Newsletter Datenschutz
Ausgabe 08 | 2013

Newsletter Datenschutz

Die Kundenzeitung der agentia wirtschaftsdienst

Liebe Leserin, lieber Leser,

wissen Sie, was echte Anonymität ausmacht? Diese Ausgabe Ihrer Datenschutz-Zeitung erklärt es Ihnen. Ebenso erfahren Sie, wie Sie mit einem einzigen Fehler beim Erstellen einer E-Mail in den Fokus der Aufsichtsbehörden für den Datenschutz geraten können. Das Bußgeldverfahren kann Sie persönlich betreffen, nicht nur Ihren Arbeitgeber!

Wenn Sie ein Smartphone nutzen, sollten Sie genau überlegen, ob Ihre vertraulichen Gespräche, E-Mails und SMS wirklich vor Lauschangriffen geschützt sind. Der dritte Beitrag dieser Ausgabe sagt Ihnen, worauf es ankommt. Genau hinsehen sollten Sie auch bei Ihrem Webbrowser. Nicht jede Zusatzfunktion ist so harmlos, wie es scheint. Unter Umständen werden all Ihre Internetaktivitäten transparent. Machen Sie am besten gleich den Wissenstest auf der letzten Seite.

Wir wünsche Ihnen viele neue Einsichten.

Ihre *Datenschutzbeauftragten der agentia wirtschaftsdienst*

1.000 Euro Bußgeld für Sie wegen "cc" statt "bcc"?!

Da Sie unseren Newsletter regelmäßig lesen, ist es Ihnen klar: "cc" und "bcc" ist bei Mails nicht dasselbe! Aber was ist, wenn Sie versehentlich doch zum "cc" gegriffen haben, obwohl die Empfänger der Mail nichts voneinander wissen sollten? Die Antwort: Das kann Sie persönlich ohne Weiteres 1.000 Euro Bußgeld kosten!

Erinnern Sie sich noch?

Unser Newsletter 6/2013 hat es geschildert: Soll eine E-Mail an eine Vielzahl von Empfängern gerichtet werden, müssen die Namen der Empfänger in das bcc-Feld eingetragen werden. Das stellt sicher, dass die Empfänger untereinander nicht erkennen können, wer die Mail sonst noch bekommen hat.

In der Praxis klappt das oft nicht. Aus Nachlässigkeit oder Unkenntnis kommt es immer wieder vor, dass bei einer Mail, die an eine Vielzahl von Empfängern gerichtet ist, die Namen der Empfänger in das cc-Feld eingefügt werden. Die Folge: Jeder Empfänger sieht die komplette Adressliste und kann sofort erkennen, wer die Mail sonst noch bekommen hat. Ein klarer Datenschutzverstoß!

Ein Bußgeld ist auch gegen Sie persönlich möglich!

Doch was sind die Folgen eines solchen Verstoßes? Dass ein Bußgeld gegen das Unternehmen, bei dem der "Täter" arbeitet, möglich ist, wird nicht überraschen. Doch Vorsicht: Auch gegen den "Täter" persönlich kann ein Bußgeld fällig sein.

Ein aktueller Fall aus Bayern

Sie meinen, das gibt es nicht? Dann sollten Sie wissen, dass das Bayerische Landesamt für Datenschutzaufsicht (BayLDA) genau in einem solchen Fall ein Bußgeld gegen die "schuldige" Mitarbeiterin eines Unternehmens verhängt hat. Das ergibt sich aus einer Pressemitteilung vom 28. Juni 2013.

Wer beim E-Mail-Versand nicht aufpasst, kann schnell bis zu 1.000 Euro los sein (Bild: Thinkstock)

Die genaue Bußgeldhöhe nennt die Datenschutzaufsicht nicht

Wie hoch das Bußgeld genau ist, verrät die Datenschutzaufsicht nicht. Seine ungefähre Höhe lässt sich jedoch relativ leicht aus den allgemeinen Rechtsgrundsätzen für Bußgeldverfahren erschließen. Liest man lediglich die Bußgeldvorschrift des Bundesdatenschutzgesetzes (BDSG), könnte man dazu neigen, sogar den persönlichen Ruin zu fürchten. Demnach kann nämlich die unbefugte Übermittlung von Daten mit einer Geldbuße von bis zu 300.000 Euro geahndet werden.

Ein Betrag bis 1.000 Euro ist aber möglich

Im vorliegenden Fall ging es zwar um eine größere Menge von Adressen (neuneinhalb Seiten der insgesamt zehn Seiten der Mail bestanden aus Mailadressen), doch ist z.B. nichts davon berichtet, dass den Betroffenen besondere Nachteile entstanden sind. Zudem hat die "Täterin" offensichtlich "nur" fahrlässig und nicht vorsätzlich gehandelt. Außerdem muss die Aufsichtsbehörde berücksichtigen, was die Täterin verdient. Bezieht man zudem ein, welche Geldstrafen bei erheblichen Delikten wie etwa einer fahrlässigen Tötung verhängt werden, gelangt man zu dem Ergebnis, dass ein Bußgeld bis etwa 1.000 Euro in Betracht kommt.

Aber auch das ist sicher noch Grund genug, bei Mails künftig extrem vorsichtig zu sein!

Wann sind Daten "anonym"?

Vom Prinzip her ist alles klar: Datenschutzvorschriften müssen nur dann beachtet werden, wenn es um personenbezogene Daten geht. Sind Daten anonym, spielen die Vorschriften dagegen keine Rolle. Aber wo liegt die Grenze? Und welche Methoden gibt es, Daten zu anonymisieren?

"Personenbezogen" contra "anonym"

"Mit dem Datenschutz musst du aufpassen. Er befasst sich aber nur mit personenbezogenen Daten. Wenn Daten anonym sind, musst du dich nicht um Datenschutz kümmern."

Solche und ähnliche Ratschläge erhält so mancher Anfänger, wenn er Kolleginnen und Kollegen fragt, worauf er denn beim Umgang beispielsweise mit Kundendaten achten muss. Falsch ist der zitierte Ratschlag an sich nicht. In der Praxis führt er aber trotzdem oft in die Irre.

Weglassen des Namens - was bewirkt das?

Das zeigt sich, wenn man einmal den sehr beliebten Tipp näher betrachtet, einfach den Namen eines Betroffenen wegzulassen.

Angenommen, es wird eine Liste gebraucht, die nur zeigen soll, in welchen Orten es Kunden des Unternehmens gibt. Wenn dann nach dem Weglassen der Namen wirklich nur eine Liste mit Ortsnamen übrig bleibt, ist diese Liste tatsächlich anonym. Anders sähe es dagegen aus, wenn die Adressen der Kunden noch in der Liste blieben, denn mit ihrer Hilfe könnte man über das Internet bei nahezu allen Kunden sehr leicht den Namen feststellen.

Noch ein Begriff: Pseudonymisierung

Schon ein kurzer Blick in das Gesetz zeigt übrigens, dass das bloße Weglassen des Namens im Regelfall genau kein Anonymisieren ist. Dort ist nämlich (siehe § 3 Abs. 6a BDSG) die Rede davon, dass das Ersetzen des Namens und anderer Identifikationsmerkmale durch ein Kennzeichen lediglich als Pseudonymisieren gilt, nämlich als ein Vorgang, der den Zweck hat, die Bestimmung des Betroffenen auszuschließen oder wesentlich zu erschweren. Das ist weniger als ein echtes Anonymisieren.

Zwei Varianten der Anonymisierung

Die Ansprüche an ein Anonymisieren sind deutlich höher. Davon, dass eine Anonymisierung geglückt ist, spricht das Gesetz erst dann, wenn personenbezogene Daten so verändert werden, dass die Einzelangaben entweder überhaupt nicht mehr oder nur noch mit einem unverhältnismäßig großen Aufwand an Zeit, Kosten und Arbeitskraft einer Person zugeordnet werden können. So die Vorgabe in § 3 Absatz 6 BDSG.

Wann sind Daten tatsächlich anonym? Die Frage ist nicht ganz so leicht zu beantworten wie es zunächst scheint. (Bild: Thinkstock)

Falls eine Veränderung von Daten dazu führt, dass sich die dann verbleibenden Einzelangaben überhaupt keiner konkreten Person mehr zuordnen lassen, spricht man von einer "absoluten Anonymisierung".

Praxisbeispiele zur Anonymisierung

Wie schwer sie zu erreichen ist, zeigt folgendes Beispiel: Ein Mitarbeiter, der erst 28 Jahre alt ist, fünf Kinder hat und unverheiratet ist, muss nicht beim Namen genannt werden, damit zumindest viele im Unternehmen sofort wissen, um wen es sich handelt.

Fälle absoluter Anonymisierung liegen normalerweise nur vor, wenn am Ende rein statistische Daten übrig bleiben. So dürfte es bei einer Belegschaft von 1.000 Personen kaum möglich sein, die zahlreichen Personen zu identifizieren, die verheiratet sind und mindestens ein Kind haben.

Absolute Anonymisierung ist in der Praxis fast unmöglich

Berücksichtigt man dies, dann lässt sich als Faustregel sagen, dass eine absolute Anonymisierung in der Praxis normalerweise nur gelingt, wenn sie Fachleute durchführen, die über entsprechende Erfahrung verfügen. Der Laie übersieht normalerweise verschiedenste Möglichkeiten von Rückschlüssen, mit deren Hilfe eine Zuordnung zu konkreten Personen dann doch wieder möglich ist.

Scheinbar anonyme Befragungen

Diese Gefahr wird in der Praxis vor allem bei scheinbar "anonymen" Befragungen relevant. Man meint, schon durch das Weglassen von Namen und Anschrift sicherzustellen, dass die Befragung anonym erfolgt, und übersieht dabei, dass sich aus den anderen vorhandenen Angaben und deren Kombination oft zahlreiche Rückschlüsse ziehen lassen.

Die relative Anonymisierung

Denkbar ist es allerdings, dass der dafür erforderliche Aufwand unverhältnismäßig groß ist. Dann spricht man von einer "relativen Anonymisierung". Bei ihr wäre es zwar möglich, noch konkrete Personen herauszufinden, allerdings erst durch umfangreiche Maßnahmen. Ab wann ein solcher Aufwand unverhältnismäßig ist, lässt sich dabei natürlich nahezu endlos diskutieren.

In jedem Fall richtig: Datensparsamkeit

Hat es nach alledem überhaupt Sinn, beispielsweise Namen und Anschriften von Betroffenen wegzulassen, weil beides bei einer Zusammenstellung nicht benötigt wird?

Die Antwort lautet: auf jeden Fall! Denn selbst dann, wenn dadurch keine Anonymisierung erreicht wird, verwirklicht eine solche Maßnahme das Prinzip der Datensparsamkeit. Es verpflichtet dazu, so wenige personenbezogene Daten wie möglich zu erheben, zu verarbeiten und zu nutzen, und ist inzwischen in § 3a BDSG ausdrücklich als Pflicht festgelegt.

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

Die E-Mail-Verschlüsselung reicht nicht

Die mobile Kommunikation mit Smartphones ist zwar extrem beliebt, aber keineswegs sicher. Erst verschiedene Zusatzmaßnahmen können verhindern, dass die mobile Datenverbindung belauscht wird.

Smartphones als Kommunikationszentrale

49 Prozent der Smartphone-Besitzer älter als 14 Jahre nutzen ihr mobiles Endgerät stets und überall. Bei den 20- bis 29-Jährigen sind es sogar 67 Prozent, so eine von TNS Infratest gemeinsam mit dem Bundesverband Digitale Wirtschaft (BVDW) e.V. durchgeführte Studie.

Ein wesentlicher Grund ist die ständige Erreichbarkeit, die damit sichergestellt ist. Schließlich kann man mit einem Smartphone nicht nur telefonieren, sondern auch E-Mails austauschen, Videotelefonate durchführen und über soziale Netzwerke kommunizieren.

Vorsicht, Lauschangriff

Genutzt werden die Smartphones als Beifahrer im Auto (74 Prozent), an Bahnhöfen oder Haltestellen (70 Prozent), innerhalb der öffentlichen Verkehrsmittel (65 Prozent), im Restaurant (65 Prozent), beim Einkaufen (60 Prozent) und natürlich auch am Arbeitsplatz (61 Prozent). Keine Frage, wenn man bei diesen Gelegenheiten vertrauliche Gespräche führen will, sind Mithörer nicht ausgeschlossen. Aber es gibt auch andere Formen von Lauschangriffen.

Auch mobile E-Mail ist gefährdet

Was vielen Nutzern nicht wirklich klar ist: Smartphones haben nicht nur die gleichen Funktionen wie ein Mini-Computer, sie unterliegen auch den gleichen Risiken. So können Unbefugte selbstverständlich auch die E-Mails, die über Smartphones verschickt oder empfangen werden, abfangen und einsehen, wenn es keine Verschlüsselung gibt.

Ohne besondere Sicherheitsmaßnahmen lassen sich E-Mails und Gespräche leicht mitlesen bzw. mithören (Bild: Thinkstock)

Für die gespeicherten E-Mails besteht bei Smartphones ohne Verschlüsselung sogar noch eine zusätzliche Gefahr: Mobile Endgeräte gehen leichter verloren und können einfacher gestohlen werden. Die gespeicherten E-Mails sind dem Dieb oder unehrlichen Finder dann schutzlos ausgeliefert.

Handy-Telefonate sind doch sicher, oder?

Selbst wenn Sie für Ihr Smartphone eine spezielle App nutzen, mit der Sie Ihre E-Mails verschlüsseln, ist die mobile Kommunikation nicht sicher: Von einer sicheren Kommunikation kann nur die Rede sein, wenn alle Kommunikationswege geschützt werden - und zwar wirklich alle.

Nun werden Sie vielleicht sagen: Ich nutze bislang nur E-Mails mit dem Smartphone, und ich telefoniere natürlich damit. Aber die Telefonate können ja nicht abgehört werden, oder etwa doch?

Auch Telefonate könnten angezapft werden

Vielen ist es nicht bewusst: Ohne zusätzliche Sicherheitsmaßnahmen können auch Handy-Telefonate belauscht werden, nicht nur akustisch in der direkten Umgebung, sondern auch elektronisch. Keine Form der mobilen Kommunikation mit dem Smartphone ist ohne Weiteres abhörsicher. Wenn keine Verschlüsselung vorgesehen ist, lassen sich mobile Telefonate, mobile E-Mails, mobile Chat-Dienste und mobile Videotelefonate komplett abhören.

Vertrauliche Kommunikation braucht immer Verschlüsselung

Wenn Sie also mit Ihrem Smartphone vertrauliche Daten austauschen oder vertrauliche Gespräche führen, achten Sie nicht nur darauf, dass Sie niemand belauschen kann, der neben Ihnen steht. Es reicht nicht, in einen benachbarten Raum zu gehen, um ungestört und ungehört telefonieren zu können.

Fragen Sie sich stets:

Welche Kommunikationsdienste nutze ich mit dem Smartphone?

Was kommuniziere ich jeweils darüber? Sind auch vertrauliche Informationen darunter, wie persönliche Daten, Angebote, Vertragsdetails oder Projektinhalte?

Sind meine mobilen Telefonate vertraulich? Wäre ein erfolgreicher Lauschangriff eine Gefahr?

Sind die Inhalte meiner mobilen E-Mails vertraulich?

Sind die Inhalte meiner SMS oder MMS vertraulich?

Haben die mobilen Chats einen vertraulichen Charakter?

Nutze ich Videotelefonie für eine vertrauliche Kommunikation?

Speichere ich vertrauliche Daten auf meinem Smartphone?

Wenn das private Smartphone betrieblich genutzt wird: Verfügt auch das private Smartphone über Verschlüsselungsfunktionen?

Klären Sie den Schutzbedarf

Wenn Sie das Gefühl haben, dass Ihre Kommunikation über das Smartphone besser geschützt werden sollte, weil Sie zum Beispiel keine Verschlüsselung nutzen können, sprechen Sie mit Ihrem Datenschutzbeauftragten. Wenn Sie Ihr privates Smartphone zu betrieblichen Zwecken nutzen, sollten Sie ebenfalls klären, wie sich die Kommunikation darüber besser absichern lässt.

Suchen Sie nicht selbst nach einer scheinbar passenden Sicherheitslösung, sondern fragen Sie im Unternehmen nach. Viele der Sicherheitslösungen für Privatpersonen reichen für die Sicherheitsanforderungen eines Unternehmens nicht aus.

Browser-Tools: Zusatznutzen oder Zusatzrisiko?

Webbrowser stecken bereits im Standardumfang voller Zusatzfunktionen. Zusätzliche Werkzeuge lassen sich leicht installieren. Damit steigt aber nicht nur der Leistungsumfang, sondern auch das mögliche Datenrisiko.

Weit mehr als Adresszeile und Browserfenster

Haben Sie sich Ihren Webbrowser auf dem Arbeitsplatz-PC oder Ihrem Privat-PC einmal genau angesehen? Kennen Sie alle Funktionen Ihres Browsers? Sicherlich nicht.

Das ist nicht verwunderlich, denn Webbrowser sind inzwischen sehr umfangreiche Softwarelösungen geworden. Dabei würde es für die Hauptaufgabe, die Anzeige von Internetseiten, durchaus reichen, wenn es eine Zeile gäbe, in die Sie die Internetadresse eintragen können, und ein Fenster, das die gewünschte Webseite darstellt.

Mehr Komfort, aber auch mehr Sicherheit?

Ein Blick auf Ihren Webbrowser zeigt Ihnen, dass er ein umfangreiches Funktionsmenü hat, wo sich zum Beispiel die für den Datenschutz so wichtigen Einstellungen wie das Cookie-Management befinden. Rechts neben der eigentlichen Adresszeile finden Sie aber beispielsweise beim Firefox-Browser ein weiteres Eingabefeld. Dort können Sie etwa Suchmaschinen oder Online-Shops auswählen, bei denen Sie eine Suche starten wollen, ohne die entsprechende Webseite über die Adresszeile anzusteuern.

Klingt komfortabel, da es eine Abkürzung ist. Doch die zusätzlichen Browser-Werkzeuge können es in sich haben.

Bewertung von Webseiten als Zusatzdienst

Eine häufige Zusatzfunktion, die Browser-Tools bieten, ist die Analyse der gerade besuchten Webseite. Je nach dem im Browser nachinstallierten Werkzeug kann die Bewertung Aussagen zur Beliebtheit einer Webseite machen, also den Besucherrang einer Webseite angeben. Oder aber die Sicherheit der Webseite wird untersucht, ob sich darauf etwa schädliche Links befinden. Eigentlich eine tolle Sache, werden Sie jetzt denken.

Tracking oder hilfreicher Service?

Allerdings sollten Sie genau überlegen, was da geschieht: Damit ein Browser-Werkzeug jede von Ihnen besuchte Webseite bewerten kann, muss das Tool auch von jeder Internetaktivität mit dem Browser wissen. Erschwerend kommt hinzu, dass die Bewertung nicht etwa innerhalb Ihres Webbrowsers erfolgt, sondern mittels Online-Verbindung beim Tool-Anbieter. Letztlich könnte also der Tool-Anbieter über alle Webseiten informiert werden, die Sie besuchen - der absolute Wunschzustand für die Werbeindustrie beim Online-Tracking.

Tools nicht wahllos installieren

Stellen Sie sich vor, der Tool-Anbieter ist unseriös und verkauft Ihre Tracking-Daten. Industriespione zum Beispiel könnten mit entsprechenden Daten eines Firmen-Internet-PCs genau sehen, welche Recherchen in Ihrem Betrieb laufen. Datendiebe könnten den gefährlichen Umstand nutzen, dass manche Webseiten, die eine Anmeldung erfordern, die Anmeldedaten ungeschützt in der aufgerufenen Webadresse transportieren. Der Diebstahl von Firmengeheimnissen könnte so ebenso möglich werden wie der Diebstahl Ihrer Online-Identität.

Deshalb sollten Sie kein Tool ungeprüft in die sogenannte Toolbar Ihres Browsers aufnehmen. Vorsicht ist auch geboten, wenn Sie eine Software installieren wollen und plötzlich ein Browser-Tool als Dreingabe angeboten wird.

Diese Punkte sollten Sie stets hinterfragen

Bevor Sie also Ihren Browser mit neuen Werkzeugen wie zusätzlichen Suchfeldern, Buttons als Abkürzung zu einem Online-Dienst oder Bewertungsdiensten bestücken, prüfen Sie:

1) Ist das Tool kostenlos? Wenn ja, wie finanziert es sich (Datennutzung für Werbung?)?
2) Welche Angaben sollen Sie bei der Registrierung machen, wenn eine vorgesehen ist?
3) Ist das Browser-Tool online mit dem Anbieter verbunden? (Tipp: Tools mit Online-Verbindung zum Anbieter erzeugen in der Regel eine Fehlermeldung, wenn man sie offline nutzen möchte.)
4) Was sagt die Datenschutzerklärung zur Sammlung, Nutzung und Weitergabe der Daten?
5) Können Sie das Tool problemlos wieder deinstallieren?

Wenn Sie unsicher sind, fragen Sie lieber Ihren Datenschutzbeauftragten!

Ist Ihr Webbrowser sicher? Testen Sie Ihr Wissen!

Frage: Ihr Webbrowser bietet zwei Eingabezeilen im Menübereich, eine größere und eine kleinere. Gibt es da Unterschiede?

a) Das kann ich so nicht sagen. Aber es lohnt sich, diese Eingabezeilen genauer anzusehen.
b) Nein, das ist reine Geschmackssache. Für kurze Webadressen reicht sicherlich die kurze Eingabezeile.

Lösung: Die Antwort a) ist richtig. Es ist nicht zu erwarten, dass zwei Werkzeuge im Browser die gleiche Funktion haben. Deshalb sollten Sie kein Browser-Tool nutzen, ohne sich die Funktion klargemacht zu machen.

Frage: Ihr Browser hat auf der rechten Seite des Menübereichs einen Statusbalken, der etwas zu der geöffneten Webseite aussagt. Wie gehen Sie vor?

a) Solange ich den Statusbalken nicht brauche, mache ich gar nichts.
b) Ich frage meinen Systemadministrator und den Datenschutzbeauftragten, wenn ich über die Funktion des Balkens im Unklaren bin.

Lösung: Die Antwort b) ist richtig. Eine Bewertung der geöffneten Webseite bedeutet in aller Regel, dass die von Ihnen besuchten Internetadressen an einen Dritten übertragen werden. Ob dies für den Datenschutz kritisch ist, sollten Sie mit dem Systemadministrator und dem Datenschutzbeauftragten klären.