BEILAGE ZUM DSD 4 | 2018

BDSW

INFO
WIRTSCHAFTSSCHUTZ

EINE PUBLIKATION DES ARBEITSKREISES WIRTSCHAFTSSCHUTZ DES BDSW

Schöner Fortschritt – fragliche Sicherheit

→ Früher, viele erinnern sich, war Telefonieren richtig anstrengend. Wer unterwegs war, musste sich eine Telefonzelle suchen. Vor vielen dieser gelben Häuschen bildeten sich Schlangen. Und manche Apparate waren kaputt. Das alles ist heute kein Thema mehr. Ein Griff zum Handy – und die Verbindung steht.

Ein schöner Fortschritt, der uns allen zugutekommt. Doch die Moderne fordert ihren Preis. Kurz gesagt: Mehr Technik – mehr Risiken. Seitdem die Mobiltelefone internetfähig geworden sind, sind auch die Risiken des weltweiten Webs dazugekommen. Das Telefonieren ist im Zeitalter des Mobilfunks bequemer und komfortabler geworden. Aber unbedingt sicherer geworden ist es nicht.

Ein Problem sind zweifelsohne die Apps. Einerseits bereichern sie unser digitales Leben. Auf der anderen Seite aber funktionieren nicht wenige von ihnen nur dann, wenn wir ihnen weitestgehende Zugriffsrechte, zum Beispiel auf die Adressliste mit allen Kontakten, einräumen. Das sind höchst sensible Daten, die – in die falschen Hände geraten – viel Unheil anrichten können.

Nicht jeder weiß, was er sich da heruntergeladen hat. Denn die ellenlangen, zum Teil schwer verständlichen Benutzungsbedingungen laden nicht gerade zur Lektüre ein. Mancher Nutzer stimmt deshalb aus Bequemlichkeit oder auch businesstypischem Zeitmangel diesen AGBs zu. Frei nach der Devise: Es wird schon alles seine Ordnung haben. Doch wie bei jedem Download sollte genauer hingeguckt werden, worauf man sich einlässt.

Es geht nicht darum, Apps generell zu verteufeln. Diese Anwendungssoftware kann großen Nutzen haben, das steht fest. Trotzdem gilt es immer abzuwägen: Sind die Vorteile einer App tatsächlich so groß, dass massive Einschränkungen der Sicherheit und der Privatsphäre hingenommen werden können beziehungsweise gibt es Apps, die mindestens das Gleiche können, aber weniger massiv in den persönlichen Datenschutz eingreifen?

Klassische Lauschangriffe – das war gestern. Heute geht es sehr viel einfacher: per App. Manche dieser Anwendungsprogramme sind in der Lage, Sprachtelefonie mitzuschneiden. Foto: Günther Gumhold/pixelio.de

Und bitte immer im Hinterkopf behalten: Prüfen Sie genau, was über Mobilgeräte kommuniziert werden sollte und was besser nicht. Empfohlen werden kann eine „Datendiät", sprich so wenig sensible Information wie möglich über Verbindungen, die zumindest theoretisch kompromittierbar sind.

So bleiben Sie auf der sicheren Seite.

Holger Köster
Vorsitzender
BDSW-Arbeitskreis Wirtschaftsschutz ←

Der Komfortgewinn und seine Schattenseiten: Apps-Risiken für die Mobilfunksicherheit

Von Klaus Henning Glitza

→ Oft kostenlos und mit faszinierenden neuen Möglichkeiten – das ist die Application Software. Zu Deutsch eine Anwendungssoftware, die kurz App genannt wird. Zusätzliche Applikationen, die heute en vogue sind. Als hoffnungsloser „Dino" gilt, wer sie nicht hat. Erst durch sie werden Mobilgeräte zu Multimediacentern.

Allerdings sind die Risiken und Nebenwirkungen vieler Apps weniger phantastisch. Dass die Sicherheit von Mobilfunkgeräten – dazu gehören neben Handys und Smartphones auch Tablets – durch fremdgesteuerte Software gefährdet werden kann, wurde von Info Wirtschaftsschutz bereits beleuchtet. Wie sieht es aber mit der Gefährdung aus, der wir durch eigenes Zutun Vorschub leisten? Bei sozialen Netzwerken ist bekannt, dass Nutzer ohne Not Informationen preisgeben, die von böswilligen Naturen missbräuchlich verwendet werden können. Bei den Handynutzern gibt es betrüblicherweise analogen Trend. Denn sie geben häufig große Teile ihrer Sicherheit und persönliche Daten preis, wenn sie sich Apps herunterladen.

Die Apps kommen oft unter Tarnkappen daher. Wer denkt schon, dass eine installierte Taschenlampe nicht nur die dunkle Umgebung beleuchtet, sondern auch die Kontaktdaten des Handynutzers in den Fokus nimmt. Selbst bei Anbietern, die landläufig als seriös gelten, werden von den Nutzern Zugeständnisse verlangt, die eigentlich stutzig machen müssten. So wird mit dem Download der App in vielen Fällen der Zugriff auf Kontaktdaten, Mikrofon, Fotodateien und Kamera sowie die Standortbestimmung erlaubt. Aus dem Mobiltelefon wird dadurch ein perfektes Spionageinstrument, das die Brandbreite von klassischen Spy-Tools häufig noch übertrifft.

Einige Foto-Apps lassen sich von den Benutzern die Urheberrechte an den Bildern übertragen. Die Fotos können dann weltweit verbreitet werden und das gilt natürlich nicht nur für harmlose Urlaubsbilder. Schauen Sie deshalb immer erst in die AGBs, bevor Sie auf „Akzeptieren" drücken.
Foto: Erwin Lorenzen / pixelio.de

Viele dieser Zugriffsmöglichkeiten gehen weit über die Anforderungen hinaus, die Apps für einen zuverlässigen Betrieb benötigen. Selbst Anbieter, die als seriös gelten, oder beliebte Apps, die millionenfach in Gebrauch sind, bilden da keine Ausnahme. Beispielhaft sei ein Play Store genannt. Wer ihn benutzt, räumt den Zugriff auf Kontaktdaten, Fotos und abgespeicherte Dokumente ein. Und schon bei der Registrierung werden – wie bei anderen Apps auch – persönliche Daten abgefragt. Nicht selten gehören neben Geburtsdatum, Adresse und Telefonnummer auch die Bankdaten dazu.

Die feindliche Übernahme der Handys vollzieht sich nicht unbedingt unmittelbar bei der Erstregistrierung. Beliebter Trick: Erst bei Updates werden die erweiterten Zugriffsmöglichkeiten implementiert. Das steht dann auch so im zum Update gehörenden „Kleingedruckten". Aber Hand auf Herz. Wer liest das schon Buchstabe für Buchstabe? Doch das sollte jeder Nutzer dringend tun – auch wenn es mühselig ist und die Texte oft einen denkbar geringen Spannungsgrad aufweisen.

Einfach auf den „Akzeptieren"-Button der Allgemeinen Geschäftsbedingungen (AGB) zu drücken, das ist alles andere als angebracht. Denn aus diesen oft seitenlangen und in verquaster Sprache abgefassten Benutzungsbedingungen geht hervor, welche Berechtigungen dem App-Anbieter eingeräumt werden. In den AGB ist häufig von der Weitergabe der persönlichen Daten an ungenannte Dritte und der Analyse des Nutzerverhaltens die Rede. Doch wohin die Daten wirklich gehen, das wird bei vielen Anbietern eine auf ewig unbeantwortete Frage bleiben. Von ausländischen Betreibern ist bekannt, dass sie noch nicht einmal antworten, wenn einschlägige Fragen gestellt werden. Und oft haben just solche Betreiber ihren Sitz in Ländern, die dem Datenschutz gegenüber äußerst liberal eingestellt sind – um es höflich auszudrücken. Ein Albtraum für alle, die auf den Datenschutz Wert legen.

Durch manche unsicheren Anwendungsprogramme gelangen die sensiblen Daten sogar in die Hände von Angreifern. Bei Apps, mit denen Bundesligavereine ihre Fans bei Laune halten, wurde festgestellt, dass sie E-Mailadressen, Handy-Identifikationsdaten und Passwörter der Benutzer unverschlüsselt übertrugen. Ein Risiko ersten Grades, denn nicht wenige Zeitgenossen nutzen identische Kombinationen von Mailadresse und Passwort auch für andere Dienste, im schlimmsten Fall Payment Services. Die Bundesligisten haben inzwischen nachgelegt und die Sicher-

Auch auf Tablets ist im Regelfall eine Vielzahl von Apps installiert. Genau wie bei Mobiltelefonen ist anzuraten: Prüfen Sie, welche dieser Applikation Sie wirklich benötigen. Auch standardmäßig installierte Apps sollten Sie mit kritischen Augen betrachten. Foto: Petra Bork / pixelio.de

Wer die Allgemeinen Geschäftsbedingungen akzeptiert, hat auch ohne Unterschrift einen Vertrag abgeschlossen. Viele Nutzer fallen aus allen Wolken, wenn sie sich die AGB genau durchlesen. Was sich etliche Anbieter an Zugriffsrechten einräumen lassen, ist schlichtweg abenteuerlich. Foto: Thorben Wengert / pixelio. de

heitslücken gestopft. Experten rechnen aber damit, dass es noch tausende andere Apps gibt, die für Angreifer in ähnlicher Weise offen sind wie ein Scheunentor.

Vorsicht ist auch bei Foto-Apps geboten. Möglicherweise lassen sich diese Applikationen Urheberrechte einräumen. Wird den AGB zugestimmt, können die App-Anbieter Ihre privaten und dienstlichen Fotos weltweit verbreiten – und das völlig „legal".

Nicht unerwähnt bleiben soll, dass auch Fake-Apps kursierten. Das sind Quasi-Transporter von Viren, Trojanern und anderer Malware, die als Apps getarnt sind. Im Vordergrund erscheinen sie ihren Nutzern als smarte Helferlein, im Hintergrund arbeiten sie nach Kräften gegen sie. Diese Camouflage-Apps sind in der Lage, neben Daten und Passwörtern auch die SMS-Kommunikation und sogar Sprachtelefonie auszuspähen. Kriminelle haben Fake-Apps oft genug eingesetzt, um im Namen der Nutzer extrem teure Premium-SMS zu versenden.

Doch in einer Zeit, in der vehement der Datenschutz eingefordert wird, tritt ein Paradoxon auf. Das Entertainment und der Komfort, den Apps bieten, lässt häufig die Sicherheitsbedenken verblassen. Oft ist das Argument zu hören, man habe ja nichts zu verbergen. Das gilt bei näherem Hinsehen nur sehr eingeschränkt für Privatpersonen, denn wer kann schon ruhigen Gewissens Kontonummern, Kontostand, schützenswerte Daten seiner Kinder, geschweige denn Details aus seinem höchstpersönlichen Lebensbereich zur Sache der Öffentlichkeit machen. Was für den Privatbereich zutrifft, gilt in sehr ähnlichem, wenn nicht noch höherem Maße für Unternehmen. Jede Firma, auch die kleinste, hat Geschäftsgeheimnisse, die aus gutem Grund zu hüten sind. Neben technischem Know-how gehören zum Beispiel immer auch Personalinterna, Kundendaten und anstehende Produkteinführungen oder Kampagnen dazu.

Und: Machen Sie sich bitte von dem Gedanken frei, dass es unwichtige Daten gebe. Denn so unbedeutend das einzelne Datum (Singular von Daten) auch vordergründig erscheinen mag, in der Verknüpfung mit anderen Daten kann es durchaus Bedeutung gewinnen. Ein paar Soft-Daten können, richtig analysiert und zusammengeführt, durchaus eine harte Information erbringen.

Wer das Internet nutzt, bewegt sich in einem Medium des immensen Datenhungers. Es gibt Firmen, die ihre Dienste gratis anbieten, aber trotzdem zu den wertvollsten Unternehmen der Welt gehören. Dass sie allen Datenschutzbestimmungen zum Trotz mit persönlichen Daten handeln und damit Milliarden machen, ist seit Jahren bekannt. Und nicht erst seit Edward Snowden weiß man, dass sich nicht nur die Werbeindustrie um solche datenbezogenen Fänge und Beifänge reißt, sondern auch andere meist ausländische und oft regierungsnahe Institutionen.

Was kann konkret gegen das Sicherheitsrisiko App unternommen werden?

Seien Sie generell wachsam bei kostenlosen Angeboten. Die Erfahrung zeigt, dass kostenpflichtige Angebote oft weitaus weniger als Datenstaubsauger fungieren – schon, weil sie sich nicht allein mit Datenhandel finanzieren müssen.

Wenn Sie unsicher sind, surfen Sie im Internet nach der fraglichen App. Oft sind dort einschlägige Benutzererfahrungen und Warnhinweise zu finden.

Prüfen Sie generell sorgfältig die AGB, auch wenn das Zeit erfordert. Nur so können Sie sich vor unakzeptablen Nutzungsbedingungen schützen.

Checken Sie unter dem Menüpunkt Einstellungen beziehungsweise Einstellungen/Datenschutz, welche Berechtigungen dort abgespeichert sind. Bei neueren Modellen kann der bereits genehmigte Zugriff auf Standortdaten, Fotos und Kontaktdaten wieder rückgängig gemacht werden.

Navigations-Apps benötigen den Zugriff auf Ihre Standortdaten, aber bei etlichen anderen Anwendungen ist es häufig mehr als fraglich, wozu die Ortungsfunktion gut sein soll. Haben Sie kein Navi auf Ihrem Mobilgerät, deaktivieren Sie diese.

Fragen Sie sich immer, ob die verlangten Berechtigungen nachvollziehbar sind. Wenn eine Handwärmer-App (ja, auch so etwas gibt es) Ihre Kontaktliste und Ihre GPS-Daten ausspähen will, wofür soll das gut sein? Viele Anwendungen entlarven sich selbst, indem sie nicht plausible Zugangsrechte einfordern.

Schränken Sie soweit wie möglich die Anzahl der Apps ein. Fragen Sie sich, was

Sie wirklich brauchen. Oft führen vereinzelte Apps ein Mauerblümchendasein. Manche „Games" werden zwei-, dreimal gespielt und haben dann ihren Reiz verloren. Löschen Sie solche Anwendungsprogramme konsequent. Positiver Nebeneffekt: Wenn Sie sich von solchem Ballast trennen, kann Ihr Betriebssystem spürbar schneller werden.

Behalten Sie stets die Statusleiste Ihres Mobilgerätes im Auge. Es tauchen dort eindeutige Symbole auf, wenn die Ortungsfunktion oder Funkschnittstellen wie Bluetooth ohne Ihr Zutun aktiviert werden. Ist dies der Fall, sollten Sie einen sicheren Prozessmonitor installieren, der die laufenden Anwendungen identifiziert. Ziehen Sie im Zweifelsfall einen ausgewiesenen Fachmann (keinen reinen Handyverkäufer) zu Rate.

Bevorzugen Sie seriöse Anbieter, aber seien Sie auch diesen gegenüber nicht allzu vertrauensselig.

Auch für Apps gilt: Der beste Datenschutz ist, wenn Sie selbst etwas tun. ←

Mobiltelefone sind unsere ständigen Begleiter. Quasi auf Schritt und Tritt. Und das beruflich wie privat. Deshalb ist es unerlässlich, diese Geräte auf mögliche, unerwünschte Risiken und Nebenwirkungen zu checken. Denn keine andere Technik ist so eng mit unserem Leben verknüpft.
Foto: Sascha E. Gaul / pixelio.de

Analysen und Hilfestellungen zum Wirtschaftsschutz

Von Dr. Berthold Stoppelkamp
Leiter des Hauptstadtbüros des BDSW und zuständiges Geschäftsführungsmitglied für den Arbeitskreis Wirtschaftsschutz

WISKOS-Bericht: Wirtschaftsspionage & Konkurrenzauspähung

→ Ein Großteil der Unternehmen des Verarbeitenden Gewerbes ergreift zu wenige Maßnahmen gegen Wirtschaftsspionage und Konkurrenzausspähung. Nach einer aktuellen Datenauswertung sind besonders die Elektronik-/Elektroindustrie (21 Prozent) und der Maschinenbau bzw. die Chemie-/Pharmaindustrie (jeweils 16 Prozent) bedroht. Zu diesem Ergebnis kommt das Fraunhofer-Institut für System- und Innovationsforschung ISI im Rahmen des Projekts WISKOS. Diese Erhebung wird alle drei Jahre durchgeführt und umfasst Angaben von 1.300 Produktionsbetrieben.

www.wiskos.de ←

Bitkom-Studie: Wirtschaftsschutz in der Industrie

→ 68 Prozent der Industrieunternehmen sind in den letzten zwei Jahren Opfer von Sabotage, Datendiebstahl oder Spionage geworden. 32 Prozent der Unternehmen wurden IT- oder Telekommunikationsgeräte gestohlen. Attacken auf die deutsche Industrie verursachten einen Gesamtschaden von 43 Milliarden Euro im Zweijahreszeitraum. **www.bitkom.org** ←

BKA-Bundeslagebild Cybercrime 2017

→ Cyberkriminalität hat in Deutschland im Vergleich zu 2016 um 4 Prozent zugenommen. 86.000 Fälle zählte das BKA. Durch Computerbetrug ist ein Schaden von 71,4 Millionen Euro entstanden. Auch kritische Infrastrukturen geraten zunehmend in das Visier von Cyberangriffen. **www.bka.de** ←

BfV-Broschüre: Nachrichtendienstlich gesteuerte Cyberangriffe

→ Nachrichtendienste setzen zunehmend zur Ausforschung von Regierungsstellen, Wirtschaftsunternehmen oder Forschungsinstituten Cyberangriffe ein. Die Broschüre informiert speziell über russische, chinesische und iranische Cyberangriffskampagnen.
www.verfassungsschutz.de ←

BDSW
BDSW BUNDESVERBAND DER SICHERHEITSWIRTSCHAFT
Verantwortlich: Dr. Berthold Stoppelkamp
Redaktion: Klaus Henning Glitza
Norsk-Data-Straße 3 · 61352 Bad Homburg
Fon: +49 6172 948050 · Fax: +49 6172 458580
Mail: mail@bdsw.de
Web: www.bdsw.de