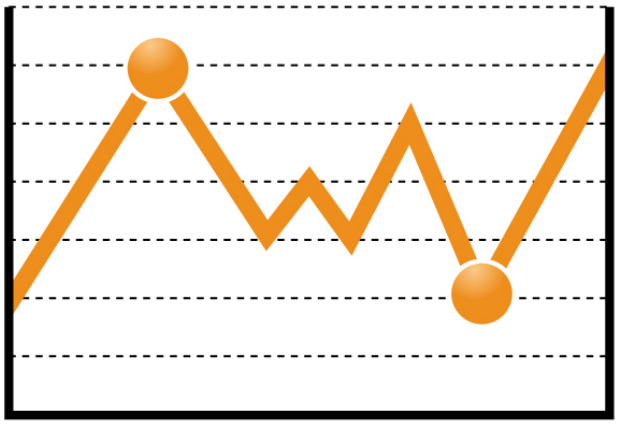
DATENSCHUTZBAROMETER 2009

– (kein) Datenschutz in Deutschland –



Datenschutz Barometer

Das Xamit Datenschutzbarometer entstand in Kooperation mit

STRATPROG, einem Think Tank des WIPN

Impressum

Herausgeber und Vertrieb
Xamit Bewertungsgesellschaft mbH
Monschauer Straße 12
40549 Düsseldorf
www.xamit.de

© Xamit Bewertungsgesellschaft mbH 2009

Alle Rechte vorbehalten. Kein Teil des Werkes darf in irgendeiner Form (Druck, Fotodruck oder in einem anderen Verfahren) ohne schriftliche Genehmigung des Herausgebers übersetzt, reproduziert oder unter Verwendung elektronischer Systeme verarbeitet, vervielfältigt oder verbreitet werden.

Rechtliche Hinweise

Alle innerhalb der Xamit-Studien genannten und ggf. durch Dritte geschützten Marken- und Warenzeichen unterliegen uneingeschränkt den Besitzrechten der jeweiligen eingetragenen Eigentümer. Allein aufgrund der bloßen Nennung ist nicht der Schluss zu ziehen, dass Markenzeichen nicht durch Rechte Dritter geschützt sind!

Inhaltsverzeichnis

© Xamit Bewertungsgesellschaft mbH

1 Einleitung

In den Medien und in der Politik spielen Datenschutz und Datensicherheit eine immer größere Rolle. So wurde unlängst in den Novellen des Bundesdatenschutzgesetzes (BDSG) der Schutz von personenbezogenen Daten gestärkt und sowohl die Bußgelder erhöht als auch die Tatbestände ausgeweitet. Dass Datenschutz schon längst kein Nischenthema mehr ist, das nur von hysterischen „Spinnern" beschworen wird, zeigen auch aktuelle Vorfälle, die ein düsteres Bild hinsichtlich der Sicherheit von persönlichen Daten zeichnen:

- Deutsche Bank gestattet selbstständigen Finanzberatern Einblick in Kundenkonten
- Berliner Firma stellt 2.500 falsche Stellenangebote beim Arbeitsamt ein, um an die Daten der Bewerber zu kommen
- Benutzer können 350.000 Rechnungen im Sparkassen-Shop einsehen
- Textildiscounter Kik spioniert Mitarbeiter und Bewerber über deren Bonität aus
- Hunderte Bewerbungsunterlagen bei ebay versteigert
- Deutsche Bank bespitzelt Aufsichtsrat

82% der Deutschen misstrauen Unternehmen beim Umgang mit persönlichen Daten

In der Gesellschaft insgesamt findet ein Umdenken statt – die Menschen haben den Eindruck, ihre Daten seien nicht mehr ausreichend geschützt. So misstrauen vier von fünf Deutschen den Unternehmen beim Schutz ihrer persönlichen Daten.[1] Dem Staat misstrauen in dieser Angelegenheit immerhin 72 Prozent der deutschen Bevölkerung.[2] Das sind keine guten Noten für eine Regierung, für die der Schutz der Persönlichkeitsrechte laut eigenen Aussagen einen hohen Stellenwert hat. So soll z.B. das Thema Datenschutz und Datensicherheit ein Schwerpunkt in der Regierungsarbeit der aktuellen Legislaturperiode sein.[3] Wir werden beobachten, wie sehr der neue Bundesinnenminister an seinen Worten gemessen werden kann und welches Datenschutzniveau in vier Jahren in Deutschland herrscht.

Mit der vorliegenden Untersuchung versucht Xamit – losgelöst von den oben erwähnten Vorkommnissen – eine empirische Antwort auf die Frage nach dem Datenschutzniveau in Deutschland zu finden und so ein möglichst realistisches Bild zu zeichnen. Dabei knüpfen wir methodisch und inhaltlich an unsere bisherigen Studien zum Thema Datenschutz und Internet an[4]:

[1] Institut für Demoskopie Allensbach (2009): Zu wenig Datenschutz? Die meisten sind mit persönlichen Daten vorsichtiger geworden. Allensbacher Bericht Nr. 6/2009
[2] Ebd.
[3] Vgl. "Wir wollen ein Land sein, das zusammenhält". Rede von Bundesinnenminister Dr. Thomas de Maizière am 11. November 2009 im Deutschen Bundestag. http://www.bmi.bund.de/cln_104/SharedDocs/Reden/DE/2009/11/rede_bt.html. Stand: 2009-11-15.
[4] Kostenfreier Download: http://www.xamit-leistungen.de/studienundtests/index.php

- „Wissen Sie, was Sie tun? Wissen Sie, wer es noch weiß? – Surfen im Internet“ über heimliche Datenerhebung bei Webstatistiken,
- „Wie Unternehmen im Internet bei Konsumenten Misstrauen säen – Kontaktformulare und Datenschutz“ über die Transparenz der Datennutzung bei Kontaktformularen,
- „Datenschutzbarometer 2008 – Datenschutz im Internet“ über das Datenschutzniveau im deutschen Internet sowie
- „Parteien und Datenschutz – Datenschutzpraxis deutscher Parteien und parteinaher Organisationen".

Alle vier Studien stellen den Umgang mit personenbezogenen Daten im Internet in den Vordergrund und untersuchten, wie stark Webseitenbetreiber Ihren Besuchern offenlegen, welche Daten erhoben werden und was mit diesen geschieht.

Im Rahmen der vorliegenden Untersuchung wird dies um zwei weitere Aspekte ergänzt: Zum einen untersuchen wir, wie ernst Unternehmer den Datenschutz im eigenen Betrieb nehmen, indem sie das Verfahrensverzeichnis als gesetzlich vorgeschriebene Grundlage des betrieblichen Datenschutzes zur Verfügung stellen (Kapitel 6). Zum anderen untersuchen wir, wie es mit der Kontrolle in den Unternehmen durch die Aufsichtsbehörden bestellt ist (Kapitel 7).

Das Datenschutzbarometer gibt einen Überblick über das Datenschutzniveau in Deutschland

Mit dem Datenschutzbarometer 2009 stellt Xamit einen einzigartigen Überblick über das aktuelle Datenschutzniveau in Deutschland zur Verfügung. Xamit wiederholt diese Untersuchung regelmäßig und in identischer Form, um die Entwicklung des Datenschutzniveaus vergleichbar zu dokumentieren.

© Xamit Bewertungsgesellschaft mbH

2 Hintergrund

Im Folgenden zeigen wir in knapper Form auf, an welchen Stellen und auf welche Weise persönliche Nutzerdaten durch Internet-Angebote erhoben werden. Sobald Daten erhoben werden, sind diese auch potentiell gefährdet. In Folge dessen droht Missbrauch.

2.1 Webshops

Mit dem Begriff Webshop werden Webseiten bezeichnet, die Waren oder Dienstleistungen zum sofortigen Online-Kauf anbieten. Dabei bestehen verschiedene Möglichkeiten, einen Webshop technisch zu realisieren. Auf die Feinheiten jeder Variante einzugehen sprengt den Rahmen der Studie. Deshalb skizzieren wir nachfolgend nur grob die generelle Funktionsweise.

Die einfachste Variante eines Webshops generiert eine E-Mail an den Betreiber, in der die bestellten Waren und der Besteller aufgeführt sind. Der Betreiber sorgt dann für die Auslieferung der Waren. Ein solcher Webshop nimmt keine Online-Abbuchungen vor und speichert keine Kundendaten, so dass Kundenkonten, mit denen der Bestellstatus eingesehen wird, fehlen. Kundendaten können folglich auch nicht aus dem Webshop gestohlen werden; wohl aber vom E-Mail-Server des Betreibers. Sicherheitslücken gefährden die Kundendaten deshalb nur im Moment des Bestellvorgangs. Ein nachträglicher Diebstahl aus dem Webshop scheitert an der fehlenden Datenhaltung.

Je komplexer die Abfrage, desto höher die Gefahr

Wesentlich anfälliger für Missbrauch und Diebstahl sind Webshops, die alle Kundendaten und Bestellungen direkt in Datenbanken beim Shop abspeichern. Solche Webshops bieten ihren Kunden Kundenkonten an, mit denen sie den Bestellstatus abfragen und ihre Kundendaten (Adresse, Zahlungsinformationen) verwalten können. Kreditkartenzahlungen sind ebenfalls möglich. Technisch nutzt diese Webshopklasse oft PHP, um die Shopsoftware auszuführen sowie eine dedizierte Datenbank, um die Artikel und Kundendaten zu speichern. Zur sicheren Aufbewahrung der Kundendaten ist es erforderlich, dass der Datenbankzugriff auf die Shopsoftware beschränkt bleibt. Die Shopsoftware ihrerseits darf die jeweiligen Kundendaten nur berechtigten Personen zugänglich machen. Andernfalls können sämtliche Kundendaten nachträglich aus der Datenbank ausgelesen und schlimmstenfalls gestohlen werden.

Die zuletzt skizzierte komplexe Variante zeigt auf, dass ein Webshop aus verschiedenen Computerprogrammen besteht. Dabei kommt mit PHP ein Programm zum Einsatz, das Skripte (kleine Programme) ausführt. Eine Shopsoftware wird demnach nicht direkt auf dem Server ausgeführt, sondern ist meistens in PHP geschrieben. Der PHP-Server führt die Shopsoftware in ähnlicher Weise aus wie ein Computer einen Browser ausführt.

Veraltete Software- und PHP-Versionen bergen Risiken

Ein Webshop kann nur dann sicher sein, wenn PHP und die Shopsoftware keine Sicherheitslücken aufweisen. Grundvoraussetzung hierfür ist, dass am betreffenden PHP-Server, der Shopsoftware sowie der Datenbank entsprechende Sicherheitseinstellungen vorgenommen wurden. Diesen Aspekt nehmen wir in der weiteren Betrachtung als gegeben an.

Sicherheitslücken kommen zudem durch Implementationsfehler („Bugs“) oder Designfehler zustande. Keine nicht-triviale Software ist frei von Fehlern. Z.B. wurden in PHP Version 4.x.x für den Bereich MySQL-Datenbank 712 Fehler behoben. Für die Version 5.2 sind es bereits 225 Fehler.[5] Um die Sicherheit von Webshops zu gewährleisten, ist es also zwingend notwendig, stets die aktuellen Programmversionen einzusetzen.

2.2 Webstatistiken

Wer eine Webpräsenz betreibt, investiert (viel) Zeit und Geld. Unternehmen und auch Privatpersonen möchten deshalb verständlicher Weise wissen, ob dieses Geld wirklich produktiv und effizient investiert ist. Eine Erfolgskontrolle von Webseiten ist für einen wirtschaftlichen Betrieb folglich unverzichtbar. Mit Hilfe von Webstatistiken – auch Web Tracking, Web Analytics oder Webcontrolling genannt – messen Unternehmen das Verhalten ihrer Website-Besucher.

Webstatistiken geben aggregierte Informationen über die Besucher von Webseiten wieder. Sie beantworten u.a. folgende Fragen:

- Über welche Wege betreten Besucher die Webpräsenz?
- Wie viele Besucher hat die Webpräsenz?
- Was unternehmen Besucher auf der Webpräsenz?

Da aussagekräftige Auswertungen einer Website Fachwissen voraussetzen, nutzen Betreiber hierfür in aller Regel externe Dienstleister – im Folgenden Statistikersteller genannt. Ein Statistikersteller erhebt die entsprechenden Daten meistens selbst und generiert hieraus regelmäßige statistische Auswertungen für den Betreiber, welche nach Aufbereitung dann keinerlei Personenbezug mehr enthalten.

Bei einer eigenständigen Datenerhebung durch den Statistikersteller bindet der Betreiber in alle Webseiten Webpixel oder einen speziellen Script-Code ein, der die Daten für den Statistikersteller sammelt und direkt an diesen sendet. Meistens werden zusätzlich Cookies eingesetzt. Welche Daten gesammelt werden, entscheidet und kontrolliert der Statistikersteller. Deshalb hat der Betreiber keine Kontrolle über Datenerhebung, Speicherung, Auswertung und weitere Nutzung der Daten.

[5] Die Entwickler von PHP betreiben unter http://www.php.net/ eine Fehlerdatenbank. Stand der Abfrage: 2009-10-23.

© Xamit Bewertungsgesellschaft mbH

Ein Beispiel: Max Mustermann surft verschiedene Webpräsenzen an. Der Betreiber kennt das Bewegungsprofil von Max Mustermann für seine eigene Webpräsenz. Weil ein Statistikersteller jedoch verschiedene Webpräsenzen betreut, besitzt er einen wesentlich umfassenderen Überblick über die Aktivitäten von Max. Je mehr Webpräsenzen also denselben Statistikersteller nutzen, desto umfangreicher, detaillierter und somit wertvoller wird dessen Datenbestand und Wissen über Max Mustermann.

Von der Einzelstatistik zum komplexen Bewegungsprofil

Derartige Personen- oder unternehmensbezogene Bewegungs- und Verhaltensprofile gehen über reine Website-Statistik weit hinaus und sind ungleich wertvoller, da sie weiterreichende Aussagen erlauben. Informiert sich ein Besucher bspw. auf den Webseiten einer Krankenkasse über eine bestimmte Krankheit, liegt die Vermutung nahe, dass er selbst (oder nahe Angehörige) an der recherchierten Erkrankung leidet. Sucht indes ein Unternehmen auf (universitären) Webseiten nach bestimmten Forschungsergebnissen und Veröffentlichungen, liegt die Vermutung nahe, dass es an einem ähnlichen Thema arbeitet.

Dem Interesse an Datentransparenz auf Seiten der Betreiber steht das Interesse nach Anonymität der Nutzer entgegen. Besucher und Unternehmen wollen unbeobachtet Webseiten nutzen!

Eine ausführliche Analyse über Webstatistiken finden Sie in unserer Studie „Wissen Sie, was Sie tun? Wissen Sie, wer es noch weiß? – Surfen im Internet“[6].

2.3 Internet-Werbung

Webseiten-Betreiber binden häufig Werbung in das eigene Angebot ein, um zusätzliche Einnahmen zu generieren. Typische Darstellungsformen dieser Werbung sind beispielsweise Banner oder Textanzeigen, die wiederum von Werbeunternehmen gestaltet und geliefert werden. Um zu verhindern, dass ein Besucher mehrfach die gleiche Werbung sieht und um nachzuvollziehen, welcher Besucher welche Werbung gesehen hat, setzen Werbeunternehmen Cookies ein oder nutzen ähnliche Techniken wie Webstatistikersteller (Kapitel 2.2).

Alle Beteiligten bestens im Bilde – nur der Besucher ahnt nichts

Ein Beispiel: Sobald Max Mustermann eine Webseite besucht, die Werbung enthält, erfährt nicht nur der Webseitenbetreiber, sondern auch das Werbeunternehmen von seinem Besuch. Dabei sieht Max Mustermann der Werbung nicht unbedingt an, von welchem Unternehmen diese stammt und wer in Folge dessen von seinem Besuch erfährt. Deshalb ist er auf die Datenschutzerklärung des Webseitenbetreibers angewiesen.

Anhand des Angebotes von Google Adsense untersuchen wir nachfolgend, ob Webpräsenzen, die Google Adsense anzeigen, auch eine

[6] Kostenfreier Download: http://www.xamit-leistungen.de/studienundtests/index.php

Datenschutzerklärung besitzen. Google verpflichtet die Nutzer von Google Adsense in § 2.6 der Allgemeinen Geschäftsbedingungen für Google AdSenseTM Online, in einer Datenschutzerklärung auf Google Adsense hinzuweisen.[7] Insbesondere ist laut Google dabei zu erwähnen, dass dieser Dienst einen Cookie setzt.

Selbstverständlich handelt es sich bei Google nicht um den einzigen Anbieter für Website-Werbung. Gleichwohl zählt Google mit den Diensten Adsense und Doubleclick zu den marktführenden und bekanntesten Anbietern und hat in Folge dessen repräsentativen Charakter. Die im Rahmen der Untersuchung ermittelten Ergebnisse sind also auf weitere Werbeunternehmen übertragbar.

2.4 Kontaktformulare

Daten werden für die verschiedensten Zwecke verwertet

Wer via Online-Kontaktformulare Waren oder Dienstleistungen bestellt oder auch nur Informationen oder einen Newsletter anfordert, gibt seine persönlichen Daten preis. Neben der Erfüllung einer konkreten Bestellung oder der Beantwortung einer Anfrage erlaubt die moderne Informationstechnik darüber hinaus, die gewonnenen Informationen für unterschiedliche Zwecke weiterzunutzen. Ohne dass es der Webseiten-Besucher (Kunde) ahnt, können

- Konsumentenprofile erstellt und ausgewertet,
- Werbung zielgerichtet versendet,
- oder auch monetäre Zusatzerlöse durch den Verkauf seiner personenbezogenen Daten generiert werden.

Unternehmen signalisieren durch eine Datenschutzerklärung, wozu sie persönliche Angaben nutzen. Diese Transparenz schafft eine wichtige Grundlage für Vertrauen. Datenschutzerklärungen liegen deshalb im Eigeninteresse von Unternehmen.

Zusätzlich regeln gesetzliche Vorschriften den Umgang mit personenbezogenen Daten. Während für den Webauftritt das Telemediengesetz (TMG) gilt, fallen die in einem Kontaktformular von privatwirtschaftlichen Unternehmen, Vereinen und anderen nicht-öffentlichen Betreibern übermittelten Daten unter das Bundesdatenschutzgesetz (BDSG).[8] Bei öffentlichen Stellen der Länder gilt indes das entsprechende Landesdatenschutzgesetz.

Ein Beispiel: Max Mustermann füllt ein Kontaktformular aus und klickt auf „absenden“. Darf der Empfänger seine Anfrage beantworten?

§ 4 Abs. 1 BDSG erlaubt eine Verarbeitung personenbezogener Daten nur dann, wenn eine Einwilligung vorliegt oder eine gesetzliche Vorschrift oder eine andere Rechtsvorschrift dies erlaubt. Aus Mangel

[7] Google (2008): Allgemeine Geschäftsbedingungen (AGBs) für AdSense. URL: https://www.google.com/adsense/localized-terms. Stand: 2009-11-20.

[8] Hoeren, Thomas (2008): Skript zum Internetrecht. Stand März 2008. URL: http://vg00.met.vgwort.de/na/8181c8ca7c1ad67f6567?l=http://www.uni-muenster.de/Jura.itm/hoeren/materialien/Skript/Skript_Maerz2008.pdf. S. 399

© Xamit Bewertungsgesellschaft mbH

an speziellen Rechtsvorschriften für Kontaktformulare bedarf es einer Einwilligung von Max Mustermann. Ob seine freiwillige Datenabgabe bereits eine Einwilligung darstellt oder dies in expliziter Form erforderlich ist, ist unter Juristen umstritten.[9]

Unstrittig dagegen ist, dass eine Einwilligung voraussetzt, dass Max Mustermann weiß, worin er einwilligen soll (siehe § 4 Abs. 3 BDSG). Denn wer würde etwas kaufen, ohne sich vorher mit dem Verkäufer über den Gegenstand und die Modalitäten zu verständigen? Erläutert die Webpräsenz,

- für welche Zwecke die Daten genutzt werden (z.B. Bearbeitung der Anfrage, Zusendung von Werbung) und
- an wen die Daten übermittelt werden,

dann weiß Max Mustermann, worauf er sich einlässt und kann einwilligen. Eine solche Erläuterung nennen wir in dieser Studie „Datenschutzerklärung". Welche Form eine solche Einwilligung haben sollte, wurde im Rahmen der zurückliegenden Xamit Studie „Wie Unternehmen im Internet bei Konsumenten Misstrauen säen – Kontaktformulare und Datenschutz"[10] ausführlich erläutert und ist im Anhang der vorliegenden Untersuchung zusammengefasst.

Datenschutzerklärung als Entscheidungsgrundlage

Unter den Begriff „Kontaktformular" fassen wir im Zuge unserer Untersuchung alle Eingabemöglichkeiten für personenbezogene Daten zusammen, also auch Newsletter-Anmeldungen oder Anmeldungen zu persönlichen bzw. Passwort-geschützten Webseitenbereichen.

[9] Ebd. S. 409
[10] Kostenfreier Download: http://www.xamit-leistungen.de/studienundtests/index.php

3 Gegenstand und Methode des Datenschutzbarometers 2009

Eine maschinelle Quellcode-Analyse von 24.376 deutschen Webpräsenzen bildet die Grundlage des Xamit-Datenschutzbarometers. Neben 1.982 Gemeinden, politischen Organisationen und 2.026 Vereinen berücksichtigt die vorliegende Xamit Studie Unternehmen aus unterschiedlichen Branchen:

- Verarbeitendes Gewerbe
- Handel, Instandhaltung und Reparatur von Kfz und Gebrauchsgütern
- Gastgewerbe und Hotels
- Grundstücks- und Wohnungswesen
- Gesundheitswesen
- Rechtsanwälte & Steuerberater
- Werbung
- Informationstechnik
- Unternehmensberatung
- Handwerk
- Medien
- Energie- und Wasserwirtschaft

Jede Branche ist mit 391 bis 4.621 Webpräsenzen vertreten. Analysiert werden jeweils maximal 1.000 Webseiten pro Webpräsenz.

Von September bis November 2009 werteten wir rund 1,6 Mio. Webseiten aus. Hierbei wurde untersucht,

Kriterien für Datenschutz im Internet

- ob und welche Shop-Software verwendet wird (Kapitel 3.1),
- ob Google Adsense verwendet wird (Kapitel 3.2),
- ob und welche Webstatistiken erstellt werden (Kapitel 3.3) und
- ob Kontaktformulare vorhanden sind (Kapitel 3.4).

In diesem Zusammenhang wurde auch das Vorhandensein von Datenschutzerklärungen geprüft. Datenschutzerklärungen enthalten charakteristische Worte („Datenschutz“, „Zweck“ usw.) um aussagekräftig zu sein. Nach diesen Worten wurde gesucht, um zu bestimmen, welche Webseiten über eine Datenschutzerklärung verfügen und welche nicht. Die Reihenfolge der Worte ist dabei irrelevant. Welche Regelungen in einer Datenschutzerklärung getroffen werden, bleibt aus methodischen Gründen unberücksichtigt.

Durch die maschinellen Analysen sind Fehlzuordnungen nicht auszuschließen. Stichprobenhafte Kontrollen zeigten allerdings keine Fehler. Daher können die Ergebnisse als valide betrachtet werden.

© Xamit Bewertungsgesellschaft mbH

3.1 Einbindung eines Webshops

Wie viele Webshops setzen aktuelle Versionen ihrer Shopsoftware ein und wie häufig werden aktuelle PHP-Versionen verwendet? Um diese Fragen zu beantworten, untersucht Xamit für jeden erkannten Webshop,

- ob eine identifizierbare Shopsoftware verwendet wird und um welche Version es sich handelt sowie
- ob und in welcher Version PHP eingesetzt wird.

Maschinelle Quellcodeanalyse von Software und PHP

Dazu untersuchten wir maschinell den Quellcode jeder Webseite daraufhin, ob charakteristische Zeichen für bekannte Standardshopsoftware vorhanden sind. Webshops, die keine bekannte Standardshopsoftware einsetzen, sondern eine Eigenentwicklung sind, konnten wir aufgrund fehlender Charakteristika nicht identifizieren.

Es gibt kein eindeutiges Merkmal, einen Webshop zweifelsfrei von einem reinen Informationsangebot zu unterscheiden. Eine Warenkorbfunktion kann mit „Warenkorb“ betitelt sein, sie muss es aber nicht. Das Wort „Warenkorb“ kommt zudem auch außerhalb von Webshops vor. Erst die Verwendung einer Shopsoftware lässt eindeutig auf einen Webshop schließen.

Die PHP-Version ermittelten wir aus dem Header der Webseite. Allerdings lassen sich Webserver so konfigurieren, dass die PHP-Version im Header gar nicht oder falsch angezeigt wird. Das Verheimlichen der Version erschwert etwa einen möglichen Angriff. Aus diesem Grund konnten wir nicht alle PHP-Installationen aufspüren. Auch lässt sich ein gehärtetes, d.h. „sicheres“ PHP[11] nicht aufspüren. Ungeachtet dessen sollte die verwandte Methodik einen ersten Überblick über die Sicherheit von Webshops verschaffen.

3.2 Einbindung von Google Adsense

Unverkennbar: „Adsense“ von Google

Für die Einbindung von Google Adsense nutzen Websites eine charakteristische Zeichenfolge in Form des entsprechenden Java Script von Google. Diese Zeichenfolge ist auf allen Webseiten, die Google Adsense aufweisen, identisch. Sobald wir die Zeichenfolge im Quelltext finden, gehen wir von einer Adsense-Nutzung aus.

3.3 Webstatistiken und Nutzer-Hinweis

Auch jeder Statistikersteller bindet eine charakteristische Zeichenfolge in die überwachten Webseiten ein, um den Seitenaufruf protokollieren zu können. Diese Zeichenfolge ist ebenfalls auf allen überwachten Webseiten identisch. Kommt eine solche Zeichenfolge auf

[11] Siehe auch http://www.hardened-php.net/suhosin/index.html

einer Webseite vor, wurde dies als Überwachung durch den zugehörigen Statistikersteller gewertet.

Einhaltung der Nutzungsbedingungen wird überprüft

Google verlangt in § 8.1 seiner Nutzungsbedingungen[12], die Nutzung von Google Analytics an „prominenter“ Stelle zu dokumentieren. Google schreibt den Wortlaut dieser Information vor und behält sich ein Kontrollrecht vor. Ob die von Google vertraglich vorgeschriebenen Formulierungen auf einer Webpräsenz, die Google Analytics nutzt, vorkommen, wurde analog untersucht.

Aus methodischen Gründen wurden lediglich diejenigen Statistikersteller berücksichtigt, die eine eigene Datenerhebung durchführen. Logfile-Analysen blieben deshalb außen vor.

3.4 Einbindung von Kontaktformularen

Für jede Webpräsenz wurde untersucht,

- ob Eingabefelder personenbezogene Daten abfragen, z. B. bei Kontaktformularen,
- ob eine Datenschutzerklärung auf der Webpräsenz vorliegt,
- ob die Datenschutzerklärung einfach und mit maximal einem Klick vom Formular aus direkt erreichbar ist.

Umfang und Qualität der abgefragten Daten

Dazu untersuchten wir maschinell den Quellcode jeder Webseite daraufhin, ob Formularfelder verwendet werden. Wenn wir ein Formularfeld fanden, analysierten wir seine Umgebung im Quellcode. Tauchten dort einschlägige Begriffe wie „Vorname“, „Straße“ etc. auf, gingen wir davon aus, dass personenbezogene Daten abgefragt werden. Diese Methode ist nicht hundertprozentig fehlerfrei, doch eine manuelle Überprüfung zufällig ausgewählter Webpräsenzen zeigte keine systematischen oder lediglich minimale Fehlzuordnungen. Deshalb können wir auch diese Ergebnisse als ausreichend valide betrachten.

[12] Google Analytics Bedingungen. URL: http://www.google.com/analytics/de-DE/tos.html. Letzter Zugriff: 2009-10-23.

© Xamit Bewertungsgesellschaft mbH

4 Ergebnisse

In diesem Kapitel stellen wir die Befunde hinsichtlich

- sicherer Software (Kapitel 4.1),
- Werbeeinblendungen (Kapitel 4.2),
- Webstastiken (Kapitel 4.3)
- und Kontaktformularen (Kapitel 4.4)

vor. Die Ergebnisse aggregieren wir in Kapitel 5 zu dem kompakten Xamit Datenschutzbarometer.

4.1 Webshops – veraltete Software noch immer weit verbreitet

Jeder zweite Webshop basiert auf veralteter Software

Insgesamt haben wir 4.961 Installationen von PHP der Version 4 und 5.071 der Version 5 identifiziert (Mehrfachnennung möglich). Damit verfügt die veraltete Version 4 noch immer über einen Anteil von 50%. 2008 waren es 66%. Nur langsam steigen die Betreiber auf die aktuelle Version 5 um. Dies ist insofern bedenklich, da die Betreuung und Fehlerbehebung von Version 4 mit der Version 4.4.9 Ende 2008 eingestellt wurde.[13] Von allen erkannten PHP-Installationen haben wir bei nur 22% die zum Zeitpunkt der Erhebung aktuelle Version (4.4.9 oder 5.3.0) entdeckt. 2008 waren es noch 29%. Ein Grund mag darin liegen, dass es einen größeren Anteil an Installation der Version 5.2.X gibt, die wir nicht gesondert erfasst haben.

Nach einer Studie des Web Application Security Consortium (WASC) sind 9% der Webpräsenzen und Webshops anfällig für das Einschleusen von SQL-Codes. Ein solches Code-Einschleusen erlaubt i.d.R. den Diebstahl von Kundendaten aus einem Webshop. PHP ist dabei ein mögliches Einfallstor. Das WASC ermittelte mit Hilfe automatischer Scanner und manueller Tests die Schwachstellen von mehr als 32.000 Webpräsenzen und Webshops.[14]

In 202 Fällen konnten wir eine bekannte Shopsoftware erkennen. xtCommerce ist mit einem Anteil von 57% (2008: 64%) unbestrittener Marktführer gefolgt von seinem OpenSource-Verwandten osCommerce mit 26% (2008: 20%). Die restlichen 17% (2008: 16%) teilen sich fünf (2008: sieben) Programme auf. Aufgrund der geringen Fallzahlen verzichten wir auf eine Aufteilung nach Branchen.

Viele Shop-Anbieter nutzen individuelle Software

Angesichts der geringen Anzahl an erkannter Shopsoftware liegt der Verdacht nahe, dass viele Webshops entweder eine kaum verbreitete Standardsoftware oder eine Eigenentwicklung nutzen. Je verbreiteter eine Standardsoftware ist, desto eher werden Sicherheitslücken gefunden und bekannt gegeben. Der Hersteller hat meistens ein vitales

[13] Siehe Ankündigung zu Version 4.4.9. URL: http://www.php.net/. Letzter Zugriff: 2009-11-30.
[14] Heise Online (2008): Studie: Fast jede Webanwendung angreifbar. URL: http://www.heise.de/newsticker/Studie-Fast-jede-Webanwendung-angreifbar--/meldung/115656. Letzter Zugriff: 2009-11-30.

Interesse daran, die Lücken schnell zu schließen, da ein hoher Marktanteil zu entsprechend vielen gefährdeten Webshops führt.

Bei Individualsoftware müsste der Shopbetreiber indes aktiv nach Sicherheitslücken suchen (lassen). Ein kostspieliges Unterfangen, welches nur äußerst selten eingesetzt wird. Wenn Kriminelle (zufällig) auf Sicherheitslücken stoßen, können sie diese unbemerkt ausnutzen. Individualsoftware bedeutet deshalb nicht per se eine höhere Sicherheit.

87% der Webshops auf PHP-Basis gefährden Kundendaten

Von den Webshops mit Standardshopsoftware setzen 56% (2008: 53%) die aktuelle Version der Shopsoftware ein. 13% (2008: 19%) der Webshops mit Standardshopsoftware und erkannter PHP-Installation setzen sowohl die aktuelle Shopsoftware als auch die aktuelle PHP-Version ein. Dieser geringe Anteil deutet darauf hin, dass viele Webshops ihre PHP-Installation nicht regelmäßig aktualisieren. Sie bleiben für Sicherheitslücken in PHP anfällig und gefährden die Kundendaten.

Bezogen auf die geringe Anzahl an untersuchten Webshops sind unsere Ergebnisse nicht repräsentativ. Gleichwohl werfen sie ein Schlaglicht auf einen beunruhigenden Sachverhalt: Gefährdete Kundendaten durch veraltete PHP-Versionen und Shopsoftware. Auch der hohe Anteil an Individualsoftware wirft Fragen nach der Sicherheit auf.

4.2 Google Adsense – Datenübertragung bleibt im Dunkeln

Wer Google Adsense auf seiner Webpräsenz einbindet, der macht Werbung für fremde Unternehmen und Produkte. Viele der untersuchten Webpräsenzen zählen allerdings nicht zu den typischen Adsense-Nutzern, so dass deren relativ geringer Anteil von 1,3% (2008: 1,2%) unter den untersuchten Webpräsenzen nicht überrascht.

Zwei Drittel der Webpräsenzen nutzen Google Adsense heimlich

Informierten 2008 erst 21% der Webpräsenzen mit Adsense ihre Besucher mit einer Datenschutzerklärung, sind es 2009 bereits 32%. Auf der anderen Seite setzen sich 68% (2008: 79%) über die Nutzungsbedingungen von Google hinweg und lassen ihre Besucher im Dunkeln darüber, dass Google ein Cookie setzt und dass Daten wie die IP-Nummer zu Google übertragen werden.

Deutliche Unterschiede zwischen den Branchen bestehen. Unternehmen aus dem Bereich „Medien“ informieren zu 65%, während kein einziger Verein eine Datenschutzerklärung veröffentlicht und die Nutzungsbedingungen von Google Adsense einhält. Aufgrund der geringen Fallzahlen verzichten wir auf eine weitere Aufteilung nach Branchen.

Die verbreitete Heimlichkeit und Neigung zum Bruch der Nutzungsbedingungen korrespondiert mit unseren Ergebnissen zur Webstatistik (Kapitel 4.3).

© Xamit Bewertungsgesellschaft mbH

4.3 Webstatistik – meist verheimlichte Datenerhebung

Aufsichtsbehörde hält Nutzung von Google Analytics für nicht gesetzeskonform

Vor gut zwei Jahren hatten wir zum ersten Mal die Nutzung von Google Analytics durch deutsche Webseitenbetreiber untersucht. Ein breites Medienecho und eine Diskussion in der Fachwelt über die rechtliche Zulässigkeit waren die Folge.[15] Im Januar 2009 erreichte die Debatte mit einer Stellungnahme des Unabhängigen Landeszentrums für Datenschutz Schleswig-Holstein (ULD) ihren Höhepunkt. Das ULD stuft die *Nutzung* von Google Analytics durch Webseitenbetreiber als nicht mit dem deutschen Datenschutzrecht vereinbar ein.[16] Zu den Gründen zählen

- die Datenübermittlung in die USA,
- die ewige Datenspeicherung ohne Löschmöglichkeit und
- die Möglichkeit, durch Datenverknüpfung ein Nutzerprofil zu erstellen.

Webseitenbetreiber, die Google Analytics nutzen, begehen damit eine Ordnungswidrigkeit. Eine Einschätzung, die der Düsseldorfer Kreis, ein Koordinierungsgremium aller deutschen Datenschutzaufsichtsbehörden für den nicht-öffentlichen Bereich, mit allgemeinen Kriterien für Webstatistiken untermauerte.[17] Der Bundesdatenschutzbeauftragte ermahnte deshalb jüngst zahlreiche Krankenkassen, Google Analytics nicht einzusetzen.[18] Uns interessiert, wie sich im Licht dieser Entwicklung die Nutzung von Google Analytics und anderen Webstatistikdiensten in den letzten 24 Monaten verändert hat.

CSU und Hessisches Statistisches Landesamt klären Webseiten-Besucher nur ungenügend über Datensammlung auf

Die CSU und das Hessische Statistische Landesamt illustrieren die Antwort deutlich. Beide nutzen Google Analytics weiter. Die CSU weist in Ihrer Datenschutzerklärung auf die Nutzung – etwas unglücklich unter Cookies platziert – hin (Abbildung 1), während das Hessische Statistische Landesamt vage bleibt (Abbildung 2):

> *„Zur Nutzungsauswertung dieser Website bedienen wir uns auch Dritten, die wir mit dieser Auswertung beauftragt haben."*

Sowohl die CSU wie auch das Hessische Statistische Landesamt suggerieren in ihrer Datenschutzerklärung, dass bei ausgeschalteten Cookies keine Datenübermittlung an Google stattfindet. Leider übersehen beide Betreiber, dass Google in jedem Fall die IP-Nummer des Besuchers erhält. Denn Google sammelt seine Daten mit Hilfe eines

[15] Vgl. Pordesch, Ulrich, Steidle, Roland (2008): Im Netz von Google. Web Tracking und Datenschutz. In: Datenschutz und Datensicherheit (DuD), Nr. 5, Jg. 2008, S. 324-329.
[16] Unabhängige Landeszentrum für Datenschutz Schleswig-Holstein (2009): Datenschutzrechtliche Bewertung des Einsatzes von Google Analytics. URL: https://www.datenschutzzentrum.de/tracking/20090123_GA_stellungnahme.pdf. Letzter Zugriff: 2009-08-05.
[17] Düsseldorfer Kreis (2009): Beschluss zur Datenschutzkonforme Ausgestaltung von Analyseverfahren zur Reichweitenmessung bei Internet-Angeboten. URL: http://www.datenschutz-mv.de/dschutz/beschlue/Analyse.pdf. Letzter Zugriff: 2009-11-30.
[18] Heise Online (2009): Bundesdatenschutzbeauftragter kritisiert Usertracking bei Krankenkassen. URL: http://www.heise.de/newsticker/meldung/Bundesdatenschutzbeaftragter-kritisiert-Usertracking-bei-Krankenkassen-864903.html. Letzter Zugriff: 2009-11-23.

Scripts, dass der Browser beim Anzeigen der Webseite automatisch von Google abholt.

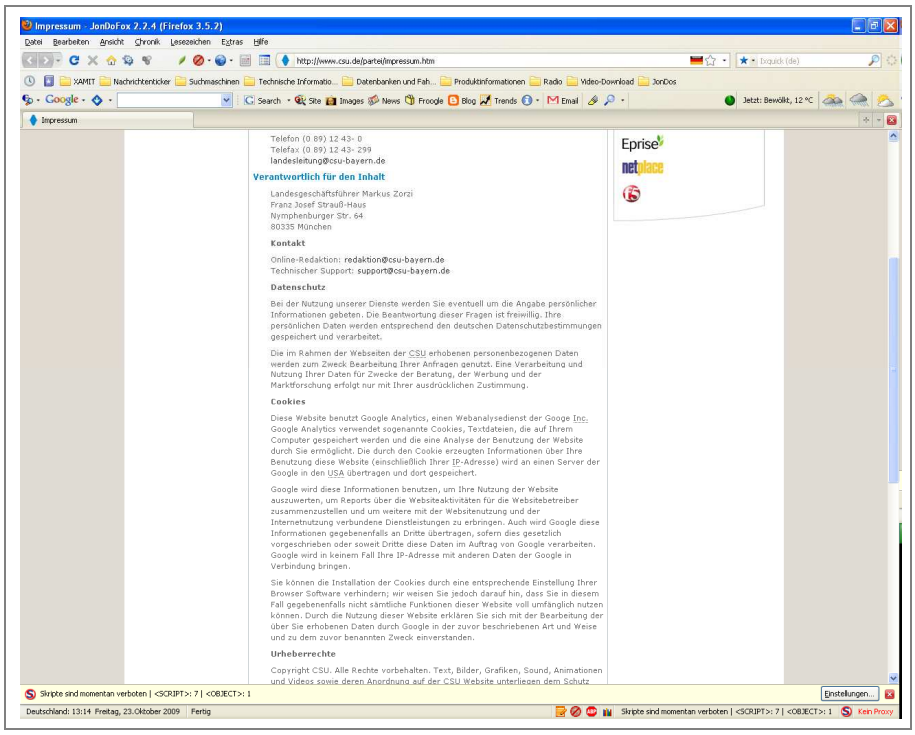


Abbildung 1: Datenschutzerklärung der CSU[19]

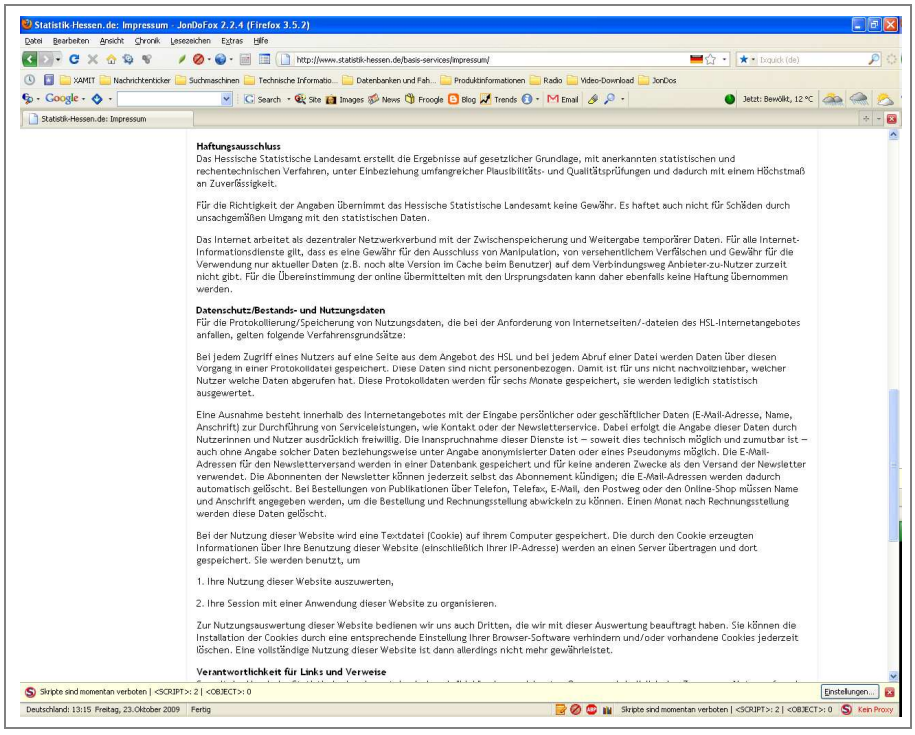


Abbildung 2: Datenschutzerklärung des Hessischen Statistischen Landesamts[20]

[19] URL: http://www.csu.de/partei/impressum.htm. Letzter Zugriff: 2009-10-23.

© Xamit Bewertungsgesellschaft mbH

Google baut Markführerschaft beim Tracking weiter aus

Zum Zeitpunkt unserer ersten Erhebung (August und September 2007) nutzten 7% der Webpräsenzen Google Analytics und 1% einen anderen Anbieter. 2008 waren es bereits 10% für Google Analytics und 2% für andere Anbieter. Heute sammelt Google Analytics auf 13% der Webpräsenzen Daten. Eine Steigerung um 31% gegenüber 2008. 4% verwenden andere Anbieter. Abbildung 3 zeigt die Nutzung nach Branchen. Insgesamt erfreut sich Google Analytics steigender Beliebtheit über alle Branchen hinweg.

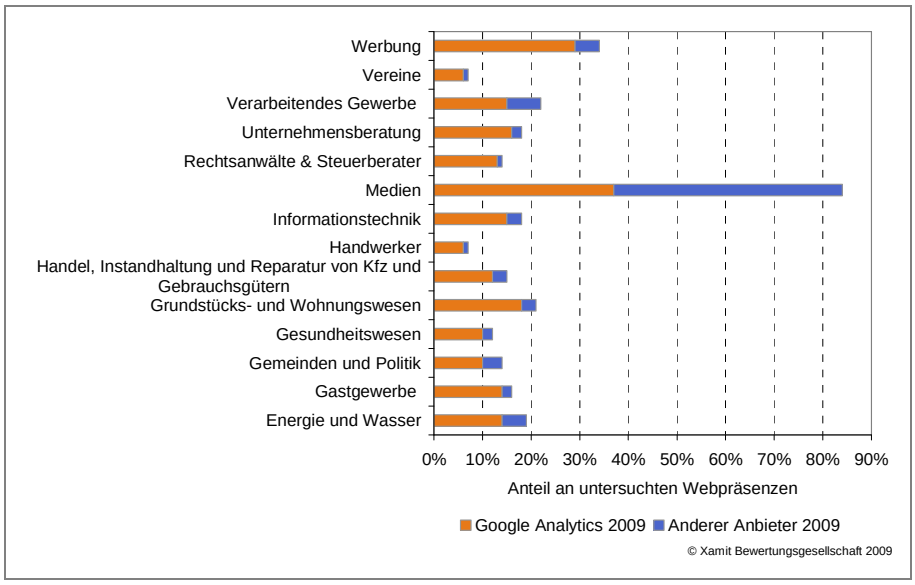


Abbildung 3: Nutzung von Webstatistiken nach Branchen

Google verlangt in § 8.1 seiner Nutzungsbedingungen, dass Betreiber die Bewegungsprofile von Besuchern nicht mit personenbezogenen Daten verknüpfen und die Nutzung von Google Analytics an „prominenter“[21] Stelle dokumentieren. Google schreibt den Wortlaut dieser Information vor und behält sich auch ein Kontrollrecht vor.

Immer noch sammeln zwei Drittel der Webpräsenzen Daten heimlich

In der Praxis ignorierten 2007 99% der von uns untersuchten Betreiber diese Kennzeichnungspflicht. Dieser Wert sinkt 2008 auf 95%, d.h. 5% informieren 2008 ihre Besucher mit dem von Google vorgegebenen Wortlaut. Weitere 19% nutzten 2008 eine Datenschutzerklärung ohne diesen Passus. Heute benutzen 15% der Betreiber den Google-Passus und 20% einen anderen Wortlaut. Die Abnahme der heimlichen Datensammlung ist eine erfreuliche Entwicklung. Trotzdem setzen aktuell immer noch 65% der Webpräsenzen Google Analytics heimlich und unter Verstoß der Lizenzbedingungen ein. Das zeigt deutlich, dass viele Betreiber entweder nicht wissen (wollen), was sie tun, oder bewusst die Interessen ihrer Besucher ignorieren, da sie keine Sanktionen fürchten müssen.

[20] URL: http://www.statistik-hessen.de/basis-services/impressum/. Letzter Zugriff: 2009-10-23.
[21] Google Analytics Bedingungen. URL: http://www.google.com/analytics/de-DE/tos.html. Letzter Zugriff: 2009-10-23.

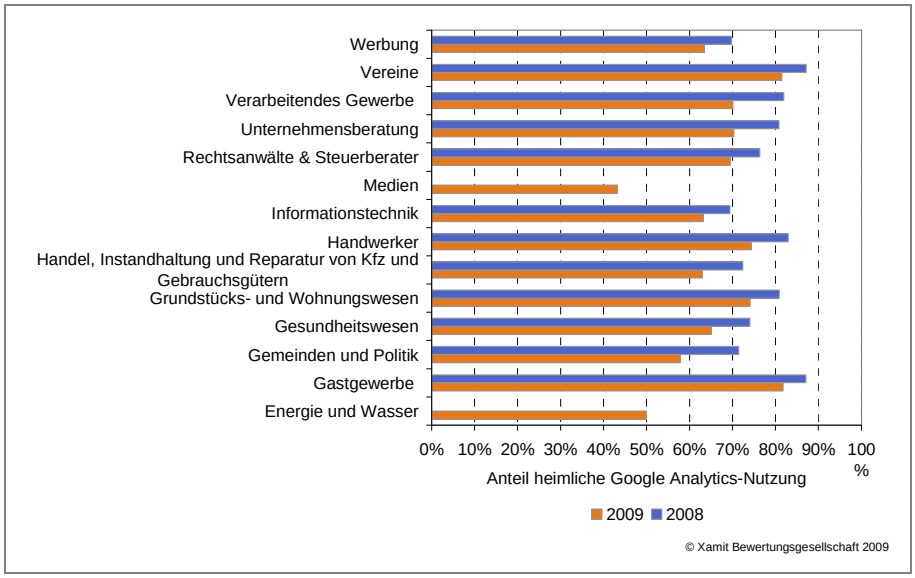


Abbildung 4: Heimliche Nutzung von Google Analytics nach Branchen

Vereine und Gastgewerbe sind die größten heimlichen Datensammler

Abbildung 4 zeigt die heimliche Nutzung von Google Analytics nach Branchen. Medien sowie Energie und Wasser sind neu hinzugekommen, so dass für 2008 noch keine Werte vorliegen. Vereine und das Gastgewerbe setzen heute mit 82% noch fast vollständig auf eine heimliche Datensammlung und nutzen die von Google vorgegebene Textpassage weiterhin sehr zurückhaltend (Abbildung 5). Erfreulicherweise nutzen inzwischen deutlich mehr Webpräsenzen den Google Passus als 2008. Ein sehr positiver Effekt der öffentlichen Debatte.

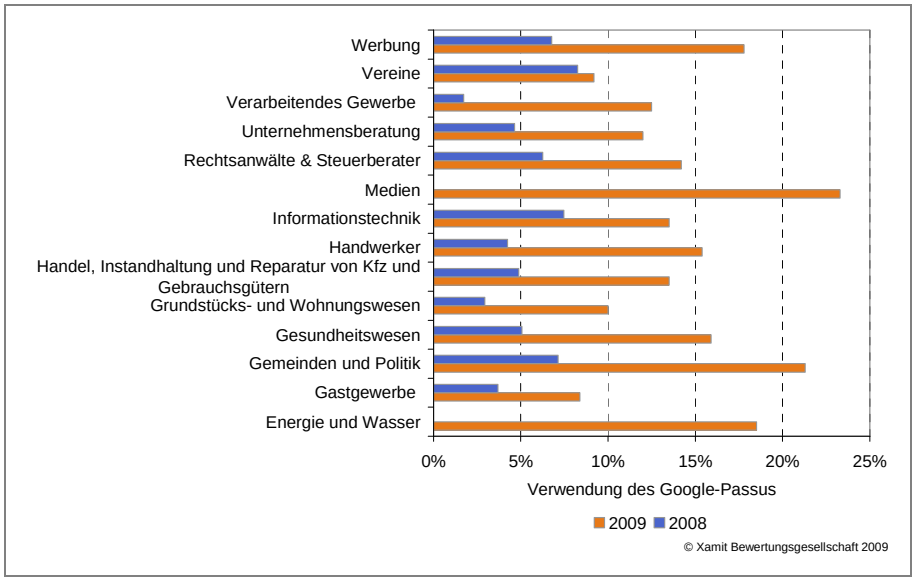


Abbildung 5: Verwendung des Google-Passus nach Branchen

© Xamit Bewertungsgesellschaft mbH

4.4 Kontaktformulare – Datenverarbeitung im Verborgenen

Im 2008 analysierten wir die Nutzung von Kontaktformularen auf deutschen Webpräsenzen. 42% der damals untersuchten Webpräsenzen setzten Kontaktformulare ein. Heute sind es 45%. Abbildung 6 zeigt die Nutzung nach Branchen. Spitzenreiter sind die Medien mit 71%.

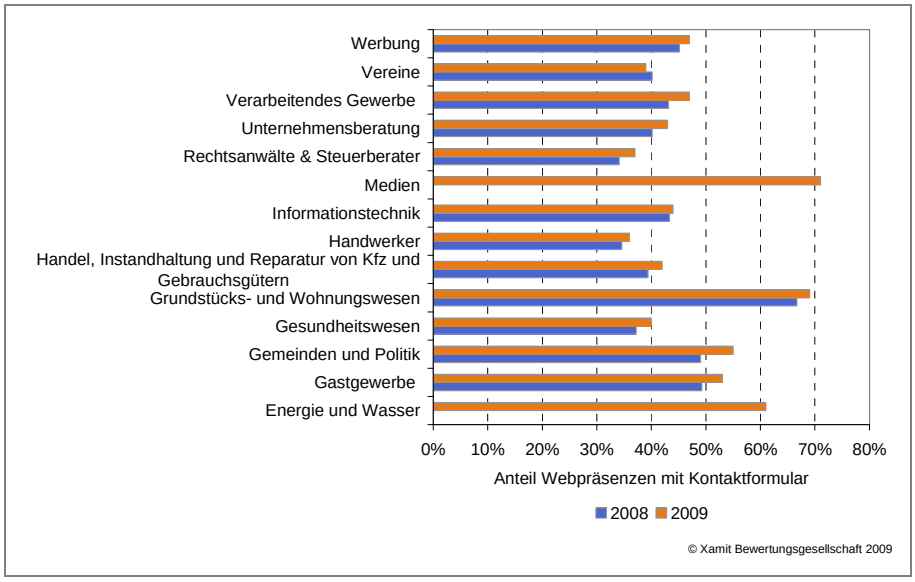


Abbildung 6: Einsatz von Kontaktformularen nach Branchen

Wie gehen die Betreiber mit den anfallenden personenbezogenen Daten um?

Information über die Verarbeitung der persönlichen Daten nimmt insgesamt zu

Von den Webpräsenzen mit Kontaktformular informieren 23% (2008: 17%) über ihren Umgang mit den erhobenen Daten. Lediglich bei 7% (2008: 5%) wird die Datenschutzerklärung entweder direkt beim Kontaktformular angezeigt oder ein Link zur Datenschutzerklärung angeboten. In Summe werben mehr Betreiber um Vertrauen in ihren Umgang mit den eingegebenen persönlichen Daten.

Abbildung 7 zeigt, wie heute die einzelnen Branchen mit den Datenschutzerklärungen umgehen. 3% (2008: 2%) aller untersuchten Webpräsenzen (mit und ohne Kontaktformular) erheben personenbezogene Daten vorbildlich, indem sie eine Datenschutzerklärung veröffentlichen und diese direkt mit dem Kontaktformular verlinken. Weitere 7% (2008: 5%) erheben die Daten und geben eine nicht verlinkte Datenschutzerklärung an. 35% (2008: 35%) aller untersuchten Webpräsenzen fragen personenbezogene Daten ab ohne eine Datenschutzerklärung zu veröffentlichen. Die restlichen 55% (2008: 58%) verzichten auf die Erhebung personenbezogener Daten.

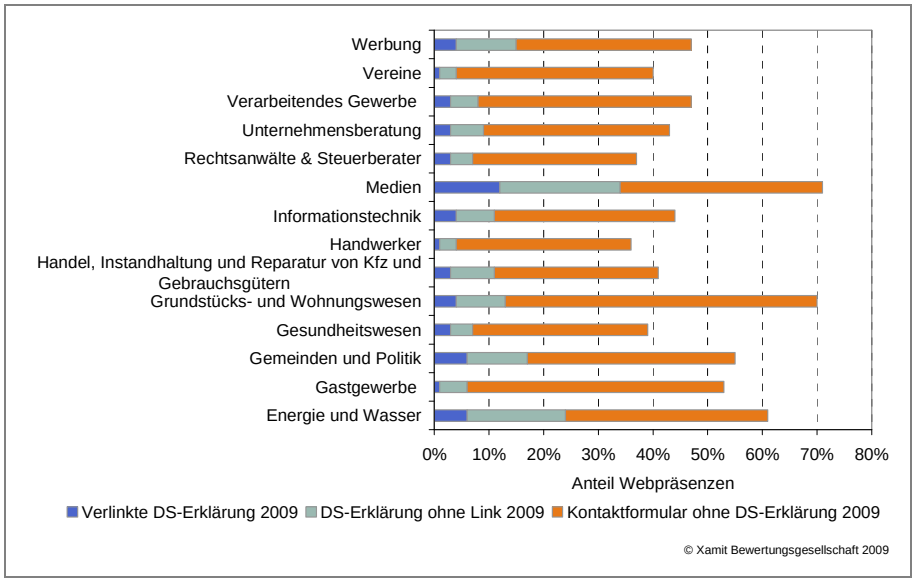


Abbildung 7: Datenschutzerklärungen bei Kontaktformularen

Immer noch machen gut drei Viertel der Webseiten keine Angaben darüber, was mit eingegebenen Daten passiert.

Insgesamt verfügen 23% (2008: 17%) der Webpräsenzen mit Kontaktformular über eine Datenschutzerklärung. Alles in allem können wir also eine leicht positive Entwicklung feststellen, was jedoch nicht darüber hinweg täuschen darf, dass immer noch 77% der Webseiten-Betreiber Ihre Besucher im Dunkeln darüber lassen, was mit den im Kontaktformular eingegebenen persönlichen Daten geschieht.

5 Das Xamit-Datenschutzbarometer 2009

Messung des Datenschutzniveaus nach objektiven Kriterien

In Kapitel 4 untersuchten wir vier einzelne Aspekte, die den Umgang mit persönlichen Daten im Internet illustrieren. Alle vier Aspekte haben wir anhand der gleichen Webpräsenzen untersucht, d.h. die Befunde sind untereinander vergleichbar. Mehr noch, eine Webpräsenz kann sowohl eine Webstatistik nutzen als auch ein Kontaktformular ohne Datenschutzerklärung. Aus diesem Grund kombinieren wir unsere Befunde zu einem Index: dem Xamit-Datenschutzbarometer. Das Datenschutzbarometer zeigt an, wie es um den Schutz persönlicher Daten im Internet bestellt ist.

Ähnlich einer Kriminalitätsstatistik zählt das Datenschutzbarometer alle Webpräsenzen, die

- heimlich Webstatistiken durch Statistikanbieter erstellen lassen,
- Google Analytics nutzen,
- Kontaktformulare ohne Datenschutzerklärung nutzen,
- Adsense ohne Datenschutzerklärung einbinden,
- unsichere Shop-Software verwenden oder
- unsichere PHP-Versionen bei Online-Shops einsetzen.

Nutzung von Google Analytics als zusätzlichen Verstoß aufgenommen

Den Verstoß „Nutzung von Google Analytics“ nehmen wir aufgrund der Stellungnahme des ULD (siehe Kapitel 4.3) neu auf. Wir passen die angegebenen Vergleichswerte für 2008 entsprechend an.

Um das Datenschutzbarometer vergleichbar mit zukünftigen Untersuchungen zu halten, setzen wir die Anzahl an Beanstandungen in Relation zur Anzahl der untersuchten Webpräsenzen.

Die Folgen eines Datenschutzvergehens hängen davon ab, welches Angebot eine Webpräsenz hat oder welchem Zweck sie dient. Eine heimliche Webstatistik eines Sockenhändlers sagt weniger Persönliches aus als die Webstatistik eines Facharztes. Wir fassen deshalb die betrachteten Branchen in folgende Klassen zusammen:

- Sensible Daten: Alle Branchen, die mit sensiblen Daten umgehen, wie das Gesundheitswesen, Rechtsanwälte und Steuerberater.
- Alltag: Hierunter fassen wir alle Branchen zusammen mit denen ein Konsument im Alltag zu tun hat, wie z.B. Handel, Gastgewerbe, Grundstücks- und Wohnungswesen und Handwerker, Energiewirtschaft und Medien.
- eGovernment: Alle staatlichen Stellen, wie z.B. Gemeinden, aber auch Parteien fallen in diese Klasse.
- Datenschutzmultiplikatoren: Unternehmen, deren Aufgabenfeld eine größere Datenschutzkompetenz erwarten lässt oder die ihre Kunden im Umgang mit personenbezogenen Daten beraten sollten, fassen wir in dieser Klasse zusammen. Dazu gehören Informationstechnik und Werbung.

- Gewerbe: Unternehmen des produzierenden Gewerbes sind hier zusammengefasst.
- Dienstleistung: Alle Dienstleistungsunternehmen, die in keine der anderen Klassen fallen, zählen hierzu, wie z.B. Unternehmensberatungen.
- Vereine: Vereine bilden eine eigene Klasse.

61% der untersuchten Webseiten geben Grund zur Beanstandung

Insgesamt haben wir Verstöße oder Gründe zur Beanstandung auf 61 von 100 untersuchten Webpräsenzen gefunden. 2008 waren es inkl. Google Analytics Nutzung 55. Eine Steigerung um 11%. Abbildung 8 vergleicht die Verstöße 2008 mit 2009.

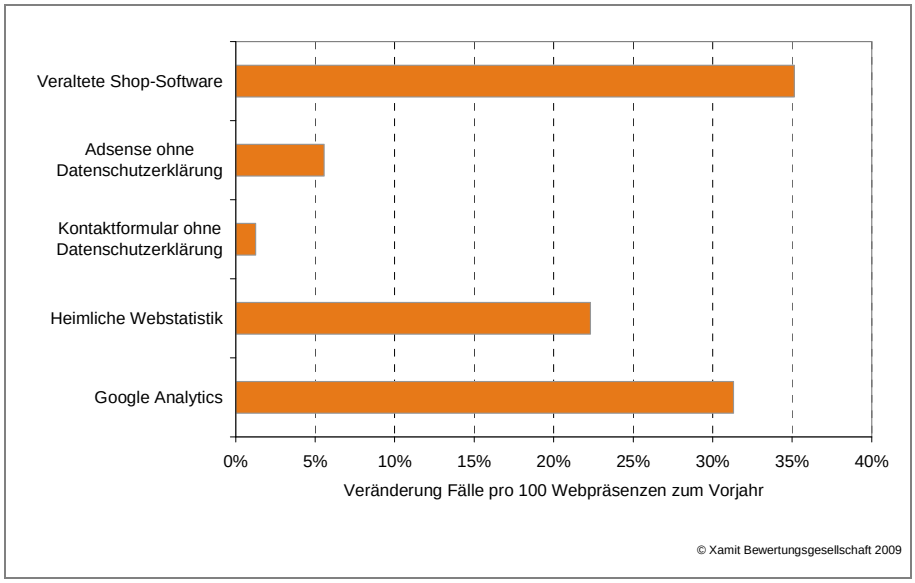


Abbildung 8: Entwicklung der Verstöße und Beanstandungen

Gerade bei Fachleuten haben die Verstöße um fast 50% zugenommen

Spitzenreiter sind – wie auch 2008 – die Datenschutzmultiplikatoren mit 77 Verstößen (2008: 52 Verstöße) pro 100 Webpräsenzen (Abbildung 9). Da viele Unternehmen und Organisationen bei ihren Online-Aktivitäten auf die Kompetenz von Werbefachleuten und IT-Fachleuten setzen, wirkt die Datenschutzsensibilität dieser Fachleute in viele andere Unternehmen hinein. Vor allem die Zunahme der Verstöße um fast 50 Prozent lässt erahnen, wohin die Reise bei diesen Unternehmen gehen könnte.

© Xamit Bewertungsgesellschaft mbH

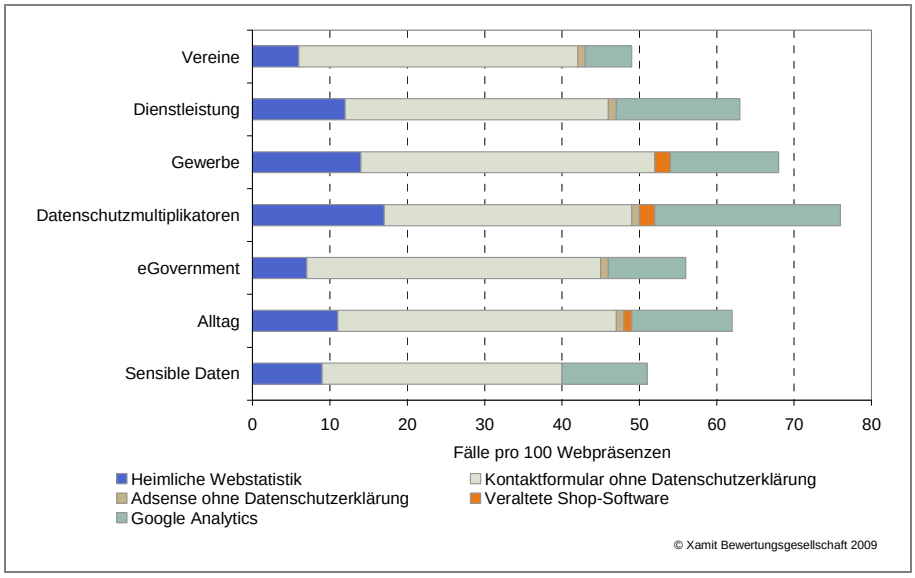


Abbildung 9: Verstöße und Beanstandungen nach Klassen

Eine regionale Verteilung nach Bundesländern zeigt Abbildung 10. Spitzenreiter ist Hamburg mit 77 Verstößen. In diese Darstellung sind diejenigen Webpräsenzen eingeflossen, deren Betreiber wir einem Bundesland zuordnen konnten. 2.240 Webpräsenzen konnten wir keinem Bundesland zuordnen, weshalb sie in den Zahlen nicht berücksichtigt sind.

In Hamburg wurden die meisten Beanstandungen festgestellt

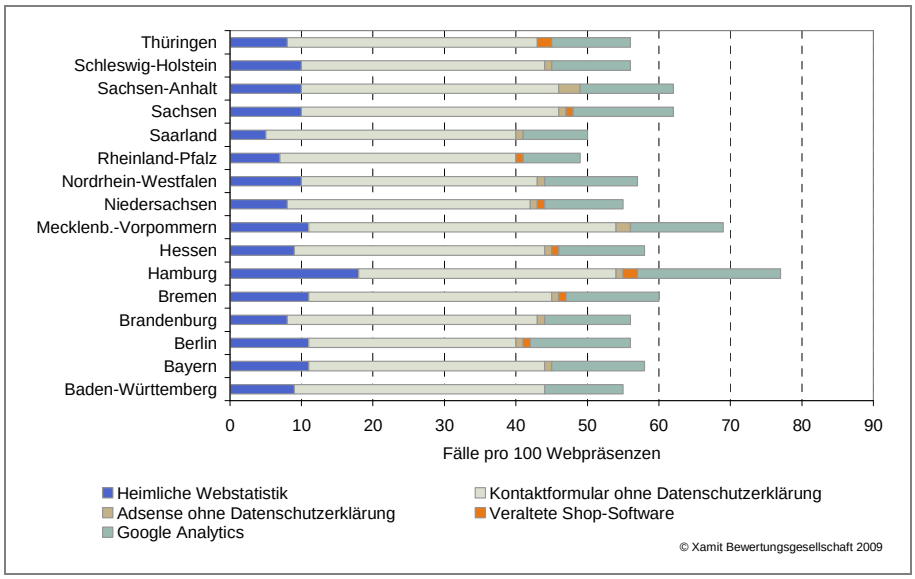


Abbildung 10: Verstöße und Beanstandungen nach Bundesländern

6 Datenschutz – keine Unternehmensaufgabe?

Datenschutzverstöße im Internet nehmen deutlich zu (siehe Kapitel 5). Liegt das am Medium Internet, welches einige Politiker als „rechtsfreien Raum“ bezeichnen? Oder liegt die Ursache tiefer? Gäbe es flächendeckende Datenschutzkontrollen analog zur Betriebsprüfung durch Finanzbehörden oder Gesundheitsämter, dann könnten deren Statistiken herangezogen werden. Flächendeckende Datenschutzkontrollen finden aber nicht statt und wären mit dem heutigen Personalbestand in den Aufsichtsbehörden auch nicht durchführbar (Kapitel 7). Wir nähern uns der Antwort deshalb über einen Umweg, dessen Prinzip wir in unserer Studie „Parteien & Datenschutz“[22] ausführlich beschrieben haben.

Das BDSG sieht als betriebliche Kontrollinstanz den betrieblichen Datenschutzbeauftragten[23] oder die Geschäftsleitung vor. Als Arbeitsgrundlage dient ein Verfahrensverzeichnis. Das Verfahrensverzeichnis beschreibt

- den Zweck der Datenverarbeitung,
- die Rechtsgrundlage,
- wer die Daten verarbeitet,
- welche Daten verarbeitet werden,
- von wem Daten verarbeitet werden und
- wohin die Daten übermittelt werden.

Das Verfahrensverzeichnis gibt es in zwei Versionen (vgl. § 4e BDSG): Im öffentlichen Verfahrensverzeichnis stehen allgemeine Informationen darüber, welche Daten zu welchen Zwecken verarbeitet werden. Dieses muss jedermann auf Verlangen zugänglich gemacht (§ 4g Abs. 2 S. 2 BDSG). Das interne Verfahrensverzeichnis enthält sensible Informationen wie z.B. IT-Sicherheitsmaßnahmen und braucht außer an die Aufsichtsbehörde an niemanden herausgegeben zu werden.

Kein Verfahrensverzeichnis – kein Datenschutz

Ohne ein Verfahrensverzeichnis fehlt der Überblick, welche personenbezogenen Daten verarbeitet werden. Damit sind Zweckänderungen, ausbleibende Löschungen, Sicherheitsprobleme und weitere Datenschutzverstöße vorprogrammiert.

Wie viele Organisationen verfügen über ein solches Verfahrensverzeichnis und sind damit in der Lage, datenschutzkonform zu handeln?

Testpersonen haben per E-Mail an die im Impressum auf der Webseite angegebene Adresse von 395 Organisationen, deren Webseite wir in Kapitel 4 analysiert hatten, um die Zusendung des öffentlichen Ver-

[22] Kostenfreier Download unter http://www.xamit-leistungen.de/studienundtests/index.php.
[23] Bei Organisationen, in denen mehr als neun Personen personenbezogene Daten automatisiert verarbeiten oder Einsicht in diese Daten haben, muss ein Datenschutzbeauftragter bestellt werden.

© Xamit Bewertungsgesellschaft mbH

fahrensverzeichnisses gebeten. Die Zusendung konnte elektronisch oder postalisch erfolgen. Der Untersuchungszeitraum reichte von Ende August bis Ende Oktober 2009.

Von den 395 versandten E-Mails waren 17 unzustellbar, d.h. 4% der im Impressum genannten E-Mail-Adressen funktionieren nicht. Diese Betreiber verstoßen damit gegen die Kennzeichnungspflicht (§ 5 Abs. 1 Nr. 2 TMG). Die folgenden Zahlen beziehen sich auf die 378 zugestellten E-Mails.

Nur 5% der angefragten Organisationen verhielten sich gesetzeskonform

5% schickten postalisch oder elektronisch ein Verfahrensverzeichnis zu. Ein Steuerberater verweigerte mit fragwürdigen Argumenten die Einsichtsnahme. 4% verstanden die Anfrage nicht und 1% reagierten mit unnötigen Gegenfragen. Die übrigen 90% antworteten gar nicht erst. Fazit: 95% der angefragten Organisationen verstießen gegen das Einsichtsrecht. Abbildung 11 zeigt die Reaktionen nach Branchen. Medien-Unternehmen hatten wir nicht angesprochen.

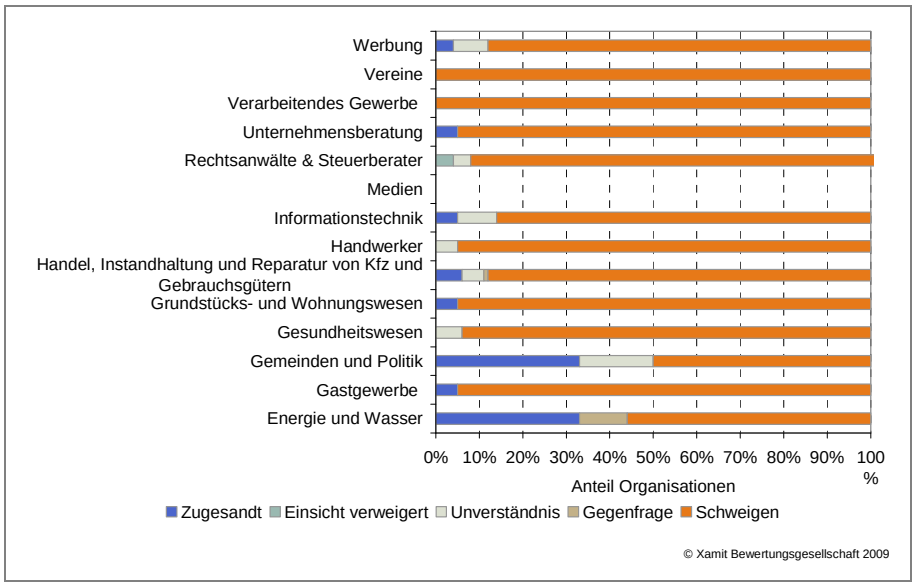


Abbildung 11: Reaktionen auf die Anforderung des Verfahrensverzeichnisses

Halten Unternehmen sich an die Datenschutzbestimmungen auch ohne Verfahrensverzeichnis? Der Blick auf eine Auswahl an Sicherheitsvorfällen, die 2009 für Medienaufmerksamkeit sorgten, weckt Zweifel:

- Angestellte der britischen Tochter der Deutschen Telekom, haben Millionen von sensiblen Kundendaten an Zwischenhändler weiterverkauft
- Deutsche Bank gestattet selbstständigen Finanzberatern Einblick in Kundenkonten
- Berliner Firma stellt 2.500 falsche Stellenangebote beim Arbeitsamt ein, um an die Daten der Bewerber zu kommen
- Benutzer können 350.000 Rechnungen im Sparkassen-Shop einsehen

- Arbeitsagentur macht Bewerberdaten Dritten ohne Kontrolle zugänglich
- Rechnungen von Hunderttausenden Libri.de-Kunden im Internet einsehbar
- Mitarbeiter der Arbeitsagentur können sensible Daten von Hartz IV-Empfängern einsehen
- Postbank gestattet Einblick in Millionen Girokonten ihrer Kunden zu Werbezwecken
- Hacker spionieren Millionen Daten bei SchülerVZ aus
- Finanzdienstleister AWD gibt weiteres Datenleck bekannt: Interne Abrechnungen im Internet veröffentlicht
- Schwere Datenpanne bei Finanzdienstleister AWD
- Deutsche Telekom: Hunderttausende Kontoverbindungsdaten von Kunden ins Ausland gelangt
- Textildiscounter Kik spioniert Mitarbeiter und Bewerber über deren Bonität aus
- Zwei 750 Liter-Container voller persönlicher Daten in Mainz entdeckt
- CDU nutzt Mitgliederadressen des Turnvereins Hanau für Werbung
- Deutsche Bank bespitzelt Aufsichtsrat
- Patientendaten auf der Straße gefunden
- Hunderte Bewerbungsunterlagen bei ebay versteigert
- Kriminelle manipulieren Geldautomat und verschaffen sich Zugriff auf 55 Konten
- Fraktionsspitze kassiert private E-Mails ein
- CDU-Stadtverbandsspitze leitet private E-Mails um
- Möglicher Missbrauch von MasterCard-Kreditkarten
- Blitzer-Videos mit Autokennzeichen live auf privatem Fernseher
- Wahlwerbung an 1.600 Grundschüler verschickt
- Das Abonnenten-Callcenter des SPIEGEL sammelt Krankendaten der Mitarbeiter
- Reporter kaufen im Internet Tausende privater Datensätze mit Bankverbindungen
- Verlust eines USB-Sticks mit gespeicherten Kopien von Daten des Elektronischen Grundbuchs der Grundbuchämter Demmin und Ribnitz-Damgarten
- Unzulässige Krankendatensammlung bei der Deutschen Bahn
- Versicherten-Daten in offenem Container
- Konto-Daten von Ratsmitgliedern auf der Straße
- Abrechnungen von Ratsmitgliedern auf der Straße gefunden
- Panne bei der Sendungsverfolgung von DHL
- Sparkasse Köln/Bonn soll Mitarbeiter- und Kundendaten ohne Anonymisierung an externen Berater geschickt haben
- Märkische Klinik: Zwei Festplatten mit Patientendaten verschwunden
- Pressefotograf erhält monatelang E-Mails mit fremden Bankdaten
- Krankenkassen dürfen Kundendaten nicht klammheimlich weitergeben
- Vertrauliche Gerichtsakten im Müllcontainer gefunden
- Lidl führte geheime Krankenakten über Mitarbeiter

© Xamit Bewertungsgesellschaft mbH

- Kundendaten von Kabel Deutschland kursieren weltweit im Internet
- Fehler im Verlagshaus Madsack macht Kundendaten sichtbar
- DSDS-Bewerberdatenbank offen im Netz
- Verlorener USB-Stick enthält Kranken-Befunde
- Bildungsträger Kolping legt sensible Daten offen
- Datenpanne bei 1&1: Verbindungsdaten liegen offen
- Hunderte Datensätze von Kunden auf der Telekom-Website offen einsehbar
- www.geldkarte.de: Nutzerdaten offen im Netz
- Deutsche Bahn späht Tausende Mitarbeiter aus

7 Politik: Alle 39.400 Jahre eine Datenschutzkontrolle

In Kapitel 6 haben wir gesehen, dass in fast allen deutschen Unternehmen nur in den seltensten Fällen die Grundlagen für einen wirkungsvollen Datenschutz geschaffen sind. Doch was passiert eigentlich, wenn ein Betrieb kein Verfahrensverzeichnis hat? Oder keinen Datenschutzbeauftragten, obwohl die kritische Zahl an Mitarbeitern längst erreicht ist? Kapitel 7.1 gibt eine Antwort auf die Frage nach der staatlichen Kontrolldichte und somit, wie es mit der Wirksamkeit des Bundesdatenschutzgesetzes bestellt ist. Danach stellen wir am Beispiel einer Aufsichtsbehörde dar, welche Arbeiten anfallen können und wie hoch die Arbeitsbelastung ist (Kapitel 7.2). Außerdem gehen wir der Frage nach, warum trotz der vielen Datenrechtsverstöße nur verhältnismäßig wenige Bußgelder verhängt werden.

7.1 Aufsicht ohne Personal

Wir haben alle 23 den Ländern unterstehenden Aufsichtsbehörden angeschrieben und ihre Stellenanzahl in Vollzeitäquivalenten erfragt.[24] Den Bundesbeauftragten für den Datenschutz und die Informationsfreiheit lassen wir unberücksichtigt, da er nur für die öffentlichen Stellen des Bundes und nur in Ausnahmen für wenige nicht öffentliche Stellen zuständig ist.

70% der Behörden haben geantwortet. Herzlichen Dank dafür! Für folgende Bundesländer liegen vollständige Angaben vor:

- Berlin
- Brandenburg
- Hamburg
- Mecklenburg-Vorpommern
- Nordrhein-Westfalen
- Rheinland-Pfalz
- Sachsen
- Sachsen-Anhalt
- Schleswig-Holstein

Für folgende Bundesländer liegen nur unvollständige Angaben vor, da von zwei Aufsichtsbehörden, jeweils eine für öffentliche und eine für nicht-öffentliche Stellen, nur jeweils eine Behörde die erbetenen Angaben zur Verfügung stellte:

- Baden-Württemberg
- Bayern
- Hessen
- Saarland
- Thüringen

[24] Wir verwenden den Begriff „Aufsichtsbehörde“ aus Gründen der Lesbarkeit in Abweichung zum BDSG sowohl für den öffentlichen wie auch für den nicht-öffentlichen Bereich. In beiden Fällen wird faktisch eine kontrollierende Aufsicht geführt.

© Xamit Bewertungsgesellschaft mbH

Alle Zahlen geben Vollzeitstellen wieder. Wenn Antworten zwischen besetzten Stellen und Planstellen differenzieren, nehmen wir die Planstellen, da sie die maximal mögliche Ausstattung widerspiegeln.

Einige befragte Behörden nehmen neben ihrer Aufsichtstätigkeit auch weitere Aufgaben war, z.B. Aufgaben basierend auf Informationsfreiheitsgesetzen. Aus diesem Grund sind die Stellenangaben nur schwer vergleichbar, denn die hier vorgestellten Zahlen berücksichtigen die unterschiedlichen Aufgaben der Aufsichtsbehörden nicht. Gleichwohl zeigen sie qualitativ auf, wie es um die Ausstattung der Datenschutzaufsicht bestellt ist.

Demnach verfügen die antwortenden Behörden 2009 über knapp 272 Stellen. Davon entfallen 256 auf das Kernpersonal, 12 auf Praktikanten und Referendare und vier auf Auszubildende und Trainees.

Das Kernpersonal nahm in vielen Aufsichtsbehörden zwischen 2007 und 2009 zu. Im Saarland, Schleswig-Holstein und Thüringen blieb der Personalbestand unverändert. Nordrhein-Westfalen baute als einziges Bundesland Personal ab (Abbildung 12).

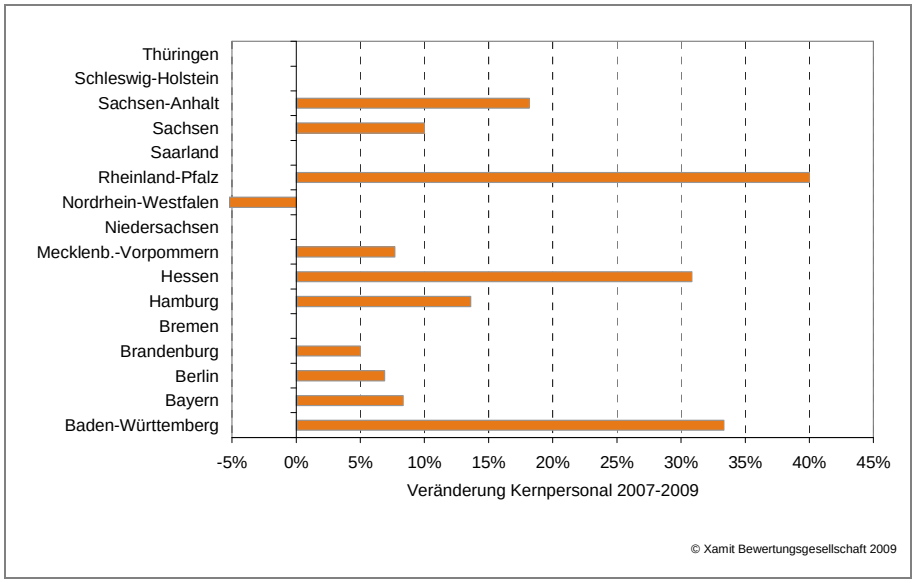


Abbildung 12: Veränderungen in der Stellenausstattung

Das Datenschutzrecht unterscheidet in öffentliche und nicht öffentliche Organisationen

Das Datenschutzrecht kennt für öffentliche (z.B. Behörden) und nicht öffentliche (z.B. Unternehmen, Vereine, Parteien) Stellen unterschiedliche Regeln. Um die Stellenanzahl in Relation zu einigen Kennzahlen zu setzen, unterteilen wir die Stellen in öffentliche und nicht öffentliche Stellen. Einige Aufsichtsbehörden arbeiten ausschließlich in einem der beiden Bereiche, so dass wir deren Stellen dem jeweiligen Bereich einfach zuordnen können. Bei Aufsichtsbehörden, die beide Bereiche abdecken, verteilen wir die Stellen – sofern wir keine anderen Angaben erhalten haben – 2/3 zu 1/3 zu Gunsten des öffentlichen Bereichs. Damit nehmen wir ein wesentlich günstigeres Verhältnis an, als bei den anderen bereichsspezifischen

Aufsichtsbehörden zu beobachten ist. Tabelle 1 zeigt die Verteilung der Stellen nach Bundesländern.

Bundesland	Nicht öffentlicher Bereich	Öffentlicher Bereich
Baden-Württemberg	8,00	k.A.
Bayern	k.A.	26,00
Berlin	10,20*	20,8*
Brandenburg	4,00	17,00
Bremen	k.A.	k.A.
Hamburg	5,50*	11,20*
Hessen	12,47	k.A.
Mecklenburg-Vorpommern	2,00	12,00
Niedersachsen	k.A.	k.A.
Nordrhein-Westfalen	15,00*	30,00*
Rheinland-Pfalz	4,60*	9,40*
Saarland	k.A.	10,00
Sachsen	7,30*	14,70*
Sachsen-Anhalt	3,50	16,00
Schleswig-Holstein	5,25	8,75
Thüringen	2,00	k.A.

Tabelle 1: Personalausstattung der Datenschutzaufsicht verteilt auf öffentliche und nicht öffentliche Stellen. Die Zahlen mit * sind geschätzt nach oben genanntem 2/3 zu 1/3-Schlüssel.

Der Kontrollgegenstand einer Aufsichtsbehörde ist z.B. ein Unternehmen oder eine andere Behörde. Eine wesentliche Kennzahl, um die Größe eines Unternehmens oder einer Behörde zu beschreiben, stellt die Anzahl der sozialversicherungspflichtigen Beschäftigten dar. Wir setzen deshalb

- die Stellen für den öffentlichen Bereich zu der Anzahl an Beschäftigten im öffentlichen Sektor (Bund[25], Land und Gemeinden) ins Verhältnis.
- die Stellen für den nicht öffentlichen Bereich zu der Anzahl an Beschäftigten im Privatsektor ins Verhältnis.

Für die Kontrolle von Behörden steht wesentlich mehr Personal zur Verfügung als für die von Unternehmen

Abbildung 13 zeigt deutlich, dass für den öffentlichen Bereich deutlich mehr Stellen pro 100.000 Beschäftigten zur Verfügung stehen als für die Kontrolle von Unternehmen, Vereinen und Parteien.

[25] Die Bundesbehörden gehören nicht zum Aufgabenbereich der hier betrachteten Aufsichtsbehörden. Deshalb zeichnen unsere Berechnungen ein zu optimistisches Bild.

© Xamit Bewertungsgesellschaft mbH

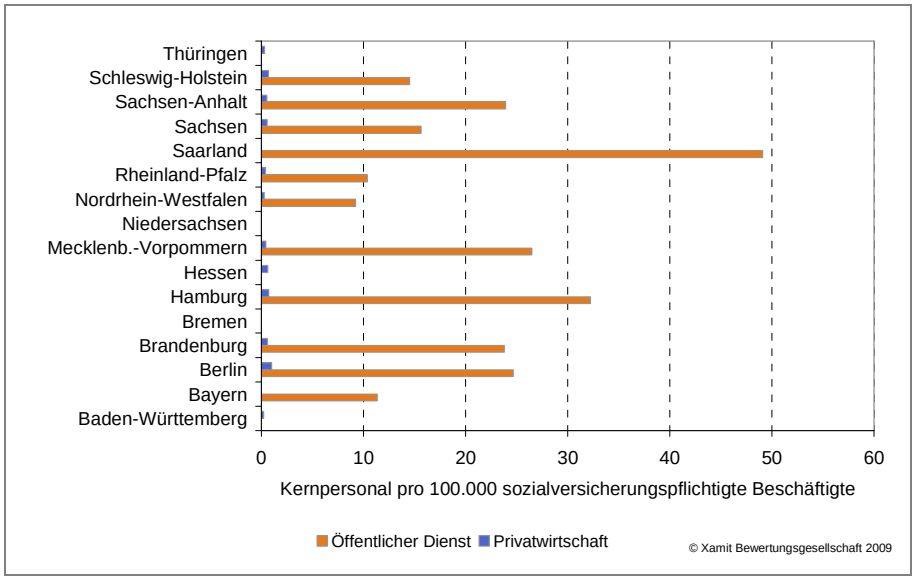


Abbildung 13: Stellenverteilung in Relation zur Anzahl sozialversicherungspflichtiger Beschäftigter

Bezogen auf die Unternehmensanzahl (also ohne Vereine, Parteien und andere Organisationen) stehen Bundesweit 2,2 Stellen pro 100.000 Unternehmen zur Verfügung.

Die Datenschutzaufsicht hat 2,2 Stellen pro 100.000 Unternehmen zur Verfügung

Zum Vergleich: Für die Finanzverwaltung waren 2008 244.600 Menschen in Bund, Ländern und Gemeinden tätig.[26] Das macht 6.888 Personen pro 100.000 Unternehmen. Steuererhebung ist also 3.131 Mal wichtiger als der Schutz von Grundrechten.

7.2 Arbeitsbelastung der Datenschutzaufsicht am Beispiel von Baden-Württemberg

Nachdem wir gesehen haben, dass die Personaldecke in den Aufsichtsbehörden für die geforderten Aufgaben recht dünn ist, wollen wir einmal exemplarisch an der Aufsichtsbehörde von Baden Württemberg ausrechnen, wie viel Zeit den Mitarbeitern zur Prüfung in den Unternehmen vor Ort bleibt. Wir treffen folgende vereinfachende Annahmen:

- Mitarbeiter verfügen über eine Netto-Arbeitszeit von acht Stunden pro Tag, d.h. sie widmen ihre volle Aufmerksamkeit ihrer Tätigkeit, ohne von kollegialen Gesprächen, Meetings oder sonstiger Kommunikation abgelenkt zu werden.
- Von den 254 Arbeitstagen im Jahr subtrahieren wir insgesamt 40 Tage für Abwesenheiten (Krankheit[27] und Urlaub).

[26] Quelle: http://www.destatis.de/jetspeed/portal/cms/Sites/destatis/Internet/DE/Content/Statistiken/FinanzenSteuern/OeffentlicherDienst/PersonalOeffentlicherDienst/Tabellen/Content75/GebietskoerperschaftenAufgabenbereiche,templateId=renderPrint.psml. Letzter Zugriff: 2009-10-21.

[27] Im Schnitt meldete sich 2007 jeder Bundesbedienstete mehr als 15 Tage pro Jahr krank. Vgl. Öffentlicher Dienst: Staatsdiener sind öfter krank. Focus online. URL:

Im Jahr 2008 standen der Aufsichtsbehörde im nicht öffentlichen Bereich in Baden Württemberg sieben Mitarbeiter zur Verfügung.[28] Das macht für Baden Württemberg insgesamt 1.498 Personentage.

In Tabelle 2 berechnen wir den durchschnittlichen Aufwand für die anfallenden, von außen eingehenden Aufgaben in den Behörden. Darunter sind alle schriftlichen Beschwerden zusammengefasst. Nach Angaben von Aufsichtsbehörden reicht die Bearbeitungsdauer dieser Vorfälle „je nach Bereich von wenigen Tagen bis zu mehr als einem Jahr in Ausnahmefällen."[29] Wir haben eine durchschnittliche Bearbeitungsdauer von zwei Tagen angenommen, die sehr konservativ geschätzt ist. Beratungsanfragen werden in den meisten Fällen von Bürgern, Unternehmen und Datenschutzbeauftragten gestellt, wir nehmen eine durchschnittliche Dauer von einem halben Tag an.

	Baden-Württemberg	
Art des Vorgangs (Zeitbedarf)	**Anzahl**	**Bedarf in PT**
Eingaben (2 Tage/Vorgang)	658	1.316
Anrufe (10 Minuten/Anruf)	2.000	42
Beratungsanfragen (½ Tag/Beratung)	239	120
Summe		**1.477**
Anzahl PT zur Verfügung		1.498
Differenz zur Ist-Situation		**21**

Tabelle 2: Arbeitsbelastung am Beispiel Baden Württembergs in 2008 anlässlich von außen eingehender Anfragen

Die Tabelle macht deutlich, dass der eigentliche Schwerpunkt der Aufsichtsbehörden auf der beratenden Tätigkeit liegt. Für Kontrollen von Unternehmen hat Baden Württemberg 21 PT im Jahr „übrig".

Wir wissen von Baden Württemberg, dass die Behörde im Jahr 2008 insgesamt zwölf solcher Kontrollen in unterschiedlicher Größenordnung durchgeführt hat.

Alle 39.400 Jahre eine Datenschutz-Kontrolle

Wenn wir uns also die verbleibenden Tage für Kontrollen anschauen, wird deutlich, dass eine abschreckende Kontrolldichte nicht erkennbar ist. Das Innenministerium von Baden-Württemberg hat in seiner Rolle als Aufsichtsbehörde für den nicht-öffentlichen Bereich im Jahr 2008 zwölf Unternehmen vor Ort überprüft.[30] Das entspricht 0,0025% aller Unternehmen dieses Bundeslandes. Bei dieser Kontrollfrequenz wartet ein Unternehmen mehr als 39.400 Jahre auf eine Datenschutzkontrolle. Von Kontroll„dichte" kann hier nicht mehr die Rede sein.

http://www.focus.de/karriere/berufsleben/arbeitsalltag/oeffentlicher-dienst-staatsdiener-sind-oefter-krank_aid_357642.html. Letzter Zugriff: 2009-11-18.

[28] Siehe Antwort des Innenministeriums zum Antrag der Landtagsfraktion der SPD (Drucksache 14/4478). S. 6.

[29] Siehe Antwort des Innenministeriums zum Antrag der Landtagsfraktion der SPD (Drucksache 14/4478). S. 4.

[30] Ebd.

© Xamit Bewertungsgesellschaft mbH

Viele Verstöße, wenige Bußgelder – warum?

Was passiert aber, wenn bei einer Kontrolle Datenschutzverstöße erkannt werden? Das ist immerhin bei 70 bis 80% der eingehenden Beschwerden der Fall.[31] Erst kürzlich machten Bußgelder in Millionenhöhe für die Datenschutzverstöße bei der Deutschen Bahn[32] und zum wiederholten Male bei Lidl[33] Schlagzeilen. Doch sind Bußgeldverfahren im Alltag der Aufsichtsbehörden bisher eher die Ausnahme als die Regel. Innerhalb eines Jahres wurden pro Bundesland gerade einmal 2,75 Bußgeldbescheide erlassen.[34] Woran liegt das?

Pro Bundesland wurden innerhalb eines Jahres nur 2,75 Bußgeldbescheide erlassen

Dass nur eine geringe Anzahl an Bußgeldverfahren eingeleitet wird, liegt unter anderem an der mangelnden personellen Besetzung der Aufsichtsbehörden. Ohne Personal können keine wirksamen Kontrollen durchgeführt und somit auch keine Verstöße aufgedeckt und Bußgelder verhängt werden. Dass nicht immer, wenn ein Datenschutzverstoß gemeldet wird, auch ein Bußgeldverfahren eingeleitet werden muss, zeigt der Fall Daimler[35]. Hier wurden zum wiederholten Male heimlich Listen mit Krankendaten von Mitarbeitern erstellt. Bisher ist das Unternehmen mit zwei Rügen der Aufsichtsbehörde davongekommen, da es sich einsichtig zeigte und die Fälle umgehend aufarbeitete.

Im Fall einer datenschutzrechtlichen Prüfung muss die verantwortliche Stelle in der geprüften Organisation sowie der Beschwerdeführer von dem Ergebnis der Prüfung informiert werden. Dann wird „darauf hingewirkt“, dass solche Verstöße künftig nicht mehr vorkommen und evtl. ein Gespräch mit der verantwortlichen Stelle geführt. Denn nach geltendem Gesetz haben die Aufsichtsbehörden fast keine Möglichkeit, verbindliche Anordnungen zu erlassen. Bei Häufungen innerhalb einer Branche setzt sich die Aufsichtsbehörde z.B. mit dem übergeordneten Verband in Verbindung. Doch nur in wenigen Fällen werden Bußgeldverfahren eingeleitet.[36] Bußgelder werden meist nur verhängt, wenn die Behörden kein anderes Mittel mehr zur Ahndung eines aufgedeckten Datenschutzverstoßes sehen.

So ist es kein Wunder, wenn Datenschutzverstöße bewusst in das unternehmerische Risiko einkalkuliert werden oder man sich auf Seite

Datenschutzverstöße als Teil des unternehmerischen Risikos

[31] S. Antwort des Innenministeriums zum Antrag der Landtagsfraktion der SPD (Drucksache 14/4478). S. 3.
[32] Datenskandal: Bahn soll Bußgeld zahlen. URL: http://nachrichten.rp-online.de/article/wirtschaft/Datenskandal-Bahn-soll-Bussgeld-zahlen/55735. Letzter Zugriff: 2009-10-20.
[33] Datenschutzaufsichtsbehörden verhängen hohe Bußgelder gegen Lidl. URL: http://www.innenministerium.baden-wuerttemberg.de/de/Meldungen/192358.html?referer=83357&template=min_meldung_html&_min=_im. Letzter Zugriff: 2008-09-11 und: Datenschutz verhängt Bußgeld gegen Lidl. URL http://www.welt.de/wirtschaft/article4353471/Datenschutz-verhaengt-Bussgeld-gegen-Lidl.html. Letzter Zugriff: 2009-08-19.
[34] Vgl. Holländer, Corinna (2009): Datensündern auf der Spur – Bußgeldverfahren ungeliebtes Instrument der Datenschutzaufsichtsbehörden? In: Recht der Datenverarbeitung (RDV), Oktober 2009. S. 215 – 222.
[35] Zweite Rüge für Daimler wegen Gesundheitsdaten. URL: http://www.swr.de/nachrichten/bw/-/id=1622/nid=1622/did=5547546/1v915hd/index.html. Letzter Zugriff: 2009-10-28.
[36] Vgl. Antwort des Innenministeriums zum Antrag der Landtagsfraktion der SPD (Drucksache 14/4478). S. 3f.

der Unternehmen einfach keine Gedanken darüber macht. Datenschutzverstöße werden also weiter den Alltag begleiten.

© Xamit Bewertungsgesellschaft mbH

8 Datenschutz = Wettbewerbsnachteil?

Vertrauen ist die Grundlage aller Geschäftsbeziehungen

Das Grundthema unserer Untersuchungsrichtung ist Vertrauen. Vertrauen ist Basis und Schmierstoff der Marktwirtschaft. Ohne Vertrauen wären fast alle Geschäfte nur zu deutlich höheren Kosten möglich – wenn überhaupt. Vertrauen beeinflusst das Geschäftsleben in vielfältiger Form. Es wirkt sich z.B. aus auf

- die Zahlungsbereitschaft und -fähigkeit des Kunden,
- die Qualität der Ware oder Dienstleistung und
- die Angemessenheit des Preises.

Durch die elektronische Datenverarbeitung tritt eine weitere Vertrauenskomponente hinzu:

- Das Vertrauen in einen fairen Umgang mit personenbezogenen (persönlichen) Daten.

Denn deren Verwendungsmöglichkeiten sind technisch keine Grenzen gesetzt. Umso wichtiger werden die gesetzlichen Beschränkungen und die Selbstverpflichtung von Unternehmen, diese Daten nur in engen Grenzen zu nutzen und Daten wirksam zu schützen.

Die Hauptlast, Vertrauen zu schaffen, liegt beim Unternehmen. Es gestaltet seinen Umgang mit personenbezogenen Daten und verantwortet, wie er seinen Website-Besuchern bzw. Kunden gegenüber auftritt. Auch der engagierte und integere Unternehmer stößt dabei allerdings schnell an Grenzen:

- Wettbewerber erzielen mit Sicherheitsmängeln und Datenschutzverstößen einen deutlichen Wettbewerbsvorteil.
- Wettbewerber, die im Umgang mit Daten nachlässig sind oder diese sogar verfälschen, schaden dem Ruf einer Branche bis hin zur gesamten Internetwirtschaft.

Dies ist die gegenwärtige Situation, in der 82% der Deutschen den Unternehmen im Hinblick auf den Umgang mit ihren gespeicherten Daten misstrauen.[37]

Kontrollen schaffen Wettbewerbsgleicheit

Fehlende Kontrollmechanismen verzerren den Wettbewerb

Durch das zunehmende Bewusstsein der Bevölkerung, dass es mit dem Datenschutz nicht zum Besten bestellt ist, könnten sich diejenigen Unternehmen als besonders kundenorientiert und vertrauenswürdig positionieren, die in punkto Datensicherheit vorbildlich arbeiten. Dazu müssen jedoch erst einmal wirksame Kontrollmechanismen geschaffen werden, die einen einheitlichen Datenschutzstandard ga-

[37] Institut für Demoskopie Allensbach (2009): Zu wenig Datenschutz? Die meisten sind mit persönlichen Daten vorsichtiger geworden. Allensbacher Bericht Nr. 6/2009.

rantieren (Kapitel 8.3). Denn nur, wenn die Kontrolldichte hoch ist, wird Wettbewerbsgleichheit geschaffen.

Freiwillige Selbstkontrolle führt auch im Straßenverkehr nicht zum Ziel

Eine ähnliche Situation zeigt sich im Straßenverkehr. Sicher ans Ziel kommt man nur, wenn nicht nur die eigenen Bremsen funktionieren, sondern auch die der übrigen Verkehrsteilnehmer. Dass Freiwilligkeit hier nicht hilfreich ist, sieht man in vielen Ländern, die keine „TÜV-Pflicht“ kennen. Der „TÜV“ und seine Wettbewerber sorgen dafür, dass jedes Auto einem technischen Mindeststandard genügt. Ob die TÜV-Pflicht eingehalten wird, ist Gegenstand polizeilicher Kontrollen, weshalb diese den Angelpunkt der wirksamen TÜV-Pflicht darstellen. Würde die Pflicht nicht kontrolliert, dann gäbe es nur wenige TÜV-geprüfte Fahrzeuge auf der Straße. Autofahrer können also darauf *vertrauen*, dass Autos auf deutschen Straßen TÜV-geprüft sind. Der TÜV (und seine Wettbewerber) in Kombination mit der *durchgesetzten* TÜV-Pflicht schaffen Vertrauen in die Verkehrssicherheit. Dieses Vertrauen nützt allen Autofahrern.

Der Datenschutz in Deutschland befindet sich in folgender Situation: Gesetzliche Pflichten der Unternehmen bestehen ebenso wie die Rechte der Betroffenen. Wie wir gezeigt haben, ignorieren jedoch fast alle Unternehmen ihre Datenschutzpflichten (Kapitel 5 und 6). Skandale sind mittlerweile an der Tagesordnung (siehe Kapitel 6). Aufsichtsbehörden leiden unter extremem Personalmangel (Kapitel 7), so dass eine flächendeckende Kontrolle faktisch nicht stattfindet. Was ist also zu tun? Kapitel 8.1, 8.2 und 8.3 zeigen mögliche Alternativen auf.

8.1 Alternative 1: Datenschutz abschaffen

Ein erster Reflex sagt: „Lasst den Datenschutz fallen. Ohne Kontrollen bringt er sowieso nichts.“ Diese Option wirkt sehr sympathisch, ließe sie sich doch als Beitrag zum Bürokratieabbau feiern. Die Entlastung wäre indes gering. Da mindestens 95% (siehe Kapitel 6) der Unternehmen Datenschutzbestimmungen verletzen, ergibt sich kein Einspareffekt. Lediglich die wenigen gesetzestreuen Unternehmen wären entlastet.

Ohne Datenschutz kein Vertrauen in die Wirtschaft

Anders sieht es bei den Folgekosten aus. Verbraucher und auch Unternehmen verlieren Vertrauen. Ein „Wildwest“-Gefühl macht sich breit. Dieses Gefühl wird von einigen heute mit dem Internet verbunden. Es würde dann für die gesamte Wirtschaft gelten:

- Kunden argwöhnen, dass ihre Daten verkauft werden.
- Arbeitnehmer wissen, dass ihre Krankengeschichten öffentlich im Unternehmen kursieren.
- Unternehmen überwachen ihre Arbeitnehmer per Kamera, Mikrofon und spionieren die Arbeitsplatzrechner aus.

Mangelnder Datenschutz kostet Umsatz

Ein solcher „Wilder Westen“ kostet Umsatz, da Misstrauen Online-Käufe verhindert, und Gewinne, da Reibungsverluste in Gestalt von Misstrauen in Unternehmen Einzug halten.

© Xamit Bewertungsgesellschaft mbH

8.2 Alternative 2: Im „Weiter so“ untergehen

„Es ist ja noch immer gut gegangen“, pflegt der Kölner zu sagen. Dies weckt eine falsche Hoffnung, denn es hat sich in den letzten zehn Jahren etwas fundamental geändert: Die elektronische Datenverarbeitung ersetzt fast vollständig den manuellen papierbasierten Datenumgang. Restriktionen, wie schlechte Such- und Verwertungseigenschaften, entfallen. Alles, was man sich vorstellen kann, lässt sich heute mit persönlichen Daten anstellen. Sie können beliebig verknüpft und derart ausgewertet werden, dass neue – überraschende – Erkenntnisse über Personen möglich sind.[38]

Beim jetzigen Datenschutzverhalten ist der Vertrauensverlust vorprogrammiert

Der tägliche Umgang mit elektronischen Daten stammt aber oft aus der Papierzeit. Skandale sind deshalb vorprogrammiert. Solche Skandale lassen die Illusion eines sicheren und gesetzeskonformen Datenumgangs bersten. Sie sind keine Einzelfälle, sondern nur die sichtbare Spitze des Eisbergs. Ein „Weiter so“ bedeutet keine ernstzunehmenden Kontrollen und damit in Konsequenz keinen wirksamen Datenschutz. Eine solche Alternative führt langfristig zum gleichen Vertrauensverlust wie Alternative 1 (Kapitel 8.1).

8.3 Alternative 3: Kontrollen stärken

Erst gestärkte Kontrollen sichern das notwendige Vertrauen. Wie kann eine stärkere Kontrolle erreicht werden?

Ein Blick auf das Steuerwesen zeigt einen Weg auf: Jedes Unternehmen muss faktisch die Steuererklärung durch einen Steuerberater erstellen lassen. Dieser fungiert als erste Kontrollinstanz. Bei prüfungspflichtigen Unternehmen kommt als zweite Instanz ein Wirtschaftprüfer. Das Finanzamt kontrolliert die Erklärung und stichprobenartig in den Außenkontrollen, ob die Berechnungen gesetzeskonform und vollständig sind. Der betriebliche Datenschutzbeauftragte entspricht in etwa dem Steuerberater und die Aufsichtsbehörde dem Finanzamt. Wenn man weiß, dass 244.600 Beschäftigte in Bund, Ländern und Gemeinden für die Finanzverwaltung arbeiten[39], schreckt der Personalbedarf erst einmal ab. Gleichwohl ließe sich Analoges für den Datenschutz mit deutlich weniger Personal bewerkstelligen.

Eine zusätzliche privatwirtschaftliche Kontrollinstanz würde datenschutzkonformes Handeln stärken

Kontrollen vor Ort könnten durch unabhängige privatwirtschaftliche Unternehmen in Analogie zum TÜV erfolgen. Abbildung 14 zeigt modellhaft, wo eine solche zweite Kontrollinstanz innerhalb der bestehenden Kontrollmechanismen angesiedelt sein könnte. Ähnliche Überlegungen gibt es bereits zum Datenschutzsiegel. Der Erfolg hängt aber davon ab, dass sichergestellt wird, dass sich alle Unternehmen, Parteien und Vereine einer regelmäßigen Kontrolle unter-

[38] vgl. z.B. Golze, Kay et al. (2009): Private Sicherheit im Spannungsfeld globaler Datenströme und konkurrierender Volkswirtschaften. 2. Auflage. URL: http://www.wipn.de/New/Private%20Sicherheit%20im%20Spannungsfeld%20V9.pdf. Letzter Zugriff: 2009-11-03.

[39] Bundesagentur für Arbeit (2009): Arbeitsmarkt in Zahlen – Beschäftigungsstatistik.. Dezember 2008.

ziehen. Hier könnte eine Registrierung der Prüfungsberichte analog zum elektronischen Handelsregister helfen. Die Aufsichtsbehörden schreiten weiterhin bei Beschwerden ein. Ein solches Modell baut auf etablierten Strukturen auf und erhöht den gelebten Datenschutz deutlich.

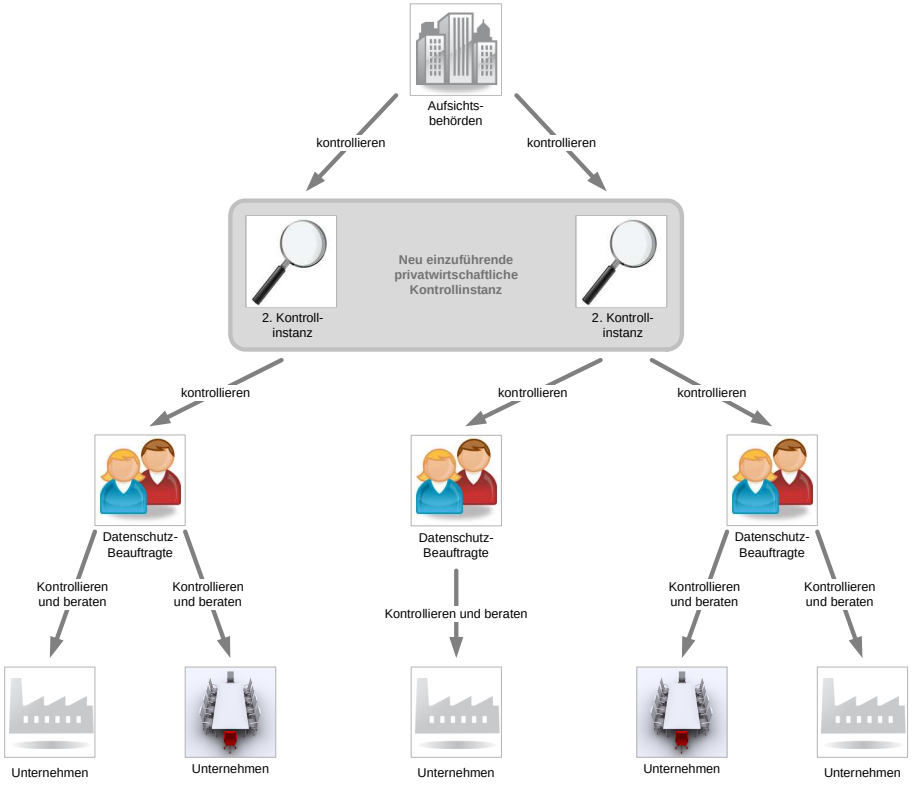


Abbildung 14: Ein abgestufter Kontrollmechanismus könnte den Datenschutz in Deutschland wirksam erhöhen

© Xamit Bewertungsgesellschaft mbH

9 Fazit

Ob Webstatistik, Webshop, Kontaktformular oder Werbung – die überwiegende Mehrheit der Unternehmen und Institutionen lässt die Besucher ihrer Internetseiten im Unklaren darüber, was mit online generierten Nutzerdaten geschieht. Die Verstöße nahmen 2009 im Vergleich zum Vorjahr um 11% zu. Zudem verstoßen 95% der Unternehmen gegen datenschutzrechtliche Vorschriften.

Beim Datenschutz ist das Vertrauen der Bürger in Unternehmen und Behörden stark gesunken

Das Vertrauen von Kunden und Bürgern in sichere und zuverlässige Geschäftsvorgänge im Internet schwindet, denn es findet in Sachen Datensicherheit zurzeit ein spürbares Umdenken in der deutschen Bevölkerung statt. Mehr Personen gehen inzwischen vorsichtiger mit den eigenen Daten um. Doch ist auch eine gewisse Hilflosigkeit auszumachen angesichts der immer häufiger öffentlich werdenden Datenskandale. Entrüstung hilft hier nicht weiter. Notwendig sind wirksame Kontrollmechanismen, die dem Datenschutz eine höhere Priorität einräumen. Der Gesetzgeber sieht die Einrichtung von Aufsichtsbehörden im Bundesdatenschutzgesetz (§ 38) explizit vor. Er geht also auch davon aus, dass erst eine Kontrolle wirksamen Schutz bietet. Solange ein Unternehmen, wie im Fall Baden Württemberg gesehen, statistisch alle 39.400 Jahre kontrolliert wird, drängt sich die Frage auf: Warum werden dann aber die Aufsichtsbehörden nicht adäquat ausgestattet?

Ohne wirksame Kontrollmechanismen kann Datensicherheit nicht gewährleistet werden

Wenn der Bundesregierung am Datenschutz genauso viel gelegen wäre wie an ihren Steuereinnahmen, lägen die Dinge wahrscheinlich anders. Eine zunehmende Bußgeldverhängung durch die Aufsichtsbehörden könnte hier schon weiter helfen. Auch, um eine positive Datenschutzkultur in den Unternehmen zu etablieren oder diese zu stärken. Die Ergebnisse des Datenschutzbarometers wie auch die aktuell in der Presse berichteten Datendiebstähle und Datenmissbräuche zeigen, dass die Gesellschaft wohl weiter um ihre persönlichsten Daten fürchten muss, solange die Datenschutzbehörden nicht adäquat ausgestattet sind und keine wirksamen Kontrollmechanismen etabliert werden. Der hiermit einhergehende Vertrauensverlust bedeutet für Unternehmen weniger Umsatz[40] und gefährdet Arbeitsplätze besonders für alle online agierenden Branchen. Ein hoher Preis für Politikversagen.

Es ist Zeit für neue Datenschutzkonzepte

Es ist für Politik, aber auch für Unternehmen, Verbraucherschützer und Datenschützer an der Zeit, überzeugende Datenschutzkonzepte vorzulegen. Denn eines ist wohl unbestritten: So, wie das Bundesdatenschutzgesetz zurzeit umgesetzt wird, kann es nicht weiter gehen. Profiteure der derzeitigen Situation wehren sich standhaft gegen den längst überfälligen Paradigmenwechsel, während sich die Mehrzahl der Behörden und Unternehmen ahnungslos gibt oder die Augen vor der Realität verschließt.

[40] Vgl. Heise Online (2005): US-Studie über die Kosten durch Identitätsdiebstahl in Unternehmen. 15.11.2005.

10 Anhang

Im Rahmen dieses Kapitels werden die aus den Ergebnissen resultierenden Handlungsempfehlungen für Webseiten-Betreiber (Kapitel 10.1) und Webseiten-Besucher (Kapitel 10.2) zusammengefasst.

10.1 Webseiten-Betreiber

Unternehmen, die ein kundenfreundliches und Vertrauen bildendes Image bevorzugen, sollten genau prüfen, welche Signale Ihre Webpräsenz an Besucher aussendet. Sobald

- ein Kontaktformular verwendet,
- Werbung Dritter angezeigt oder
- eine Webstatistik angefertigt

wird, darf eine Datenschutzerklärung nicht fehlen. Eine Datenschutzerklärung sollte

- verständlich formuliert sein,
- den Zweck für die Datennutzung angeben,
- die Zusendung von Werbung regeln,
- die Übermittlung an Dritte erläutern,
- direkt im Umfeld des Kontaktformulars, der Newsletteranmeldung etc. platziert sein oder durch einen gut sichtbaren und erkennbaren Link erreichbar sein und
- im vorbildlichen Fall auf das Auskunftsrecht oder das Widerspruchsrecht mit Wirkung für die Zukunft hinweisen.

Wer einen externen Dienstleister für die Webstatistik beauftragt, sollte einen Vertrag abschließen, der die Datenschutzrechte sichert und festlegt, ob und in welchem Umfang der Dienstleister die erhobenen Daten für eigene Zwecke nutzen darf. Ein solcher Vertrag ermöglicht eine Datenverarbeitung im Auftrag gemäß § 11 BDSG zu konstituieren, für die das Datenschutzrecht Privilegien vorsieht. Eine Zustimmung zu der Dienstleister-AGB ohne weiteren Vertrag reicht indes nicht aus!

Wer personenbezogene Daten in einer Datenbank sammelt (z.B. in einem Webshop), geht eine besondere Verpflichtung ein. Diese Daten müssen sicher aufbewahrt und vor den neugierigen Augen Unbefugter geschützt werden. Wer veraltete Software (PHP, Shop-Software) nutzt, lässt Sicherheitslücken offen, die zu einem Datendiebstahl einladen. Suchmaschinen helfen potentielle Opfer schnell zu finden. Der nachfolgende Angriff läuft dann teilweise vollautomatisch ab. Die Haltung „Mein Shop ist klein. Wer will bei mir einbrechen?“ gefährdet die Existenz des Unternehmens!

© Xamit Bewertungsgesellschaft mbH

Weiterführende Informationen zu Webstatistiken und Kontaktformularen finden Sie in unseren Studien[41]:

- „Wissen Sie, was Sie tun? Wissen Sie, wer es noch weiß? – Surfen im Internet“ und
- „Wie Unternehmen im Internet bei Konsumenten Misstrauen säen – Kontaktformulare und Datenschutz“

10.2 Webseiten-Besucher

Ein Website-Besucher hat zwar keinen direkten Einfluss auf die Art und Weise der Datenverarbeitung durch den Betreiber, doch kann er durch sein Verhalten vorbildliche Webpräsenzen unterstützen und somit auch seine eigenen Daten schützen. In Ermangelung wirksamer Standards und Kontrollen hilft nur Selbstschutz:

- Datenschutzerklärungen lesen.
- Betreiber ohne eine nach persönlicher Einschätzung akzeptablen Datenschutzerklärung meiden.
- Dateneingaben auf das erkennbare Minimum reduzieren und Pflichtfelder im Zweifel mit sinnlosen Eingaben zufriedenstellen.
- Schwarze Schafe bei der zuständigen Aufsichtsbehörde[42] oder den Verbraucherzentralen[43] anzeigen.

Jeder Mensch und jedes Unternehmen hat Geheimnisse. Alle Informationen, die nicht für die Öffentlichkeit bestimmt sind, brauchen Schutz. Wer will seine Krankengeschichte im Internet lesen? Welches Unternehmen will seine Forschungspläne mit der Konkurrenz teilen? Bereits mit einfachen und kostenlosen Mitteln können Privatpersonen und Unternehmen ihre Surfspuren verringern:

- Browser so einstellen, dass Cookies höchstens für die aktuelle Sitzung angenommen werden[44].
- Bei sensiblen Themen einen Anonymisierungsdienst verwenden[45].
- Bei Nutzung von Firefox Scripte selektiv mit der Firefox-Erweiterung „noscript“ [46] steuern, so dass Cookies von Google und Co. gar nicht erst gesetzt werden können. Ein vergleich-

[41] Kostenfreier Download: http://www.xamit-leistungen.de/studienundtests/index.php

[42] Jedes Bundesland hat eine eigene Aufsichtsbehörde für den Datenschutz. Eine entsprechende Liste stellt der „Bundesbeauftragten für den Datenschutz und die Informationsfreiheit“ zur Verfügung. URL: http://www.bfdi.bund.de/cln_027/nn_531524/DE/AnschriftenUndLinks/AnschriftenUndLinks__node.html__nnn=true. Letzter Zugriff: 2008-03-13

[43] URL: http://www.verbraucherzentrale.de. Letzter Zugriff: 2008-03-13

[44] Anleitungen für unterschiedliche Browser finden Sie im Internet. Bspw. hier: http://www.informationelle-selbstbestimmung-im-internet.de/node4.html

[45] Kostenlos und relativ einfach zu installieren ist An.On der Universität Dresden (http://anon.inf.tu-dresden.de/). Von dem Dienst Tor raten wir ab, da er gerne genutzt wird, um Passwörter auszuspähen.

[46] Zu viele Webpräsenzen benötigen Scripte, um zu funktionieren. Deshalb stößt ein generelles Abschalten schnell an praktikable Grenzen. Bezugsquelle: http://www.erweiterungen.de/detail/NoScript/

bares Werkzeug ist uns für den Internet Explorer nicht bekannt.
- Keine Toolbar von Google, Yahoo, Alexis u.a. im Browser einsetzen, da diese Toolbars das Surfverhalten protokollieren.

Anonymität im Internet wird immer wichtiger, da auch die staatliche Überwachung weiter zunimmt. Nach der Vorratsdatenspeicherung wird nun diskutiert, welche weiteren digitalen Spuren für die staatliche Überwachung von Interesse sind[47].

[47] Heise Online (2008): EU-Innenpolitiker wollen sämtliche digitalen Nutzerspuren überwachen. URL: http://www.heise.de/newsticker/EU-Innenpolitiker-wollen-saemtliche-digitalen-Nutzerspuren-ueberwachen--/meldung/115770. Letzter Zugriff: 2008-11-05.

© Xamit Bewertungsgesellschaft mbH

11 Weitere Studien von Xamit zum Thema Datenschutz

Alle Studien und ausgewählte Fachbeiträge finden Sie als kostenlosen Download auf unserer Webpräsenz.[48]

Xamit-Studie "Parteien und Datenschutz - Datenschutzpraxis deutscher Parteien und parteinaher Organisationen"

Keine der im Bundestag vertretenen Parteien handelt beim Thema Datenschutz uneingeschränkt gesetzeskonform. Untersucht wurden u.a. der Umgang mit Online-Spenden oder das Vorhandensein eines datenschutzrechtlich vorgeschriebenen Verfahrensverzeichnisses. In Summe werden etwa ein Drittel der denkbaren Verstöße auch begangen. Das heißt, entsprechende gesetzliche Vorschriften werden von den Parteien und deren verwandten Organisationen vielfach ignoriert.

Datenschutzbarometer 2008 – Datenschutz im Internet

Das Datenschutzbarometer 2008 stellt eine in dieser Form erstmalig durchgeführte Überprüfung von insgesamt 26.209 deutschen Internetpräsenzen dar. 45 von 100 Webseiten verstoßen gegen die gesetzlichen Bestimmungen oder weisen sonstige Indikatoren für ein mangelhaftes Schutzniveau auf.

Wie Unternehmen im Internet bei Konsumenten Misstrauen säen

Gut 85 Prozent aller Unternehmen und Behörden in Deutschland, die durch den Einsatz von Dialoginstrumenten personenbezogene Daten ihrer Website-Besucher sammeln, verzichten auf jegliche Information dahingehend, was mit diesen Daten geschieht. So lautet das Ergebnis einer repräsentativen Studie der Xamit Bewertungsgesellschaft mbH, bei der im Februar 2008 mehr als 815.000 Webseiten privater Firmen und öffentlicher Institutionen begutachtet wurden.

Wissen Sie, was Sie tun? Wissen Sie, wer es noch weiß? – Surfen im Internet

Wer protokolliert das Surfverhalten im World Wide Web? Wer ist Marktführer beim Web Tracking? Werden Besucher über eine Datenerhebung informiert? Wer kann technisch Bewegungsprofile mit Namen verknüpfen?

[48] http://www.xamit-leistungen.de/studienundtests/index.php

12 Beiträge von Xamit in Fachmedien

Nur ein Vollzugsdefizit? – Parteien vernachlässigen den Datenschutz. FIfF-Kommunikation 4/2009 (in Druck).

Datenschutz im Internet: Alarmierende Ergebnisse des Xamit Datenschutzbarometers 2008. Datenschutz und Datensicherheit 10/2009.

Vertrauensvolle Datenverwendung: Basis des Geschäftserfolges. direkt marketing 5/2009

Umgang mit Datenschutzerklärungen im Internet. Datenschutz und Datensicherheit 1/2009

Datenschutz bei Webstatistiken. Datenschutz und Datensicherheit 4/2008.

© Xamit Bewertungsgesellschaft mbH

Xamit Bewertungsgesellschaft mbH

Der IT-Spezialist für den Mittelstand – unabhängig, neutral, zuverlässig.

Unser Leistungsspektrum:

- **Xamit Firmen Check – Mit Sicherheit zum Erfolg.**
  Beim Xamit Firmen Check nehmen wir Ihr Unternehmen fachmännisch unter die Lupe, analysieren die Sicherheit Ihrer IT-Systeme, zeigen Schwachstellen auf und erarbeiten mit Ihnen ein Konzept zur Optimierung Ihre Sicherheit oder Ihres Datenschutzes.

- **Xamit Projekt Check – Rechnen Sie mit Gewinn.**
  Der Xamit Projekt Check ist Ihre Versicherung für effizientes Arbeiten. Wir machen Ihre Software-Projekte transparent. Die Risiken werden kalkulierbar. Ihr Erfolg wird planbar.

- **Xamit Studien und Tests**
  Wir bieten aktuelle Studien und Tests sowie weitergehende detaillierte Informationen zu IT-relevanten Themen.

Xamit-Leistungen stehen für begutachtete Kompetenz und Qualität: Das Unternehmen ist geprüftes Mitglied im Beraternetzwerk des IBWF Instituts e.V. und gehört darüber hinaus der Gesellschaft für Datenschutz und Datensicherung e.V. (GDD) sowie dem Berufsverband der Datenschutzbeauftragten Deutschlands (BvD) an.

Ihre Vorteile mit Xamit:

- Anerkanntes Fachwissen,
- neutrale Beratung und
- Unabhängigkeit.

Setzen Sie nicht leichtfertig Ihr Unternehmen aufs Spiel. Sichern Sie Ihren Erfolg.
Rufen Sie uns an.

Xamit Bewertungsgesellschaft mbH

Zülpicher Str. 6
40549 Düsseldorf

Tel.: 0211 / 58 300 330
Fax: 0211 / 58 300 331

E-Mail: info@xamit.de
WWW: www.xamit.de