

## Serie: Der kleine Lauschangriff (Teil 3)

# Wege in die Wohnung

Natürlich haben Lauschangriffe nur eines zum Ziel: das Erlangen von Informationen. Klar, daß dabei gezielte Abhörmaßnahmen ein gewichtiger Faktor sind. Doch bekanntlich heiligt der Zweck die Mittel, und so werden alle zur Verfügung stehenden Hilfsmittel eingesetzt, wenn es darum geht, das Informationspuzzle weiter zu ergänzen. Dieter Görrisch zeigt alltägliche und weniger alltägliche Mittel zur Informationsbeschaffung.

**Die lieben Nachbarn:** Heute kann man Telefonnummern-CDs sehr preiswert in jedem Kaufhaus erwerben. Nicht nur, daß sich damit problemlos Rückschlüsse von einer Telefonnummer auf deren Besitzer ziehen lassen, auch die gesamte Nachbarschaft des Lauschoppers samt deren Telefonnummern wird in Sekundenschnelle komfortabel ermittelt. Telefonanrufe bei den auf diese Weise ermittelten Personen bringen oft erstaunliche Details über Lebenswandel, Arbeitgeber oder Sozialverhalten des Lauschoppers ans Licht, sofern sich der Anrufer als alter Klassenkamerad, Arbeitskollege oder gar Kripobeamter am Telefon aus gibt.

Es ist schon fast unglaublich, mit welcher Sorglosigkeit diskrete Informationen über Nachbarn und Freunde an völlig unbekannte Anrufer gegeben werden. Profis von Nachrichtendiensten werden übrigens



Der spurlose Einbruch in die Wohnung geht in der Regel der Installationen von Wanzen voraus.  
Foto: Görrisch

in dieser Art der Informationsgewinnung geschult (sog. Befragungstechnik) und kitzeln durch bewußte Gesprächstechnik und Verhaltensweise die gewünschten Informationen aus den Gesprächspartnern.

**Anrufbeantworter und Mailboxen:** Auch das unbefugte Abhören von Anrufbeantwortern oder Handy-Mailboxen gehört zum Repertoire des Lauschangriffs. Dort werden nicht selten brisante Dinge ausgesprochen und abgespeichert, weshalb sich ein Lauschangriff hier immer lohnt. Natürlich verlangen sowohl Anrufbeantworter als auch Mailboxen zunächst die Eingabe einer PIN-Nummer, bevor sie ihre Geheimnisse preisgeben.

Diese zwei- (!) bis vierstelligen DTMF-Tonfolgen, werden gewöhnlich mit handelsüblichen Fernabfragesendern erzeugt. Profis arbeiten hier mit modifizierten Tongeneratoren, die verschiedenste DTMF-Tonkombinationen in kurzer Zeit ausgeben können und so den Dekoder im Anrufbeantworter überlisten. Grundsätzlich soll es auch mit künstlich erzeugtem Rauschen möglich sein, den DTMF-Dekoderchip zu täuschen, da in diesem Rauschteppich statistisch gesehen alle Frequenzen (also auch die benötigten Tonkombinationen) enthalten sind.

Doch meist ist es die Unvorsichtigkeit der Leute selbst, die einen Lauschangriff auf Anrufbeantworter und Mailboxen noch erleichtert. Die PIN-Nummer ist bei Auslieferung der Geräte oft auf einen Standardwert gesetzt (Beispiel: 0000) und sollte vom Kunden selbst individuell einprogrammiert werden. Dies wird leider immer wieder vergessen, weshalb es Lauschprofis zunächst einmal mit häufig verwendeten Standard-PINs der Hersteller versuchen und oft genug Erfolg damit haben.

Kaum bekannt und nicht in der Bedienungsanweisung dokumentiert ist auch die Tatsache, daß manche Anrufbeantworter sogar aktiv werden, obwohl sie gar nicht eingeschaltet sind. Läßt man den Apparat nur lange genug klingeln (etwa 15 mal) schaltet sich das Gerät nämlich trotzdem (ohne Ansagetext) auf die Leitung und erwartet Fernsteuerkommandos. Tatsächlich hilft in diesen Fällen nur das völlige Trennen des Gerätes von der Telefonleitung, um alle Manipulationen grundsätzlich auszuschließen.

**Eindringen in Wohnungen:** Im Rahmen eines Lauschangriffs kann auch die eigene Wohnung



### Der Autor

Dieter Görrisch, Jahrgang 1960, war bereits im Alter von 13 Jahren mit dem Radio- und Bastelvirus infiziert. So mußte schließlich auch die berufliche Ausbildung diesem Weg folgen.

Nach dem Abitur schloß sich beinahe zwangsläufig ein Studium der Elektrotechnik an, das 1989 abgeschlossen wurde. Erster beruflicher Einsatz in der Fördertechnik, danach mehrjährige Tätigkeit bei einem Mobilfunkbetreiber im Bereich Netzqualitätssicherung und Richtfunktechnik.

Parallel dazu die ersten journalistischen Beiträge für mehrere Zeitschriften. Jetzt selbstständig in den Bereichen Sicherheits- und Kommunikationstechnik, Dokumentation und als freier Mitarbeiter mehrerer Fachzeitschriften tätig. Unter dem Rufzeichen DL1MEH seit 10 Jahren auf KW, UKW und ATV aktiv.

Ziel von Durchsuchungen oder Manipulationen (beispielsweise das Anbringen von Abhöreinrichtungen) werden. Da solche Aktionen unerkant bleiben sollen, dürfen weder Zerstörungen noch sichtbare Spuren hinterlassen werden.

**Wie schnell Profis mit heutigen Methoden Sicherheitsschlösser aufsperrern können, ist bedauerlicherweise kaum bekannt. Es stehen gleich mehrere Verfahren zur Verfügung, das raffinierteste ist zweifellos der sog. „Elektro-Pick“.**

Das batteriebetriebene, kaum bananengroße Gerät trägt an seiner Spitze ein etwa 10 cm langes Metallblatt, das in den Schließkanal des Sicherheitsschlusses eingeführt wird. Auf Knopfdruck versetzt der eingebaute Elektromotor des Elektro-Picks dieses Metallblatt und damit die Sperrstifte im Schließkanal des Schlosses in Vibration. Gleichzeitig wird auf den Schließrotor des Schlosses mit einem Hilfswerkzeug ein leichtes Drehmoment ausgeübt. Da die Sperrstifte unter dem Einfluß des Elektro-Picks zu schwingen beginnen, verlieren sie zeitweise ihre Sperrwirkung und der Rotor läßt sich drehen – das Schloß ist geöffnet. Auch das Wiederverschließen solcher „gepickten“ Schlösser mit einem weiteren Spezialwerkzeug, dem sog. „Flipper“, ist kein größeres Problem. Irgendwelche Spuren an Schloß oder Türe bleiben nicht zurück.

**Verräterische Videoüberwachung:** In einigen Anwesen gewährt gar der Eigentümer selbst großzügigen Einblick in seine Wohnung: drahtlos, über sog. Video-Links. Mit dem Monitor verbundene Überwachungskameras haben oft genug eine größere Reichweite als gemeinhin angenommen. Sie arbeiten fast ausnahmslos im 2,4 GHz ISM-Band (2400,00 bis 2483,50 MHz) nach

dem Prinzip der einseitigen Funkstrecke, ähnlich wie eine analoge TV-Richtfunkstrecke. Zum Empfang dieser völlig unverschlüsselt übertragenen Videoübertragungen genügt ein 2,4 GHz Videoempfänger mit Frequenzdemodulation.

Den Profis stehen für solche Anwendungen natürlich kompakte und tragbare Geräte zur Verfügung, die einfach in die Nähe des Lauschobjektes gebracht werden können. Vertrauliche Videosignale sollten wegen der Abhörsicherheit stets über Drahtverbindungen weitergeleitet werden. In Zukunft stehen für drahtlose Videoübertragungen dieser Art auch digitalisierte Übertragungsverfahren zur Verfügung, mit denen sich die Video-Informationen gegen unbefugtes Abhören vorher verschlüsseln lassen.

Diese Technik ist für Privatanwender derzeit leider noch zu teuer.

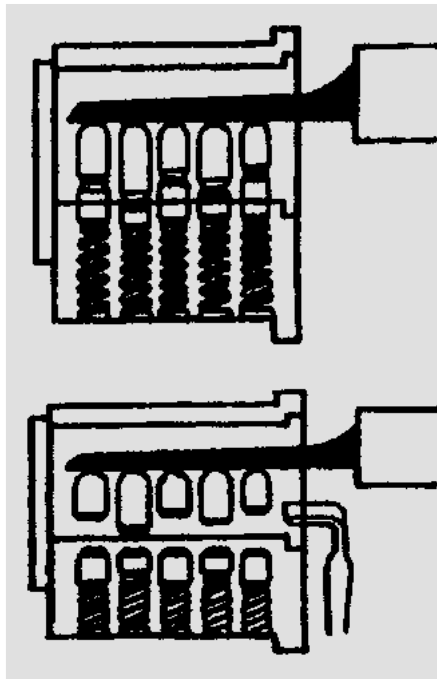
Wer sich näher für Schlösser und Schließtechnik interessiert und vielleicht seinen Schlüssel hin und wieder mal vergißt, sollte sich die folgende Internetseite genauer ansehen:

<http://www.home.t-online.de/home/SSD-Archiv.htm>.

Dort erfährt man u.a., wie leicht das Schlösserknacken ist und daß es nicht strafbar ist, ein solches Öffnungswerkzeug zu besitzen, es sei denn man hat die Absicht, damit kriminell zu werden ...

*Dieter Görrisch*

Wir danken der Firma Josef Guschelbauer-Elektronik aus Bad Vilbel (siehe Anzeige im Heft) für die Bereitstellung eines „Elektro-Picks“ zu Testzwecken.



## So funktioniert ein Elektro-Pick-Sperrwerkzeug

**Bild oben:** Einführen des Pickstiftes in das Schoß, wobei er auf allen Schließstiften sauber aufliegen muß.

Alle Sperrstifte sind noch verriegelt, der Rotor des Schlosses ist blockiert.

**Bild unten:** Nachdem der Schließrotor unter Mitwirkung eines Hilfswerkzeuges, dem sog. „Spanner“ mit Drehmoment beaufschlagt wurde, wird der Elektro-Pick aktiviert. Der Pickstift beginnt zu vibrieren und schlägt auf die Sperrstifte (hier fünf Stück).

Diese beginnen ebenfalls unkontrolliert zu bewegen und verlieren zeitweise ihre Sperrwirkung, der Rotor kann sich drehen, das Schloß ist geöffnet!