Handys - Komfort nicht ohne Risiko

Tipps zum Datenschutz

Landesbeauftragter
für Datenschutz und Informationsfreiheit
Nordrhein-Westfalen

Herausgeber:

LDI NRW

Landesbeauftragter für
Datenschutz und Informationsfreiheit
Nordrhein-Westfalen
Ulrich Lepper

Kavalleriestr. 2-4
40213 Düsseldorf

Tel.: 0211 - 38424 - 0
Fax.: 0211 - 38424 - 10
Mail: poststelle@ldi.nrw.de

Diese Veröffentlichung kann neben anderen Broschüren zu Datenschutz und Informationsfreiheit unter www.ldi.nrw.de abgerufen werden.

Handys - Komfort nicht ohne Risiko

Mobiltelefone sind aus dem täglichen Leben nicht mehr wegzudenken. Sie sind klein, leicht und daher problemlos mitzunehmen, so dass eine ständige Erreichbarkeit gegeben ist. Sie bieten je nach Ausstattung und gewähltem Vertragsrahmen neben der Sprachkommunikation eine Reihe zusätzlicher Möglichkeiten wie Aufnahme und Versand von Fotos, Surfen im Internet, Bestellung und Abspielen von Musik oder die Nutzung als Ortungs- und Navigationsgerät.

Die Vielfältigkeit dieser Alleskönner beinhaltet aber auch Risiken. So erlauben sie verdeckte oder gar missbräuchliche Nutzungen, wie unbemerktes Mithören von Gesprächen, ungewollte Ortung oder heimliches Fotografieren. Die Betriebssoftware kann durch gezielte Aktionen so verändert werden, dass die Geräte überwacht oder als Wanze verwendet werden können.

Fotografie

Handys haben heute zum großen Teil hochwertige digitale Kameras integriert. Mit Ihnen können somit schnell Fotos erstellt werden und beispielsweise per MMS (Multimedia Messaging Service) direkt weitergeleitet oder sogar direkt ins Internet gestellt werden. Die fotografierten Personen sind damit oft gar nicht einverstanden.

Fotos, die eine identifizierbare Person zeigen, sind meist so lange unproblematisch, wie sie nur für persönliche und private Zwecke verwendet werden. Allerdings muss auch hier unbedingt die Intimsphäre beachtet werden. Das heimliche Hineinfotografieren in Wohnungen oder andere gegen Einblick geschützte Räume kann sogar mit Freiheitsstrafe bis zu einem Jahr oder Geldstrafe bestraft werden.

Die Zulässigkeit der Veröffentlichung von Fotos richtet sich nach dem Kunsturhebergesetz. Danach ist die Verbreitung von Bildern beispielsweise im Internet grundsätzlich nur erlaubt, wenn alle betroffenen Personen auf dem Foto eingewilligt haben.

In Ausnahmefällen ist eine Einwilligung aber nicht erforderlich, wenn der oder die Abgelichtete nur einen Teil einer Landschaftsaufnahme oder den Teil einer größeren Veranstaltung darstellt. So ist es auch zulässig ein Bild von einem Badestrand voller Menschen oder auch von einem Karnevalsumzug zu veröffentlichen, selbst wenn einzelne Personen darauf erkennbar sind. Die Personen dürfen aber nicht herausgestellt oder angezoomt werden.

Datenaustausch über Bluetooth

Viele Geräte besitzen neben dem Mobilfunk eine zweite Funkschnittstelle, über die im Nahbereich - meist bis circa 10 Meter - eine Kommunikation zu anderen elektronischen Geräten, wie PCs, PDAs oder schnurlose Headsets aufgebaut werden kann. Über diese Verbindung kann dann ein Datenaustausch oder eine Sprachübertragung erfolgen. Diese so genannte Bluetooth-Schnittstelle kann mit verschiedenen Sicherheitseinstellungen betrieben werden. Sie ist aber wie jede Funkschnittstelle angreifbar. So ist es beispielsweise über Bluetooth möglich, Nachrichten auf Geräte zu senden oder über den Zugriff auf Kalender oder Adressbücher Daten zu verändern oder zu entwenden.

Die Bluetooth-Schnittstelle sollte daher immer dann deaktiviert werden, wenn sie nicht benötigt wird. Sie sollte nur bei Bedarf und in sicherer Umgebung in Betrieb genommen werden.

Surfen im Internet

Um im Web zu surfen, wird ein Internetbrowser benötigt. So genannte Smartphones beinhalten diese Möglichkeit. Sie besitzen die Funktionalitäten von Handy und PDA (Personal Digital Assistent) und bieten viele Varianten der Datenkommunikation. Smartphones haben im Allgemeinen ein Betriebssystem, das es den Nutzerinnen und Nutzern ermöglicht, nach Belieben eigene Programme zu installieren und auszuführen. Im Grundsatz sind diese Geräte somit den gleichen Risiken ausgesetzt wie beispielsweise PCs oder Laptops. Sie hinterlassen bei entsprechender Nutzung und gerade durch den mobilen Gebrauch viele Datenspuren und sind genau wie Laptops vor Ausspionierung, Schadsoftware, Verlust oder Diebstahl zu schützen. So wurde mittlerweile spezielle "Spyware" für Smartphones entdeckt, die Daten über Anrufe, SMS und Internetaktivitäten auf dem mobi-

len Gerät sammelt und diese Daten versteckt zur Auswertung an einen Internetserver sendet.

Navigation

Handys, die mit einem GPS-Empfänger (Global Positioning System - satellitengestütztes System zu Standortbestimmung) und entsprechender Software ausgestattet sind, können auch zur Navigation eingesetzt werden. GPS-Systeme arbeiten nur passiv, das heißt, sie empfangen lediglich Signale, die weiter verarbeitet werden können. Deshalb können diese Systeme von sich aus nicht zur Überwachung eingesetzt werden, es sei denn, die eingesetzte Software leitet ermittelte Standortdaten automatisch an Dritte weiter. Beim Kauf oder Einsatz ist deshalb darauf zu achten, dass derartige Funktionen nur gewollt möglich sind.

Das elektronische Gedächtnis

Die komfortable Nutzung von Mobilfunkgeräten führt zur Speicherung vieler persönlicher Daten unterschiedlicher Qualität. So werden selbstverständlich die Kontaktdaten aller Kommunikationspartnerinnen und -partner in elektronischen Telefonbüchern gespeichert. Dies gilt ebenso für Termine, Erinnerungen oder auch Fotos. Diese Speicherung nimmt die Besitzerin oder der Besitzer des Handys noch selber aktiv vor. Die Speicherung der letzten Anrufdaten oder SMS-Meldungen erfolgt aber automatisch, wenn nicht auf eine Löschung geachtet wird. Die Speicherung der Daten ist so lange unproblematisch, wie sich die Geräte in persönlichem Besitz befinden. Da sie aber Aufschluss über Aktivitäten, Aufenthaltsorte und -zeiten, Bewegungen, Kommunikationspartnerinnen und -partner oder das soziale Umfeld geben können, sollte man sich vor Verkauf oder Reparatur eines Handys der gespeicherten Daten bewusst sein und darüber nachdenken, welche Daten zu löschen sind.

Das Handy als Wanze

Das Abhören von Räumen mit Wanzen ist aus vielen Darstellungen hinlänglich bekannt. Auch ein Handy kann für diese Zwecke verwendet werden. Im einfachsten Fall wird ein eingeschaltetes Handy, mit dem zuvor eine Gesprächsverbindung

aufgebaut wurde, im Raum liegengelassen. Alle im Raum geführten Gespräche werden, sofern das Mikrofon des Handys sie erfasst, zu einem Zielgerät übertragen.

Möglich ist es aber auch, Geräte von außen als Abhöranlage zu steuern. Sind bei einem "liegen gelassenen" Handy die Leistungsmerkmale, "Automatische Anrufannahme" und "Lautlosbetrieb" aktiviert, kann von außen sogar zu einem beliebigen Zeitpunkt abgehört werden. Erst ein Anruf versetzt das Handy dann in den Gesprächszustand. Zwar schließen sich bei vielen Geräten die Leistungsmerkmale "Automatische Anrufannahme" und "Lautlosbetrieb" gegenseitig aus und das Leistungsmerkmal "Automatische Anrufannahme" kann im allgemeinen nur in Kombination mit einer Freisprecheinrichtung genutzt werden; durch eine geschickte Auswahl von Ruftonoptionen und den Einsatz externer Sprechgarnituren (Mikrofon und Ohrhörer) kann der beschriebene Effekt aber trotzdem erreicht werden. Somit ist ein Handy allein durch die Nutzung von Standardmerkmalen und frei verfügbarer Technik schon als recht leistungsfähiges Abhörgerät zu betreiben.

Auch durch Hard- und Softwaremanipulationen können die Funktionen von Handys verändert werden. So können je nach Gerätetyp durch die Übermittlung von Service-SMS die Grundeinstellungen verändert, zusätzliche Funktionen aktiviert oder sogar unbemerkt Spionagesoftware in Handys eingebracht werden.

Ortung per Handy

Rund um die Handynutzung werden eine Reihe von Zusatzdienstleistungen angeboten. Basis dieser Dienstleistungen sind häufig die aktuellen Standortdaten der Handys. Sind Mobilfunkgeräte eingeschaltet, stehen sie mit örtlichen Sendeanlagen in Verbindung und sind über diese relativ genau lokalisierbar. Bei Ortungsdiensten handelt es sich um Angebote, die in der Regel eine Beziehung zwischen Telekommunikationsanbietern (Mobilfunk), Ortungsdienstleistern und Besitzerinnen oder Besitzern von Handy-Verträgen (zum Beispiel Eltern, Firmen) sowie den Nutzerinnen und Nutzern (zum Beispiel Kind, Angestellte/r) zum Gegenstand haben.

Im Fall der Ortung von Kindern wollen im Allgemeinen Eltern über das Handy des Kindes dessen aktuellen Standort abfra-

gen. Bei der KFZ-Ortung handelt es sich in der Regel um Arbeitgeberinnen und Arbeitgeber, die über den Abruf des Fahrzeugstandortes per Handy den Fahrzeugeinsatz optimieren möchten. Angeboten werden aber auch Dienste, bei denen beispielsweise auf Anfrage der nächste Pizza-Bäcker oder die nächste Apotheke mitgeteilt werden können. In allen Fällen liegen gleiche technische Funktionsweisen zu Grunde.

Die mit Hilfe der Mobilfunktechnik ermittelten Standortkoordinaten werden an den Dienstanbieter weitergeleitet. Hier erfolgt eine Umsetzung dieser Koordinaten in eine beschreibende Information, zum einen bei der Anfrage über das Internet in eine Kartendarstellung mit der Angabe des Ortes und zum anderen im Fall der Anfrage per SMS in eine entsprechende textliche Mitteilung mit Straße oder Ort.

Standortdaten dürfen von den Telekommunikationsunternehmen nur dann an Dritte wie beispielsweise Ortungsdienstleister weitergegeben werden, wenn die Besitzer der Geräte hierin eingewilligt haben und bei Überlassung von Geräten an weitere Personen, wie in Familien oder in Arbeitsverhältnissen, diese über die erteilte Einwilligung unterrichtet werden. Liegen diese Einwilligungen vor, können die Daten für Lokalisierungsdienste genutzt werden.

Die Dienstleistung ist deshalb aus der Sicht des Datenschutzes problematisch, weil Mitbenutzende von Geräten häufig über erteilte Einwilligungen nicht umfassend informiert wurden und sich über die Konsequenzen dauerhafter Überwachungsmöglichkeit nicht im Klaren sind.

Überwachung

Neben der Ortung für private Zwecke können auch Sicherheitsbehörden unter festlegten gesetzlichen Voraussetzungen Handys orten und abhören. Neben der allgemeinen Telefonüberwachung und den hierüber möglichen Zugriff auf die Telekommunikationsdaten gibt es spezielle Geräte, so genannte IMSI-Catcher (International Mobile Subscriber Identity - netzinterne Teilnehmerkennung), die es erlauben, nahezu unbemerkt örtliche Bereiche darauf zu überwachen, ob in ihnen ein bestimmtes Geräte in Betrieb ist. Die Geräte simulieren hierfür eine Basisstation, indem sie eine zusätzliche eigene Funkzelle aufbauen, die sich genau wie eine Originalzelle verhält. Über diese

Station laufen dann alle Verbindungswünsche der Handys, die sich im Einflussbereich des Überwachungsgerätes befinden. Weil die Geräte mit einer etwas stärkeren Leistung arbeiten, melden sich alle Handys in dieser neuen Funkzelle und nicht bei der eigentlichen Basisstation an. Die Nutzerinnen und Nutzer bemerken hiervon nichts. Von allen in seiner Reichweite befindlichen Handys kann der IMSI-Catcher neben der IMSI auch die IMEI (International Mobile Station Equipment Identity - Endgerätekennung) abrufen. Technisch bedingt können während der aktiven Überwachung von keinem umgeleiteten Handy Gespräche geführt oder empfangen werden. Selbst Notrufe zu Polizei, Feuerwehr oder ärztlichem Notdienst sind von keinem der in der neuen Funkzelle eingebuchten Handys möglich.

Bei derartigen Überwachungen ist immer eine beträchtliche Anzahl Unbeteiligter ebenfalls betroffen. Die Datenschutzbeauftragten des Bundes und der Länder haben den Einsatz der IMSI-Catcher besonders deshalb abgelehnt, weil sie das Recht unbeteiligter Dritter auf unbeobachtete Kommunikation mit hoher Intensität beeinträchtigen.

Es wird deutlich, dass Handys neben ihren vielfältigen Möglichkeiten eine Reihe von Datenschutzrisiken und missbräuchlichen Anwendungsmöglichkeiten bieten. Einen garantierten Schutz dagegen gibt es nicht. Den Nutzerinnen und Nutzern von Handys sollten jedoch die Einsatzmöglichkeiten ihrer Geräte bekannt sein, damit sie für sich bewusst entscheiden können, wie und bei welchen Gelegenheiten sie ihr Gerät einschalten und welche Funktionen sie nutzen. Deshalb ist es wichtig, dass Mobilfunkgeräte in ihren Anleitungen transparent beschrieben und in der Nutzung der Dienste einfach zu handhaben sind. Weiter sollte der Netzbetrieb so ausgestaltet sein, dass Missbrauchsmöglichkeiten so weit wie möglich ausgeschlossen sind. Bei der Vielfältigkeit der Angebote bedarf es von Seiten der Telekommunikationsindustrie einer offenen und umfassenden Information der Kundschaft nicht nur über die Möglichkeiten sondern auch über die Risiken der Mobilfunkkommunikation.

Schließlich sollten Handys weder in fremde Hände gegeben noch unbeobachtet liegen gelassen werden. Nur so kann vermieden werden, dass Dritte heimlich Software auf das Handy laden oder unberechtigt Onlinedienste für das Handy bestellen, um später die Besitzerin oder den Besitzer auszuspionieren.

Literatur und Links

Bundesamt für Sicherheit in der Informationstechnik (BSI): GSM-Mobilfunk Gefährdungen und Sicherheitsmassnahmen, http://bsi.de/literat/doc/gsm/index.htm

BSI Mobile Kommunikation - Handys**:**
http://www.bsi-fuer-buerger.de

Claudia Eckert: IT-Sicherheit, Oldenbourg Wissenschaftsverlag, 2006