audatis.INFO
Newsletter für Datenschutz + Datensicherheit in kleinen und mittleren Unternehmen

Ausgabe 2 / 2012
bundesweit

Nützliche App oder doch ein 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

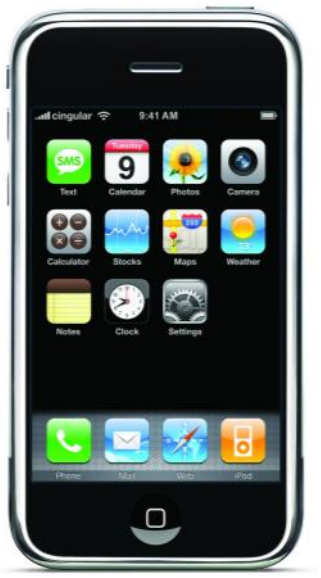
Im mobilen Internet finden Sie Abertausende kostenloser Apps für Ihr Smartphone, die praktische Funktionen anbieten: von der mobilen Navigation über den virtuellen Einkaufszettel und den mobilen Terminkalender bis hin zum scheinbar lustigen Handy-Spielchen. Doch nicht jede App will nur spielen, manche 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 Daten-dieben 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, ... (*Fortsetzung auf Seite 3*)



Schwerpunkt dieser Ausgabe: Die Sicherheit Ihrer mobilen Apps!
Mit Test auf Seite 3.

IN DIESEM NEWSLETTER

IM NÄCHSTEN NEWSLETTER

Sicherheit + Cloud Computing
Veranstaltungen 2012 / 3
Aktuelle Themen
Datensicherung: wann und wie?

audatis
Datenschutz und Informationssicherheit | NEWSLETTER

Persönlich adressierte Werbung 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.

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 für Werbung notwendig! Der Gesetzgeber hat hier verschiedene Ausnahmen vorgesehen.”

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 und Geburtsjahr.

Geregelt ist dies in § 28 Absatz 3 Satz 2 BDSG. 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 Telefon-büchern) erhoben werden. Auch dazu ist keine Einwilligung erforderlich.

Gewinnspiele zum Locken

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.

Adresshandel und -mittlung

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 Unter-nehmens 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 Auftrags-verhältnis gilt rechtlich nicht als Daten-übermittlung. 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. (WN)

Fortsetzung von Seite 1

Nützliche App oder doch Spion?

… 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, avast! Free Mobile Security 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! (WN)

Links zu einigen kostenlosen Sicherheitslösungen für Ihr Smartphone:

avast! Free Mobile Security:

http://ds-its.eu/avast

AVG Mobilation für Android:

http://ds-its.eu/avg

Lookout Mobile Security:

http://ds-its.eu/lookout

Nutzen Sie nur sichere Apps? Jetzt testen!

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.

Datenschutz-schulung für Ihre Mitarbeiter

Datenschutz kann als Wettbewerbs- und Marketingvorteil genutzt werden, um das Vertrauen von Kunden und Geschäftspartnern zu gewinnen. Vorausgesetzt es beteiligen sich alle Mitarbeiter und Führungskräfte.

Für viele Datenschutzbeauftragte ist die Motivierung der Mitarbeiter zur Umsetzung der Datenschutzvorschriften eine Sisyphos-Aufgabe und wird als Arbeitsbehinderung, etc. abgetan. Noch schlimmer ist die Situation, wenn sogar die Führungskräfte nicht von der Notwendigkeit des Datenschutzes und der entsprechenden Einhaltung im Unternehmen überzeugt sind dann fehlt den Mitarbeitern das Vorbild und sie werden sich erst recht nicht an die Datenschutzanforderungen halten.

audatis Training hat die Probleme der Datenschutzbeauftragten, aber auch die Argumente der Mitarbeiter und Manager, analysiert und daraus ein Datenschutz-Schulungskonzept zur Sensibilisierung von Mitarbeitern im Unternehmen entwickelt (Datenschutz-Awareness). Dieses enthält:

- Abstimmung der Inhalte mit dem betrieblichen DSB
- Auswahl der Zielgruppen
- Erstellung der Schulungsunterlagen (PDF + PPT)
- Schulung durch unsere Referenten bei Ihnen vor Ort (pro Gruppe ca. 1,5 Std.)
- Integration von Live-Hackings und Beispielen aus Betrieb und Privatleben

Bei Interesse oder Fragen: training@audatis.de

Veranstaltungen und Seminare zu Datenschutz und Datensicherheit von Mai bis Juli 2012

Im **Bereich Datenschutz** finden folgende Veranstaltungen zwischen **Mai und Juli 2012** statt:

14.05. - 15.05. **Seminar: Datenschutzassistent mit TÜV-Zertifikat (W)** 09:00 - 17:00 in Köln [**dsastuv**]

21.05. **Workshop: Datenschutz für Unternehmer und Freiberufler (W)** 16:30 - 20:00 in Herford [**dswuf**]

18.06. - 19.06. **DuD 2012: Fachkonferenz Datenschutz + Datensicherheit (F)** 09:00 - 17:00 in Berlin [**dud2012**]

19.06. **Seminar: Erstellen und Pflegen des Verfahrensverzeichnisses (W)** 09:00 - 17:00 in München [**dsvztuv**]

28.06. **Workshop: Datenschutz für Unternehmer und Freiberufler (W)** 16:30 - 20:00 in Bielefeld [**dswuf**]

29.06. **Seminar: Datenschutz für IT-Leiter und IT-Experten (W)** 09:00 - 17:00 in Bielefeld [**dsitl**]

Für die Sparte **Datensicherheit** konnten wir folgende Veranstaltungen für Sie zwischen **Mai und Juli 2012** finden:

11.06. - 15.06. **Seminar: IT-Security-Beauftragter mit TÜV-Zertifikat (W)** 09:00 - 17:00 in Berlin-Spandau [**isbtuv**]

21.06. - 22.06. **Seminar: IT-Sicherheit für Datenschutzbeauftragte (W)** 09:00 - 17:00 in Bielefeld [**isitsds**]

26.06. - 27.06. **Seminar: IT-Sicherheit für Datenschutzbeauftragte (W)** 09:00 - 17:00 in Frankfurt am Main [**isitsds**]

03.07. **Seminar: Professioneller Umgang mit Datenpannen (W)** 09:00 - 17:00 in München [**isdptuv**]

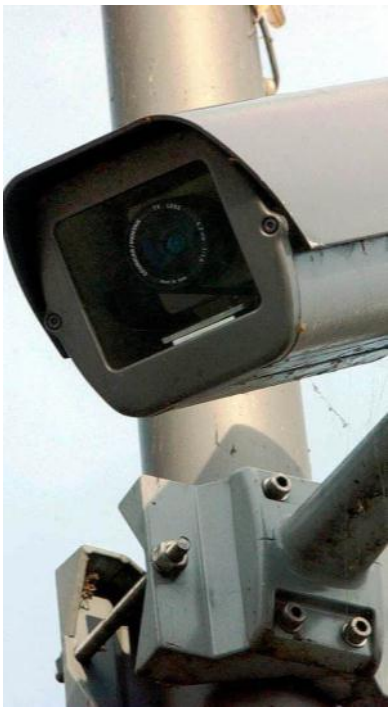
10.07. - 11.07. **Seminar: IT-Sicherheit für Datenschutzbeauftragte (W)** 09:00 - 17:00 in Bremen [**isitsds**]

17.07. - 18.07. **Seminar: IT-Sicherheit für Datenschutzbeauftragte (W)** 09:00 - 17:00 in Dresden [**isitsds**]

(F) = Fachtagung / Forum
(O) = Online / Webinar
(W) = Weiterbildung / Seminar

Sie finden **weitere Informationen** zu den Veranstaltungen und die Veranstalter über folgenden Shortlink: **http://ds-its.eu/CODE** dabei ersetzen Sie den CODE durch den entsprechenden Wert in [eckigen Klammern], welcher unter jedem Veranstaltungshinweis steht.

Videoüberwachung im Betrieb



Durch die geringen Kosten wird Videoüberwachung in immer mehr Unternehmen als Mittel zur Abschreckung und zum Nachweis von Straftaten eingesetzt. Doch der Einsatz solcher Videotechnik sollte gründlich geplant werden, um Datenschutzverstöße zu vermeiden.

Die Videoüberwachung ist als Mittel zur Verhinderung oder Aufklärung von Sach-, Personen- oder Vermögensschäden sehr beliebt. Allerdings müssen auch die Rechte auf informationelle Selbstbestimmung von Mitarbeitern oder unbeteiligten Dritten (z.B. Passanten oder Kunden) berücksichtigt werden.

Datenschutzrecht beachten

Aus datenschutzrechtlicher Sicht ist die Videoüberwachung grundsätzlich unzulässig, sofern nicht

a) eine Einwilligung des/der Betroffenen vorliegt oder

b) eine gesetzliche Norm diese rechtfertigt.

Hier ist die Art der Videoüberwachung entscheidend, um zu klären welche rechtliche Norm hierfür zuständig ist.

- Videos vom Außengelände (sofern öffentlich zugänglich) werden in §6b BDSG geregelt.
- Werden Aufzeichnungen oder Live-Überwachungen innerhalb der Betriebsgebäude durchgeführt können teilweise die §28 bzw. 32 BDSG im Rahmen einer Interessensabwägung herangezogen werden.

Weiterhin sollte berücksichtigt werden, dass eine Videoüberwachung auch mitbestimmungspflichtig ist und ein evtl. vorhandener Betriebsrat nach §87 BVerfG beteiligt werden muss.

Die Überwachung von Sozialräumen ist im Normalfall nicht gestattet.

Das Filmen der Mitarbeiter am Arbeitsplatz benötigt eine entsprechend stichhaltige Rechtfertigung (z.B. konkreter Verdacht auf eine Straftat) und muss sich weiteren Rechtsnormen unterwerfen.

Im Regelfall lassen sich nach §§4, 4a BDSG die Einwilligung der Betroffenen bzw. stellvertretend eine Betriebsvereinbarung einholen, allerdings dürfen dadurch keine Persönlichkeitsrechte verletzt werden.

Bedenken Sie auch die allgemeinen Vorschriften des BDSG, die ebenfalls für eine Videoüberwachung gelten:

Datensparsamkeit nach §3a BDSG: Sofern die Daten ihren Zweck erfüllt haben, müssen sie gelöscht werden. Eine grundlos unbefristete Aufbewahrung von Videoaufzeichnungen ist also nicht statthaft. Je nach Zweck kann eine Aufzeichnung länger als 24h unzulässig sein. Dies muss jedoch im Einzelfall geklärt werden.

Vorabkontrollen nach §4d Abs. 5 BDSG sind vor Beginn der Videoüberwachung im Regelfall durch den Datenschutzbeauftragten durchzuführen.

Im Strafgesetzbuch sollte man sich mit §201 und §201a vertraut machen, die eine unberechtigte Ton- und Bildaufzeichnung unter Strafe stellen. Im Regelfall wird eine Videoüberwachung ihren Zweck auch ohne Ton erfüllen. Hier gilt es im Vorfeld die Technik zu prüfen, damit nicht unfreiwillig eine Tonaufzeichnung durchgeführt wird, die nur mangels Lautsprecher am Überwachungsstand nicht entdeckt wird.

Evtl. besteht auch die Verpflichtung zur Benachrichtigung der Betroffenen nach §33 BDSG, wenn diese im Rahmen der Videoüberwachung identifiziert werden können. (CR)

Mit unserer Checkliste können Sie die wichtigsten Fragen abarbeiten und entsprechend dokumentieren:

http://ds-its.eu/chkvideo

“Bis zu 99% aller Videoüberwachungen verstoßen laut Niedersachsens Landesbeauftragtem für Datenschutz gegen das Datenschutzrecht.”

Unsere Online-Services für Sie

Sie setzen ein **Webanalyse-Tool** auf Ihrer Webseite ein? Dann sollte es Sie interessieren, ob dieses auch datenschutzkonform genutzt wird bzw. werden kann. Testen Sie selbst:

http://ds-its.eu/wac

Wie ist es um das Datenschutzniveau in Ihrem Unternehmen bestellt? Halten Sie die wichtigsten Vorgaben ein? Oder gibt es noch wesentliche Baustellen? Der **Datenschutz-Schnelltest** für Unternehmen liefert die Antworten in wenigen Minuten online und als PDF zum Ausdrucken:

http://ds-its.eu/dst

Neuer Ratgeber und Lexikon

Ab sofort bieten wir auf unseren Webseiten unter der Rubrik „**Ratgeber**“ einige kostenlose Informationsangebote für die berufliche und private Beschäftigung mit dem Datenschutz und der Datensicherheit an.

In unserem „**Business Ratgeber**“ finden Sie Checklisten und Dokumente, die Ihnen den Arbeitsalltag erleichtern sollen. Neben Aufbewahrungsfristen stehen Prüflisten für den Einsatz von Videoüberwachung oder die Auswahl technischer und organisatorischer Maßnahmen gem. §9 BDSG zur Verfügung.

Unter „**Home & Family**“ bekommen Sie Anleitungen zum Einsatz von Passwortsafes oder Videoerklärungen zu Themen des Datenschutzes und Ihrer Rechte als Betroffener. Außerdem haben wir Empfehlungen zu Sicherheitsprodukten wie Antiviren-Software, Firewalls oder Smartphone-Sicherheitslösungen und Verschlüsselungsprodukten zusammengetragen. Diese können häufig auch in kleinen Unternehmen oder von Freiberuflern genutzt werden und bieten entsprechende Anhaltspunkte zur Auswahl von Datensicherheitsprodukten.

Im Bereich „**Lexikon**“ finden Sie zahlreiche Begriffe aus dem Umfeld von Datenschutz und Datensicherheit erklärt. Diese Rubrik wird nach und nach erweitert und enthält auch Erklärungen per Video, um die Sachverhalte leicht verständlich darzubieten.

Die Videos von audatis können auch von Unternehmen genutzt werden. (KH)
http://ds-its.eu/rat

Hat Ihnen unser Newsletter gefallen?

Dann empfehlen Sie diesen doch gerne weiter:

www.audatis.de/online/newsletter

Die nächste Ausgabe dürfen Sie in Q3 / 2012 erwarten.

Impressum

audatis - Datenschutz und Informationssicherheit
Consulting | Training | Services
Inh. Carsten Ripper

Hauptsitz / Büro Ostwestfalen:

Dreyener Str. 20
32130 Enger

Büro Rhein-Main-Neckar:

Wehrstr. 30
69488 Birkenau

Redaktion:

V.i.S.d.P. Carsten Ripper (CR)
Kerstin Hilß (KH)

Erscheinungsweise: 4 x jährlich

Kontaktmöglichkeiten

So können Sie uns zu allen Fragen oder Anregungen erreichen:

Telefon: (05224) 999 260 - 90
Telefax: (05224) 999 260 - 99

E-Mail: info@audatis.de (allgemein)
E-Mail: newsletter@audatis.de (Newsletter-Redaktion)

Internet: www.audatis.de
Facebook: www.facebook.com/audatis
Twitter: twitter.com/audatis