Mobiltelefone können abgehört oder als Mikrofone sowie Kameras zum Ausspionieren verwendet werden.

Smartphone als Wanze

Abgehörte Mobiltelefone, verwanzte Urlaubsdomizile, Trojaner auf Laptops, Mikrofone, versteckte Überwachungskameras: Wie erkennt man, ob man abgehört wird, und wie schützt man sich davor?

Mit zunehmenden technologischen Möglichkeiten besteht die Gefahr, dass jedes Wort mitgeschnitten wird und Geheimnisse an falsche Ohren geraten. Manche Vermieter von Feriendomizilen sehen die Überwachung als einen Schutz des Eigentums, und immer öfter werden Geschäftsgeheimnisse gezielt ausspioniert. Auch wenn nicht jeder und jede gefährdet ist, so ist doch die „Datensammlung auf Verdacht" technisch möglich und kann Privatpersonen gleichsam als „Beifang" erwischen.

In George Orwells Buch „1984" waren die Proponenten nicht einmal in der Natur sicher vor dem Abhören. Im Freien ist man heute wohl weniger sicher, als in den eigenen vier Wänden, seit eine Überwachung aus größerer Distanz durchführbar ist – sei es durch hochfliegende Drohnen, Richtmikrofone oder Teleobjektive. Abwehrmaßnahmen im Freien sind schwierig.

Mobiltelefone, Laptops, Tablets sowie digitale Assistenten sind in vielen Fällen der geeignetste Abhörweg. Mobiltelefone können entweder bei aktiven Verbindungen mitgehört werden oder als Mikrofone und Kameras verwendet werden, die nebenbei zuverlässig die Position und das Bewegungsprofil der überwachten Person liefern. Damit ein Telefon zu einer Wanze wird, die auch im Ruhezustand sendet, ist es nötig, einen Trojaner zu installieren.

„Digitaler Wachhund". Was möglich ist, zeigt die von Edward Snowden entwickelte Android-App „Haven", die ein Android-Telefon in eine Abhöranlage verwandelt – von ihm entwickelt als „digitaler Wachhund", den man auf einem Android-Mobiltelefon installieren kann, um es beispielsweise in seinem Hotelzimmer liegen zu lassen, damit man unerwünschte Besuche erkennen kann.

Ende-zu-Ende-Verschlüsselung. Wird ein Mobiltelefon abgehört, verbraucht das Energie. Ein Telefon, das im Ruhezustand warm ist und dessen Akku schnell leer wird, könnte einen Trojaner beherbergen. Doch nicht immer ist das ein Zeichen, dass man abgehört wird, denn es könnte die Hotspot-Funktion eingeschaltet sein, der Akku alt oder das Ladegerät defekt sein.

Wenn Behörden Telefongespräche überwachen lassen, besteht in vielen Fällen für die Betroffenen kaum eine Chance, dies mitzubekommen, denn die Überwachung erfolgt normalerweise bei den Telekomanbietern oder auf Netzwerkebene. Erst wenn jemand Ende-zu-Ende-verschlüsselte Kommunikation verwendet, wie es beispielsweise *Signal* oder *Telegram* für Chats und für Sprache bieten, ist Abhören über Provider und Netzwerk nicht mehr möglich. Bei einer Ende-zu-Ende-Verschlüsselung sind auch die Gespräche vor Abhören geschützt. In diesem Fall muss der Abhördienst eine Spionagesoftware am Mobiltelefon installieren, die die Sprachdaten noch vor der Verschlüsselung abhören kann.

Abhörmaßnahmen erkennen. Kameras und Mikrofone, gut versteckt und strategisch positioniert, ermöglichen lückenlose Überwachung. In den meisten Fällen werden diese Abhöreinrichtungen entweder mit einem Sender ausgestattet oder nicht allzu weit von einem solchen entfernt sein. Der weitverbreitete Tipp, doch auf Funkstörungen bei Mobiltelefon, Radio und Fernsehen zu achten, dürfte weniger hilfreich sein, um Sicherheit darüber zu erlangen, ob man abgehört wird. Wenn Kameras Infrarot verwenden, beispielsweise zur Beleuchtung im Dunkeln, kann diese Beleuchtung noch allenfalls mit einfachen Mitteln entdeckt wer-

FOTO: JO PANUWAT /STOCK.ADOBE.COM

Aufnahme aus einem Hausinneren mit einer Drohnen-Kamera.

FOTO: INGO BARTUSSEK/STOCK.ADOBE.COM

den. So kann man mit einer Mobiltelefonkamera, deren Empfindlichkeit im Infrarot-Bereich vorher festgestellt werden muss, den abgedunkelten Raum nach Infrarot-Lichtquellen – oft in Form von Lichtblitzen – absuchen.

Einfacher und zuverlässiger ist die Suche nach Hochfrequenz-Quellen, also nach den zugehörigen Sendern. Auch wenn es inzwischen eine Unzahl von billigen Geräten gibt, die eine zuverlässige Detektion von Kameras (mittels Infrarot-Licht) und Sendern verspricht, sind die Erfahrungen mit diesen Geräten schlecht oder gemischt.

Klarheit über Spionagesender bieten professionelle Geräte etwa von *Gigahertz Solutions (www.gigahertz-solutions.de)* oder von *Aaronia (https://aaronia.de/spektrumanalysator/)*. Nur durch Geräte, die zuverlässig das gesamte Funkspektrum abdecken und in einem sehr breiten Empfindlichkeitsbereich arbeiten, sind zuverlässige Detektionen möglich. Damit sind auch Sender, die an der Außenhülle von Gebäuden befestigt sind, leicht ortbar.

Schutz vor Abhörung ist erst durch die Kombination von Detektoren und Störeinrichtungen möglich – was derzeit wohl eher nur von Behörden und gut ausgestatteten Diensten verwendet wird. Dabei besteht in diesem Bereich noch aus ganz anderen Gründen Bedarf: Oft ist Mobilfunkkommunikation nicht erwünscht – beispielsweise in Justizvollzugseinrichtungen oder in Schulen und generell in Bildungseinrichtungen, speziell während Prüfungen.

Gigahertz Solutions hat eine Lösung entwickelt, die unter der Marke *Gigahertz Security (www.gigahertz-security. de)* angeboten wird, und die derzeit im Prototyp-Stadium ist: Es besteht in Deutschland die Kooperation mit Justizvollzugsanstalten, um sicherzustellen, dass Insassen der Anstalt keine Kommunikation über unerlaubte Wege nach außen führen können. Dazu wird eine breitbandige Detektion in Echtzeit durchgeführt und Kommunikation unterdrückt, die innerhalb eines klar abgrenzbaren räumlichen Bereichs versucht wird. Legale Kommunikation, etwa über DECT-Telefone der Vollzugsbeamten, wird davon nicht gestört.

Dieses System erkennt und unterbindet Kommunikation, die beispielsweise mit aus den Fenstern gehaltenen Mobiltelefonen versucht wird, ohne dabei die Kommunikation anderer Mobiltelefone zu stören, die sich außerhalb des geschützten Bereichs befinden. Dadurch ist dieses System auch in dichtverbautem Gebiet einsetzbar. In dieser Lösung ist auch die Erkennung von mobilen Geräten im Standby-Modus enthalten. Da diese nur auf geringe Distanz möglich ist, erfordert diese Detektion Personenschleusen.

Abschirmung. Für den rein passiven Schutz gibt es Materialen, die hochfrequente Strahlung abschirmen. Einen Überblick bietet *Gigahertz Solutions,* die Produkte haben, die auch als Schutz gegen Elektrosmog dienen (*www.gigahertz-solutions. de/de/abschirmung).*

Michael Werzowa

Zum Autor:
Michael Werzowa, Experte für Netzwerk- und Datensicherheit, Vorstand der IoT Austria – The Austrian Internet of Things Network