Infobrief Datenschutz
Ausgabe 04 | 2013

agentia wirtschaftsdienst

Newsletter Datenschutz

Die Kundenzeitung der agentia wirtschaftsdienst

Liebe Leserin, lieber Leser,

ob auf der kleinen Vereinsfeier oder auf der großen politischen Bühne in der EU: Der Datenschutz spielt in weitaus mehr Bereichen eine Rolle, als man glaubt. Das zeigen die ersten beiden Beiträge. Der erste Artikel erklärt Ihnen, worauf Sie beim Fotografieren während einer Vereinsveranstaltung achten sollten, der zweite macht Sie mit den Aufgaben des Europäischen Datenschutzbeauftragten vertraut.

Wie Sie persönlich mithelfen können, Hackerangriffe abzuwehren, das erfahren Sie im dritten Beitrag dieser Ausgabe. Versäumen Sie nicht, den Selbsttest auf der letzten Seite zu machen, wenn Sie wissen wollen, wie man Ihren aktuellen Aufenthaltsort über das Internet feststellen kann. Tipps gegen die heimliche Ortung im Netz liefert Ihnen der vierte Artikel.

Interessante Einblicke in den modernen Datenschutz wünschen Ihnen

Ihre *Datenschutzbeauftragten der agentia wirtschaftsdienst*

Fotos bei Vereinsveranstaltungen - was ist zu beachten?

Ein Bild sagt mehr als 1.000 Worte! Das ist sicher richtig, und deshalb wird gerade bei Vereinsveranstaltungen munter drauflosfotografiert. Schön, wenn alle ihre Freude dabei haben. Nicht so schön, wenn es danach Ärger gibt. Lesen Sie deshalb, was bei solchen Fotos zu beachten ist!

Ein Vorsitzender hat richtig Ärger

Der Vereinsvorsitzende hatte sich wirklich nichts Böses dabei gedacht, doch jetzt war ihm mulmig. Dabei war der Spielnachmittag ein voller Erfolg gewesen, weit über 100 Kinder hatten teilgenommen. Auf den Bildern, die er davon gemacht hatte, winkten ihm Kinder wie Eltern fröhlich zu. Aber dass er die Bilder auf die Vereins-Homepage gestellt hatte, das verkrafteten die Eltern jetzt überhaupt nicht.

Einverständnis und Einverständnis sind zweierlei

Der Vorsitzende war in eine klassische Falle getappt! Natürlich konnte er davon ausgehen, dass die Kinder und Eltern, die er abgelichtet hatte, damit einverstanden waren. Fröhliches Winken in Richtung des Fotografen, bewusstes "In-die-Kamera-Lächeln" - das sind klare Anzeichen dafür, dass jemand mit einem Foto einverstanden ist.

Das bedeutet aber noch nicht, dass er zugleich einer Veröffentlichung dieses Fotos zustimmt. Wenn man ein Foto von jemandem veröffentlichen will, muss man ihm dies irgendwie ankündigen und muss sicherstellen, dass er auch mit dieser Veröffentlichung einverstanden ist. Das Einverständnis in eine Aufnahme und das Einverständnis in ihre Veröffentlichung sind also zwei verschiedene Dinge!

Das "Recht am eigenen Bild" beachten!

Eigentlich gebietet das ja schon die Höflichkeit. Weil das Vertrauen darauf aber nicht immer ausreicht, existiert hierfür eine ausdrückliche gesetzliche Regelung. Sie ist in einem speziellen Gesetz enthalten, das die etwas irreführende Bezeichnung "Kunsturheberrechtsgesetz" trägt. Es enthält Regelungen für das "Recht am eigenen Bild". Über Google ist der relativ kurze Text leicht zu finden.

Sollen Fotos von Kindern veröffentlicht werden, müssen die Eltern einwilligen (Bild: Thinkstock)

Für Kinder entscheiden die Eltern

Wenn es um Kinder geht, ist natürlich der Wille der Eltern maßgeblich. Das gilt übrigens auch bei eher "großen Kindern" knapp unter 18 Jahren. Denn auch sie sind eben noch nicht volljährig. Daher hätte der Vorsitzende in unserem Beispiel die Eltern fragen müssen, bevor er Bilder einzelner Kinder veröffentlicht.

Besonderes gilt bei Menschenmengen ...

Anders sieht es übrigens aus, wenn es um das Foto einer Menschenmenge geht. Falls der Vorsitzende zum Abschluss der Veranstaltung alle teilnehmenden Kinder als fröhliche Gruppe fotografiert hat, dürfte er dieses Foto veröffentlichen, ohne lange zu fragen. Das ergibt sich aus einer ausdrücklichen Regelung des Gesetzes.

... und auch bei Prominenten

Und falls ein Prominenter bei der Veranstaltung war, etwa ein bekannter Politiker, der für den Fotografen mit einigen Kindern gespielt hat, dann darf auch dieses Foto veröffentlicht werden, ohne vorher lange zu fragen. Denn ein Politiker ist eine Person der Zeitgeschichte. Und wer sich neben einer solchen Person aufhält, muss eine Veröffentlichung des Fotos dulden. Auch das steht im Gesetz.

Wann hilft Ihnen der Europäische Datenschutzbeauftragte (EDSB)?

Auch für Fachleute ist es nicht immer einfach, den Überblick über die verschiedenen Datenschutzbehörden zu behalten. Wäre es da nicht bequem, sich gleich an den Europäischen Datenschutzbeauftragten zu wenden, wenn man eine Beschwerde hat? Lesen Sie, wann das der richtige Weg ist und wann nicht.

Deutschland hat besonders viele Gesetze

Für den Datenschutz gibt es in allen Mitgliedstaaten der Europäischen Union nationale Gesetze. In Deutschland sind dies sogar noch ein paar Gesetze mehr als in allen anderen Mitgliedstaaten. Das hängt damit zusammen, dass Deutschland eben eine "Bundesrepublik" ist, in der die Bundesländer neben dem Bund eine eigenständige Rolle spielen.

Neben dem BDSG stehen Landes-Datenschutzgesetze

Jedes Bundesland hat deshalb ein eigenes Datenschutzgesetz. Es gilt allerdings nur für die öffentlichen Stellen des jeweiligen Bundeslandes. Daneben gibt es meist (wenn auch nicht immer) noch zahlreiche Sonderregelungen, vom Datenschutz in Schulen bis hin zum Datenschutz in Krankenhäusern.

Für private Wirtschaftsunternehmen haben diese Landesgesetze höchstens dann Bedeutung, wenn sie als Dienstleister für entsprechende Behörden tätig sind. Für ihren eigenen Tätigkeitsbereich sind sie dagegen ohne Belang. Für private Wirtschaftsunternehmen ist vielmehr das Bundesdatenschutzgesetz maßgeblich, also eine Regelung des Bundes.

Die Überwachung der Gesetze ist meistens Ländersache

Wer hat nun die Einhaltung dieser vielen Gesetze zu überwachen? Bei den Datenschutzgesetzen der Länder gibt es insoweit keine Überraschungen. Über ihre Einhaltung wacht der jeweilige Landesbeauftragte für den Datenschutz oder eine vergleichbare Institution (etwa das "Unabhängige Landeszentrum für Datenschutz" in Schleswig-Holstein). Aber wer überwacht die Einhaltung des Bundesdatenschutzgesetzes?

Naheliegend scheint auf diese Frage die Antwort, dass dies beim Bundesdatenschutzgesetz wohl der Bundesbeauftragte für den Datenschutz sein müsse. Das trifft jedoch

Der Europäische Datenschutzbeauftragte überwacht, wie europäische Einrichtungen mit den Daten ihrer Mitarbeiter, aber auch mit denen von EU-Bürgern umgehen (Bild: Thinkstock)

nicht zu. Vielmehr ist auch das eine Aufgabe der Bundesländer! In den meisten Bundesländern wird sie vom jeweiligen Landesbeauftragten für den Datenschutz wahrgenommen. Bayern hat dafür eine eigene Behörde, das "Landesamt für Datenschutzaufsicht". Lediglich die Datenschutzaufsicht über Unternehmen der Post und der Telekommunikation ist tatsächlich eine Aufgabe des Bundesbeauftragten!

Einfach ist diese Zuständigkeitsverteilung nicht gerade. Sie ist aber hier - wie auch in anderen Lebensbereichen - der Preis dafür, dass Deutschland eben kein Zentralstaat ist. Anders sieht es dagegen zum Beispiel in Frankreich aus: Dort gibt es eine einzige zentrale Datenschutzkommission, die für alle Unternehmen des Landes zuständig ist.

Beim EDSB geht es nur um Institutionen der Europäischen Union

Wenn Sie bis hierher durchgehalten haben, möchten Sie spätestens jetzt endlich auch etwas zum Europäischen Datenschutzbeauftragten hören. Seine Aufgabe wird besonders deutlich bei Personen, die direkt bei der Europäischen Union beschäftigt sind, etwa bei der Europäischen Kommission in Brüssel, die Tausende von Mitarbeitern hat.

Ob die Europäische Kommission mit den Daten ihrer Mitarbeiter korrekt umgeht, kann eine nationale Datenschutzinstanz nicht überprüfen. Hierfür braucht es eine Instanz auf europäischer Ebene, und das ist der Europäische Datenschutzbeauftragte.

Wichtige Themen sind dabei Personaldaten und Subventionsdaten

Er befasst sich jedoch nicht nur mit Personaldaten. Inzwischen kommt es relativ häufig vor, dass europäische Instanzen auch mit Daten normaler Bürger aus der Europäischen Union umgehen. Das betrifft etwa Landwirte, bei denen eine europäische Instanz überprüft, ob sie Subventionen zu Recht erhalten haben oder nicht. Es mag sich wie Science Fiction anhören, aber in diesem Bereich überwacht die Europäische Union zum Teil sogar mittels Satellitenaufnahmen, auf welchen Feldern was angebaut wird. Wehe, ein Landwirt hat dann eine Subvention dafür beantragt, dass er ein Feld aus Naturschutzgründen nicht nutzt, und dann findet sich dort doch Mais!

Auch für Beschwerden im Zusammenhang mit solchen Überwachungen ist der Europäische Datenschutzbeauftragte zuständig.

Der EDSB ist aber keine Oberaufsicht für ganz Europa

Was er jedoch ganz klar nicht ist: eine zusätzliche Instanz für Fälle, in denen Sie mit der Entscheidung einer nationalen Datenschutzaufsichtsbehörde nicht einverstanden sind. Er darf nur Maßnahmen und Entscheidungen von Institutionen der Europäischen Union überprüfen, aber nicht Entscheidungen nationaler Behörden.

Für den Fall, dass Sie tatsächlich einmal in eine Situation kommen, in der er zuständig ist, finden Sie unter folgendem Link ein besonderes Beschwerdeformular: *http://kurzlink.de/beschwerde_eu*.

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

Das Erfolgsgeheimnis der Hacker

Apple, Facebook und Yahoo sind nur drei Beispiele für bekannte Unternehmen, die kürzlich erfolgreich von Hackern angegriffen wurden. Wie schaffen Hacker das, trotz professioneller Sicherheitssoftware aufseiten der Opfer? Sie werden überrascht sein: Die Antwort hat mit Ihnen zu tun.

Versagt die IT-Sicherheit?

Wenn Privatpersonen feststellen müssen, dass sie Opfer eines Angriffs aus dem Internet geworden sind, kommt schnell der Verdacht auf, dass sie sich nicht ausreichend geschützt haben. Unprofessionelle, veraltete Sicherheitssoftware oder sogar der Verzicht auf Sicherheitslösungen scheinen die Ursachen zu sein.

Doch bei großen Unternehmen, die ihr Geschäft im Internet machen und sich mit den Gefahren gut auskennen sollten, ist dies mehr als unwahrscheinlich.

In den seltensten Fällen entsprechen Hacker dem üblichen Klischee vom absoluten Technik-Profi. Oft zielen sie mehr auf die Nutzer als auf die Technik ab. (Bild: Thinkstock)

Ein Blick in die Hackerwelt liefert Antworten

Um zu verstehen, warum die Hacker selbst große, bekannte Unternehmen mit Erfolg attackieren können, lohnt es sich, die Angriffe einmal ganz genau anzusehen.

Vielleicht stellen Sie sich einen Hackerangriff so vor, dass der Angreifer ein absoluter Profi ist, der auf die falsche Seite geraten ist. Mit umfangreichen Programmier-Tricks, leistungsstarken Rechnern und selbst gebastelter Angriffssoftware bezwingt er die Sicherheitssoftware und kommt so in die IT-Systeme seiner Opfer. In Wirklichkeit ist dies aber nur in den seltensten Fällen so.

Hacking: anders als erwartet

Werden Hacker enttarnt, sind es häufig keine kriminell gewordenen IT-Sicherheitsexperten, sondern Internetkriminelle, die sich ihre Angriffswerkzeuge aus dem Netz besorgen, ihre Opfer nach finanziellen Motiven aussuchen oder sich als ehemalige Beschäftigte an ihrem Ex-Arbeitgeber rächen wollen. Der Erfolg des Hacking basiert auch nicht auf technischer Überlegenheit der Angreifer, wie das folgende Beispiel zeigt:

Hacking ist wie Fischen gehen

Der Angriff auf den Technologiekonzern Apple im Februar 2013 zum Beispiel basierte auf dem Auslegen eines Köders im Internet.

Apple und andere Technikunternehmen verdanken ihre Marktpositionen unter anderem einer innovativen Produktentwicklung. Also dachten sich die Angreifer, lohnende Opfer im Apple-Konzern sind die Produktentwickler. Die Hacker griffen nicht die Computer der Entwickler direkt an, sondern manipulierten eine Webseite, die für Apple-Entwickler interessant ist. Mit dem Besuch der verseuchten Webseite machten die Entwickler ungewollt eine Hintertür zu ihren Computern auf.

Es kommt auf Sie an!

Viele andere Hacking-Vorfälle lassen sich ähnlich erklären: Hacker bezwingen in aller Regel nicht die Firewall oder zerstören gar die Sicherheitssoftware, wie man es sich vielleicht vorstellt. Sie gehen den Weg über den Nutzer, verleiten ihn zu einer unbedachten Aktivität und hoffen, dass bestimmte Sicherheitsempfehlungen wieder einmal unbeachtet bleiben.

Das Erfolgsgeheimnis der Hacker sind wir alle, die Internetnutzer, die ausgenutzt, getäuscht und manipuliert werden.

So wehren Sie sich gegen Hacking

Hacker nutzen ihr Wissen über das Verhalten der Nutzer aus: Die Angriffe sind erfolgreich, weil Sicherheitswarnungen häufig missachtet werden, und sie sind erfolgreich, weil Internetnutzer leicht durchschaubar sind. Die Hacker wissen, wo sich die gewünschten Opfer im Internet aufhalten werden, und schlagen genau dort zu.

Umgehen Sie "Wasserloch"-Attacken

Diese Angriffstechnik nennt man auch "Wasserloch-Attacke", weil dem Angreifer klar ist, dass sein Opfer zum "Wasserloch", also zu einer bestimmten Webseite, kommen wird.

Natürlich können Sie nicht auf den Besuch der für Sie wichtigen Webseiten verzichten, schließlich sind sie wie Wasserlöcher notwendig. Doch Sie sollten folgende Tipps gegen Hacking beherzigen:

Tipps gegen Hacking

1. Nutzen Sie professionelle IT-Sicherheitssoftware auf allen Endgeräten, die Sie verwenden.

2. Aktualisieren Sie jede Anwendung, die Sie nutzen, natürlich auch Ihre Sicherheitssoftware.

3. Vergessen Sie auch Mini-Anwendungen nicht, wie zum Beispiel Erweiterungen für Ihren Browser oder die Apps auf Ihrem Smartphone.

4. Selbst wenn Sie alles aktualisieren und gute Sicherheitssoftware nutzen: Fühlen Sie sich nicht komplett sicher im Internet. Nehmen Sie Sicherheitswarnungen ernst.

5. Denken Sie daran, dass gerade besonders beliebte und renommierte Webseiten Gefahren enthalten können. Die Angreifer lauern an den Wasserlöchern.

6. Wenn Sie das Gefühl haben, dass etwas bei einer Software oder bei einem Endgerät nicht mehr stimmt, scheuen Sie nicht davor zurück, Ihre IT-Administratoren und Ihren Datenschutzbeauftragten zu kontaktieren.

Verfolgt auf Schritt und Tritt

Ortung geht auch ohne GPS und Satelliten. Selbst wenn Sie ein Handy ohne Navigationsfunktion nutzen, können Sie Ihre aktuelle Position verraten. Nicht nur die Online-Werbung ist an Ihrem Aufenthaltsort interessiert.

Überraschung beim Frühstück

Stellen Sie sich vor, Sie befinden sich auf einer Dienstreise im benachbarten Ausland. Während des Frühstücks im Hotel wollen Sie sich nochmals den Weg zur Messehalle ansehen. Ihr Smartphone hat zwar keine spezielle Navigationssoftware, aber Google Maps liefert Ihnen alle Informationen, die Sie brauchen. Deshalb starten Sie die entsprechende App und sind nach kurzer Zeit erstaunt, Ihre aktuelle Position gar nicht eingeben zu müssen, um den besten Weg zur Messehalle angezeigt zu bekommen. Ihr Smartphone weiß schon, wo Sie sind. Die angezeigte Position ist tatsächlich Ihr Hotel.
Wie ist das möglich?

Das verräterische WLAN

Wenn Sie GPS und eine Navigationssoftware genutzt hätten, wäre Ihnen alles klar. Über die Satellitenverbindung wären Sie geortet worden. Aber eigentlich sind Sie doch nur im Internet! Um Kosten für die Datenverbindung zu sparen, haben Sie das angebotene WLAN im Hotel dafür genutzt.

Das aber ist des Rätsels Lösung. Durch die Nutzung des WLAN-Hotspots im Hotel kennt Google Maps Ihren Aufenthaltsort. Das gilt natürlich nicht nur für WLAN im Hotel, sondern für jedes WLAN, das mit seiner Kennung und seinem Standort von Google oder einem anderen Internetkonzern registriert wurde.

Webseiten nutzen Standortdaten

Die Auswertung von Standortinformationen ist auch nicht auf Kartendienste oder Suchmaschinen beschränkt. Viele Webseiten versuchen, die Standortdaten zu nutzen, um die Inhalte entsprechend anzupassen. Insbesondere die Online-Werbung soll für Sie relevanter werden, wenn die Standortdaten ausgewertet werden. Man spricht hierbei auch von standortbezogenem Surfen (Location-aware Browsing).

Firefox-Browser meldet Wunsch nach Standortdaten

Solange das standortbezogene Surfen mit Ihrem Wissen und Ihrer Einwilligung geschieht, ist daran nichts auszusetzen, im Gegenteil. Wenn Sie über eine Suchmaschine nach "Messehalle" suchen, werden Ihnen dann direkt die Messehallen passend zu Ihrem Standort angezeigt. Wenn die Standortdaten aber heimlich gesammelt und ausgewertet werden, ist Ihre Privatsphäre in Gefahr.

Der Browser Mozilla Firefox meldet sich immer dann, wenn eine Webseite nach Standortdaten fragt, also nach Ihrer aktuellen IP-Adresse und nach Ihrem aktuellen Internetzugang, also zum Beispiel dem WLAN im Hotel.

Transfer zulassen oder blockieren

Wenn Sie Ihre Standortdaten nicht übermitteln lassen wollen, können Sie es dem Browser untersagen, oder aber Sie erlauben den Datentransfer. Denkbar ist es auch, das standortbezogene Surfen komplett zu verbieten. Möglich ist dies, indem Sie im Firefox-Browser

- in der Adressleiste about:config eingeben,
- geo.enabled in die Filter-Zeile eintragen
- und auf die Einstellung geo.enabled doppelklicken.

Denken Sie aber daran, dass diese Einstellung nur auf den im Beispiel genannten Firefox-Browser wirkt, nicht aber auch andere Programme oder Internetdienste umfasst, die ebenfalls Ihre Standortdaten lesen könnten. Schließlich werden die entsprechenden Daten von Ihrem jeweiligen Internetzugang übermittelt und stehen jeder Internetanwendung zur Verfügung.

Werden Sie nicht selbst zum Verräter

Zudem bringt es wenig, dem Browser zu verbieten, Standortdaten zu übertragen, und dann selbst bei Facebook & Co. den aktuellen Aufenthaltsort zu melden. Wer in einem sozialen Netzwerk wie Facebook als Nachricht einträgt, dieses oder jenes Hotel sei toll, man frühstücke dort gerade, muss sich nicht wundern, wenn Dritte die aktuelle Position kennen.

Sehen Sie sich einmal bei Facebook die integrierte Kartenansicht an. Wer seine Orte eingetragen hat, hinterlässt dort eine sichtbare Spur, in der Regel für alle anderen Facebook-Nutzer oder sogar für andere Internetnutzer.

Üben Sie sich also in Datensparsamkeit, auch an schönen Orten!

Vermeiden Sie eine ungewollte Ortung im Internet?

Frage: Um nicht ungewollt geortet zu werden, schalten Sie bei Nichtgebrauch die GPS-Funktion Ihres Smartphones ab. Reicht das?

a) Leider nicht. Positionsdaten lassen sich auch aus dem genutzten Mobilfunk- und Internetzugang gewinnen.
b) Ohne GPS geht die Navigation bei mir nicht, eine Ortung kann also nicht mehr stattfinden.

Lösung: Die Antwort a) ist richtig. Die Ortung über GPS ist nur ein Weg. Auch bei der Internetnutzung hinterlässt man Positionsdaten. Bei Smartphones werden so theoretisch Bewegungsprofile der Nutzer möglich.

Frage: Sie wollen Ihre aktuelle Position nicht im Internet preisgeben. Genügt es dazu, den Browser entsprechend einzustellen?

a) Nein, denn jede Anwendung mit Internetzugang könnte meine IP-Adresse, die WLAN-Kennung und weitere Positionsdaten auswerten und weiterleiten.
b) Da alle Webseiten über den Browser angezeigt werden, ist dies ausreichend.

Lösung: Die Antwort a) ist wieder richtig. Bei einem Smartphone zum Beispiel ist der Browser nur eine App von vielen. So können etwa auch Apps der sozialen Netzwerke Standortdaten abfragen. Inzwischen wurden viele Spionage-Apps entdeckt, deren Aufgabe es ist, die Positionen des Nutzers aufzuzeichnen und Dritten zu melden.