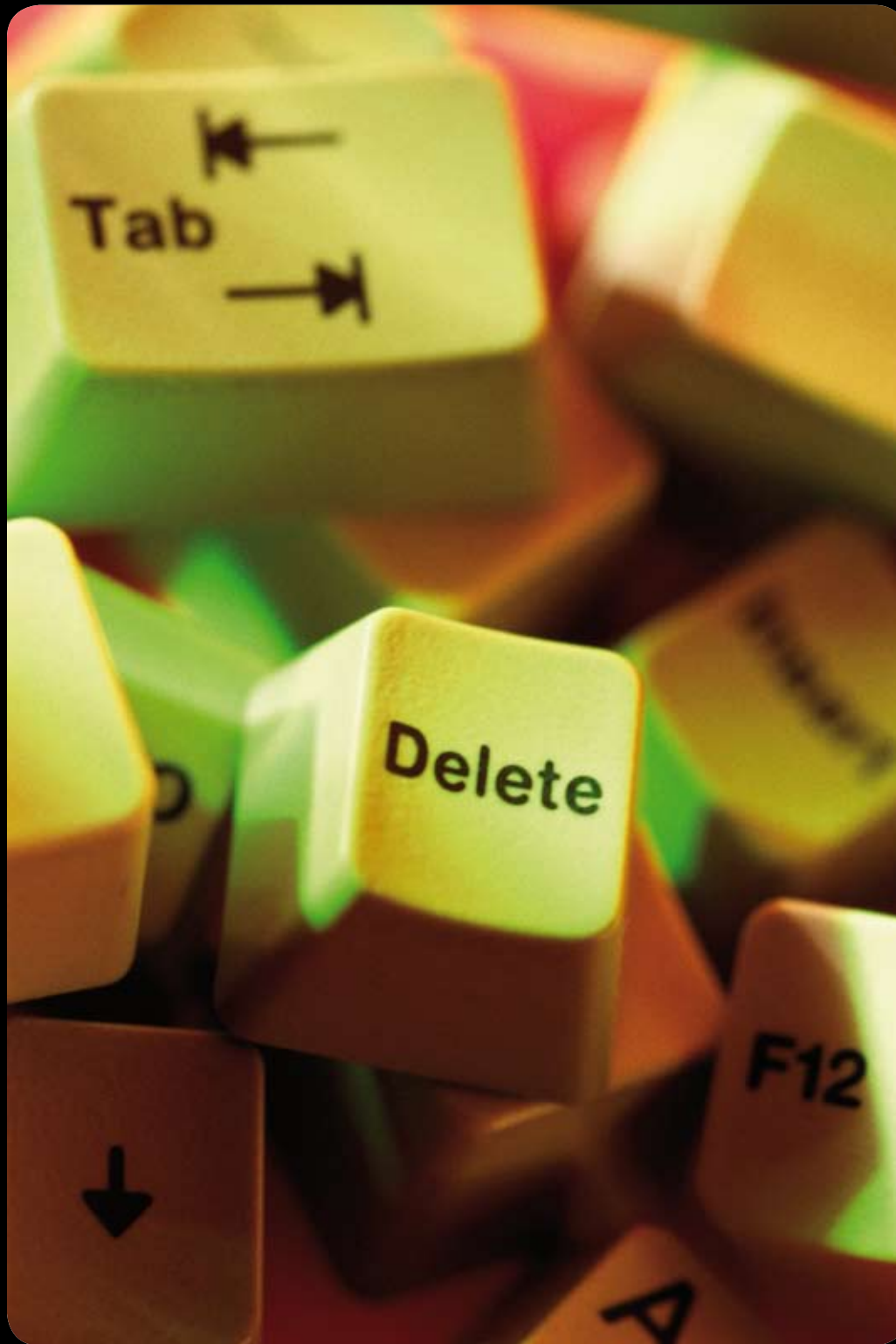


Datenschutz newsbox



Ausgabe

7

07/2010

Google Analytics entschärft	2
Neuaufgabe der BfDI-Info „Die Datenschutzbeauftragten in Behörde und Betrieb“	3
Gemeinsame Studie des BSI und der ASW zur IT-Gefährdungslage bei KMU	3
3. GDD-Sommer-Workshop	3
GDD Privacy Panel - Erste Ergebnisse	4

Innenministerium veröffentlicht Studie zu Identitätsdiebstahl	5
Online-Werbung und Datenschutz	5
Data-Mining als digitale „Glaskugel“	5
Ist datenschutzkonformes Cloud-Computing möglich ?	6
Microsoft errichtet Meldestelle für gestohlene Zugangsdaten	6

Umfrage „IT-Sicherheitsstandards und IT-Compliance 2010“	7
Kryptografische Absicherung des DNS	7
Der Bundesinnenminister hält Grundsatzrede zur Internetpolitik	7
Quick Freeze datenschutzfreundlicher als Vorratsdatenspeicherung	8
Neuerscheinung: Praxishilfe zur BDSG-Novelle II (2009)	8



Editorial:

Das Sommerloch ist eine Bezeichnung der Massenmedien, besonders der Tagespresse und der Nachrichtenagenturen, für eine nachrichtenarme Zeit, die vor allem durch die Sommerpause der politischen Institutionen und Sport-Ligen ferner auch der kulturellen Einrichtungen bedingt ist.

Ob auch in der Welt des Datenschutzes dieses Jahr ein solches Sommerloch zu erwarten ist, kann angesichts der zahlreichen Ereignisse im Bereich des Datenschutzes getrost bezweifelt werden. So taugen die Anzahl der Pressemeldungen des Bundesbeauftragten für den Datenschutz und die Informationsfreiheit, die Meldungen der Nachrichtenagenturen zum Thema Datenschutz sowie die rege Aktivität auf dem Datenschutz-Forum des BfDI als verlässlicher Indikator dafür, wie der kollektive Puls der Datenschutz-Welt im Moment schlägt.

Nach diesem Puls zu urteilen, sieht es eher danach aus, dass dies ein heißer Sommer wird...hoffentlich auch, was die Temperaturen angeht, wünscht Ihr

RA Levent Ferik
Gesellschaft für Datenschutz und
Datensicherheit e.V.

Google Analytics entschärft

Google kämpft im Moment an vielen Fronten und ist bestrebt verloren gegangenes Vertrauen bei seinen Nutzern wieder gut zu machen. Dabei steht nicht nur der Dienst Google Street View im Fokus der Medien und der Datenschutz-Aufsichtsbehörden, sondern auch der Webanalysedienst Google Analytics.

Google Analytics ist ein leistungsfähiges Werkzeug, das Webmaster kostenlos auf ihren Seiten einbinden können, um die Zugriffe zu analysieren. Google Analytics identifiziert dabei Ein- und Ausstiegspunkte, erstellt Statistiken und verzeichnet die Anfragen auf einer Landkarte. Dabei gibt der Webmaster jedoch sehr viele Informationen an Google weiter.

Bereits Ende 2009 forderten die obersten Datenschutz-Aufsichtsbehörden, dass Websurfer zumindest eine Möglichkeit bekommen müssen, der Erfassung durch Google Analytics zu widersprechen. Es scheint so, dass Google eben dieses „Opt-out“ offensichtlich nun umsetzen möchte und zwar in Form einer Browser-Erweiterung.

Die Erweiterung soll verhindern, dass der Browser den Google Analytics-Code ausführt. Nach Installation der Erweiterung soll Google keinerlei Daten beim Aufruf der Seite erhalten. Allerdings erfährt Google allein durch den Skript-Download trotzdem von jedem Aufruf der betreffenden Seiten, sodass herkömmliche Werbe- und Skriptblocker die Privatsphäre zuverlässiger schützen.

Der Dienst erfährt aber nicht nur auf Seiten der Seitenbesucher eine Entschärfung. Auch für die Betreiber der Webserver, auf denen der Dienst läuft, gibt es eine neue Möglichkeit, der von den Aufsichtsbehörden geforderten Rechtskonformität zumindest ein wenig mehr entgegen zukommen.

Webmaster können bei der Implementierung künftig „IP-Masking“ aktivieren. Dabei verspricht Google, vor jeder weiteren Verarbeitung der anfragenden IP-Adresse die letzten 8 Bit zu löschen. Seitenbetreiber haben damit die Möglichkeit Google Analytics ergänzt um den Code „_anonymizelp()“ und angepasster Datenschutzerklärung einzusetzen.

Ob diese neue Funktion allein dazu führen wird, die Nutzung von Google Analytics als zulässig zu erachten, werden zukünftige Aussagen der Aufsichtsbehörden zum Thema Google Analytics hoffentlich klären. Festhalten lässt sich jedoch jetzt schon, dass der Google-Analytics-Konkurrent eTracker, dem der Hamburgische Datenschutzbeauftragte bereits vor geraumer Zeit eine BDSG-konforme Funktionalität bescheinigt hat, eine ähnliche Funktionsweise besitzt.

Quelle: Heise Online

Neuaufgabe der BfDI-Info „Die Datenschutzbeauftragten in Behörde und Betrieb“

Der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit hat seine Broschüre Info 4 „Die Datenschutzbeauftragten in Behörde und Betrieb“, die die wichtigsten Rechtsvorschriften für interne Datenschutzbeauftragte vorstellt und praktische Hinweise gibt, neu aufgelegt.

In der Neuaufgabe (Stand: Mai 2010) sind die mit der BDSG-Novelle im September 2009 in Kraft getretenen Regelungen berücksichtigt.

Die Position und Unabhängigkeit des Datenschutzbeauftragten ist nunmehr durch einen verbesserten Kündigungsschutz deutlich gestärkt worden. Eine Kündigung ist nur zulässig, wenn Tatsachen vorliegen, die zur Kündigung aus wichtigem Grund ohne Einhaltung einer Kündigungsfrist berechtigen. Das gleiche gilt für den Zeitraum eines Jahres nach Beendigung der Bestellung zum Beauftragten für den Datenschutz.

Gesetzlich geregelt ist jetzt auch, dass die Behörden beziehungsweise Betriebe dem Beauftragten für den Datenschutz zur Erhaltung seiner erforderlichen Fachkunde die Teilnahme an Fort- und Weiterbildungsveranstaltungen zu ermöglichen und deren Kosten zu übernehmen haben.

In Zukunft werden die Bedeutung und die Aufgabe der internen Datenschutzbeauftragten noch weiter wachsen, weil funktionierender Datenschutz und bürger- beziehungsweise kundenfreundliche Verfahren immer wichtiger werden und sich im nicht-öffentlichen Bereich zu einem Wettbewerbsvorteil entwickeln.

Zu den Hauptaufgaben des Datenschutzbeauftragten gehört die Überwachung der Einhaltung der Datenschutzvorschriften von der Erhebung der Daten, über die Institutionalisierung von Unterrichtungspflichten gegenüber Betroffenen bis hin zur ordnungsgemäßen Beachtung von Lösungsfristen. Wichtiges Ziel ist die Schaffung von Transparenz in der Datenverarbeitung.

Besonders zu erwähnen ist in diesem Zusammenhang die seit September 2009 geltende Verpflichtung für nicht-öffentliche Stellen, die Aufsichtsbehörde und die Betroffenen bei Datenschutzpannen unverzüglich zu benachrichtigen. Der Gesetzgeber hat in der amtlichen Begründung zu der Gesetzesänderung ausdrücklich darauf hingewiesen, dass der betriebliche Datenschutzbeauftragte bei Ermittlung von Datenschutzpannen und deren Bewältigung beteiligt werden muss.

Quelle: Webseite des Bundesbeauftragten für den Datenschutz und die Informationsfreiheit (BfDI)

Gemeinsame Studie des BSI und der ASW zur IT-Gefährdungslage bei KMU

Das Bundesamt für Sicherheit in der Informationstechnik (BSI) und die Arbeitsgemeinschaft für Sicherheit der Wirtschaft e.V. (ASW) wollen gemeinsam eine Studie durchführen, um die IT-Gefährdungslage bei kleinen und mittleren Unternehmen (KMU) zu ermitteln. Auf Grundlage von Interviews mit Geschäftsführung und Systemadministratoren „vor Ort“ wird der Bedarf an Sensibilisierung, Beratung und Schutz von sicherheitskritischen technologieorientierten Unternehmen festgestellt, auf Wunsch werden konkrete Empfehlungen an die KMU für IT-Sicherheitsmaßnahmen gegeben. Der Aufwand in den Unternehmen für Vorbereitung, Durchführung und Nachbereitung wird bei ca. drei Arbeitstagen liegen. Die Studie wird nur durchgeführt, wenn sie auf ausreichendes Interesse bei Unternehmen stößt. Weitere Informationen finden Sie unter nachfolgender Adresse:

Quelle: Kurzmitteilungen des BSI

3. GDD-Sommer-Workshop am 2. – 4. August 2010 in Timmendorfer Strand

Für Datenschutzbeauftragte und -berater sowie Datenschutzdienstleister findet am 2. – 4. August 2010 in Timmendorfer Strand der 3. GDD-Sommer-Workshop statt.

Die GDD-Sommer-Akademie bietet zugleich den Nachweis der gem. § 4f BDSG geforderten gesetzlichen Fachkunde gegenüber den jeweiligen Auftraggebern, Arbeitgebern und den Aufsichtsbehörden.

Das vollständige Seminar-Programm finden Sie auf der DATAKONTEXT-Homepage.

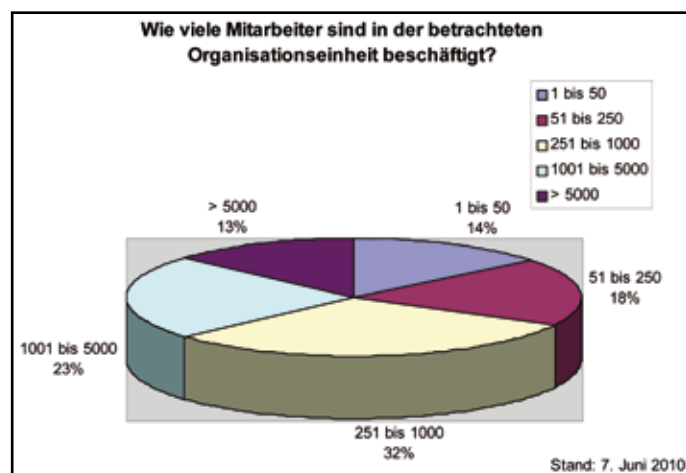
GDD Privacy Panel – Erste Ergebnisse

Nachdem die **GDD** im Jahre 1996 erstmals eine breit angelegte Umfrage zur Datenschutzpraxis und zur Stellung des Datenschutzes durchgeführt hat und diese Studie im Jahre 2004 wiederholt hat, um den zwischen diesen Jahren erheblich veränderten gesetzlichen Rahmenbedingungen für Unternehmen und Behörden bzw. für die Datenschutzbeauftragten Rechnung zu tragen, ist die **GDD** in diesem Jahr dazu übergegangen, diese Umfrage online durchzuführen und mit weiteren umfangreichen webbasierten Auswertungsmöglichkeiten auszustatten.

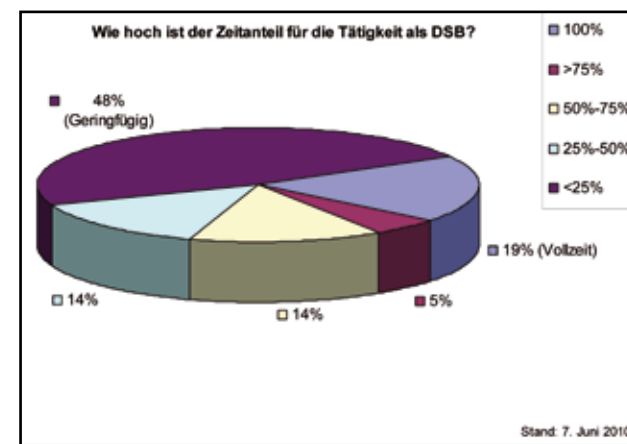
Der sog. Ersterhebungszeitraum des am Anfang März 2010 gestarteten **GDD** Privacy Panels endete am 3. Mai 2010. Seit Abschluss der Ersterhebungsphase haben die Teilnehmer die Möglichkeit die Ergebnisse der Datenschutzumfrage einzusehen. Dabei können sich die Teilnehmer nach von Ihnen auswählbaren Kriterien die Ergebnisse der Umfragen anzeigen und diese grafisch darstellen lassen. Sowohl die Teilnahme am **GDD** Privacy Panel, als auch die Nutzung der Auswertungsmöglichkeit steht allen Interessierten ganzjährig zur Verfügung.

Schon jetzt lassen sich aus den Ergebnissen der Umfrage Erkenntnisse hinsichtlich des Standes der Aufgaben und der Stellung des Datenschutzbeauftragten in der betrieblichen oder behördlichen Praxis gewinnen.

Bislang haben sich 197 Datenschutzbeauftragte bzw. –verantwortliche am **GDD** Privacy Panel beteiligt. Bereits bei der prozentualen Beteiligung der Teilnehmer ist zu erkennen, dass die Zahl der teilnehmenden Unternehmen mit einer Mitarbeiteranzahl <50 Mitarbeiter im Vergleich zum Jahre 2004 zugenommen hat. Waren im Jahre 2004 bloß 8% der Unternehmen mit einer Mitarbeiteranzahl von <50 MA unter den Teilnehmern, sind es nun 14%. Diese Auffälligkeit kann damit erklärt werden, dass das Thema Datenschutz immer mehr auch von kleineren Unternehmen als Qualitäts- und Wettbewerbsfaktor betrachtet wird.



Umgekehrt lassen jedoch die Ergebnisse zum Zeitbudget des Datenschutzbeauftragten und der Frage, ob der Datenschutzbeauftragte so rechtzeitig über neue Verfahren informiert wird, dass er seiner Pflicht zur Vorabkontrolle nachkommen kann, Rückschlüsse darauf zu, wo die Unternehmen noch Optimierungsbedarf haben. So üben nur 19% der Datenschutzbeauftragten ihre Tätigkeit in Vollzeit aus und nur 7, 6% geben an, dass sie so rechtzeitig in neue Verfahren im Unternehmen eingeweiht werden, so dass sie eine Möglichkeit zur Vorabkontrolle haben.



Auffällig ist auch, dass zwischen Wunsch und Wirklichkeit auch beim Thema Datenschutz oft eine große Lücke klafft.

44% der Datenschutzbeauftragten beantworten die Frage „Wie wichtig ist die formelle Verankerung des Datenschutzes für einen funktionierenden Datenschutz in Ihrem Unternehmen Ihrer Meinung nach“ mit der Antwortoption: „Sehr wichtig“.

Leider können in einer Nachfolgefrage nur 15% bestätigen, dass der Datenschutz auch tatsächlich im Unternehmen optimal verankert ist.

Alle Ergebnisse der Datenschutzumfrage können Sie sich als Teilnehmer des **GDD** Privacy Panel unter der Rubrik „Reports“ anzeigen lassen. Wer sich bislang nicht für das **GDD** Privacy Panel angemeldet hat, kann dies unter <https://www.gdd.de/gdd-privacy-panel-1> nachholen. Dort finden sich auch weitere Informationen zum Panel.

Innenministerium veröffentlicht Studie zu Identitätsdiebstahl

Auf Initiative des Bundesministeriums des Innern (BMI) und im Auftrag des Bundesamtes für Sicherheit in der Informationstechnik (BSI) haben führende deutsche Experten eine interdisziplinäre Studie mit dem Titel „Identitätsdiebstahl und Identitätsmissbrauch im Internet – Rechtliche und technische Aspekte“ erstellt.

Die Autoren der Studie sind Prof. Dr. Georg Borges von der Ruhr-Universität Bochum und Prof. Dr. Carl-Friedrich Stuckenberg von der Universität des Saarlandes sowie Prof. Dr. Jörg Schwenk und Dr. Christoph Wegener (beide von der Ruhr-Universität Bochum).

Die Studie führt aus, inwiefern Identitätsdiebstahl und Identitätsmissbrauch heute die Sicherheit von E-Government und E-Business bedrohen. Sie nimmt darüber hinaus eine detaillierte Bewertung des geltenden Rechts in Bezug auf Identitätsdiebstahl vor und zeigt sowohl bereits erzielte Erfolge als auch neue Lösungsansätze und offene Fragen im Kampf gegen Diebstahl und Handel von digitalen Identitäten auf.

Die Studie zeigt auch auf, dass sich die Vorgehensweise der Täter in den letzten Jahren geändert hat: Die Schadprogramme gelangen heute vorwiegend durch Schwachstellen im Betriebssystem beziehungsweise in Softwarepaketen auf die Nutzer-PCs. 2009 wurden die meisten Sys-

teme durch den bloßen Besuch von Internetseiten („Drive-by Infection“) und präparierte PDF-Dokumente angegriffen. Als Gegenmaßnahmen schlagen die Autoren Standardsicherheitsmaßnahmen (Virenschutzprogramme, Firewall sowie regelmäßige Updates des Betriebssystems und der Anwendungen) vor. Notwendig sei zudem eine umfassende Aufklärung der Internetnutzer. Für die Zukunft prognostiziert das BMI, dass Identitätsdiebstahl und -missbrauch noch nicht absehbare Formen annehmen werden, da neue Techniken und Plattformen immer neue Angriffsszenarien ermöglichen.

Quelle: ZDNet

Online-Werbung und Datenschutz

Die Artikel 29-Gruppe der europäischen Datenschutzbeauftragten hat eine Stellungnahme zu den datenschutzrechtlichen Anforderungen für Werbe-Netzwerke und Anbieter von Internetseiten veröffentlicht („Online Behavioural Advertising“). Hauptkritikpunkt in der Stellungnahme ist, dass die Online-Werbung vielfach nicht den Vorgaben des europäischen Datenschutzrechts entspricht.

Der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit, Peter Schaar, der Mitglied der Art. 29-Gruppe ist, erklärt hierzu: „Leider werden die europarechtlichen Vorgaben beim „behavioural advertising“ häufig nicht beachtet. Dies gilt insbesondere für die Vorgabe, dass cookies nur mit ausdrücklicher Einwilligung des Nutzers auf dessen Rechner abgelegt werden dürfen. Auch die Information über die Sammlung von Nutzerdaten ist häufig mangelhaft. Wir haben deshalb in unserer Stellungnahme die einschlägigen datenschutzrechtlichen Anforderungen klargestellt. Unser Papier soll helfen, Online-Werbung und Datenschutz in Einklang zu bringen. Die Datenschutzbehörden werden europaweit verstärkt darauf achten, dass die datenschutzrechtlichen Vorgaben eingehalten werden.“

Quelle: Webseite der Europäischen Kommission
und Webseite des BfDI

Data-Mining als digitale „Glaskugel“

Nach Einschätzung von Data-Mining-Experten lässt sich mit einer Verknüpfung vieler Einzelinformationen sogar eine Scheidung oder Trennung eines Nutzers vorhersagen.

Im Bereich des Data-Minings existieren Vorhersagemodelle, die das Risiko für Zahlungsausfälle aufgrund von demografischen Daten vorhersagen. Besitzt man Informationen über Alter, Wohnort, Beruf und Kinder, vergleicht man diese mit den Daten von Personen, die in einer ähnlichen Situation sind und schaut, wie oft in diesem Personenkreis die Zahlungen ausgefallen sind. Diese Daten stammen oftmals von Datenhändlern, die diese zum Verkauf anbieten. Es geht hier also nicht um Esoterik oder den Blick in die Glaskugel zum Vergnügen, sondern um die Erstellung möglichst genauer Kundenprofile zwecks Gewinnsteigerung.

Weitere interessante Details über diesen Geschäftsbereich verrät der Artikel unter nachfolgender Adresse.

Quelle: Zeit.de

Ist datenschutzkonformes Cloud-Computing möglich?

Nach Ansicht des Schleswig-Holsteinischen Landesdatenschützers Thilo Weichert sind personenbezogene Daten beim Cloud-Computing nicht sicher.

Derzeit bestehende Cloud-Angebote seien fast durchgängig mit dem geltenden Datenschutzrecht nicht vereinbar, sagte Thilo Weichert auf dem 4. Österreichischen IT-Rechtstag in Wien. Cloud-Computing, bei privaten Nutzern wie in Wirtschaftsunternehmen immer verbreiteter, sei generell unzulässig, wenn außerhalb der Europäischen Union personenbezogene Daten verarbeitet würden, so Weichert. Aber auch bei innereuropäischen Angeboten würden die organisatorischen und technischen Sicherheitsmaßnahmen und die Ressourcenanbieter nicht hinreichend transparent gemacht. Weichert: „Zwar spielen Integrität und Vertraulichkeit auf dem Cloud-Markt

heute eine Rolle, doch für die Anwender bleibt die Cloud eine Black Box, die ihnen die Wahrnehmung ihrer Verantwortung unmöglich macht. Wer heute in einer Public Cloud Personendaten verarbeitet, handelt regelmäßig unverantwortlich und rechtswidrig.“

Auch der Berliner Datenschutzbeauftragte Alexander Dix geht in seinem aktuellen Jahresbericht (Seite 14 ff.) davon aus, dass die Verarbeitung von Personendaten, die außerhalb der EU stattfindet laut dem deutschen Datenschutzrecht nicht zulässig sein kann. Insbesondere, wenn es um den Schutz von sensiblen Daten gehe, sei es unumgänglich zu wissen, wo diese gespeichert werden und wer darauf zugreifen kann.

Nach der Bewertung des Landesdatenschützers seien beim Cloud-Computing datenschutzkonforme Lösungen technisch und vertraglich möglich; diese wür-

den aber bislang nicht praktiziert. Weitere wichtige Details und welche Anforderungen an ein datenschutzkonformes Cloud-Computing zu stellen sind, können Sie dem aktuellen Tätigkeitsbericht (http://www.datenschutz-berlin.de/attachments/669/Jahresbericht_2009.pdf?1269595949) des Berliner Beauftragten für den Datenschutz und Informationsfreiheit entnehmen (Seite 14 ff.)

Beachten Sie in diese in diesem Zusammenhang auch die Veröffentlichung eines Leitfadens (http://www.bitkom.org/de/themen/36129_61111.aspx) zum Thema Cloud-Computing durch den Bundesverband Informationswirtschaft, Telekommunikation und neue Medien e.V. (BITKOM).

Quelle: Webseite Infolaw – Forschungsverein für Informationsrecht und Immaterialgüterrecht

Microsoft errichtet Meldestelle für gestohlene Zugangsdaten

Je nach Einzelfall kann es vorkommen, dass man im Internet auf Listen stößt, die zahlreiche gestohlene Daten enthalten, etwa Kreditkartendaten, eBay- und Bankzugangsdaten und dergleichen. Sicherheitsspezialisten, entdecken dieser Arten von Daten beruflich bedingt, oft auf sogenannten Drop Zones, d.h. auf manipulierten Servern, in denen Trojaner ausgespähte Daten abgelegt haben.

Für diese Fälle hat Microsoft in Kooperation mit mehreren US-amerikanischen Organisationen und Unternehmen eine neue Sicherheitsinitiative vorgestellt. Mit der „Internet Fraud Alert“ genannte Meldestelle soll der Diebstahl von persönlichen Daten bekämpft werden.

Die Meldestelle soll als zentraler Anlaufpunkt für Sicherheitsspezialisten, Internet Provider, Behörden und andere dienen, um im Internet entdeckte, gestohlene Daten wie Nutzernamen, Passwörter und Kreditkartennummern zu melden. Die Meldestelle will dann die betroffenen Unternehmen informieren, damit diese entsprechende Gegenmaßnahmen ergreifen und ihre Kunden informieren können. Handlungsbedarf sieht Microsoft in diesem Bereich, da es sich bislang als schwierig erwies, die Informationen über gestohlene Daten an den Richtigen weiterzuleiten.

Quelle: Spiegel.de und Microsoft.com

Umfrage „IT-Sicherheitsstandards und IT-Compliance 2010“

Secumedia führt zusammen mit ibi research (Universität Regensburg) eine Umfrage zum Einsatz von IT-Sicherheitsstandards und zu Compliance-Management in Behörden und Unternehmen durch. Betrachtet werden Standards bzw. IT-Frameworks wie IT-Grundschutz, ISO/IEC 27001/2 oder CobiT, die in vielen Institutionen zur Verbesserung der Informationssicherheit, zur Prozessoptimierung

und/oder zur Sicherstellung der IT-Compliance-Konformität eingesetzt werden. Eine zahlreiche Teilnahme an der Umfrage trägt dazu bei, den Status Quo hinsichtlich der Verwendung und Verbreitung von Standards bzw. IT-Frameworks zu ermitteln, Verbesserungspotenziale aufzudecken, sowie die vorhandene IT-Unterstützung zu analysieren. Die Umfrageresultate werden auf dem

BSI-Grundschutz-Tag am 20.10.2010 im Rahmen der IT-Sicherheitsmesse it-sa in Nürnberg vorgestellt. Die Umfrage wird online ab dem 10.5. bis zum 15.7.2010 durchgeführt, Startpunkt ist <http://www.grundschutz.info/studie>

Quelle: Bundesamt für Sicherheit in der Informationstechnik

Kryptografische Absicherung des DNS

Die Public Internet Registry (PIR) hat auf dem 38. Treffen der Internet Corporation for Assigned Names and Numbers (ICANN) in Brüssel verkündet, ab sofort von jedem signierte Domainnamen entgegenzunehmen. Mit der für den 15. Juli geplanten Veröffentlichung eines aktiven Schlüssels für die zentrale Rootzone steht damit den acht Millionen .org-Domaininhabern eine lückenlose Absicherung ihrer Adressen gegen Cache-Poisoning und Man-in-the-Middle-Angriffe zur Verfügung. DNSSEC (DNS Security Extensions) sei ein großer Schritt zu einem sichereren DNS, allerdings kein magisches Allheilmittel, sagte ICANN-Präsident Rod Beckstrom. DDoS-Angriffe oder auch Phishing bleiben eine Bedrohung.

Von DNSSEC erwarten sich die Experten mehr Sicherheit gegen Angriffe auf das Domain Name System (DNS), da Antworten des Systems über den Abgleich eines Schlüsselpaars auf ihre Authentizität überprüft werden können. Seit Anfang Januar bietet die deutsche Registry Denic eine signierte Variante der de-Zone auf einer eigenen Infrastruktur an.

Quelle: Heise Security

Der Bundesinnenminister hält Grundsatzrede zur Internetpolitik

Bundesinnenminister Thomas de Maizière (CDU) ist bei einer Grundsatzrede zum Internet auch auf Fragen des Datenschutzes eingegangen. In seinen „14 Thesen zu den Grundlagen einer gemeinsamen Netzpolitik der Zukunft“ zeichnete de Maizière ein differenziertes Bild. Einerseits warnte er vor Gesetzgebungsaktivismus und mahnte eine bessere Umsetzung bestehenden Rechts an. Ein spezielles Gesetz zu Google Street View lehnt er ab. Soziale Netzwerke wie etwa Facebook forderte er auf, „rücksichtsvolle Grundeinstellungen“ zu verwenden. Der Einzelne sollte sich zur Wehr setzen können, „wenn etwas Falsches oder Ehrenrühriges über ihn im Internet kursiert“, etwa mit einem Recht darauf, bei Suchergebnissen Gegendarstellungen anzeigen zu lassen. Bei anonymen Schmähungen ist er für einen Löschantrag.

Im Netz sollten die „Abwehrrechte gegenüber dem Staat“ gewährleistet sein, um einen „technisch möglichen“ Missbrauch des Internets als „totalitäres Überwachungsinstrument“ zu verhindern. Andererseits dürfe es auch keine „schrakenlose Anonymität“ geben - Ermittler dürften im Netz im Vergleich zur offline-Welt nicht privilegiert oder benachteiligt werden.

Quelle: Sueddeutsche.de

Quick Freeze datenschutzfreundlicher als Vorratsdatenspeicherung

Bei einer Veranstaltung des Verbands der Anbieter von Telekommunikations- und Mehrwertdiensten (VATM) sprach sich der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit, Peter Schaar, am 14.06.2010 in Köln erneut für den Verzicht auf die Vorratsdatenspeicherung von Telekommunikationsdaten aus.

Schaar sagte: „Eine sinnvolle Alternative zur Vorratsdatenspeicherung ist das „Quick Freeze“-Verfahren, das sich in anderen Staaten, etwa in den USA, seit Jahren bewährt hat. Bei der vom Bundesverfassungsgericht kürzlich gestoppten Vorratsdatenspeicherung werden ganz überwiegend Daten von unschuldigen Bürgern gespeichert. Aus ihnen lässt sich ein nahezu vollständiges Profil von Kom-

munikationsbeziehungen der gesamten Bevölkerung gewinnen. Dabei gibt es Maßnahmen, die zu wesentlich geringeren Eingriffen in den Datenschutz und in das Telekommunikationsgeheimnis führen und zugleich eine effektive Strafverfolgung gewährleisten.“

Von der Bundesregierung erwarte der Bundesdatenschutzbeauftragte, dass sie sich im Zuge der anstehenden Überprüfung der europäischen Vorratsdatenspeicherungs-Richtlinie verstärkt für Alternativen einsetzt, die deutlich datenschutzfreundlicher sind.

Bei „Quick Freeze“ handelt es sich um ein zweistufiges Verfahren um Telekommunikationsdaten zu sichern, die im Rahmen der Strafverfolgung, bei Urheberrechtsverstößen oder zur Gefahrenabwehr erforderlich sind. In der ersten Stufe werden die Anbieter von Telekommunikations-

diensten verpflichtet, bestimmte, in der Anordnung näher benannte Verkehrsdaten nicht zu löschen. Dies können etwa die Daten eines Netzknotens, von dem aus Hacker-Angriffe erfolgt sind, oder Daten einer bestimmten Person, die einer Straftat verdächtig ist, sein. Innerhalb einer vorgegebenen Frist (in den USA handelt es sich dabei um einen Monat, wobei die Frist auf Antrag um einen weiteren Monat verlängert werden kann) müssen die Ermittlungsbehörden den Nachweis erbringen, dass ihnen die vorgehaltenen Daten nach den gesetzlichen Vorgaben in einem Ermittlungsverfahren übermittelt werden müssen. Diese Auskunft bedarf einer richterlichen Genehmigung. Sofern innerhalb der Frist keine entsprechende Anordnung ergeht, sind die Daten zu löschen.

Quelle: Virtuelles Datenschutzbüro

Neuerscheinung: Praxishilfe zur BDSG-Novelle II (2009)

Die aktuelle Praxishilfe der **GDD** e.V. ist ab sofort lieferbar und behandelt folgende Themen:

- Adresshandel und Werbung
- Markt- und Meinungsforschung
- Beschäftigtendatenschutz
- Informationspflicht bei Datenschutzpannen
- Datenvermeidung und Datensparsamkeit
- Gestärkte Datenschutzkontrolle

Die Praxishilfe ist als Print- und digitale Version lieferbar.

Weitere Infos finden Sie auf der Homepage: www.datakontext.com

