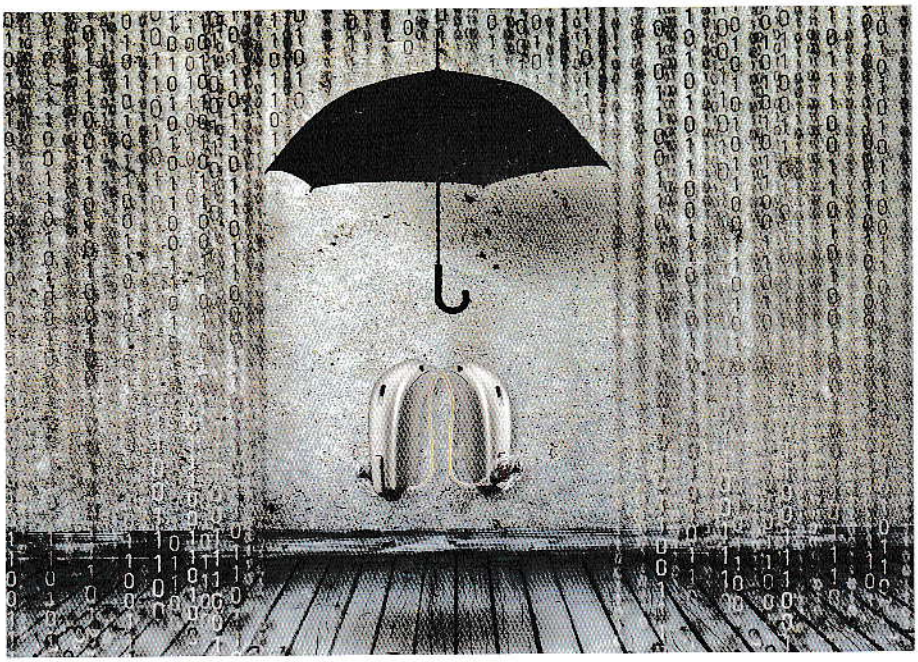
Datenschutz

Wie sicher sind Hörsysteme?

Längst ermöglichen Hörsysteme ihren Nutzern mehr als gutes Hören – sie ersetzen die Kopfhörer beim Musikhören oder das Headset beim Telefonieren. Manche sind sogar internetfähig und werden über das Smartphone gesteuert. Und das Optimieren der Hörsysteme geschieht per Fernwartung durch den Hörakustiker. Doch wie sieht es hier in Sachen Datensicherheit aus?

Hörsysteme sind heute kleine internetfähige Computer, mit deren Hilfe man wieder gut hören kann, in bestimmten Situationen sogar besser als Normalhörende. Dies wird durch aufwendige Signalverarbeitung möglich, um zum Beispiel Sprachanteile von Lärm zu befreien. Mit Umsetzung von neuen Patenten können sogar verschiedene Sprecher aus unterschiedlichen Richtungen identifiziert werden und dann mit speziellen Mikrofonschaltungen optimal in eine Balance gebracht werden – ohne dass dabei wichtige Umgebungsgeräusche wie ein heranrollendes Auto überhört werden. Insgesamt ermöglichen die neuesten Entwicklungen bei Hörsystemen eine Leichtigkeit des Hörens.



Stehen Hörsysteme tatsächlich unter einem Cyberschutzschirm? Foto: Byoungjoo/iStockphoto

Datenaustausch dank moderner Technik

Diese Leichtigkeit des Hörens wird durch das bessere räumliche Hören und durch eine gemeinsame Signalverarbeitung beider Geräte mittels drahtlosen Datenaustausches erreicht. Hierfür wird eine induktive, schwach magnetisch pulsierende Technik genutzt (Near Field Magnetic Induction (NFMI)). Damit ist es für moderne Hörgeräte möglich, die Information von allen verwendeten Mikrofonen für jedes Hörsystem gemeinsam zu nutzen. Pro Hörsystem sind dies zwei, somit liefern bei einer binauralen Versorgung vier Mikrofone Informationen, zum Beispiel von wo ein Vogel zwitschert. Zusätzlich wird die NFMI-Technik seit über zehn Jahren bei vielen Hörsystemen genutzt, um über einen Adapter (Streamer) zu telefonieren, den Fernsehton zu hören oder um die Hörsysteme mit einer Fernbedienung zu regulieren. Der Vorteil der NFMI-Technik ist, dass die Streaming-Funktionalitäten mit minimalem zusätzlichen Energieaufwand möglich wird, die Hörgerätebatterien also lange halten. Der Nachteil ist eine sehr geringe Reichweite von maximal einem Meter. Deshalb ist ein Streamer notwendig, um – mittels stromfressender Funktechnik – größere Reichweiten zu erzielen.

Heute können die modernsten Hörgeräte drahtlos mit der Bluetooth-Low-Energy (BLE)-Funktechnik im Bereich von 2,4 GHz mit Smartphones zum Telefonieren und zum Hören sämtlicher Audioquellen ohne zusätzlichen Streamer genutzt werden. Musik, Sprachnachrichten, Videotelefonie, WhatsApp-Filme oder komplette Videofilme können in beiden Ohren, wenn möglich auch in Stereo, direkt in die Hörsysteme funken, ohne weiteres Zubehör und in bester Klangqualität. Sowohl über NFMI oder Streamer als auch über BLE können diverse Apps in den verwendeten Smartphones genutzt werden. Die App kann als Fernbedienung für die Hörsysteme verwendet werden oder zur Einstellung bestimmter Programme, der Lautstärke und der Wunschklänge in der Tinnitusrehabilitierung.

Ebenfalls können die NFMI- und 2,4-GHz-Kanäle zur Anpassung und Programmierung der Hörsysteme durch den Hörakustiker verwendet werden, ohne dass der Kunde oder die Geräte selbst verkabelt werden müssen. Die Wireless-Funktionen ermöglichen es sogar, moderne Hörsysteme durch eine Fernwartung anzupassen. Der Kunde muss nicht mehr ins Hörakustikfachgeschäft, um Modifikationen in den Hörgeräten durchführen zu lassen. Hierfür benötigt der Hörgeräteträger aber moderne Hörsysteme und eine spezielle App auf dem Smartphone. Der anpassende Hörakustiker braucht seinerseits einen internetfähigen Rechner

mit der entsprechenden Anpasssoftware, die auch über eine gesicherte Verbindung einen Kontakt zum Smartphone des Hörgeräteträgers herstellen kann. Jetzt kann der Hörakustiker mit seinem Kunden nicht nur zu jeder Zeit und an jedem Ort der Welt videogestützte Telefonate führen, er kann ebenso die Hörsystemanpassung per Fernwartung optimieren.

Immer wenn Funksysteme, Datenübertragung oder gar das Internet ins Spiel kommen, wird speziell in Deutschland nach der Sicherheit für eben diese Systeme gefragt. Angesichts der Meldungen über Sicherheitslücken scheint diese Skepsis nicht unbegründet – werden doch die Funksignale von Autoschlüsseln mit einfachen Mitteln gekapert oder Bankzugänge gehackt. Als prominentes Opfer einer Abhöraktion wird immer wieder Angela Merkel genannt, auf deren Handy sich Fremde Zugang verschafft haben. Die Liste könnte endlos fortgesetzt werden. Auch bei Hörsystemen fragen Hörakustiker und Hörsystemträger immer wieder nach, ob diese abgehört, gehackt oder fremdgesteuert werden und dadurch sensible Gesundheitsdaten womöglich in fremde Hände gelangen können.

Philosophisch könnte man anmerken, dass es zumindest theoretisch keine Sicherheit gibt. Die Menschheitsgeschichte hat uns gelehrt, dass bisher jedes von Menschen entwickelte Sicherheitssystem auch von Menschen umgangen und damit ausgehebelt werden kann. Die Frage ist allerdings, welchen Aufwand man hierfür betreiben muss und welchen Vorteil man dadurch erzielen kann. Da der Aufwand in vielen Fällen sehr hoch und der Nutzen sehr gering ist, gibt es rein praktisch betrachtet in vielen Anwendungen eine große Sicherheit. Das gilt speziell für Hörsysteme.

Kopplung – Der kritische Moment

Um überhaupt zwei technische Komponenten per Funk verbinden zu können, müssen diese gekoppelt werden. Das kann in offenen Systemen wie im Radio geschehen. Ein Radiosender sendet auf einer Frequenz und jeder Radioempfänger kann sich mit der gleichen Frequenz koppeln – also alle können das Programm hören. Bei der hier beschriebenen Anwendung soll nur ein Nutzer seine Hörsysteme mit seinem Smartphone koppeln. Oder ein Hörakustiker möchte für einen Kunden die Hörsysteme anpassen, muss diese also mit seinem Anpassrechner koppeln. Dazu werden jeweils die zu koppelnden Hörsysteme in einen Kopplungsmodus gebracht; das geschieht bei Hörsystemen beispielsweise durch Aus- und wieder Einschalten. Dann sind die Geräte für wenige Minuten im Kopplungsmodus und nur dann können sie gekoppelt werden. Aus Sicherheitsgründen wird zumindest von einigen Herstellern die Kopplungsreichweite, zum Beispiel auf 30 cm, stark begrenzt.

Zur drahtlosen Anpassung verwendet der Hörakustiker diverse Schnittstellen, wie zum Beispiel Noahlink Wireless oder Fitting Link. Diese stellen den Funkkontakt zum PC her. Eindringlinge müssten demnach genau in der Kopplungszeit die zu koppelnden Hörsysteme mit wie auch immer hergestellten Schnittstellen direkt nebeneinander platzieren, was schon sehr schwierig und auffällig wäre. Hinzu kommt, dass jede Firma eigene Protokolle verwendet, um die Hörsysteme zu koppeln. Kann mit einer Telefonnummer nur ein Anschluss erreicht werden, so muss man die „Telefonnummer" der Hörsysteme kennen, um mit ihnen Kontakt aufzubauen. Passiert dies nicht in kurzer Zeit, verlassen die Hörsysteme den Kopplungsmodus – aus Sicherheitsgründen und um Strom zu sparen. Ein erneuter Hackerangriff könnte also erst dann stattfinden, wenn die Geräte wieder im Kopplungsmodus sind.

Da die Reichweite der NFMI-Technik nicht groß ist, müssten sich potenzielle Eindringlinge zumindest mit der zum Hacken verwendeten Technik in direkter Nähe zu den eingeschalteten Hörsystemen befinden. Direkt heißt unter einem Meter; das

gilt nicht nur für die Kopplung, sondern für den gesamten Zeitraum des Abhörens. Hörgerätenutzer tragen ihre Streamer wie selbstverständlich um den Hals, wenn sie telefonieren möchten. Wenn Hacker jedoch unauffällig einen Streamer bei den Abzuhörenden unterbringen möchten, gestaltet sich das schon schwieriger.

Die Bluetooth-Schnittstelle ist ursprünglich entwickelt worden, um kabelgebundene Anwendungen am Computer – wie zum Beispiel eine Maus – auch drahtlos verwenden zu können. Ein wesentliches Entwicklungsziel war die absolut sichere Verbindung von zwei Komponenten, damit beispielsweise diverse Computer nicht durch eine Maus plötzlich ferngesteuert werden können. Deshalb wird mit einem Frequenzsprungverfahren gearbeitet, bei dem die Funkfrequenz 1600-mal pro Sekunde gewechselt wird. Wenn also hier nicht während der Kopplungsphase eine Verbindung aufgebaut ist, ist es praktisch unmöglich, in eine bestehende Verbindung einzudringen.

Wie sicher sind Apps?

Wird ein Smartphone gehackt, kann natürlich auch auf jede App zugegriffen werden. Die Firma Apple hat sehr strenge Auflagen, an die sich jeder halten muss, der Made for iPhone (MFi) anbietet. Im Apple-eigenen App Store werden nur von Apple geprüfte Apps zugelassen. Das ärgert viele Softwareentwickler, die alternative Anwendungen für die Apple-Smartphones anbieten möchten. Der Vorteil dieser geschlossenen und absolut kontrollierten Apple-Welt ist die hohe Funktionssicherheit und – in den bereits genannten Grenzen – die Sicherheit gegenüber Angriffen. Da einige Nutzer auf ihrem iPhone auch nicht lizensierte Apps installieren möchten, haben findige Softwareentwickler es geschafft, aus dem Apple-Gefängnis durch ein „Jailbreak" auszubrechen. Wer diese Anwendung nicht kennt, kann schon mal beruhigt sein; er wird ein sicheres Smartphone haben. Wer sein Gerät allerdings entfesselt, öffnet damit die Tore für alle unerwünschten Anwendungen – auch von außen.

Anders sieht es in der deutlich größeren Anwenderschar der Android-Smartphones aus. Google hat ganz bewusst sein Android-System offen gehalten, damit den Softwareentwicklern viele Freiheiten gelassen werden. Diese Offenheit beflügelt die Fantasie und Energie, leider auch die der Kriminellen. Es ist also tendenziell leichter, ein Android-System anzugreifen. Die dafür notwendige Software ist zwar in Deutschland verboten, kann aber über illegale Wege im Internet beschafft werden.

Im Gegensatz zu Hörsystemen sind Smartphones sehr einfach zu hacken. Foto: CarmenMurillo/iStockphoto

Welche Gefahr droht bei Hörsystemen?

Wenn die Frage gestellt wird, ob ein Hörgerät gehackt werden kann, muss auch gefragt werden, welche Gefahren damit verbunden sind. Einige Hörsystemnutzer wünschen sich, ihre Geräte selbstständig zu optimieren – eventuell sogar mit Ideen, die vom Hersteller noch nicht angedacht worden sind. Diese Forderung wurde zum Beispiel auf der Tagung des Chaos Computer Clubs 2013 aufgestellt. Wer ernsthafte und kompetente Ideen hat, sollte bei seinem Hörakustiker einen verständnisvollen Partner finden, der mit ihm die Ideen durchspielt.

Falls ein Hacker von außen die Einstellung ohne Wissen des Nutzers ändern möchte, müssten die schon beschriebenen, fast unüberwindbaren Hürden zur Kopplung überwunden werden. Zusätzlich müsste der Eindringling eine Software zur Einstellung mit riesigem Aufwand entwickeln, oder er müsste vorab wissen, welche Hörgeräte von welchem Hersteller am Ohr sind. Zusätzlich muss er dann genau für diese Geräte und die dort verwendete Firmware eine passende Software bereithalten. Falls er alle Hürden überwunden hat, wozu sollte er dann die Änderung vornehmen? Mit falsch dosierten Medikamenten könnte man einen unliebsamen Mitmenschen schwer schädigen oder sogar umbringen; mit falsch eingestellten Hörsystemen erreicht man im Zweifelsfall Ärger. Als Reaktion würden die Geräte schlicht vom Ohr genommen werden, um dann beim Hörakustiker die Einstellungen überprüfen zu lassen. Würde jemand den ganzen Aufwand betreiben, um einen Menschen zu ärgern? Schwer vorstellbar, Klingelstreiche sind da viel einfacher.

Eine häufig genannte Furcht ist die, dass persönliche Daten ausgeforscht werden könnten. Dies sind durchaus berechtigte Sorgen, da über ausgespähte Informationen alle möglichen privaten Verhaltensweisen aber auch Gesundheitsdaten zum eigenen Nachteil verwendet werden können. Wenn zum Beispiel ausgelesen wird,

wann die Hörgeräte morgens eingeschaltet werden, wann sie sich vom Wohnort entfernen und wann sie wieder auf dem Rückweg sind, könnte ein potenzieller Einbrecher die Wohnung leer räumen, wenn der Bewohner nicht zu Hause ist. Theoretisch ist das möglich. Falls so ein Ausspähen aber tatsächlich geplant ist, geht das viel einfacher: Über ein eingeschaltetes Smartphone lassen sich mit illegaler Software praktisch alle Aktivitäten des Nutzers überwachen. Das geht soweit, dass auch die im Handy eingebauten Mikrofone und Kameras zum verbrecherischen Ausspähen genutzt werden können. Wer hier große Sorgen hat, kann sehr einfach gegensteuern: kein Smartphone benutzen.

Fazit

Die Kopplung mit einem Hörsystem zum Zwecke des Ausspähens ist ziemlich schwierig. Viel einfacher geht dies über die vom Nutzer zusätzlich verwendeten Smartphones, speziell wenn es ein Android-Modell ist. Diejenigen, die größte Bedenken in Bezug auf Datensicherheit haben, sollten also generell auf die Nutzung von Mobiltelefonen verzichten. Wer halbwegs sicher telefonieren möchte, sollte die wenigen öffentlichen, mit Bargeld zu fütternden Fernsprecher wählen – und zwar an wechselnden, nicht wohnortnahen Standorten. Auf diese Art und Weise hat Altkanzler Helmut Kohl versucht, die verschiedenen Geheimdienste auszutricksen. Anders handelte seine Nachfolgerin Angela Merkel. Sie ist ein bekennender Handy-Fan und hat es den Diensten in dieser Hinsicht ziemlich leicht gemacht. Den reinen NFMI-Betrieb auszuforschen, ist fast unmöglich oder extrem aufwendig, potenzielle Spione würden sicher andere, einfachere Wege nutzen. Die gute Nachricht lautet also: Hörsysteme selbst können ohne Bedenken genutzt werden (siehe auch Seite 35 in dieser Ausgabe).

Horst Warncke

Literatur

Oticon (2016) Whitepaper „Opn Clinical Evidence"

WETTBEWERBS
RECHT

Bildnachweis: vectezy.com

Werbung mit Wirkaussagen – Paragraf 3 HWG beachten!

Einen Praxisfall der Wettbewerbszentrale sowie eine neuere Gerichtsentscheidung möchten wir zum Anlass nehmen, auf das spezialgesetzliche Irreführungsverbot des Paragrafen 3 Heilmittelwerbegesetz (HWG) hinzuweisen. Eine Irreführung im Sinne dieser Norm ist unter anderem dann anzunehmen, wenn Medizinprodukten, Verfahren oder Behandlungen eine therapeutische Wirksamkeit oder Wirkung beigelegt wird, die sie nicht haben (Paragraf 3 Satz 2 Nr. 1 HWG). Weiterhin erfasst die Vorschrift zum Beispiel auch den Fall, dass der fälschliche Eindruck erweckt wird, ein Erfolg könne mit Sicherheit erwartet werden, Paragraf 3 Satz 2 Nr. 2a HWG.

Eine Irreführung in diesem – zuletzt genannten – Sinne hat die Wettbewerbszentrale zum Beispiel in einem Fall angenommen, in dem ein Hörakustiker gegenüber Trägern von Hörgeräten damit geworben hatte, die Geräteeinstellungen so zu optimieren, dass ein „30 Prozent besseres Verstehen" erreicht wird. Da die Werbung außer einer Geld-zurück-Garantie keinerlei Einschränkungen enthielt und die individuellen Gegebenheiten der Hörgeräteträger vollkommen unberücksichtigt ließ, wurde fälschlich der Eindruck eines mit Sicherheit zu erwartenden Erfolges erweckt. Die Sache konnte durch die Abgabe einer Unterlassungserklärung außergerichtlich beigelegt werden.

Das Oberlandesgericht (OLG) Stuttgart hat sich kürzlich mit einem Fall befasst, in dem einem Medizinprodukt eine heilsame beziehungsweise leistungssteigernde Wirkung beigelegt wurde, die fachlich umstritten ist (OLG Stuttgart, Urteil vom 08.06.2017, Az. 2 U 154/16 – nicht rechtskräftig). In den Urteilsgründen haben die Richter darauf hingewiesen, dass der Werbende in einem solchen Fall zur Vermeidung einer Irreführung nach Paragraf 3 Satz 2 Nr. 1 HWG darauf hinweisen muss, dass seine Überzeugung von der Wirksamkeit seines Produktes nicht unumstritten ist. Das OLG hat außerdem festgestellt, dass das Vorhandensein einer CE-Kennzeichnung den Werbenden grundsätzlich nicht davon entbindet, den Nachweis der Richtigkeit der von ihm verwendeten Wirkaussagen zu führen.

Fazit: Eine eigene Werbung mit Wirkaussagen sollte stets auch auf die Einhaltung dieser spezialgesetzlichen Vorgaben hin überprüft werden.

Sabine Siekmann ·
Wettbewerbszentrale Büro Hamburg