third-party-blocker

privacy bags for mobile phones and other devices

((why?))

Abschalten hilft nicht
— Abschirmen ist notwendig

Die technischen Möglichkeiten zur Ortung von Personen und zum Abhören von Räumen durch Mobiltelefone, Smartphones und PDAs sind seit Jahren bekannt. Weder die Telefondienstanbieter noch die Gesetzgebung reagieren angemessen auf die stetig zunehmende Verletzung der Privatsphäre von Nutzern solcher Geräte. Im Gegenteil - sie bieten Dienste an, die das Orten und Abhören durch Dritte ermöglichen. Nicht nur Verfolgungsbehörden nutzen zunehmend die Mobiltelefone von Privatpersonen, um diese zu belauschen und zu orten. Auch Eltern lassen sich „zur Sicherheit“ den aktuellen Aufenthaltsort ihrer Kinder übermitteln, Eifersüchtige „tracken“ ihre Partner/innen, Arbeitgeber „verfolgen“ ihre Außendienstmitarbeiter lückenlos. Die Möglichkeiten, Handynutzern hinterher zu schnüffeln, enden leider nicht mit dem Ausschalten der Geräte.

Software-Manipulation: Mit einer Software ab 100 Euro kann jeder Handys zu gut getarnten Spionagewerkzeugen umrüsten. Das Programm *FlexiSpy* z.B. erlaubt nicht nur, sämtliche SMS über das Internet mitzulesen und alle Anrufe zu protokollieren. Es kann unbemerkt Gespräche oder Geräusche in der Umgebung des Handys abhören. Das funktioniert auch dann, wenn der Nutzer das Handy „ausgeschaltet“ hat: Eine Veränderung der Gerätesoftware täuscht dem Nutzer lediglich vor, das Gerät sei ausgeschaltet (Klingelton, Vibrationsalarm und Display sind deaktiviert). Tatsächlich bleiben Lauschfunktionen (z.B über automatische Rufannahme) aktiv.

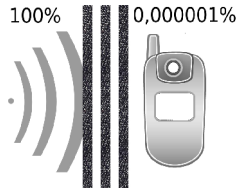
Wer ein fremdes Handy über diese Methode ausspionieren will, braucht es nur wenige Minuten lang in die Hände zu bekommen. Das Lauschprogramm wird mittels Speicherkarte und weniger Tastenklicks installiert. Bei Bluetooth-Geräten lässt sich die Software sogar über Funk auf das Telefon übertragen. Je nach Handytyp lässt sich solche Spionage-Software auch per „Service-SMS“ oder „Update“ auf das Handy übermitteln. Für den Besitzer ist das Programm praktisch unsichtbar.

Hardware-Manipulation: Darüber hinaus können in Handys problemlos Wanzen untergebracht werden. In der Regel wird dabei der Akku des Handys der Zielperson gegen einen optisch gleichen Akku getauscht, in dem eine Abhörwanze eingebaut ist. Diese manipulierten Akkus kann man für die gängigen Handys für etwa 200 Euro im Internet ersteigern.

Wenn sich die Anwesenheit eines Mobiltelefons bei Besprechungen sensiblen Inhalts nicht vermeiden lässt, hilft der third-party-blocker, **ungebetene Zuhörer auszuschließen.**

((the principle))

Der *third-party-blocker* ist eine Tasche, die elektronische Geräte von ihrer Außenwelt abschirmt. **Drei Lagen Gewebe aus leitendem, Silber-ummanteltem Garn verhindern eine elektromagnetische Signalübertragung** über die gesamte (im Mobilfunkbereich genutzte) Frequenzbreite zwischen dem Inneren und Äußeren der Tasche. **Das gilt sowohl für alle Handynetze, als auch für GPS, Bluetooth, wireless LAN und RFID-Frequenzen.**



Das funktioniert wie beim Auto, welches als „Faradayscher Käfig“ vor Blitzeinschlag schützt: Eine geschlossene Hülle aus gut leitendem Material schirmt elektrostatische Felder bzw. elektromagnetische Strahlung ab. Eine Übertragung der Umgebungsgespräche sowie eine Ortung über ein solches (eventuell manipuliertes) Gerät wird dadurch verhindert.

Die Eindringtiefe hochfrequenter elektromagnetischer Strahlung in eine gut leitende Hülle ist sehr gering. Daher genügt eine dünne Schicht, um die gewünschte Abschirmung zu erreichen. Durch drei Schichten des

leitenden Gewebes beim *third-party--blocker* sind Dämpfungswerte von mindestens 80 dB (über das gesamte relevante Frequenzspektrum hinweg) gewährleistet. Dies entspricht einer Reduktion der Signalstärke im Inneren der Tasche um mehr als 99,999999%. In die verschlossene Tasche gelangen also maximal 0,000001% der Umgebungsfeldstärke. Damit ist eine effektive Abschirmung auch hochempfindlicher Empfänger garantiert.

((how to use))

Der *third-party-blocker* soll niemanden in falscher Sicherheit wiegen. Um einen möglichst hohen Schutz der Privatsphäre zu gewährleisten, wird die Nutzung wie folgt empfohlen:

Das Funktionsprinzip des *third-party-blockers* beruht darauf, dass die Tasche eine geschlossene(!), leitende Hülle um das abzuschirmende Gerät bildet. Der Verschluss ist dazu so konzipiert, dass ein (mindestens) **zweimaliges Einrollen** der Verschlusskante die beiden inneren und die äußere Stoffschicht jeweils leitend abschließt. **Klettverschluss straff schließen!**

Veränderungen am Verschlusssystem, Löcher oder Schlitze im Stoff sind zu vermeiden (also kein Knopfloch oder ähnliches anbringen). Das technische Gewebe der Innen- und Außenhaut ist relativ robust. Die Tasche ist **bei 30°C waschbar.** Chemische Reinigung, Bleichen, Trocknen, Bügeln müssen jedoch vermieden werden. Diese können den Silberanteil des Gewebes und damit die Abschirmwirkung verringern.

Sicherheit gegen Ortung und Identifizierung des Geräts:
Es besteht vollständiger Schutz, wenn sich das Gerät in der Tasche befindet, und diese wie beschrieben verschlossen wird. Weder über einen eventuell vorhandenen GPS-Empfänger noch über die Suche nach Signalübertragungsstationen (Handynetze, wirelss LAN, ...), erhält das Gerät oder ein Angreifer Informationen über den Aufenthaltsort des Geräts.

Das gilt unabhängig davon, ob ein Schnüffelangriff über die Software oder die Hardware erfolgt. Es empfiehlt sich, das Gerät auszuschalten, damit das Gerät bei der kontinuierlichen, erfolglosen Netzsuche nicht unnötig Strom verbraucht.

Sicherheit gegen Abhören der Geräte-Umgebung:
1) Der beste Schutz besteht darin, KEIN Gerät dabei zu haben
2) Hohe Sicherheit bietet, Gerät und ausgebauten Akku in die Tasche zu stecken.
3) Mittlere Sicherheit bietet, das Gerät ausgeschaltet in die Tasche zu stecken.
4) Geringe Sicherheit bietet der Ausbau des Akkus (ohne Tasche)
5) Keine Sicherheit bietet das Ausschalten des Geräts (ohne Tasche)

Zur Erläuterung nehmen wir ein modernes Handy: Die Tasche verhindert jegliche Signal-ÜBERTRAGUNG, egal ob die Software (z.B. automatische Rufannahme trotz Ausschalten) oder die Hardware (z.B. Akkuwanze) des Handys manipuliert wurde. Um eine Sprach-AUFZEICHNUNG in den Handyspeicher (mit eventuell später erfolgender Übertragung) zu behindern, sollte zusätzlich der Akku entfernt werden. Dieser sollte ebenfalls in die Tasche gesteckt werden! Bei älteren Handys/Geräten ohne Speicher zur Sprachaufzeichnung entfällt die Unterscheidung zwischen 2) und 3).

((never trust – test it!))

Die korrekte Funktion des *third-party-blocker* kann man jederzeit selbst überprüfen: Gerät im eingeschalteten Zustand in die Tasche stecken und Tasche wie beschrieben verschließen. Jede Kontaktaufnahme (z.B. Anrufen des Handys in der Tasche) sollte nun scheitern. Das Telefon klingelt nicht, der Anrufende erreicht lediglich die mailbox (des Handynetzbetreibers).

((questions?))

Weitere Informationen finden sich unter www.third-party-blocker.de
Fragen oder Anmerkungen bitte an info@third-party-blocker.de

third-party-blocker