Wenn Sicherheitsmaßnahmen unsicher machen

Big Brother wider Willen

Technischer Fortschritt im Bereich der Display-Technik wirkt sich nicht nur auf den eigenen Computerarbeitsplatz aus, sondern auch auf andere Geräte. Heute muss man auch bei Babyphonen nicht mehr auf Video verzichten – und fertig ist das Spionagegerät.

Der Empfänger hat ein farbiges TFT-Display. Der Sender ist eine kleine Kamera, die das Ton- und Videosignal per Funk überträgt. Fertig ist die Baby-Überwachung, und ein sicheres Gefühl stellt sich ein. Manchmal allerdings wird dieses Gefühl auch empfindlich gestört – wenn man als Eltern nämlich das Baby des Nachbarn anstelle des eigenen sieht oder gar plötzlich Fernsehen schaut. Man könnte nun einfach den Kanal seines Senders und des Empfängers umstellen – aber wenn man mit Datensicherheit beruflich zu tun hat, dann stellt sich an dieser Stelle noch auf ganz anderer Ebene ein recht ungutes Gefühl ein.

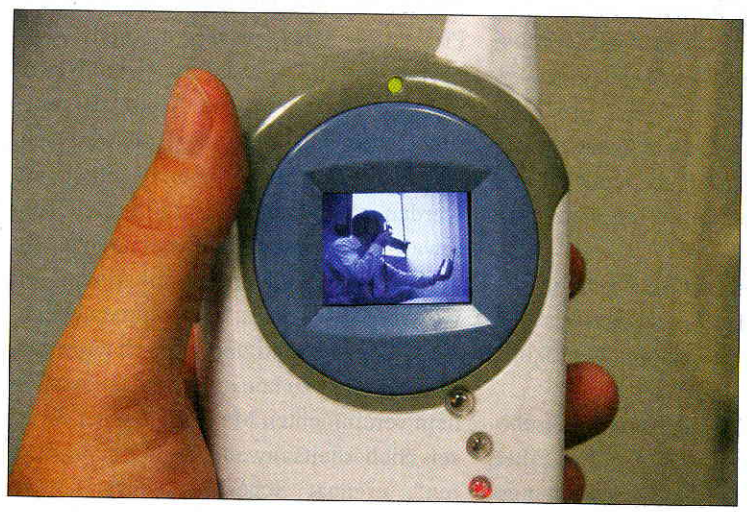
Wer den handlichen Empfänger einfach einmal mitnimmt auf eine Tour „in die Stadt", erlebt eine noch größere Überraschung als im heimischen Wohngebiet: Er sieht – neben dem einen oder anderen Fernsehprogramm – alle möglichen Szenen: Hauseingänge, Parkplätze, den Empfangsbereich bei Firmen, interne Büros, Ladengeschäfte und Privatwohnungen.

Die Babies und deren Bettchen sind klar in der Unterzahl. Funküberwachungskameras dagegen scheint es fast überall zu geben. Mit etwas Glück sieht man sich selbst vorbeigehen – Big Brother wider Willen.

Der Hintergund: Video-Babyphone, aber auch Funk-Überwachungskameras, verwenden für die drahtlose Übertragung dieselben Frequenzen um 2.4 GHz. Die Empfänger funktionieren also mit allen Sendern zusammen und umgekehrt. Der Babyphone-Empfänger empfängt die Überwachungskamera genauso gut wie der Empfänger eines Überwachungskamera-Sets das Signal der Videoeinparkhilfe. Zusätzlich gibt es Sets zur drahtlosen Übertragung von Kabelfernsehen – auch auf denselben Kanälen. Es handelt sich dabei allerdings nicht um WLAN nach 802.11.

Nur durch die Wahl der Kanäle kann eingeschränkt werden, was man empfängt oder nicht. Die handelsüblichen Geräte sind dabei auf 3 bis 4, umfangreichere drahtlose Videoüberwachungsanlagen auf ein bis zwölf Kanäle beschränkt. Aber auch hier liegen alle Kanäle auf festen Frequenzen. Kanal 4 einer Überwachungskamera ist auch bei einem TV-Übertragungsset Kanal 4. Um fremde Signale aufzufangen, müssen daher nur die entsprechenden Kanäle durchprobiert werden.

Warum aber fällt niemandem auf, dass die Signale seiner Kameras unverschlüsselt und für praktisch jeden mit dem passenden Empfänger erreichbar ausgestrahlt werden, wenn sowohl das Band als auch die Kanäle standardisiert sind? In der Realität liegen die Sender selten so nah zusammen, dass sie sich stören. Das Signal der Videoüberwachungskamera im Hauseingang wird das Video-Babyphone im zweiten Obergeschoss desselben Gebäudes nicht stören – schlimmstenfalls ist der Empfang ein bisschen schlechter. An manchen Kreuzungen in Großstädten sieht dies allerdings anders aus: Hier ist manchmal Kanal 1 überbelegt, und Bilder überdecken sich, weil abschirmende Mauern und Fenster fehlen. Erst, wenn man sich einem Sender nähert, beginnt sich dessen Signal durchzusetzen. Typischerweise können die Videosignale 20 bis 40 Meter entfernt von der Kamera empfangen werden. In wenigen Ausnahmen reicht der Übertragungsbereich auch erheblich weiter. Die Positionierung und der Typ der Kamera sind hier entscheidend: Eine Kamera, die in einem voll verglasten Büro in der Nähe des Fensters montiert ist kann auch in 100 Metern noch empfanger werden. Abgesehen von der Kanalwahl gib es keinerlei Schutzmechanismen. Es existiert weder ein Verschlüsselungsstandard



Manchmal überwacht man sich auch selbst: Ungesicherte Videosysteme führen zu überraschenden Begegnungen.
Quelle: Syss

auf den man aufbauen könnte, noch gibt es einen guten Grund für den Hersteller, sich um dieses Problem zu kümmern. Überwachungskameras sparen das Verlegen von Kabeln ein, die einen großen Kostenfaktor bei der Installation darstellen.

Genau dies macht die Kameras für den Endverbraucher so attraktiv. Bei der Verwendung drahtloser Kameras ist weder das

Weiterführende Literatur und Links

„Einblicke in die Privatsphäre", ZDF REPORTER, 22.03.2007, http://www.zdf.de/ZDFmediathek/inhalt/26/0,4070,5254938-0,00.html. Der Beitrag zeigt unter die Kamera einer Apotheke. Man kann außerhalb des Gebäudes zusehen und mithören, wie die Apotheker mit Patienten über Rezepte und Behandlungen reden.
„Wardriving & Wireless Penetration Testing", Chris Hurley et al, Syngress.
Paragraph 202b StgB: http://dejure.org/gesetze/StGB/202b.html

Durchbohren von Wänden nötig noch das teilweise mühevolle Kaschieren von Leitungen, was vor allem an einem schönen Altbau sehr aufwändig sein kann. Da der Käufer eines solchen Gerätes von dieser Einsparung so viel wie möglich profitieren möchte, würde er ein teureres Gerät, das ein verschlüsseltes Signal verschickt, nicht kaufen. Die unglaubliche Verbreitung derartiger Systeme liegt somit sicherlich an den Preisen von Kamera- und Empfänger-Sets. Eine Kamera mit Handempfänger kostet in der Regel weniger als 200 Euro.
Dies hat verschiedene Konsequenzen. Zum einen sind derartige Kameras nicht immer als Schutz vor Diebstählen geeignet. Ein Dieb nämlich kann sehen, was die Kamera auch sieht, und kann sich deshalb bei einem eventuellen Einbruch ohne weiteres im „toten Winkel" der Kamera halten. Die Kamera hilft ihm außerdem, zu entscheiden, wie er in ein Objekt eindringt. Wird die Eingangstür überwacht, wählt er eben ein Fenster und so weiter. Hinzu kommt, dass nicht immer nur Bilder übertragen werden. Sehr oft unterstützen Kameras dieser Art auch Audio, insbesondere natürlich die Babyphone. Damit kann mitgehört werden, was im privaten oder beruflichen Umfeld besprochen wird, und Abschalten lässt sich die Audio-Funktion oft nicht. Ein weiterer Punkt ist, dass der mögliche Mithörer seinen Empfänger bequem in der Manteltasche tragen und über Kopfhörer mithören kann. Entdeckt wird er nicht. Mit dem passenden Zusatzgerät vermag der Lauscher oder Mit-Seher das Signal auch aufzuzeichnen.

WLAN mit WPA2 wäre nötig

Will man derartige Kamerasysteme absichern, scheitert man zwangsläufig an den fehlenden Verschlüsselungsmethoden. Jede Form des Videoschutzes, die man einfach durch den Kauf des passenden Empfängers umgehen kann, ist einfach nichts wert. Es bleibt daher nur der Umstieg auf ein drahtgestütztes System oder der Einsatz von Kameras, die WLAN-Technik zur Übertragung verwenden und mindestens WPA2 unterstützen. Auch lassen sich die Geräte nicht nachträglich erweitern. Da mit dem Produkttyp Kosten gespart werden sollen, fehlen die entsprechenden Optionen. Auch die Sendestärke kann nicht reguliert werden. Hier ist ohnehin Vorsicht geboten: Da es sich beim Übertragungsbereich der Geräte um das 2.4-GHz-Band handelt, können Empfangsgeräte mit WLAN-Antennen ausgestattet werden, um deren Leistung zu verbessern. Sich wegen der kurzen Reichweite des Signals in Sicherheit zu wiegen, wäre also verfehlt.
Man kann also nur raten, auf diese Technik zu verzichten. Sie zeigt, was passiert, wenn nicht oder unzureichend verschlüsselte Signale einem unbestimmten Benutzerkreis zugänglich gemacht werden. Ein System, bei dem man nur das passende Empfangsgerät kaufen muss, um dessen Signale zu empfangen und zu verstehen, ist von Prinzip her unsicher. Es kann daher nur an Stellen zum Einsatz kommen, bei dem ein Schutz wirklich unnötig ist.

Sebastian Schreiber/wj

Zu den rechtlichen Aspekten des Themas lesen Sie bitte das Interview auf Seite 44.

Sebastian Schreiber ist Geschäftsführer des auf Sicherheitstests spezialisierten Unternehmens Syss in Tübingen

Rechtliche Aspekte

Die technische Situation bei drahtlosem Videofunk ist im Grunde recht übersichtlich – rechtlich allerdings wirft das Thema gleich eine ganze Reihe von Fragen auf. Um die Probleme klären, hat Syss für die LANline ein Interview mit einem auf IT Sicherheits- und Datenrecht spezialisierten Anwalt geführt.
Dr. Jyn Schultze-Melling LL.M. ist Technologie-Anwalt bei der internationalen Wirtschaftskanzlei Nörr Stiefenhofer Lutz in München und dort Spezialist für das IT-Sicherheits- und Datenschutzrecht.

LANline/Syss: Macht sich jemand strafbar, der mit einem Babyphone durch die Innenstadt läuft und sich Bilder von Überwachungs-Kameras anschaut?

Schultze-Melling: Seit ungefähr drei Jahren macht sich hierbei zunächst einmal der strafbar, der solche Überwachungskameras unbefugt einsetzt und dabei den „höchstpersönlichen Lebensbereich" der Betroffenen verletzt – ein anschaulicher Klassiker hierbei sind zum Beispiel die ganz unauffällig videoüberwachte Umkleidekabine im Kaufhaus oder heimlich überwachte Kindermädchen. Ebenso wird zwar eigentlich auch derjenige bestraft, der dermaßen illegal hergestellte Videos speichert, vervielfältigt oder Dritten zugänglich macht. Wer aber nur mit einem Babyphone in der Hand durch die Innenstadt läuft, wird kaum Ärger mit dem Staatsanwalt bekommen – bloßes Zuschauen ist bislang zumindest strafrechtlich nicht relevant. Aber Vorsicht: Ganz anders sieht es aus, wenn solche illegalen Aufnahmen aufgezeichnet werden und dann zum Beispiel auf Videoportalen wie Youtube und Co. landen – dies kann zu Strafanzeigen führen.
Hinzu kommt noch ein weiterer wichtiger Aspekt: Das Abfangen der Daten von Funküberwachungskameras mit dem Babyphone berührt auch datenschutzrechtliche und persönlichkeitsrechtliche Themen, und hier können Verstöße mit Unterlassungsverfügungen, Schadenersatzklagen und empfindlichen Geldbußen enden.

Dr. Jyn Schultze-Melling LL.M. ist Technologie-Anwalt bei der internationalen Wirtschaftskanzlei Nörr Stiefenhofer Lutz in München

LANline/Syss: Können solche Signale unter Umständen legal aufgezeichnet werden?

Schultze-Melling: Wie gesagt ist das bloße Zuschauen nicht strafbar, es sei denn, man hat die Kamera selbst aufgestellt. Auch das Mitschneiden ist strafbar. Ansonsten hat man es hier in erster Linie mit datenschutzrechtlichen Fragen zu tun. Abgesehen von einigen Ausnahmefällen ist laut Bundesdatenschutzgesetz die Videoüberwachung öffentlicher Räume nur von öffentlichen Stellen oder von Privaten zur Wahrung ihres Hausrechts zulässig, wobei eine Überwachung natürlich eine gewisse Dauer voraussetzt.
Ist man also weder Polizeibeamter auf Verbrecherjagd noch der Hausherr, der seine Geschäftsräume überwacht, oder kann man auch sonst keine guten Gründe vorbringen, warum man einen öffentlich zugänglichen Platz per Video überwachen muss, gilt ein striktes Überwachungsverbot, sobald über die Kamera Personen zu erkennen sind. Das gilt natürlich prinzipiell auch für eine „Überwachung" mit dem Babyphone und erst recht für die Aufzeichnung der Bilddaten.

LANline/Syss: Verhält es sich anders, wenn man bei der Installation eines solchen Empfängers zufällig ein privates oder gar dienstliches Gespräch mithört?

Schultze-Melling: Grundsätzlich gilt hier das Gleiche. Wenn ich also zufällig auf die richtige Frequenz einer Überwachungskamera komme und dadurch dem Nachbarn ins Schlafzimmer schauen kann, sollte ich das Babyphone lieber abschalten, sobald ich das bemerke. Handelt es sich um einen Büroraum, sollte man dasselbe tun und vielleicht in Erwägung ziehen, die betroffene Firma zu informieren. Der für diese Erkenntnis notwendige kurze Augenblick ist aber rechtlich kein Problem.

LANline/Syss: Kann ich mich als Besitzer einer solchen (Funk-)Kamera gegen Mithören- und -sehen zur Wehr setzen?

Schultze-Melling: Rechtlich kaum – Sie bekommen in der Regel ja nicht einmal mit, wer ihre Überwachungskameras anzapft und Sie auf diesem Wege belauscht und beobachtet.
Hinzu kommt, dass Sie aufgrund der bereits beschriebenen datenschutzrechtlichen Vorschriften ja ohnehin jedem mitteilen müssen, dass er überwacht wird – für manche Zeitgenossen dürften daher die charakteristischen Hinweisschilder in öffentlichen Räumen quasi eine Aufforderung zum Zuschauen darstellen.

LANline/Syss: Bei den von uns beschriebenen Geräten kann man nicht oder nur schwer verhindern, das Dritte das Signal empfangen und somit sehen und eventuell auch hören, was die Kamera sieht oder deren Mikrofon hört. Welche Konsequenzen hat diese technische Eigenfür den Einsatz dieser Kameras im Firmenumfeld?

Schultze-Melling: Abgesehen von den beschriebenen strafrechtlichen Konsequenzen, mit denen sich die Verantwortlichen konfrontiert sehen können, muss ganz klar gesagt werden: Hier geht es auch um Know-how-Schutz!
Wenn ich als Geschäftsführer eine derartige Kamera in meiner Firma aufstellen lasse, um zum Beispiel meine Mitarbeiter in einem Großraumbüro zu kontrollieren, und ein Modell mit Audio-Übertragung erwische, dann habe ich mich ja praktisch erfolgreich selbst verwanzt. Das Gleiche gilt natürlich auch für die Industrie: Als Konkurrent kann mir ein ausführlicher Blick in die neuen Produktionshallen des Wettbewerbers extrem viel wert sein – noch dazu, wenn ich dafür noch nicht einmal durch die Fabriktore schleichen muss.

LANline/Syss: Welche Konsequenzen kann es haben, wenn jemand ein dienstliches Telefonat meiner Mitarbeiter mit einem Kunden aufzeichnet und veröffentlicht?

Schultze-Melling: Abgesehen davon, dass es sich hierbei auch um ein strafbares Datenabfangen im Sinne des nagelneuen Paragraph 202b StGB handeln könnte, kann jemand, der sich auf diese Weise unbefugt Betriebsgeheimnisse verschafft, schon auf der Grundlage des geltenden Wettbewerbsrechts mit einer Freiheitsstrafe von bis zu drei Jahren bestraft werden.