Newsletter Datenschutz
Ausgabe 06 | 2014

agentia wirtschaftsdienst

Newsletter Datenschutz

Die Kundenzeitung der agentia wirtschaftsdienst

Liebe Leserin, lieber Leser,

darf der Online-Dienst Google Maps für die betriebliche Reisekostenabrechnung genutzt werden? Die Antwort auf diese Frage finden Sie in dieser Ausgabe. Sie mag ebenso überraschen wie das Gerichtsurteil zum Einscannen von Personalausweisen.

Doch nicht nur in der Rechtsprechung gibt es Unerwartetes. Auch die Vielfalt der Datenrisiken bei Smartphones ist vielen Nutzern noch unbekannt. Für die richtige Wahl der mobilen Sicherheitslösung aber müssen Sie wissen, wovor Sie Ihre Daten schützen müssen. Wenn es aber einmal zum Ernstfall kommt, zum Diebstahl Ihrer Passwörter, sollten Sie umgehend und richtig handeln können. In dieser Ausgabe erhalten Sie deshalb eine Anleitung, was bei Identitätsdiebstahl unbedingt zu tun ist. Dann sind Sie auch auf böse Überraschungen vorbereitet.

Wir wünschen Ihnen eine spannende Lektüre,

Ihre Datenschutzbeauftragten der agentia wirtschaftsdienst

Reisekostenabrechnung mit Google Maps - rechtlich kein Problem!

Google Maps ist eine praktische Sache. Oft nutzen Unternehmen es, um Abrechnungen von Dienstreisen durchzuführen oder um solche Abrechnungen zu überprüfen. Liegt darin eine technische Überwachung, die besondere rechtliche Vorkehrungen verlangt und zum Beispiel ein Mitbestimmungsrecht des Betriebsrats auslöst? Das Bundesarbeitsgericht hat dies verneint und damit grünes Licht für die Verwendung von Google Maps gegeben.

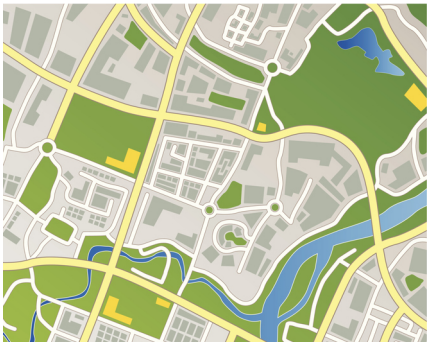
Routenvorschläge des Systems - mehr nicht!

Wie Google Maps funktioniert, ist rasch erklärt: Es handelt sich um einen Routenplaner, bei dem man eingibt, von wo nach wo man fahren möchte. Dann schlägt das System im Normalfall mehrere Routen vor. Von der Entfernung her sind sie meist unterschiedlich lang, wobei nicht selten eine kilometermäßig längere Strecke die zeitlich kürzere ist. Was ihm wichtiger ist, die Zeitersparnis oder die Kürze der Strecke, muss jeder Nutzer des Systems selbst beantworten - diese Entscheidung nimmt Google Maps ihm nicht ab.

Der Mensch entscheidet, nicht Google Maps

Dieser Punkt ist aus Sicht des Bundesarbeitsgerichts entscheidend für die Beantwortung der Frage, ob die Verwendung von Google Maps in einem Unternehmen als Einsatz einer technischen Überwachungseinrichtung anzusehen ist. Das Gericht verneint diese Frage und hebt dabei vor allem Folgendes hervor:

- Anders als etwa ein GPS-System ermittelt Google Maps nicht, welche Wegstrecke bei einer konkreten Fahrt tatsächlich zurückgelegt worden ist. Deshalb speichert das System auch keine Informationen über das Fahrverhalten bei einer konkreten Fahrt.



Der Einsatz von Google Maps für Abrechungszwecke ist in Unternehmen nicht mitbestimmungspflichtig (Bild: Thinkstock/Jorgenmac)

- Das System macht lediglich Routenvorschläge unter den Aspekten "Entfernung" und "Fahrzeit", trifft jedoch keine Festlegung, welche Route gewählt werden muss.

- Bei der Abrechnung von Dienstreisen ist es lediglich ein Hilfsmittel für die Beteiligten. Wenn etwa ein Unternehmen festlegt, dass nur die Kosten für die kürzeste Fahrtstrecke erstattet werden, dann ändert die Verwendung von Google Maps für die Durchführung der Abrechnung nichts an dieser Regelung.

- Das System selbst hat keinen Einfluss darauf, was ein Sachbearbeiter mit den Informationen tut, die er durch das System gewinnt.

Google Maps ist daher keine technische Überwachungseinrichtung

Im Ergebnis ist Google Maps deshalb nach Auffassung des Gerichts nicht als technische Überwachungseinrichtung anzusehen. Das hat unter anderem zur Folge, dass kein Mitbestimmungsrecht des Betriebsrats besteht.

Eine andere Frage: Stimmt wirklich alles?

Ob die Berechnungen, die das System durchführt, immer zutreffen, war allerdings nicht Gegenstand des Verfahrens. Wer hieran einmal Zweifel hat, sollte die Ergebnisse beispielsweise durch Notieren des Kilometerstands am Tachozähler überprüfen und Abweichungen reklamieren.

Das Scannen von Personalausweisen ist ausnahmslos verboten!

Wenn der Betroffene damit einverstanden ist, darf man mit seinen Daten (nahezu) alles machen - so glauben viele. Dass dies für Personalausweise nicht gilt, hat das Verwaltungsgericht Hannover kürzlich entschieden. Es hat nämlich das Scannen von Personalausweisen generell und ohne Ausnahme untersagt - sogar für den Fall, dass der Betroffene damit einverstanden ist. Ein Sieg für den Datenschutz? Lesen Sie, warum man darüber durchaus geteilter Meinung sein kann!

Auslieferungsvorgänge bei einem Logistikdienstleister

Ein Logistikdienstleister muss täglich Hunderte von Fahrzeugen ausliefern. Dabei werden die Fahrzeuge in der Regel durch Fahrer von Speditionen abgeholt. Um einen Nachweis dafür zu haben, wer als Abholer da war, und auch, um Betrügereien zu verhindern, scannte der Dienstleister die Personalausweise der Abholer ein und speicherte die Scans auf einem Rechner. Nach Abschluss des Vorgangs (etwa durch Bezahlen der Rechnung für das Fahrzeug) wurden die Scans binnen weniger Tage wieder gelöscht.

Untersagungsanordnung der Datenschutzaufsicht

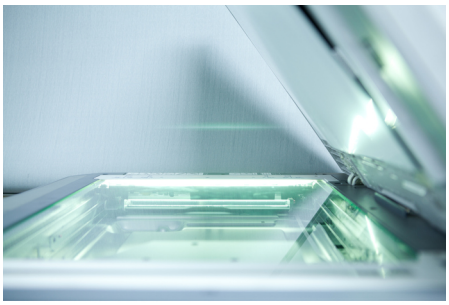
Die zuständige Datenschutzaufsichtsbehörde war mit diesem Vorgehen überhaupt nicht einverstanden. Sie vertrat die Auffassung, dass es gegen die Vorschriften des Personalausweisgesetzes verstößt, und ordnete gegenüber dem Dienstleister an, dass er das Einscannen von Personalausweisen künftig unterlassen muss. Das sah der Dienstleister nicht ein und klagte gegen diese Anordnung vor dem Verwaltungsgericht Hannover.

Erfolglose Klage gegen die Anordnung

Das Gericht wies seine Klage allerdings zurück. Nach Meinung des Gerichts trifft die Auffassung der Datenschutzaufsicht zu: Personalausweise dürfen nicht eingescannt werden, und zwar nicht einmal dann, wenn der Betroffene damit einverstanden ist.

Enge Vorgaben des Personalausweisgesetzes

Das Gericht begründet dies mit der Vorgabe des § 20 Absatz 2 Personalausweisgesetz. Demnach darf der Personalausweis - von wenigen Ausnahmefällen etwa im Polizeibereich abgesehen - weder zum automatisierten Abruf personenbezogener Daten noch zur automatisierten Speicherung personenbezogener Daten verwendet werden. Wenn ein Personalausweis eingescannt wird, dann erfolgt jedoch gerade die automatisierte Speicherung der personenbezogenen Daten, die im Ausweis enthalten sind. Somit ist das Scannen von Personalausweisen unzulässig.



Wer kennt das nicht: Spätestens beim Abschluss eines Mobilfunkvertrags war es bisher üblich, dass der Personalausweis eingescannt wurde. Das ist nach einem neuen Urteil nun nicht mehr zulässig. *(Bild: Thinkstock/dingming zhang)*

Bewusstes Scan-Verbot durch den Gesetzgeber

Dies war die ausdrückliche Absicht des Gesetzgebers. Die Gesetzesbegründung besagt nämlich ausdrücklich, dass Verfahren wie das Scannen von Ausweisdaten ausgeschlossen sein sollen. Das sollte verhindern, dass die eingescannten Daten auf elektronischem Weg weitergegeben und für Zwecke genutzt werden können, die das Gesetz nicht vorsieht.

Eine Einwilligung des Betroffenen ist nicht möglich

Die naheliegende Überlegung, dass es dem Ausweisinhaber möglich sein müsste, seine Einwilligung zum Einscannen zu erteilen, weist das Gericht zurück. Eine solche Möglichkeit sehe das Personalausweisgesetz gerade nicht vor. Darin unterscheide sich dieses spezielle Gesetz von den allgemeinen Regelungen des Bundesdatenschutzgesetzes, in denen die Einwilligung des Betroffenen als Rechtfertigung für einen bestimmten Umgang mit personenbezogenen Daten ausdrücklich vorgesehen ist (siehe dort § 4 und § 4a).

Möglich bleiben schwerfällige Alternativen

Als Ausweg in solchen Situationen ist nach Meinung des Gerichts folgender Weg möglich:

1. Der Ausweisinhaber legt seinen Ausweis zur Einsichtnahme vor.

2. Der Dienstleister notiert sich die Daten, die zur Identifikation des Ausweisinhabers erforderlich sind.

Ob dieser Ansatz den Bedürfnissen der Praxis gerecht wird, darf man durchaus bezweifeln. Ein solches Vorgehen verursacht nicht nur einen erheblichen Zeitaufwand. Vielmehr besteht dabei auch immer das Risiko, dass Daten fehlerhaft notiert werden.

Zudem enthalten solche Notizen anders als ein Scan kein Bild des Ausweisinhabers, was eine spätere Identifikation enorm erschwert. Außerdem ist seitens eines Betroffenen stets die Behauptung möglich, er jedenfalls sei nicht vor Ort gewesen und habe auch keinen Ausweis vorgelegt. Woher die angeblich über ihn notierten Daten stammen würden, sei ihm völlig unklar.

Übereifer des Gesetzgebers?

Im Ergebnis spricht vieles dafür, dass der Gesetzgeber mit der geschilderten Regelung über das Ziel hinausgeschossen ist. Solange das Gesetz nicht geändert wird, müssen Unternehmen wie Bürger allerdings damit leben, dass Personalausweise eben nicht eingescannt werden dürfen. Dass sich damit manche Abläufe verkomplizieren, ist nicht zu ändern.

Impressum

agentia wirtschaftsdienst
dipl.-inform. udo wenzel
budapester straße 31
10787 berlin

tel.: 030 2196 4390
fax: 030 2196 4393

udo.wenzel@agentia.de
thorsten.ritter@agentia.de

Smartphone-Risiken: Trojaner sind nicht alles

Smartphones und Tablets gehören inzwischen zu den Hauptangriffszielen der Datendiebe. Ein mobiler Virenschutz allein reicht nicht zur Abwehr. Alle mobilen Bedrohungen müssen bei der Wahl der Sicherheitslösung bedacht werden.

Smartphones sollten nicht nur mit einerm Virenschutz versehen sein, sondern auch passende Sicherheits-Apps nutzen, um umfassende Sicherheit zu gewährleisten
(Bild: Thinkstock/leszekglasner)

Smartphones im Fadenkreuz

Sicherheitsbehörden wie das Bundesamt für Sicherheit in der Informationstechnik (BSI), Datenschützer und Sicherheitsforscher sind sich einig: Mobile Endgeräte wie Smartphones und Tablets gehören zu den bedrohten Arten, wenn es um IT-Risiken geht. Die Zahl der Schadprogramme, die speziell für Smartphones, allen voran für Android-Smartphones, entwickelt werden, hat in den letzten Monaten drastisch zugenommen.

Warum sind Smartphones solch beliebte Angriffsziele?

Für diese besondere Gefährdung mobiler Endgeräte gibt es Gründe:

1. Einerseits ist die Zahl der Smartphone-Nutzer massiv angewachsen, gleichzeitig werden die mobilen Internetverbindungen immer preiswerter.

2. Andererseits sind die Smartphones weiterhin deutlich schlechter geschützt als die PCs und Notebooks, sodass die mobilen Internetverbindungen zu idealen Einfallstoren für Hacker werden.

3. Als weiterer Punkt kommt hinzu, dass Smartphones eine Vielzahl an Daten vorhalten oder zugänglich machen, die Datendiebe auf den Plan rufen.

Wo der Virenschutz nicht helfen kann

Auf Seiten der IT-Sicherheitslösungen ist natürlich auch viel passiert: Es gibt zahlreiche Lösungen - Security-Apps -, die mobile Endgeräte nach Viren und Trojanern durchsuchen. Eine Sicherheitslösung, die sich allein auf das Trojaner- und Virenrisiko beschränkt, greift allerdings viel zu kurz. Es gibt eine ganze Reihe mobiler Datenrisiken, die nichts mit einem Trojaner zu tun haben, aber trotzdem die personenbezogenen Daten auf den Smartphones gefährden.

Ein Beispiel sind Smartphone-Apps, die keine direkt schädliche Funktion in sich tragen, wie dies klassische Schadsoftware tut. Vielmehr sind diese Apps viel zu neugierig und sammeln Nutzerdaten, die sie für ihre Funktion gar nicht brauchen und die der Nutzer auch nicht preisgeben will. Hier sind insbesondere die aktuellen Standortdaten des Nutzers zu nennen. Eine Vielzahl von Apps sammelt diese Standortdaten und speichert Bewegungsprofile, ohne Zustimmung und Wissen des Nutzers.

Vielfältige Risiken bedingen umfassende Gegenmaßnahmen

Zu den Risiken, denen ein mobiler Virenschutz nicht beikommen kann, gehören insbesondere

- der Geräteverlust mit gleichzeitigem Datenverlust,

- die Geräterückgabe mit darauf verbleibenden, ungeschützten Restdaten,

- die Vermischung privater und geschäftlicher Daten,

- Phishing-Attacken über mobile Nachrichten und

- die Nutzung ungeschützter WLAN-Hotspots, die Lauschangriffe auf die Internetverbindungen möglich macht.

IT-Sicherheitslösungen für Smartphones und Tablets sollten diese Risiken möglichst vollständig abdecken. Fehlende Sicherheitsfunktionen zur Risikoabwehr sollten sich über Zusatzmodule leicht ergänzen lassen. Dazu aber müssen die Nutzer wissen, dass die mobile Sicherheitslösung nicht vollständig ist.

Welche mobilen Schutzfunktionen nicht fehlen dürfen

Der Vielfalt der mobilen Risiken kann ein Nutzer nur begegnen, wenn auf Smartphones unter anderem Sicherheitsscanner installiert sind, die nicht nur nach schädlichen Apps oder Dateien suchen, sondern auch nach unerlaubten Datenzugriffen. Benötigt wird zudem eine Funktion zur Fernlöschung der Daten im Fall des Geräteverlusts oder Diebstahls. Der interne Speicher des Smartphones und die Speichererweiterung mittels Speicherkarten müssen mit einer mobilen Verschlüsselung geschützt werden können.

SMS-Filter, Trennung von privater und betrieblicher Nutzung

Da Spam nicht nur als E-Mail auf Smartphones gelangen kann, werden auch sogenannte SMS-Filter benötigt. Wird ein und dasselbe Smartphone sowohl zu betrieblichen als auch zu privaten Zwecken genutzt, darf die strikte Trennung betrieblicher sowie privater Apps und Daten nicht fehlen.

Privates Smartphone nicht vergessen

Da der Datenschutz nicht nur am Arbeitsplatz, sondern auch im Privatleben eine zentrale Rolle spielen muss, sollten Sie sich Ihr privates Smartphone einmal genau ansehen, auch dann, wenn Sie es nicht betrieblich einsetzen. Es gibt für Privatpersonen verschiedene Security-Apps, die kostenlos sind, aber umfangreiche Schutzfunktionen bieten.

Informieren Sie sich über aktuelle Tests

Geben Sie sich nicht mit einem reinen Virenschutz auf Ihrem Smartphone oder Tablet zufrieden, sondern nutzen Sie eine Lösung, die wirklich mobile Datensicherheit anbietet und nicht nur die mobile Sicherheit im Namen trägt. Am besten nutzen Sie bei der Auswahl Ihrer mobilen Sicherheitslösung die aktuellen Tests von Institutionen wie der Stiftung Warentest oder die Ergebnisse anderer Verbraucherschutzorganisationen.

Was Sie tun müssen, wenn Ihre Online-Identität gestohlen wurde

Erst 16 Millionen gehackte E-Mail-Konten, dann weitere 18 Millionen: Das Bundesamt für Sicherheit in der Informationstechnik (BSI) warnt vor massenhaftem Identitätsdiebstahl im Internet. Doch was muss man als Opfer tun?

Es geht nicht "nur" um E-Mails

Bei der Analyse krimineller Aktivitäten im Internet haben Forschungseinrichtungen und Strafverfolgungsbehörden rund 16 Millionen Datensätze zu gehackten E-Mail-Konten entdeckt. Und dieser Datendiebstahl ist kein Einzelfall: Bereits im April 2014 meldete das BSI, dass Internetkriminelle weitere 18 Millionen E-Mail-Zugänge gekapert haben, darunter drei Millionen allein aus Deutschland.

So schlimm die Vorstellung ist, dass Hacker die E-Mails der Opfer ausspähen konnten, es kommt noch schlimmer: Obwohl davon immer wieder abgeraten wird, verwenden viele Internetnutzer ihre E-Mail-Zugangsdaten auch für weitere Online-Dienste wie zum Beispiel für soziale Netzwerke.

Die eigene Identität im Internet wird gestohlen

Was es bedeutet, wenn die eigenen Zugangsdaten gestohlen werden, wird bei sozialen Netzwerken wie Facebook besonders gut sichtbar: Der Datendieb erhält Zugang zum Online-Profil des Opfers und kann es manipulieren und missbrauchen. Der Internetkriminelle kann die Identität des Opfers übernehmen und in dessen Namen aktiv sein.

Anzeichen für einen Identitätsdiebstahl

Die typischen Anzeichen für einen Identitätsdiebstahl sind die folgenden:

- glaubhafte und nachprüfbare Hinweise, dass Spam-Mails, Spam-SMS, unerwünschte Briefe/Fax-Sendungen oder Anrufe mit dem eigenen Namen als Absender/Anrufer aufgetreten sind

- angebliche Online-Profile in sozialen Netzwerken, die man nie selbst angelegt hat

- falsche Buchungen im Bank-/Kreditkartenkonto

- Gebühren für Online-Dienste oder Mobilfunk-Dienste, die man nicht selbst verursacht hat (Beispiel: kostenpflichtige Downloads, kostspielige SMS)

Jeder braucht ein Notfallprogramm

Natürlich ist es das erste Ziel, dass es gar nicht zu einem solchen Identitätsdiebstahl kommt. Die Wahl komplexer, starker Passwörter gehört wie alle anderen Passwortrichtlinien zur Abwehr solcher Angriffe. Doch nicht immer haben Sie es in der Hand, Ihre Zugangsdaten zu schützen. Mitunter werden Ihre Passwörter beim Provider nicht ausreichend geschützt, und Ihre Daten werden von den Servern des Anbieters gestohlen.

Deshalb brauchen auch Internetnutzer ein Notfallprogramm für den Fall eines Identitätsdiebstahls, die den Selbstdatenschutz sehr ernst nehmen. Man kann sogar sagen: Das Notfallprogramm gehört dazu.

Sofortmaßnahmen: Rechner scannen, neue Passwörter

Wenn Sie Opfer eines Identitätsdiebstahls im Internet werden sollten, müssen Sie in Absprache mit Ihrer Systemadministration folgende Schritte ergreifen:

1) Zuerst müssen alle von Ihnen genutzten Rechner, ob Desktop, Notebook, Tablet oder Smartphone, mit einem aktuellen, professionellen Anti-Viren-Programm durchsucht werden, ob sich Schadprogramme darauf befinden.

2) Dann gilt es, alle Passwörter, die Sie nutzen, zu ändern, für Ihr E-Mail-Programm und für alle Online-Dienste wie zum Beispiel die sozialen Netzwerke.

3) Wenn Sie bestimmte Passwörter nicht selbst ändern können, informieren Sie sofort den Betreiber des betreffenden Dienstes.

4) Warnen Sie Ihre ggf. betroffenen Kontakte, soweit möglich, auf einem zweiten Kommunikationsweg, also zum Beispiel per Telefon.

5) Überprüfen Sie die Sicherheits- und Datenschutzeinstellungen der von Ihnen genutzten Online-Dienste.

Wissen Sie, was bei Identitätsdiebstahl zu tun ist?

Frage: Sie bekommen eine E-Mail, die besagt, dass Ihr E-Mail-Passwort gestohlen wurde. Was tun Sie?

a) Ich klicke auf den Link in der E-Mail, um sofort mein Passwort zu ändern.
b) Ich bin vorsichtig und klicke nicht auf den Link, denn die Warnung könnte auch ein Angriffsversuch sein.

Lösung: Die Antwort b) ist richtig. Prüfen Sie immer zuerst, ob der Hinweis auf einen Identitätsdiebstahl von einer glaubhaften Stelle kommt. Klicken Sie nie auf Links in solchen Mails, denn oftmals startet damit der echte Passwortdiebstahl.

Frage: Sie werden von vertrauenswürdiger Seite über einen Identitätsdiebstahl informiert. Was muss nun geschehen?

a) Zuerst prüfe ich den Rechner, den ich zuletzt genutzt habe, ob sich darauf Malware befindet.
b) Als ersten Schritt nutze ich einen zuverlässigen Malware-Scanner für alle Geräte, die ich nutze.

Lösung: Die Antwort b) ist erneut richtig. Sie müssen alle Geräte auf Verseuchung untersuchen lassen, denn der Datendiebstahl kann über jedes von Ihnen genutzte Gerät erfolgt sein. Oftmals liegt sogar eine längere Zeit zwischen dem Hinweis auf Identitätsdiebstahl und der Attacke, weshalb der zuletzt genutzte Rechner bei der Malware-Suche nicht ausreicht.