter des gerade auf Urlaub befindlichen System-Administrators ausgibt, der eine wichtige Umstellung vornehmen müsse; vorgibt, im Auftrag des Vorstands zu handeln oder die besondere Dringlichkeit einer Maßnahme vorzuschützt.

Die *Signal Intelligence (SIGINT)* stellt auf die Informationsgewinnung durch technische Maßnahmen ab, also Lausch- und Spähangriffe, Abhören der Telekommunikation und Auffangen von Funkübertragungen sowie Angriffe auf die Informationstechnologie.

**Gegenmaßnahmen.** „Die Marketingabteilung ist der natürliche Feind des Sicherheitsbeauftragten“, betonte Reiser. Bei veröffentlichten Berichten oder im Fachgespräch auf Messständen sollte der Stolz auf die eigene Leistung oder die des Unternehmens durch kriti-



Müller Reifenhandel GmbH  
Grieshofgasse 14, 1120 Wien  
Tel: 813 96 87-0  
Fax: 815 61 79  
office@muellner-reifen.at  
www.muellner-reifen.at

- Reifen
- Felgen
- Schneeketten
- Autobatterien
- Kundenräderdepot
- umweltgerechte Altreifenentsorgung

## WIRTSCHAFTSTREUHÄNDER

Mag. Dr.

# WOLFGANG SCHULLA

**Buchprüfung, Steuerberatung**

Allgemein beoideter und gerichtlich zertifizierter Sachverständiger

2120 Wolkersdorf, In Gruben, Annahof 1/4  
Tel: 02245-5758, Fax: 02245-83322, www.doktor-schulla.at



### Manipulierter Stempel.

Der Mensch und seine Schwächen als Risikofaktor – eine breite Palette. Sensibilisierung der Mitarbeiter gegenüber den Arten der Human Intelligence ist oberstes Gebot – auch auf der Vorstandsebene. Jeder Mitarbeiter sollte aus diesem Gesichtspunkt nur so viel wissen, als er zur Erfüllung seiner Aufgaben braucht (Need-to-Know-Prinzip).

Bei Arbeitsende sollte nichts unversperrt herumliegen (Clean-Desk-Policy). Gegenüber Besuchern sollte ein gesundes Misstrauen bestehen – der Besucherausweis sollte gegen den Personalausweis getauscht werden. Für Besucher sollten eigene Räume eingerichtet werden („steriler“ und „nicht steriler“ Bereich). Bei behaupteten Reparaturarbeiten wäre beim Auftraggeber nachzufragen. Sensible Räume (Telefonzentrale, EDV, Datenträgerarchiv, Serverraum, Hauptverteiler) sollten nicht im Klartext beschriftet werden.

Vorsicht bei der Annahme von Gast- und Werbegeschenken – sie könnten Lauscheinrichtungen enthalten und sollten wie Einlaufstücke in der Poststelle die Röntgenstraße durchlaufen. Das gilt auch für Sammlerstücke und Kunstgegenstände, von denen der Schenkende weiß, dass sie im nächsten Umfeld der Zielperson aufgestellt werden. Handys für die Vorstandsebene sollten nicht unter dem Firmennamen bestellt, sondern direkt im Laden gekauft werden, um Manipulationen zu verhindern.

Auf Reisen dürfen wichtige Dokumente wie etwa Vertragsentwürfe, Angebote, Studien niemals in fremden Büros oder Hotelzimmern zurückgelassen und Laptops sowie Datenträger (CDs, DVDs, USB-Sticks) niemals unbeaufsichtigt gelassen werden. Daten sollen darauf nur (hardwaredmäßig) verschlüsselt gespeichert werden. Allenfalls können „Spieldaten“ zur Verfügung gestellt werden, um das Risiko einschätzen zu können und den Gegner zu beschäftigen.

Foto: KURT HECKISCH

Pötzleinsdorfer Höhe 2  
A - 1180 Wien  
Tel.: 440 75 84  
Tel. oder Fax:  
440 35 58  
STADLER  
blumen@blumen-stadler.at

Ihr kreatives Team  
Sonn- und Feiertag geöffnet (Wien 18)  
Zustellung in ganz Wien  
www.blumen-stadler.at

Blumenstudio:  
Wilhelminenstraße 40  
A - 1160 Wien  
Tel.: 480 38 77  
STADLER  
blumen@blumen-stadler.at

Blumen for you - Blumen für Sie

1230 WIEN, HOCHWASSERGASSE 2  
TEL.: 01/616 33 50  
FAX: 01/616 33 50/20  
E-MAIL: eltech@aon.at

**ELTECH**  
ELEKTROINSTALLATIONEN GES.M.B.H.

ÄRZTEHEIM  
BETRIEBS GES. M. B. H.

1100 Wien, Dr. Eberle-Gasse 3

☎ 01/617 11 90  
Fax 01/617 11 90/17  
e-mail: office@aerzteheim.at  
www.aerzteheim.at

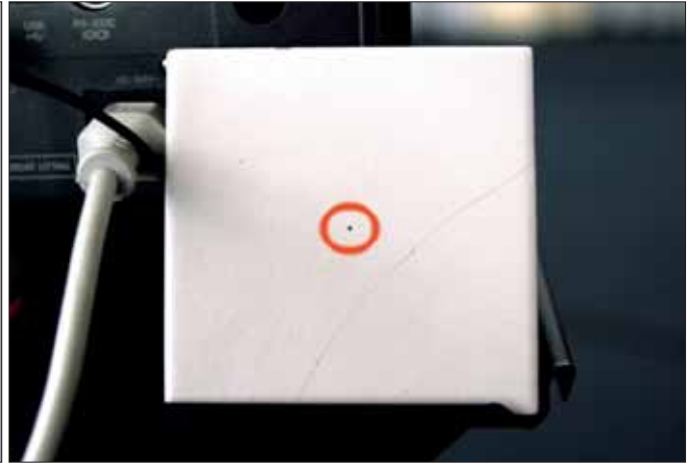


Warum sollten Sie als Pensionist/in auf Komfort, den Sie seit jeher gewohnt waren, verzichten?  
Gerade im fortgeschrittenen Seniorenalter sollten Sie die Annehmlichkeiten eines langen Lebensabends entsprechend genießen. Wir bieten Ihnen mit unserem wunderschönen Ärzteheim die Möglichkeit dafür.

Besichtigen kann man unser Seniorenheim Montag bis Freitag  
Um Voranmeldung wird gebeten



**Manipulierte Elektrosteckdose: Abhörgeräte können überall versteckt sein.**



**Minikamera hinter einer Fliese: Aufnahmen durch ein Stecknadel großes Loch.**

Dokumente, Laptops und Datenträger sollten bei Linienflügen nur im Handgepäck mitgeführt werden. Persönliche Dinge wie Kleidungsstücke, Koffer, Mobiltelefone dürfen auch für kurze Zeit nicht unbeaufsichtigt gelassen werden.

Unvermeidbare persönliche Unterredungen in Lokalen sollten nicht im Klartext, sondern verklausuliert erfolgen – bei bekannten Sachverhalten ist es ohnehin nicht nötig, Namen und konkrete Fakten zu nennen. Verzichtet werden sollte auf das „Stammlokal“. Statt dessen sollten Gaststätten ohne erkennbares Schema öfters gewechselt werden. Tischreservierungen sollten nicht auf den Firmennamen oder den tatsächlichen Namen bekannter Personen vorgenommen werden.

Luxuszimmer und Suiten sind weltweit als Abhörriisiko anzusehen. Auch mit einer Überwachung der Telefonanschlüsse muss gerechnet werden. Dass sich die Verwendung von Handys im Hotel als nicht möglich erweist, kann an einer absichtlichen Störung des Netzes liegen, durch die ein Ausweichen auf die – überteuerte und möglicherweise abgehörte – Festnetzanlage des Hotels erzwungen werden soll. Sogar mit einer Kameraüberwachung, etwa durch präparierte TV-Geräte, muss gerechnet werden. Die vielfach verwendeten, als Magnetkarten gestalteten „Plastikzimmerschlüssel“ sind leicht reproduzierbar und können nicht als sicher eingestuft werden. Und wenn ein Eindringling erst einmal das Schild „Nicht stören“ außen an die Zimmertür gehängt hat, kann er sicher sein, stundenlang ungestört „arbeiten“ zu können. Welches Zimmermädchen prüft schon nach, ob der, der das Zimmer be-

tritt, in dem sie gerade aufräumt, auch der berechnete Nutzer ist?

Wenn es, wie bei Konferenzen oder für Delegationen, um hohe Sicherheitsansprüche geht, sollen ganze Flügel oder Etagen angemietet werden, abgesichert durch eigenes Service- und Sicherheitspersonal. Kritische Gegenstände wie Telefone, TV-Geräte, Radiowecker, sollen von vornherein entfernt und durch geprüfte eigene Geräte ersetzt werden. Wie bei Restaurants sollte die Reservierung von Hotelzimmern nicht auf den Firmennamen oder den Namen bekannter Personen erfolgen. Kleine Hotels oder Pensionen sind unter Sicherheitsaspekten mitunter kalkulierbarer als internationale Hotelketten. In ganz verschiedenen Fällen können in mehreren verschiedenen Hotels Konferenzräume vorbestellt werden, oder die Teilnehmer treffen sich an dem angegebenen Ort und werden von dort an einen bisher geheim gehaltenen Ort transportiert.

Das Benutzen fremder Infrastrukturen etwa im Fall von angemieteten Büroräumen stellt ein Sicherheitsrisiko dar; die tatsächliche Identität des Nutzers sollte verschleiert werden. Ein hohes Sicherheitsrisiko sind fremde Telekommunikationseinrichtungen. Verschlüsselungstechnik, und zwar eine solche, die möglichst nahe an der Quelle (dem Mikrofon, dem Scanner) ansetzt, bietet Abhilfe, doch kann Verschlüsselung in manchen Ländern verboten sein. In diesem Fall, oder wenn kein Chiffriergerät zur Verfügung steht, kann man die zu übermittelnde Information aufsplitten und auf verschiedenen Übertragungswegen übermitteln. Abhilfe bietet auch die Steganografie, bei der Informationen in um-

fangreichen Dateien wie Bildern verpackt werden. Etwa fünf Prozent der Größe einer Datei kann auf diese Weise unauffällig genutzt werden, das entspricht etwa 10 bis 20 A4-Seiten bei einem herkömmlichen digitalen Bild.

**Bei Lausch- und Spähangriffen** sind der Fantasie der Täter keine Grenzen gesetzt. „Das scheinbar Unmögliche muss als ganz klare Option angesehen werden“, erläuterte Lauschabwehrspezialist Fink. Abhöreinrichtungen sind leichter zu tarnen als Videokameras, die zumindest ein Blickfeld benötigen. Massiv erscheinende Gegenstände (Aschenbecher, Rahmen von Gemälden) können Lausch- und Spährichtungen enthalten, auch belanglos erscheinende Dinge (Türstopper, Verkleidungen, Schreibgeräte, Verteilerdosen).

Der Trend geht zur Manipulation vorhandener Anlagen. Wer technisch an einen Laptop mit eingebautem Mikrofon herankommt, braucht nicht mehr in den Raum einzudringen. Bei einer angesteckten Webcam observiert sich in solchen Fällen der Benutzer selbst. Eine Überbrückung der Hörergabel des Telefons ermöglicht es, mitzuhören, was im Raum gesprochen wird; über eine manipulierte Sprechtafel einer Durchsageanlage können Räume abgehört werden, weil jeder Lautsprecher in Umkehrung des physikalischen Prinzips wie ein Mikrofon wirkt. Dazu kommen Angriffsmöglichkeiten auf digitale Telekommunikationsanlagen, beispielsweise, wenn serienmäßig eingebaute Abhörmöglichkeiten entweder nicht ausgeschaltet oder nachträglich aktiviert werden.

*Kurt Hickisch*