Infobrief Datenschutz
Ausgabe 04 | 2012

agentia wirtschaftsdienst

Newsletter Datenschutz

Die Kundenzeitung der agentia wirtschaftsdienst

Liebe Leserin, lieber Leser,

mit einem Smartphone können Sie viel mehr als telefonieren. Die darauf installierten Anwendungen oder Apps machen Smartphones zu Mini-Computern. Doch so manche App spioniert Sie aus. Lesen Sie in dieser Ausgabe, wie Sie solche Apps erkennen.

Und noch eine neuartige Gefahr verdient Ihre Aufmerksamkeit: QR-Codes - kleine Quadrate mit schwarz-weißen Strichen darin - versprechen Ihnen auf Plakaten und Prospekten Gutscheine oder nützliche Downloads. Stattdessen kommt vielleicht ein Trojaner auf Ihr Handy. Zusätzlich erfahren Sie heute, wie Sie sich verhalten sollten, wenn eine E-Mail eintrifft, die vertraulich behandelt werden soll, und welche Daten für Werbemaßnahmen eingesetzt werden dürfen und welche nicht.

Ich wünsche Ihnen viele wichtige Erkenntnisse mit dieser neuen Ausgabe und stehe gerne für Rückfragen zur Verfügung! Ihr *Udo Wenzel, Datenschutzbeauftragter*

QR-Codes: Auf schnellstem Weg zum Datenklau?

Die Mini-Quadrate mit schwarz-weißem Muster sind fast überall zu finden, sie prangen auf Plakaten, Versandkatalogen und Produktverpackungen. Statt der angebotenen Zusatzinformation können QR-Codes aber auch Spionagesoftware aufs Smartphone laden.

Schluss mit dem lästigen Abtippen

Ein Blick in den Wochenprospekt vieler Discounter reicht aus, um auf einen QR-Code zu stoßen. Neben der Produktabbildung sehen Sie den zweidimensionalen Strichcode, den Sie mit Ihrem Smartphone einfach abfotografieren können, um im Gegenzug z.B. ein Produktvideo zur neuen Kaffeemaschine angezeigt zu bekommen. Früher nannte die Werbung eine Internetadresse für weitere Informationen, doch wer will schon abtippen?

Schnelle Antwort aus mobilem Internet

Die Mini-Anwendung oder App zum Einlesen der als QR-Code bezeichneten Mini-Quadrate ist oft bereits auf dem Smartphone installiert oder kostenlos zu haben. QR-Code steht für "Quick Response Code", und eine schnelle Antwort bekommen Sie tatsächlich. Die Frage ist nur, wie diese Antwort aussieht.

QR-Codes sind Links in Bildform

Wenn Sie einen QR-Code mit Ihrem Smartphone einlesen, wird das zweidimensionale Muster in eine Internetadresse übersetzt. Die meisten Apps für QR-Codes öffnen dann diese Internetadresse automatisch zum Beispiel im mobilen Browser. Sie sehen dann nach kurzer Zeit das Produktvideo oder den versprochenen Online-Gutschein. Bald können Sie sogar Konzertkarten über den QR-Code buchen und mit Ihrem Smartphone bezahlen.

Internetverbindung mit unbekanntem Ziel

Da wir Menschen den QR-Code nicht lesen können, wissen wir auch nicht, wohin er uns führt: Wirklich zum Produktvideo? Tatsächlich zur Konzertkasse und zur Bezahlmöglichkeit? Oder zu einer gefälschten Webseite, die die Bankverbindung stehlen möchte? Nicht nur das: Statt des Produktvideos könnte auch ein Trojaner übertragen werden. Mit einem QR-Code starten Sie eine Verbindung mit unbekanntem Ziel, das auch zu einem Datendiebstahl führen könnte!

Datendiebe missbrauchen QR-Codes

Internetkriminelle haben bereits begonnen, gefälschte QR-Codes zu verteilen. Die Smartphones der Opfer wurden mit Trojanern infiziert, die automatisch kostspielige Premium-SMS-Dienste auf Kosten der Betroffenen bestellt haben. Statt der gewünschten Information erhielten die Opfer eine extrem hohe Mobilfunkabrechnung! Weitere Attacken werden erwartet, denn die Manipulation von QR-Codes ist leider ganz einfach.

Jeder kann schädliche QR-Codes erzeugen

Im Internet gibt es kostenlose Möglichkeiten, zu jeder Internetadresse einen QR-Code zu erzeugen, auch zu einer verseuchten Webadresse, die zu einem Schadprogramm führt. Den manipulierten QR-Code kann man dann ausdrucken und einfach auf ein Plakat kleben - fertig ist die Smartphone-Attacke.

Deshalb: **Nutzen Sie nur QR-Code-Scanner (Apps), die Ihnen eine Vorschau der zu öffnenden Internetadresse anzeigen. Verwenden Sie aktuelle Anti-Viren-Software auf Ihrem Smartphone und zum Beispiel den kostenlosen Norton Snap QR Code Reader, der anzeigt, ob der QR-Code auf eine sichere Seite führt, oder ob sich dahinter eine gefährliche Webseite verbirgt.**

Vertraulichkeitsvermerke bei Mails - sind sie wirklich völlig egal?

Fast jede Mail, die im Büro eintrifft, enthält am Ende einen Vertraulichkeitsvermerk. Üblicherweise sagt man, dass der Adressat einer Mail einen solchen Vermerk einfach ignorieren kann. Seien Sie vorsichtig: So einfach ist die Sache nicht!

Jeder kennt den üblichen Text

"Diese Mail enthält vertrauliche und rechtlich geschützte Informationen. Wenn Sie nicht der richtige Adressat sind und diese Mail irrtümlich erhalten haben, informieren Sie bitte sofort den Absender und vernichten Sie diese Mail."

Mancher kann diese und ähnliche Texte schon nicht mehr sehen und fragt sich: Was soll das eigentlich? Wenn jemand mir eine Mail schickt, soll er sich eben vorher überlegen, ob sie in meine Hände geraten soll. Und wenn er sie mir schickt, ist es doch wohl meine Sache, was ich mit dieser E-Mail tue.

Mails an einen falschen Adressaten

Daran ist jedenfalls so viel richtig, dass es nicht Ihr Problem ist, wenn jemand eine Mail irrtümlich an Sie als falschen Adressaten versendet. Dann hat der Absender wahrscheinlich sogar seine Pflichten verletzt. Das gilt vor allem dann, wenn er personenbezogene Daten anderer Personen (etwa von Kunden) an Sie geschickt hat, obwohl diese Daten Sie gar nichts angehen.

Übertreiben muss man es nicht. Doch die Vertraulichkeitsvermerke in E-Mails sind auch nicht nur reine Dekoration.

Sie selbst haben damit jedoch nichts zu tun. Wenn Sie den Absender über die Fehlleitung informieren, ist das ein reiner Akt der Höflichkeit, zu dem Sie nicht verpflichtet sind. Weiterverbreiten - etwa im Freundeskreis - dürfen Sie eine solche Mail allerdings nicht.

Das wäre eine Übermittlung personenbezogener Daten, für die es keine Rechtfertigung gibt.

Mails im Rahmen einer Geschäftsverbindung oder eines Rechtsstreits

Aber wie sieht es aus, wenn Ihr Unternehmen mit dem Absender einer Mail in einer dauernden Geschäftsverbindung steht und Sie durchaus der richtige Adressat sind? Oder wenn Ihr Unternehmen mit dem Absender in einem Rechtsstreit liegt, in dessen Rahmen Mails gewechselt werden?

Viele glauben, dass geschäftliche Mails rechtlich nicht geschützt sind und ohne Weiteres weitergegeben oder veröffentlicht werden dürfen. Das stimmt so aber nicht.

Das musste sich auch ein Unternehmen sagen lassen, das Mails, die im Zusammenhang mit einem Rechtsstreit mit einem anderen Unternehmen gewechselt worden waren, einfach auf die eigene Webseite stellte. Das Ziel war dabei, die Öffentlichkeit über den Rechtsstreit zu informieren.

Das sind die maßgeblichen Kriterien

Jedenfalls im konkreten Fall wollte das Landgericht Saarbrücken von einem Recht zur Veröffentlichung dieser E-Mails nichts wissen. Vielmehr wies das Gericht auf folgende Aspekte hin:

- Ein Vertraulichkeitsvermerk bringt deutlich zum Ausdruck, dass der Absender eine Weitergabe oder Veröffentlichung einer Mail nicht wünscht.

- Wenn eine solche Mail an eine bestimmte Person oder ein bestimmtes Unternehmen gerichtet ist und gezielt dorthin gesandt wurde, muss der Absender nicht mit einer Veröffentlichung rechnen.

- Eine Veröffentlichung ist dann nur in besonderen Situationen zulässig, wenn etwa ein berechtigtes Interesse der Öffentlichkeit besteht, etwas über den Vorgang zu erfahren, oder wenn der Absender in dieser Angelegenheit selbst schon an die Öffentlichkeit getreten ist.

- Ansonsten muss eine Veröffentlichung einer solchen Mail unterbleiben.

Intern ist eine Weitergabe möglich

Im Ergebnis hat ein Vertraulichkeitsvermerk in solchen Fällen somit die Wirkung, dass zumindest eine Veröffentlichung nicht erlaubt ist. Was natürlich dennoch geht, ist die Weitergabe einer solchen Mail an einen Vorgesetzten, um ihn zu informieren.

Mails mit Vertraulichkeitsvermerken sollten das Unternehmen nicht verlassen

Nach außen sieht es anders aus

Sie sehen also: Völlig gleichgültig ist ein Vertraulichkeitsvermerk nicht. Wer aber mit Mails so umgeht, wie dies allgemein üblich ist, muss einen solchen Vermerk nicht fürchten. Kritisch wird es erst, wenn eine solche Mail den Bereich des Unternehmens verlässt. Aber davon werden Sie Normalfall ohnehin die Finger lassen.

Vorsicht ist besser als Nachsicht

Was die Mails angeht, die Sie selbst verschicken, sollten Sie sich allerdings nicht zu sehr auf einen Vertraulichkeitsvermerk verlassen. Schauen Sie vor allem genau hin, ob der richtige Adressat angegeben ist. Zugegeben: Dieser Ratschlag ist banal - aber der Alltag zeigt, wie wichtig er ist.

Impressum

Redaktion:
Dipl.-Inform. Udo Wenzel
Datenschutzbeauftragter

Anschrift:
agentia wirtschaftsdienst
Budapester Straße 31
10787 Berlin
Telefon: 030 / 2196 4390
E-Mail: udo.wenzel@agentia.de

Kommt persönlich adressierte Werbung wirklich immer unerwünscht?

Über persönlich adressierte Werbung wird meist eher negativ geredet. Viele glauben, das alles sei eine rechtliche Grauzone. Dabei gibt es durchaus klare gesetzliche Regeln. Im Folgenden sind einige Regeln geschildert, die in der Praxis besonders wichtig sind.

Auch Werbung hat zwei Seiten

Wie so viele Dinge kann man Werbung von zwei Seiten betrachten. Wer im Interesse seines Arbeitsplatzes darauf hofft, dass das eigene Unternehmen mehr Umsatz macht, wird sich über den Erfolg einer Werbekampagne freuen. Wer persönlich adressierte Werbung ins Haus bekommt, ist darüber nicht immer so glücklich.

Nicht immer ist eine Einwilligung nötig

Viele meinen, persönlich adressierte Werbung dürfe man nur bekommen, wenn man ausdrücklich erklärt hat, dass man damit einverstanden ist. Das ist eine Möglichkeit, die in der Praxis tatsächlich Bedeutung hat. Das Gesetz lässt jedoch weit mehr zu.

Das "Listenprivileg"

Eine besondere Rolle spielen dabei Listen mit Adressdaten. Dazu gehören etwa Listen von Kunden, die schon einmal bei einem Unternehmen gekauft haben. Solche Listen darf jedes Unternehmen zusammenstellen. Allerdings dürfen darin nur bestimmte Daten enthalten sein, die das Gesetz einzeln aufzählt. Es handelt sich um:

- Namen
- Titel oder akademischen Grad
- Anschrift
- Geburtsjahr

Die Details entscheiden

Geregelt ist dies in § 28 Absatz 3 Satz 2 Bundesdatenschutzgesetz. Dabei ist jede Einzelheit wichtig. So ist etwa ausdrücklich gesagt, dass das Geburtsjahr in einer solchen Liste enthalten sein darf. Der genaue Geburtstag wäre dagegen nicht erlaubt - und wird in der Praxis für Werbemaßnahmen auch nicht gebraucht.

Werbung bei "Bestandskunden"

Solange ein Unternehmen solche Listen von "Bestandskunden" benutzt, ist eine Einwilligung der Kunden nicht erforderlich. Diese Variante ist nämlich gesetzlich vorgesehen.

Angaben aus "allgemein zugänglichen Verzeichnissen"

Manchmal taucht in der Praxis das Problem auf, dass bestimmte Angaben fehlen. Beispielsweise ist zwar bekannt, in welchem Ort ein Kunde wohnt, es fehlen aber Straße und Hausnummer. Hier hilft eine Möglichkeit weiter, die ebenfalls im Gesetz vorgesehen ist. Das Gesetz erlaubt es nämlich, dass Daten aus allgemein zugänglichen Verzeichnissen (zum Beispiel aus Adressbüchern oder Telefonbüchern) erhoben werden. Auch dazu ist keine Einwilligung erforderlich.

Adresshandel - gesetzlich vorgesehen!

Großes Misstrauen löst es meistens aus, wenn ein Unternehmen nicht Daten verwendet, die es selbst vom Kunden bekommen hat, sondern aus dem "Adresshandel". Die gesetzlichen Regelungen hierzu sind recht kompliziert. Pauschal kann man aber sagen, dass Adresshandel im Prinzip erlaubt ist.

Nicht jede persönlich adressierte Werbung ist unzulässig!

Preisausschreiben und Gewinnspiele

Ein gängiger Weg, um an Adressen zu kommen, ist das Durchführen von Preisausschreiben oder Gewinnspielen. Solche Daten dürfen dann an Unternehmen verkauft werden, die damit Werbemaßnahmen durchführen wollen.

Das Verfahren der "Adressmittlung"

Schwieriger wird es, wenn ein Unternehmen Daten seiner Kunden einem anderen Unternehmen überlassen will, damit sie dazu benutzt werden können, Werbeschreiben zu verschicken. In der Praxis wurde dafür ein Verfahren entwickelt, das die Übermittlung der Daten von einem an das andere Unternehmen vermeidet: Weitergegeben werden dann nicht die Daten, sondern das Werbematerial, das verschickt werden soll. Der "Eigentümer" der Daten verwendet sie dazu, das Werbematerial des anderen Unternehmens zu verschicken.

Manchmal will er diesen Service nicht selbst anbieten. Dann wird ein neutraler Dritter eingeschaltet, der sogenannte Adressmittler. Er erhält vom einen Unternehmen die Adressdaten und vom anderen Unternehmen das Werbematerial. Dann führt er beides zusammen und verschickt die persönlich adressierten Schreiben.

Genaue Vorgaben für die Auftragsdatenverarbeitung

Auf den ersten Blick wundert man sich, warum die Einschaltung eines Dienstleisters etwas möglich macht, das sonst rechtlich nicht denkbar wäre. An das Unternehmen, das Werbung treiben will, dürften die Daten nämlich nicht übermittelt werden.

Des Rätsels Lösung: Der Dienstleister wird als Auftragnehmer des Unternehmens tätig, das über die Adressdaten verfügt. Und die Weitergabe von Daten in einem Auftragsverhältnis gilt rechtlich nicht als Datenübermittlung. Allerdings muss in einem schriftlichen Vertrag genau festgelegt sein, was der Auftragnehmer mit den Daten zu machen hat, und nach Durchführung des Auftrags muss er die Daten entweder wieder zurückgeben oder löschen.

Werbung kühl betrachten!

Macht man sich bewusst, welch wichtige Rolle Werbung im Wirtschaftsleben hat, und bedenkt man, dass keineswegs immer eine Einwilligung des Betroffenen erforderlich ist, sollte eine sachliche Betrachtung des Phänomens Werbung ohne Probleme möglich sein.

Nützliche App oder Handy-Spion?

Fast eine Milliarde Mini-Anwendungen wurden 2011 in Deutschland auf Smartphones geladen, darunter leider auch Apps, die den Nutzer heimlich ausspionieren. Erfahren Sie hier, wie Sie sichere und gefährliche Apps unterscheiden können.

Handy-Spaß für null Euro

Im mobilen Internet finden Sie Abertausende kostenloser Apps für Ihr Smartphone, die praktische Funktionen anbieten: von der mobilen Navigation über den virtuellen Einkaufszettel und den mobilen Terminkalender bis hin zum scheinbar lustigen Handy-Spielchen. Doch nicht jede App will nur spielen, manche beißen auch. So sind in den letzten Monaten immer wieder Apps entdeckt worden, die heimlich Nutzerdaten sammeln, etwa die Positionsdaten, also wo sich der Smartphone-Anwender aufgehalten hat.

Vorsicht: Sie zahlen vielleicht mit Ihren persönlichen Daten!

Nicht nur kostenlose Apps sind mit Vorsicht zu genießen. Auch Apps, die Sie kaufen, könnten mehr in sich tragen als die gewünschte Funktion. Wie aber lassen sich gefährliche Apps erkennen? An ihrem Namen leider nicht, ganz im Gegenteil. Oftmals werden bösartige Apps mit einem ganz ähnlichen Namen versehen, wie ihn beliebte und seriöse Apps tragen. Da viele Nutzer die Apps über die Suchfunktion des App-Marktplatzes finden, können ähnliche Bezeichnungen den Datendieben weitere ahnungslose Opfer liefern.

Sichere Marktplätze für Apps gibt es nicht

Wenn Sie sich in Sicherheit wähnen, weil Sie nur Apps für Ihr Smartphone oder Tablet nutzen, die auf offiziellen App-Marktplätzen wie dem iTunes App Store oder Android Market (seit kurzem Google Play genannt) zu finden sind, täuschen Sie sich leider. Auch Apps, die Apple geprüft und freigegeben hat oder die Google mit dem Prüfdienst Bouncer untersucht hat, entpuppten sich als schädliche Spionagesoftware oder als Betrugsmasche. Deshalb sollten Sie grundsätzlich Sicherheitsvorkehrungen treffen, wenn Sie eine neue App oder eine Aktualisierung für eine bereits installierte App nutzen möchten.

So prüfen Sie die Zuverlässigkeit einer App in fünf Schritten:

1. Achten Sie auf die Bewertungen und Kommentare anderer Nutzer, die auf den Marktplätzen zu jeder App veröffentlicht werden.

2. Sehen Sie sich bei Apps für Ihr Android-Smartphone auf dem Marktplatz genau an, welche Berechtigungen der App bei der Installation erteilt werden sollen (z.B. Zugriff auf Ihre Positionsdaten, Ihre E-Mails, Ihre SMS oder Ihr Telefonbuch).

3. Überlegen Sie, ob diese Berechtigungen wirklich für die Funktionen der App erforderlich sind. Wenn nicht: Finger weg!

4. Lesen Sie die Datenschutzerklärung und die Nutzungsbedingungen zu der App. Wenn es keine gibt, ist Vorsicht angesagt.

5. Nutzen Sie mobile Sicherheitssoftware auf Ihrem Smartphone, die es zu privaten Zwecken oftmals sogar kostenlos gibt.

Spezielle Prüffunktionen für Apps haben zum Beispiel die Anwendungen McAfee Mobile Security 2.0 und Lookout Premium App for Android.

Auch bei Apps gilt: Weniger ist mehr

Im Durchschnitt haben Smartphone-Nutzer in Deutschland 17 verschiedene Apps auf ihrem mobilen Endgerät. Wenn es bei Ihnen ähnlich aussieht, werden Sie bestimmt den Aufwand für die Prüfung der Apps scheuen, zumal bei jeder Aktualisierung einer App auch gefährliche Funktionen hinzukommen könnten.

Machen Sie deshalb mit beim App-Fasten: Installieren Sie nicht jede App, die sich interessant anhört und irgendeine witzige Funktion haben soll. Viele Apps sind nutzlos und verbrauchen nur Datenvolumen beim Herunterladen und auf dem Speicher Ihres Smartphones. Einige Apps sind sogar richtig gefährlich und stehlen Ihre Daten oder überwachen Sie heimlich.

Sparen Sie sich also Apps, die Sie nicht wirklich brauchen, dann ist die Kontrolle, wie sicher eine App ist, auch kein so großer Aufwand!

Nutzen Sie nur sichere Apps? Machen Sie den Test!

Frage: In einer Zeitschrift lesen Sie von einer kostenlosen App, mit der Sie tolle Rabattgutscheine abrufen können. Der Anbieter ist ein bekannter Markenhersteller. Installieren Sie die App?

a) Natürlich, wer will schon auf Rabatte verzichten.
b) Ja, denn die App kommt von einem seriösen Anbieter.
c) Kommt darauf an: Wenn mich die Rabatte interessieren, werde ich prüfen, ob die App auch sicher ist.

Lösung: Antwort c) ist richtig. Auch eine scheinbar lukrative App von einem bekannten Anbieter kann gefährlich sein. Zum Teil werden die Konten bekannter Anbieter auf App-Marktplätzen geknackt und die Apps verseucht.

Frage: Ein Kollege erzählt Ihnen von einer tollen App, die die perfekte Busverbindung zur Arbeitsstelle heraussuchen kann. Zu finden ist die App auf einem offiziellen App-Marktplatz wie Google Play. Was denken Sie?

a) Ganz gleich, wer eine App empfiehlt und wie nützlich sie erscheint - ich prüfe zuerst, ob die App auch sicher ist.
b) Auch die Apps von offiziellen App-Marktplätzen können heimlich Nutzerdaten stehlen.
c) Wenn mein Kollege gute Erfahrungen gemacht hat, habe ich keinen Grund zur Sorge. Natürlich will auch ich die App.

Lösung: Die Antworten a) und b) sind richtig. Ihr Kollege ist vielleicht von der Funktion begeistert; ob die App sicher ist, hat er wahrscheinlich noch gar nicht geprüft. Machen Sie es anders, auch bei Apps von offiziellen Marktplätzen. Gerade besonders interessante Apps könnten nämlich ein Lockangebot von Datendieben sein.