Infobrief Datenschutz
Ausgabe 10 | 2011

Newsletter Datenschutz

Die Kundenzeitung der agentia wirtschaftsdiesnt

Liebe Leserin, lieber Leser,

Computerviren gehören schon fast zu unserem Alltag. Doch Gefahren, an die man sich gewöhnt, werden meist unterschätzt. Wissen Sie wirklich, wo überall Viren und Trojaner lauern können? Machen Sie im ersten Artikel die Probe aufs Exempel. Testen sollten Sie auch, ob Sie einen Betrugsversuch am Telefon oder per E-Mail erkennen. Raffinierte Datendiebe versuchen geschickt, Ihr Vertrauen zu erschleichen. Lassen Sie es nicht dazu kommen!

Wenn Sie schon immer wissen wollten, was man eigentlich genau unter personenbezogenen Daten versteht: Auch darauf bietet Ihnen diese Ausgabe eine Antwort. Sie haben davon gehört, dass Peilsender mit GPS billig zu haben sind? Aber darf man sie tatsächlich einsetzen? Lesen Sie hier, was (nicht) geht.

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

Aus der Gerüchteküche: Stimmt es ...?

Computerviren gibt es bereits seit mehr als 25 Jahren. Fast jeder Internetnutzer hat schon einmal von Viren, Würmern und Trojanern gehört. Sicherlich haben Sie auch schon viele Ratschläge bekommen, wie Sie sich vor Computerviren schützen können. Doch sind diese auch richtig, oder handelt es sich nur um Halbwahrheiten?

Gibt es Computerviren wirklich nur auf Windows-Rechnern?

Viele Nutzer eines Mac-Rechners fühlen sich sicher. Denn sie haben gehört, es gebe keine Viren für diese Computer. Das ist falsch! Viren für Windows-Rechner sind nur deshalb bekannter, weil es einfach mehr Computer gibt, die unter einem Windows-Betriebssystem laufen. Die steigende Verbreitung der Apple-Produkte iPhone und iPad macht nun Mac-Systeme für Datendiebe zunehmend interessant. Die Zahl der Viren, die Mac-Rechner befallen, wird steigen. Auch Mac-Nutzer brauchen also einen Anti-Viren-Schutz.

Machen Anti-Viren-Programme den Rechner zu langsam?

25 Prozent der Internetnutzer deaktivieren ihr Anti-Viren-Programm, wenn ihnen der private Rechner zu langsam wird, so ein Umfrageergebnis von Avira. Machen Sie das bloß nicht! Anti-Viren-Programme machen den Rechner sicherer und blockieren ihn nicht. Achten Sie lieber auf die Wahl einer Anti-Viren-Lösung, die wenig Computerressourcen in Anspruch nimmt, aber trotzdem sicher ist. Hinweise finden Sie in den Vergleichstests renommierter Computer-Fachzeitschriften.

Lauern Computerviren nur auf unseriösen Webseiten?

Zwei Drittel aller Internetnutzer glauben, sie könnten sich keine Computer-Viren einfangen, wenn sie bestimmte unseriöse Webseiten nicht besuchen. Von wegen! Gerade auf seriösen Webseiten wie dem Online-Auftritt einer Zeitung oder eines Fernsehsenders können Datendiebe Viren versteckt haben. Auf diesen Webseiten sind die Nutzer weniger misstrauisch und deshalb leichter zu täuschen. Seien Sie also überall im Internet auf der Hut!

Wer nichts anklickt, hat nichts zu fürchten?

Durch das Anklicken eines Hyperlinks auf Webseiten oder in E-Mails kann man sich Computer-Viren auf den Rechner laden. Stimmt es dann umgekehrt, dass Sie nicht in Gefahr sind, wenn Sie eine Webseite oder E-Mail nur öffnen, aber nichts anklicken? Nein! Bereits das Öffnen einer Webseite in Ihrem Browser kann Computerviren auf Ihren Rechner bringen. Nur ein aktueller Anti-Viren-Schutz und die regelmäßige Aktualisierung von Webbrowser und E-Mail-Programm können davor schützen.

Sind E-Mails, die tatsächlich von Freunden oder Kollegen kommen, wirklich sicher?

Die Absenderangaben in einer E-Mail lassen sich leicht fälschen. Nur weil als Absender ein Freund von Ihnen genannt ist, muss die E-Mail nicht von ihm kommen. Aber wenn Sie genau wissen, wer der Absender ist, weil die E-Mail telefonisch angekündigt wurde, besteht dann keine Gefahr? Doch! Wenn der Rechner Ihres Freundes mit Viren verseucht ist, können es auch die E-Mails sein. Spezielle Computerschädlinge können sogar E-Mails im Namen und von dem Rechner einer Person verschicken, ohne dass sie etwas ahnt.

Glauben Sie also nicht jede Halbwahrheit, die Sie über Computer-Viren hören. Vertrauen Sie auf eine gute Sicherheitssoftware, regelmäßig aktualisierte Anwendungen und Ihren gesunden Menschenverstand. Computerviren sind überall möglich, wo Daten ausgetauscht werden, im Internet, im internen Netzwerk, auf USB-Sticks, auf DVDs und auch auf Ihrem Handy!

Was sind eigentlich "personenbezogene Daten"?

Den Begriff hat fast jeder schon einmal gehört. Und aus dem Alltag im Unternehmen weiß man: Wenn Daten personenbezogen sind, muss der Datenschutz beachtet werden. Aber was gehört eigentlich alles dazu? Lernen Sie die wichtigsten Beispiele für personenbezogene Daten kennen!

Personenbezug und Datenschutz: zwei unzertrennliche Geschwister

"Das ist personenbezogen, deshalb unterliegt es dem Datenschutz." Dieser Satz fällt häufig, wenn es darum geht, ob der Datenschutz zu beachten ist.

Dass alles, was mit dem Namen eines Arbeitnehmers, eines Kunden oder einer sonstigen Person versehen ist, personenbezogen ist, liegt auf der Hand. Aber was ist, wenn kein Name dabeisteht? Ist das Thema "Personenbezug" damit erledigt? So einfach ist die Sache leider nicht!

Die gesetzliche Regelung im Bundesdatenschutzgesetz ist erstaunlich kurz

Die gesetzliche Regelung zu diesem Thema ist kurz und knapp: "Personenbezogene Daten sind Einzelangaben über persönliche oder sachliche Verhältnisse einer bestimmten oder bestimmbaren natürlichen Person." So sagt es § 3 Absatz 1 des Bundesdatenschutzgesetzes.

Alles, was mit konkreten Namen zu tun hat, ist immer personenbezogen

Wenn bei etwas der Name dabeisteht, haben wir den klassischen - und sehr einfachen - Fall, dass es um eine ganz bestimmte Person geht.

Was genau über diese Person gesagt ist, macht dann keinen Unterschied, es ist immer personenbezogen. Das gilt für den Vermerk "zahlt schleppend" in einer Kundendatei genauso wie für den Hinweis "war Mitarbeiter des Monats August 2011" in einer Personalakte.

Auch besondere Eigenschaften charakterisieren eine Person

Schwieriger wird es, wenn der Name einer Person nicht genannt ist, es aber doch klar wird, um wen es geht.

Wenn etwa aus einer Personalübersicht zu sehen ist, dass eine Frau, die in der Buchhaltung tätig ist, zum vierten Mal Elternzeit beantragt hat, wird auch ohne den Namen klar sein, um wen es dabei geht.

E-Mail-Adressen können wie Namen wirken

Nicht anders sieht es bei einer E-Mail-Adresse aus, wenn sie zwar keinen Namen enthält, aber jeder in der Firma weiß, wer sich dahinter verbirgt. Statt Buchhaltung3@firma.de könnte man dann beispielsweise gleich "Frau Müller" sagen. Damit ist die Mailadresse personenbezogen.

Natürlich stimmt es, dass Außenstehende diesen Bezug nicht herstellen können. Aber auch sie könnten beispielsweise jemanden im Unternehmen fragen und würden schnell herausbekommen, dass es bei dieser E-Mail-Adresse um Frau Müller geht.

E-Mail-Adressen sind in vielen Fällen ebenfalls personenbezogene Daten

IP-Adressen sind ein Streitfall

Schwieriger liegen die Verhältnisse, wenn es um eine IP-Adresse geht, ohne die kein PC eine Verbindung zum Internet aufbauen kann. Häufig wird diese Adresse einem PC nur so lange zugeteilt, wie der Nutzer sich im Netz bewegt. Verlässt er das Netz wieder, kann dieselbe Adresse schon nach wenigen Sekunden einem anderen PC zugeordnet sein.

Dennoch sind fast alle Datenschützer der Auffassung, dass auch eine solche IP-Adresse personenbezogen ist. Denn selbstverständlich kann jedes Rechenzentrum und jeder Internet-Provider schnell Auskunft darüber geben, wann eine bestimmte IP-Adresse einem bestimmten PC zugewiesen war.

Allerdings: Jedenfalls bei einem Provider wird man vergebens danach fragen. Solche Daten unterliegen nämlich dem Fernmeldegeheimnis. Freilich ist dieses Geheimnis nicht mehr viel wert, wenn ein Staatsanwalt mit einer richterlichen Anordnung vor der Tür steht. Insofern bietet es eben nur begrenzten Schutz.

Bilder mit und ohne Balken

Das Bild einer Person gehört selbstverständlich ebenfalls zu den personenbezogenen Daten, auch wenn kein Name dabeisteht.

Hilft es, wenn man einen Balken über den Augen anbringt? Die Antwort lautet: meistens nicht. Denn bei vielen Menschen sind die Kinnpartie und die Frisur so charakteristisch, dass jedenfalls ihr Umfeld sie wiedererkennt. Das reicht dann aus, um den Personenbezug zu bejahen. Anders wäre es natürlich, wenn das Gesicht völlig "verpixelt" ist.

Ein Telefon, mehrere Nutzer - was nun?

In der Praxis kommt es manchmal vor, dass mehrere Personen ein und dasselbe Telefon nutzen. Sofern die entsprechende Personengruppe nicht allzu groß ist (bis zu etwa drei oder vier Mitarbeitern), bewirkt ein solcher Gruppenbezug, dass alle Daten über Gespräche mit diesem Telefon als personenbezogen gelten.

Und zwar handelt es sich dann um personenbezogene Daten jeder einzelnen Person, die das Telefon zumindest ab und zu benutzt. Denn wenn von dort aus zum Beispiel teure Auslandsgespräche geführt oder Sexnummern angerufen werden, geraten ja alle Mitglieder der Gruppe in Verdacht.

Impressum

Redaktion:
Udo Wenzel
Datenschutzbeauftragter

Anschrift:
agentia wirtschaftsdienst
Dipl.-Inform. Udo Wenzel
10787 Berlin
Telefon: 030 / 2196 4390
E-Mail: udo.wenzel@agentia.de

Überwachung der Ex mit einem GPS Sender - eine gute Idee?

Mancher Mann wüsste ganz gerne, was seine Ex den ganzen Tag so macht. Beispielsweise, um ihr den Unterhalt kürzen zu können, wenn sie heimlich arbeitet. Ein GPS-Sender an ihrem Auto könnte da ganz nützlich sein. Oder lieber nicht?

Die Unterhaltspflicht drückt

Ein unterhaltspflichtiger Mann hatte es dick, wie man so sagt: Jeden Monat 680 Euro an seine frühere Frau überweisen, und das, obwohl er sich sicher war: Sie ist eine neue Lebensgemeinschaft eingegangen und hätte deshalb entweder überhaupt keinen Anspruch auf Unterhalt mehr oder jedenfalls nicht in dieser Höhe.

Die Ex-Frau soll überwacht werden

Bloß: Wie soll man so etwas nachweisen? Ein befreundeter Detektiv wusste Rat. Er schlug vor, am Auto der Frau heimlich einen GPS-Sender anzubringen. So könnte man ein Überwachungsprotokoll erstellen, und es wäre schnell klar, wann sie sich wo bewegte und wie oft sie mit dem neuen Partner zusammen ist.

Ein Detektiv wird beauftragt

Das gefiel dem Mann, und er vergab einen entsprechenden Auftrag an den Detektiv. Irgendwelche Skrupel, was das Persönlichkeitsrecht der Frau angeht, hatten die beiden Herren offensichtlich nicht. Der Detektiv wollte das Geschäft machen und der unterhaltspflichtige Mann die monatliche Zahlung sparen. Da stellt man etwaige Bedenken schon einmal zurück.

Mithilfe eines Detektivs und eines GPS-Senders sollten die Unterhaltszahlungen ein Ende haben

Die Überwachung kostet 3.700 Euro

Richtig billig war das Ganze freilich nicht. Über 3.700 Euro kostete die Überwachung. Aber immerhin: Als er seine Ex mit den Überwachungsprotokollen konfrontierte, gab sie sofort kleinlaut bei. Sie gestand, dass sie ihren früheren Mann die ganze Zeit getäuscht und zu Unrecht Unterhalt bezogen hatte.

Man einigte sich schnell darauf, dass der Mann künftig nichts mehr zu zahlen hat.

Der Mann fordert die Detektivkosten erfolglos von der Frau

Damit allein gab er sich aber nicht zufrieden. Er verlangte von ihr, dass sie auch noch die Detektivkosten zahlt. Als sie sich weigerte, verklagte er sie.

Das Gericht erteilte ihm freilich eine deutliche Abfuhr. Es schrieb ihm ins Stammbuch, dass er das Persönlichkeitsrecht der Frau in erheblicher Weise verletzt habe. Und Kosten für rechtswidrige Aktionen müssten eben nicht ersetzt werden.

Gespart hat er im Ergebnis trotzdem

Immerhin: Letztlich hatte sich die Sache für ihn gelohnt. Denn die 3.700 Euro, auf denen er sitzen blieb, machten sich bei bisher 680 Euro Unterhaltszahlung pro Monat ja schon nach einem guten halben Jahr bezahlt.

Das Ganze war ein Spiel mit dem Feuer

Wie sehr der Mann mit dem Feuer gespielt hatte, zeigt allerdings ein anderer Fall, den das Landgericht Lüneburg entschieden hat. Dort hatte ein Detektiv ebenfalls einen Peilsender eingesetzt. Allerdings meldete sich bei ihm kein Ex-Ehemann, sondern die Staatsanwaltschaft.

Andernorts griff der Staatsanwalt ein

Sie verstand keinerlei Spaß. Vielmehr präsentierte sie ihm einen Beschlagnahmebeschluss für den Peilsender mit allem Zubehör.

Die Begründung: Es liege der Verdacht einer Straftat nach dem Bundesdatenschutzgesetz vor, nämlich der Verdacht der unbefugten Erhebung und Verarbeitung von personenbezogenen Daten.

Per GPS (Global Positioning System) lässt sich weltweit alles und jedes, das mit einem entsprechenden Peilsender versehen ist, orten

Das Gericht lässt den Sender beschlagnahmen

Niemand - so das Gericht - müsse es sich gefallen lassen, in dieser Art und Weise überwacht zu werden. Dafür gebe es überhaupt keine Rechtsgrundlage. Zudem werde das Persönlichkeitsrecht des Betroffenen in schwerer Weise verletzt. Sein Privatleben werde hier bis in Einzelheiten hinein ausspioniert.

Weder Mann noch Frau sind Unschuldslämmer

Erzählt man diese beiden Fälle im Bekanntenkreis, empören sich meistens die Frauen darüber, "wozu Kerle alles fähig sind".

Damit haben sie durchaus Recht. Allerdings gibt es auch noch eine zweite Seite der Medaille, die man nicht vergessen sollte. Wenn eine Frau weiterhin Unterhalt fordert und sich bezahlen lässt, obwohl sie genau weiß, dass sie keinen Anspruch darauf hat, bewegt sie sich im Bereich des Betrugs. Und Betrug gehört auch zu den Straftaten.

Vielleicht könnte man deshalb einmal auf die möglicherweise etwas unpopuläre Idee kommen, dass beide Seiten sich an die Gesetze halten sollten. Dann würde die Frau nichts verlangen, was ihr nicht zusteht, und der Mann würde keinen Spion in Marsch setzen ...

Vorsicht, Betrüger am Werk!

Der Anruf, der angeblich von einem neuen Kollegen kommt, die E-Mail, die scheinbar von der Systemadministration stammt, oder der Besucher, der sich in den Konferenzraum verirrt hat - überall kann ein Betrugsversuch dahinterstecken. Wie aber können Sie erkennen, ob man Sie täuschen und ausspionieren will?

Pizza-Dienst willkommen!

In der Entwicklungsabteilung ist es wieder spät geworden. Kein Wunder, dass der Chefentwickler eine Pizza bestellt hat. "Ich bringe sie schnell zu meinem Kunden, der hat Hunger, und die Pizza soll ja nicht kalt werden", und schon ist der Pizza-Bote an dem Pförtner vorbei und in Richtung Büros verschwunden.

Wenige Minuten später kommt er zurück, verabschiedet sich kurz und ist weg. Als der Entwicklungsleiter das Gebäude verlassen will, fragt der Pförtner, wie die Pizza denn geschmeckt habe. "Welche Pizza?", so die erstaunte Antwort.

Datendiebe kommen nicht nur über das Internet

Tatsächlich gelangen auf diesem Weg so manche Industriespione in Büros und Konferenzräume, in denen Notebooks oder USB-Sticks unbewacht auf dem Tisch liegen. Oder sie können ein Foto von den Notizen auf dem Flipchart machen und so Details der Unternehmensplanung ausspähen.

Nicht jeder Angriff auf vertrauliche Daten erfolgt über das Internet. Viele Attacken finden direkt vor Ort statt oder nutzen das gute, alte Telefon. Der angebliche Anruf des Systemadministrators, der eben einmal das Passwort des Nutzers braucht, ist schon klassisch. Die Kreativität der Betrüger reicht aber viel weiter.

So arbeiten die Betrüger

Um einen Angriff starten zu können, beschaffen sich die Datendiebe zuerst passende Informationen aus dem Internet, wobei insbesondere soziale Netzwerke wie Facebook & Co. tiefe Einblicke in private Daten gewähren können. Auf Basis der Informationen wird meist ein Vertrauensverhältnis zum Opfer aufgebaut.

So könnte der Entwicklungsleiter aus unserem Beispiel auf Facebook veröffentlicht haben, das er sich gerne eine Pizza bestellt, wenn es abends später wird. Das Wissen um diese Gewohnheit hilft bei der Täuschung des Pförtners.

Die Gefühle der Opfer werden ausgenutzt

Bei den Betrugsversuchen schlüpfen die Datendiebe in eine passende Rolle, oder sie missbrauchen menschliche Eigenschaften wie Hilfsbereitschaft, Neugierde oder Angst.

Oftmals nutzen die Betrüger auch fachliche Schwächen aus und verleiten die Opfer zu riskanten Handlungen, die ein erfahrener Mitarbeiter nie machen würde. Damit das Opfer kaum Zeit zum Nachdenken hat, geht es meist um etwas angeblich Dringendes, etwa um einen Bericht, den die Geschäftsleitung sofort haben möchte, um einen gefährlichen Computer-Virus oder um eine letzte Mahnung.

Seien Sie kritisch!

Die Betrugsversuche sind vielfältig und raffiniert.

Wie können Sie aber einen Betrüger von einem echten Anrufer, Besucher oder Facebook-Kontakt unterscheiden? Skepsis und gesunder Menschenverstand sind gefragt:

1. Misstrauen Sie tollen Angeboten, denn niemand hat etwas zu verschenken.

2. Glauben Sie nicht einfach der Absenderangabe bei einer E-Mail, auch nicht der in Ihrem Display angezeigten Telefonnummer. Selbst sie könnte gefälscht sein.

3. Lassen Sie sich nicht hetzen, sondern klären Sie zuerst die Echtheit einer Anfrage, zum Beispiel, indem Sie den Absender einer E-Mail anrufen. Nutzen Sie dabei nicht die in der E-Mail angegebene Rufnummer, sondern eine Nummer aus offiziellen Verzeichnissen.

4. Lassen Sie externe Personen nicht ohne Begleitung durch die Firma gehen.

5. Beantworten Sie keine Fragen von Unbekannten zu Kollegen, Projekten oder Firmendetails, auch nicht, wenn es sich angeblich um Journalisten, Kunden oder Geschäftspartner handelt. Prüfen Sie immer zuerst die Identität.

Lassen Sie sich leicht täuschen? Testen Sie sich!

Frage: Vergangene Woche hat Ihr Unternehmen eine neue Niederlassung gegründet. Heute meldet sich einer der Mitarbeiter der Niederlassung und bittet Sie um ein aktuelles Telefonverzeichnis der Zentrale. Wie reagieren Sie?

a) Ich freue mich über den Anruf des neuen Kollegen und helfe ihm, wo ich kann. Die Telefonliste sende ich ihm gleich per Fax.
b) Ich frage den Assistenten unserer Geschäftsführerin, welche Fax-Nummer denn die neue Niederlassung hat, und vergleiche die Angaben.
c) Ich suche die Rufnummer der neuen Niederlassung aus unserem Verzeichnis und rufe den Kollegen zurück.

Lösung: Die Antworten b) und c) sind richtig. Durch die Pressemeldung in der vergangenen Woche könnte jeder wissen, dass es eine neue Niederlassung gibt. Ohne weitere Prüfung geben Sie deshalb keine Telefonliste heraus.

Frage: Ein Handwerker klopft an Ihre Büroscheibe und bittet Sie darum, die Außentür zu öffnen. In der Herrentoilette sei ein Rohr undicht. Bevor alles unter Wasser stehe, müsse er schnell in das Gebäude. Machen Sie die Tür auf?

a) Nein, zuerst frage ich unseren Hausmeister, ob ein Handwerker bestellt wurde.
b) Wenn der Hausmeister Bescheid weiß, sorge ich dafür, dass jemand den Handwerker begleitet.
c) Natürlich mache ich die Tür auf. Wer will schon nasse Füße?

Lösung: Diesmal sind die Antworten a) und b) richtig, allerdings nur in Verbindung. Selbst wenn ein Handwerker bestellt wurde, sollte er nicht ohne Begleitung durch das Firmengebäude gehen.