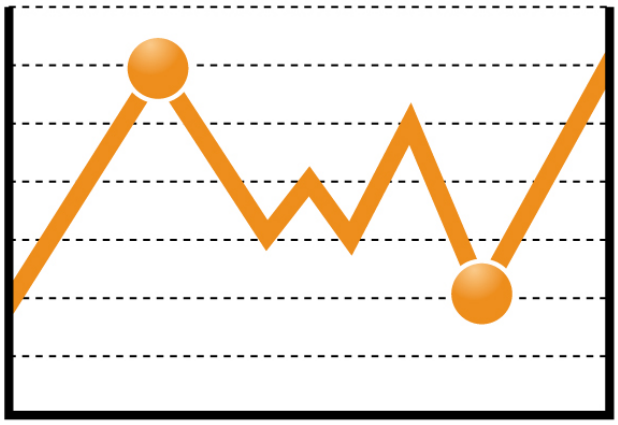
DATENSCHUTZBAROMETER 2008

– Datenschutz im Internet –

2. überarbeitete Fassung



Datenschutz Barometer

Impressum

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

Rechtliche Hinweise

Die Xamit-Studien werden mit größtmöglicher Sorgfalt erstellt. Trotzdem kann die Xamit Bewertungsgesellschaft mbH keine Haftung für die Nutzung der Xamit-Studien übernehmen. Haftungsansprüche gegen die Xamit Bewertungsgesellschaft mbH, welche sich auf Schäden materieller oder ideeller Art beziehen, die durch die Nutzung oder Nichtnutzung der Xamit-Studien verursacht wurden, sind grundsätzlich ausgeschlossen, sofern seitens des Autors kein nachweislich fahrlässiges oder grob fahrlässiges Verschulden vorliegt.

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

1 Einleitung

Durch die Elektronisierung vieler persönlicher Daten sind nicht nur neue Dienstleistungen möglich geworden, sondern auch neue Formen der Kriminalität. Aktuelle Vorfälle zeichnen ein düsteres Bild hinsichtlich der Sicherheit von persönlichen Daten:

- PricewaterhouseCoopers: Email-Adressen und Passwörter von Bewerbern gestohlen
- Tele 2: Voice-Mailboxen ohne Schutz
- Süddeutsche Klassenlotterie: bis zu 17.000 Kontodaten im Umlauf
- O2 Großbritannien: MMS freizugänglich
- TNS Infratest: 40.000 Kundenprofile ungeschützt im Internet
- HSH Soft- und Hardware Vertriebs GmbH: deutsche Einwohnerdaten ungeschützt im Internet

Es entsteht der Eindruck, Daten seien heutzutage nirgendwo sicher. Stimmt dieser Eindruck? Mittels der vorliegenden Untersuchung versucht Xamit – losgelöst von den oben erwähnten Vorkommnissen – eine empirische Antwort zu finden und somit ein möglichst realistisches Bild zu zeichnen. Dabei knüpfen wir methodisch und inhaltlich an unsere bisherigen Studien zum Thema Datenschutz und Internet an:[1]

- „Wissen Sie, was Sie tun? Wissen Sie, wer es noch weiß? – Surfen im Internet“ über heimliche Datenerhebung bei Webstatistiken sowie
- „Wie Unternehmen im Internet bei Konsumenten Misstrauen säen – Kontaktformulare und Datenschutz“ über die Transparenz der Datennutzung bei Kontaktformularen.

Beide 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 ergänzt um einen weiteren Aspekt: Die Transparenz bei Werbeeinblendungen. Auch Banner etc. sind dazu geeignet, personenbezogene Daten zu den Werbung platzierenden Unternehmen zu übermitteln. Doch informiert der Webseitenbetreiber seine Besucher darüber?

Mit dem Datenschutzbarometer 2008 stellt Xamit einen einzigartigen Überblick über das aktuelle Datenschutzniveau im Internet zur Verfügung. Xamit wird diese Untersuchung regelmäßig und in identischer Form wiederholen, um die Entwicklung des Datenschutzniveaus zu dokumentieren.

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

2 Hintergrund

Im Folgenden zeigen wir in knapper Form auf, an welchen Stellen und auf welche Weise persönliche Nutzerdaten durch Internet-Angebote erhoben und damit auch gefährdet sind und in Folge dessen Missbrauch oder gar illegale Handlungen drohen.

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 Email-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 Scripte (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.

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.

Veraltete Software- und PHP-Versionen bergen Risiken

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 338 Fehler behoben.[2] 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.

Ein Beispiel: Max Mustermann surft verschiedene Webpräsenzen an. Der Betreiber kennt das Bewegungsprofil von Max Mustermann für

[2] Die Entwickler von PHP betreiben unter http://www.php.net/ eine Fehlerdatenbank. Stand der Abfrage: 12.09.2008

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“.[3]

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 Datenschutzerklärung besitzen. Google verpflichtet die Nutzer von Google Adsense in § 1 der Allgemeinen Geschäftsbedingungen, in

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

einer Datenschutzerklärung auf Google Adsense hinzuweisen.[4] Insbesondere ist dabei zu erwähnen, dass dieser Dienst ein 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

Verwertung gesammelter Daten ist schier unbegrenzt

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).[5] 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 an speziellen Rechtsvorschriften für Kontaktformulare bedarf es einer Einwilligung von Max Mustermann. Ob seine freiwillige Datenabgabe

[4] Google (2008): Allgemeine Geschäftsbedingungen (AGBs) für AdSense. URL: https://www.google.com/adsense/localized-terms. Stand: 2008-10-28.

[5] 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

bereits eine Einwilligung darstellt oder dies in expliziter Form erforderlich ist, ist unter Juristen umstritten.[6]

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,

Datenschutzerklärung als Entscheidungsgrundlage

dann weiß Herr Mustermann, worauf er sich einlässt und kann einwilligen. Eine solche Erläuterung nennen wir in dieser Studie „Datenschutzerklärung". Welche Form eine solche Einwilligung aufweisen sollte, wurde im Rahmen der zurückliegenden Xamit Studie „Wie Unternehmen im Internet bei Konsumenten Misstrauen säen – Kontaktformulare und Datenschutz" [7] ausführlich erläutert und ist im Anhang der vorliegenden Untersuchung dokumentiert.

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

[6] 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. 409

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

3 Gegenstand und Methode des Datenschutzbarometers

Eine maschinelle Quellcode-Analyse von 26.209 deutschen Webpräsenzen bildet die Grundlage des Xamit-Datenschutzbarometers. Neben 2.218 Gemeinden und 2.122 Vereinen berücksichtigt die vorliegende Xamit Studie mittelständische 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

Jede Branche ist mit 982 bis 5.181 Webpräsenzen vertreten. Analysiert werden jeweils maximal 1.000 Webseiten pro Webpräsenz.

Von September bis November 2008 werteten wir mehr als 1,3 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.

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 indes 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[8] nicht aufspüren. Ungeachtet dessen sollte die verwandte Methodik einen ersten Überblick über die Sicherheit von Webshops verschaffen.

3.2 Einbindung von 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

[8] 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[9], 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 gravierenden Fehlzuordnungen. Deshalb können wir auch diese Ergebnisse als ausreichend valide betrachten.

[9] Google (2007): Google Analytics Bedingungen. URL: http://www.google.com/analytics/de-DE/tos.html. Stand: 2007-10-01.

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 weit verbreitet

Nur jeder 3. Webshop basiert auf aktueller PHP-Technik

Insgesamt haben wir 6.226 Installationen von PHP der Version 4 und 3.322 der Version 5 identifiziert (Mehrfachnennung möglich). Damit verfügt die veraltete Version 4 noch immer über einen Anteil von 66%. Dies ist insofern bedenklich, da die Betreuung mit der aktuellen Version 4.4.9 eingestellt wird.[10] Von allen erkannten PHP-Installationen haben wir bei nur 29% die aktuelle Version (4.4.9 oder 5.2.6) entdeckt.

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.[11]

In 162 Fällen konnten wir eine bekannte Shopsoftware erkennen. xtCommerce ist mit einem Anteil von 64% unbestrittener Marktführer gefolgt von seiner OpenSource-Verwandten osCommerce mit 20%. Die restlichen 16% teilen sich sieben Programme auf. Aufgrund der geringen Fallzahlen verzichten wir auf eine Aufteilung nach Branchen.

Anbieter setzen häufig auf Individuallösungen

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

[10] Siehe Ankündigung zu Version 4.4.9. URL: http://www.php.net/. Letzter Zugriff: 12.09.2008.
[11] Heise Online (2008): Studie: Fast jede Webanwendung angreifbar. URL: http://www.heise.de/newsticker/Studie-Fast-jede-Webanwendung-angreifbar--/meldung/115656. Letzter Zugriff: 12.09.2008

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.

81 Prozent der Shops mit Standardsoftware auf PHP-Basis sind anfällig für Angriffe von außen

Von den Webshops mit Standardshopsoftware setzen 53% die aktuelle Version der Shopsoftware ein. 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 1,2% unter den untersuchten Webpäsenzen nicht überrascht. Aufgrund der geringen Fallzahlen verzichten wir auf eine Aufteilung nach Branchen.

Nutzungsbedingungen werden mehrheitlich außer Acht gelassen

21% der Webpräsenzen mit Adsense informieren ihre Besucher über eine Datenschutzerklärung. Auf der anderen Seite setzen sich 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. Die verbreitete Heimlichkeit und Neigung zum Bruch der Nutzungsbedingungen korrespondiert mit unseren Ergebnissen zur Webstatistik (Kapitel 4.3).

4.3 Webstatistik – Allgemeines Festhalten an verheimlichter Datenerhebung

Vor gut einem Jahr 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. Doch hat sich die Nutzung von Google Analytics und anderen Webstatistikdiensten in den letzten 12 Monaten verändert?

NRW Landtag lässt Website-Besucher weiter im Dunkeln

Der Landtag von NRW illustriert die Antwort deutlich. Er nutzt Google Analytics – fast möchte man sagen trotzig – weiter. In der Datenschutzerklärung wird zwar auch auf die Nutzung hingewiesen (Abbildung 1), allerdings sorgt die Erklärung für mehr Verwirrung als Aufklärung. Der Landtag verspricht die Anonymisierung der IP-Adresse: „Nach Beendigung des Kommunikationsvorgangs wird die IP-Adresse anonymisiert." Gleichzeitig überträgt er die IP-Nummer nicht anonymisiert an Google in die USA. Die Legislative von NRW zeigt eine bemerkenswerte Einstellung zum Recht und zum Datenschutz ihrer Bürger.

Update: Der Landtag von NRW hat in Folge der Berichterstattung über dieses Datenschutzbarometer die Nutzung von Google Analytics eingestellt.

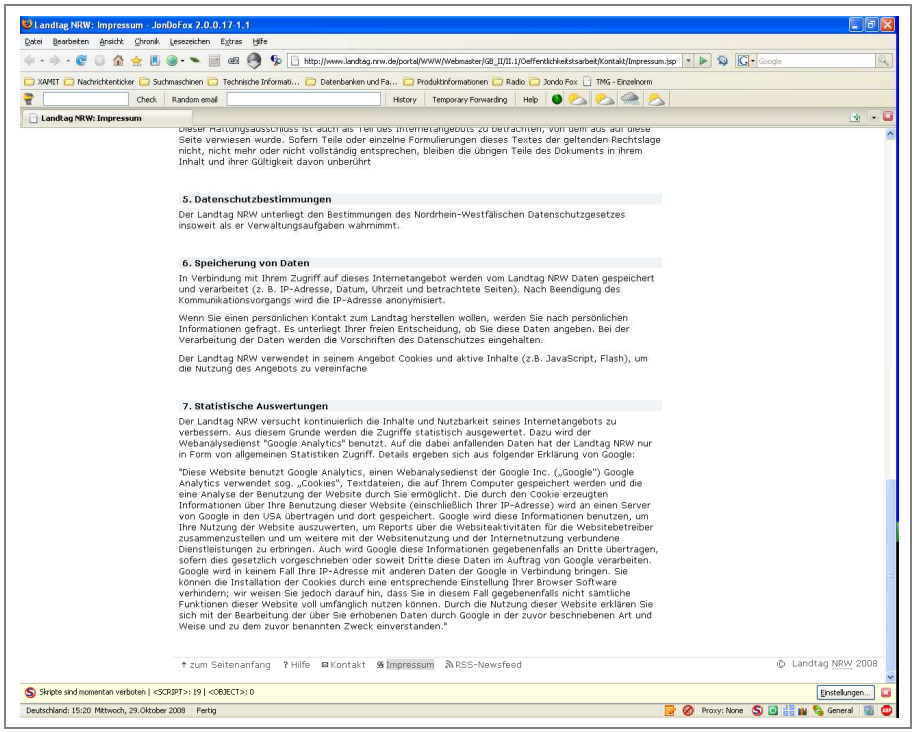


Abbildung 1: Datenschutzerklärung des Landtags von NRW[12]

Google baut Markführerschaft beim Tracking aus

Zum Zeitpunkt unserer ersten Erhebung (August und September 2007) nutzten 7% der Webpräsenzen Google Analytics und 1% einen anderen Anbieter. Jetzt sind es 10% mit Google Analytics und 2% anderer Anbieter. Abbildung 2 zeigt die Nutzung nach Branchen. Insgesamt erfreut sich Google Analytics steigender Beliebtheit über alle Branchen hinweg.

[12] URL: http://www.landtag.nrw.de/portal/WWW/Webmaster/GB_II/II.1/Oeffentlichkeitstsarbeit/Kontakt/Impressum.jsp. Letzter Zugriff: 2008-10-29.

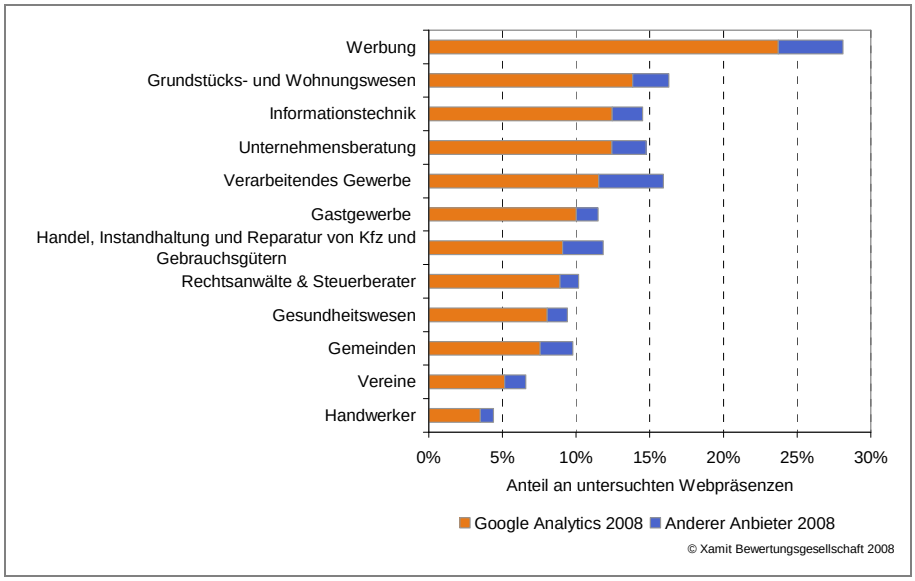


Abbildung 2: Nutzung von Webstatistiken nach Branchen

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“ Stelle dokumentieren.[13] Google schreibt den Wortlaut dieser Information vor und behält sich ein Kontrollrecht vor.

Datenschutz-konformes Tracking bleibt die große Ausnahme

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% nutzen eine Datenschutzerklärung ohne diesen Passus. Die Abnahme der heimlichen Datensammlung ist eine erfreuliche Entwicklung. Allerdings zeigt der Anteil an heimlicher Datensammlung, dass viele Betreiber entweder nicht wissen (wollen), was sie tun, oder bewusst die Interessen ihrer Besucher ignorieren, da sie keine Sanktionen fürchten müssen.

[13] Google (2007): Google Analytics Bedingungen. URL: http://www.google.com/analytics/de-DE/tos.html. Stand: 2007-10-01.

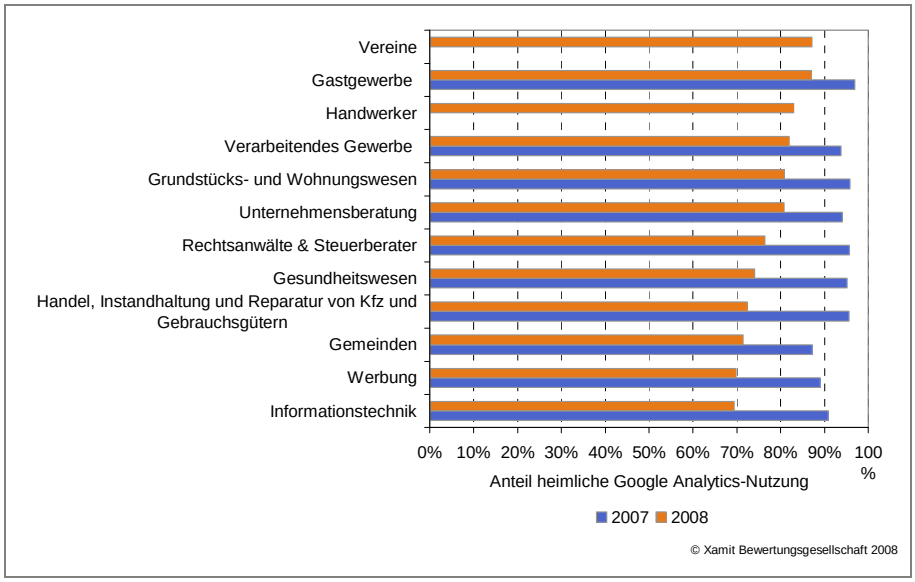


Abbildung 3: Heimliche Nutzung von Google Analytics nach Branchen

Abbildung 3 zeigt die heimliche Nutzung von Google Analytics nach Branchen. Handwerker und Vereine sind neu hinzugekommen, so dass für 2007 noch keine Werte vorliegen. Das Gastgewerbe setzte im Jahr 2007 mit 97% noch fast vollständig auf eine heimliche Datensammlung und nutzt die von Google vorgegebene Textpassage weiterhin sehr zurückhaltend (Abbildung 4). Erfreulicherweise nutzen inzwischen deutlich mehr Webpräsenzen den Google Passus als 2007. Ein sehr positiver Effekt der öffentlichen Debatte.

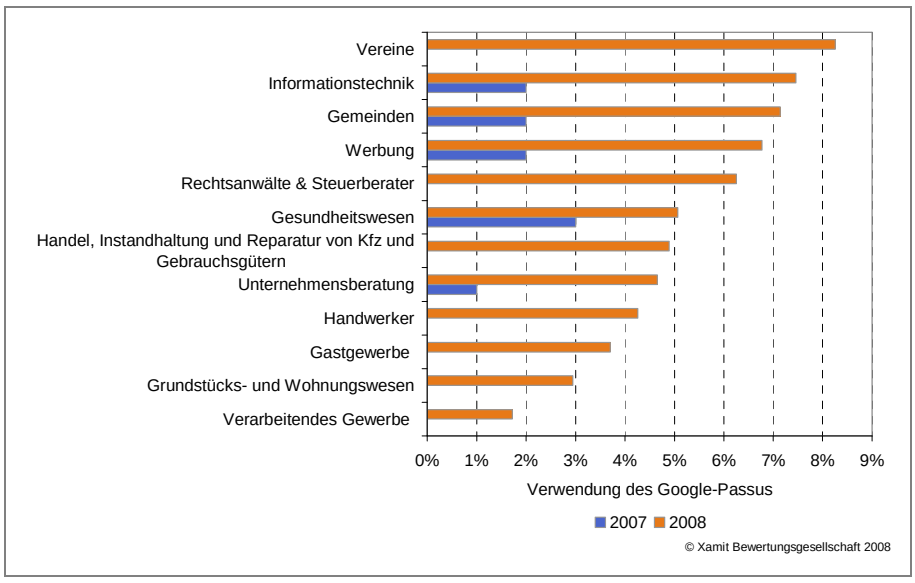


Abbildung 4: Verwendung des Google-Passus nach Branchen

Dr. Roland Steidle und Dr. Ulrich Pordesch kommen in einer technischen und rechtlichen Analyse zu dem Schluss, dass gegen den Einsatz von Google Analytics und vergleichbarer Angebote erhebliche

rechtliche Bedenken bestehen.[14] Die Bedenken beruhen auf der Übertragung der IP-Nummer an Google. Eine wirksame (und damit praktisch nicht umsetzbare) Einwilligung eines jeden Besuchers oder die Kürzung der IP-Nummer wären notwendig, um die Bedenken auszuräumen, so die Autoren. Weil Google auch Cookies setzt und über eigene Dienste mit einer personalisierten Anmeldung (Google Calender, Apps, Mail etc.) verfügt, reicht u.E. eine Kürzung der IP-Nummer nicht aus. Google bleibt weiterhin in der Lage, die Surfspuren zu einem Bewegungsprofil zusammenzuführen.

Definition von „personenbezogen“ bleibt juristisch umstritten

Aus diesem Grund greift die Argumentation einiger Webseitenbetreiber, die IP-Nummern eben nicht als personenbezogene Daten ansehen, zu kurz. Eine Auffassung, die von einigen Gerichten gestützt[15] und von anderen abgelehnt[16] wird. Der Bundesverband Digitale Wirtschaft (BVDW) hält eine Verwendung von Google Analytics dann für erlaubt, wenn ein entsprechender Datenschutzhinweis auf der Webseite angebracht wird.[17]

Das Unabhängige Landeszentrum für Datenschutz Schleswig-Holstein (ULD) und der Berliner Beauftragte für Datenschutz und Informationsfreiheit haben im Juli 2008 eine Prüfung von Google Analytics eingeleitet.[18] Von der Untersuchung sind sowohl Google wie auch Betreiber, die Google Analytics nutzen, betroffen. Ein Ergebnis wurde bis dato öffentlich nicht bekannt.

4.4 Kontaktformulare – Datenverarbeitung bei Nacht

Im Februar 2008 analysierten wir die Nutzung von Kontaktformularen auf deutschen Webpräsenzen. 41% der damals untersuchten Webpräsenzen setzten Kontaktformulare ein. Heute sind es 42%. Abbildung 5 zeigt die Nutzung nach Branchen. Spitzenreiter damals wie heute ist das Grundstücks- und Wohnungswesen mit 67%.

[14] Steidle, Roland; Pordesch, Ulrich (2008): Im Netz von Google. Web-Tracking und Datenschutz. In: Datenschutz und Datensicherheit (DuD), 5/2008. S. 324-329.
[15] Amtsgericht München, Az. 133 C 5677/08 vom 30.09.2008
[16] Amtsgericht Berlin Mitte, Az. 5 C 314/06 vom 27.03.2007
[17] BVDW (2008): Verwendung von Google Analytics – Datenschutzhinweis ist Pflicht! URL: http://www.bvdw.org/index.php?id=98&tx_ttnews[tt_news]=2828&cHash=c5befa5716&no_cache=1&sword_list[0]=google%20analytics. Letzter Zugriff: 2008-10-29.
[18] ULD (2008): Datenschützer prüfen Google Analytics – Pressemitteilung. URL: https://www.datenschutzzentrum.de/presse/20080807-google-analytics.htm. Letzter Zugriff: 2008-10-29.

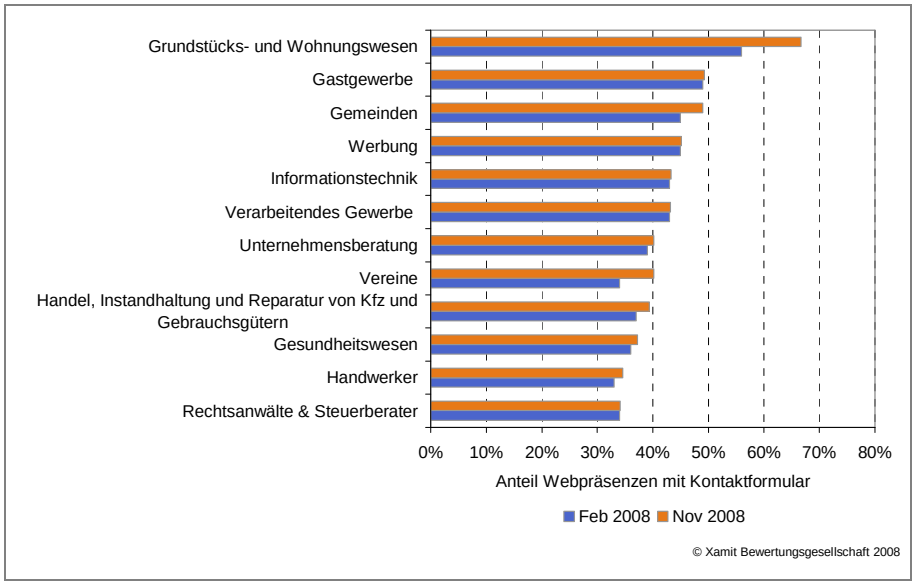


Abbildung 5: Einsatz von Kontaktformularen nach Branchen

Wie gehen die Betreiber mit den anfallenden personenbezogenen Daten um?

Von den Webpräsenzen mit Kontaktformular informieren 17% (Februar 2008: 15%) über ihren Umgang mit den erhobenen Daten. Lediglich bei 5% (Februar 2008: 2%) 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.

Bundesregierung und Ministerium reagieren auf Xamit Studie

Nachdem wir in unserer Studie „Wie Unternehmen im Internet bei Konsumenten Misstrauen säen – Kontaktformulare und Datenschutz“ berichtet hatten, dass die Bundesregierung und das Bundesministerium für Wirtschaft und Technologie Kontaktformulare ohne Datenschutzerklärung verwenden, haben beide Institutionen mittlerweile ihre Kontaktformulare mit einer Datenschutzerklärung verlinkt.

Abbildung 6 zeigt, wie heute die einzelnen Branchen mit den Datenschutzerklärungen umgehen. 2% (Februar 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 5% (Februar 2008: 4%) erheben die Daten und geben eine nicht verlinkte Datenschutzerklärung an. 35% (Februar 2008: 35%) aller untersuchten Webpräsenzen fragen personenbezogene Daten ab ohne eine Datenschutzerklärung zu veröffentlichen. Die restlichen 58% (Februar 2008: 59%) verzichten auf die Erhebung personenbezogener Daten.

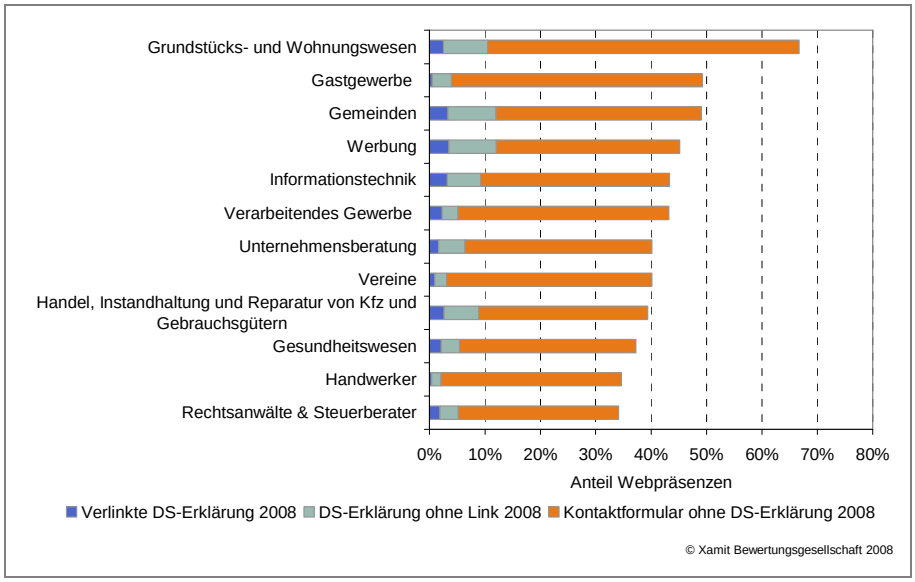


Abbildung 6: Datenschutzerklärungen bei Kontaktformularen

Insgesamt verfügen 17% (Februar 2008: 14%) der Webpräsenzen mit Kontaktformular über eine Datenschutzerklärung. Anders formuliert: 83% der Betreiber lassen Ihre Besucher im Dunkeln, was mit den im Kontaktformular eingegebenen persönlichen Daten geschieht.

5 Das Xamit-Datenschutzbarometer 2008

Einzigartige 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 wie 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,
- Kontaktformulare ohne Datenschutzerklärung nutzen,
- Adsens ohne Datenschutzerklärung einbinden,
- unsichere Shop-Software verwenden oder
- unsichere PHP-Versionen bei Online-Shops einsetzen.

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

Die Folgen eines Datenschutzvergehens hängen davon ab, welches Angebot oder welchem Zweck eine Webpräsenz dient. Eine heimliche Webstatistik eines Sockenhändlers sagt weniger Persönliches aus als die Webstatistik eines Onkologen. 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 mit denen ein Konsument im Alltag zu tun hat wie z.B. Handel, Gastgewerbe, Grundstücks- und Wohnungswesen und Handwerker.
- eGovernment: Alle staatlichen Stellen, wie z.B. Gemeinden, 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 passen, zählen hierzu, wie z.B. Unternehmensberatungen.
- Vereine: Vereine bilden eine eigene Klasse.

Insgesamt haben wir Verstöße oder Gründe zur Beanstandung auf 45 von 100 untersuchten Webpräsenzen gefunden. Spitzenreiter sind die Datenschutzmultiplikatoren mit 52 Verstößen pro 100 Webpräsenzen (Abbildung 7). 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. Hier liegt eindeutig einiges im Argen.

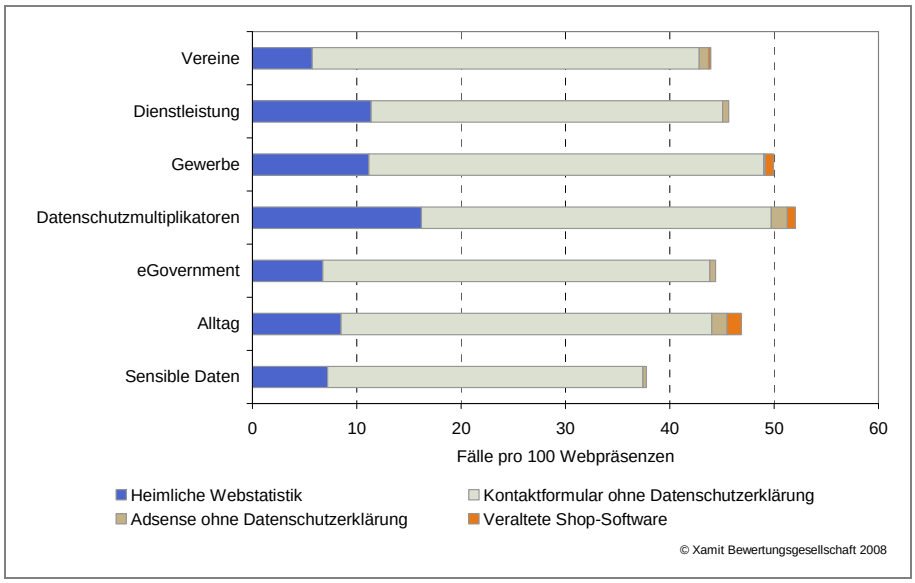


Abbildung 7: Verstöße und Beanstandungen nach Klassen

Ausgerechnet Fachleute gehen mit schlechtem Beispiel voran

Eine regionale Verteilung nach Bundesländern zeigt Abbildung 8. Spitzenreiter ist Hamburg mit 52 Verstößen. Webpräsenzen, deren Betreiber wir einem Bundesland zuordnen konnten sind in diese Darstellung eingeflossen. 4.603 von 26.209 Webpräsenzen konnten wir keinem Bundesland zuordnen, weshalb sie in den Zahlen nicht berücksichtigt sind.

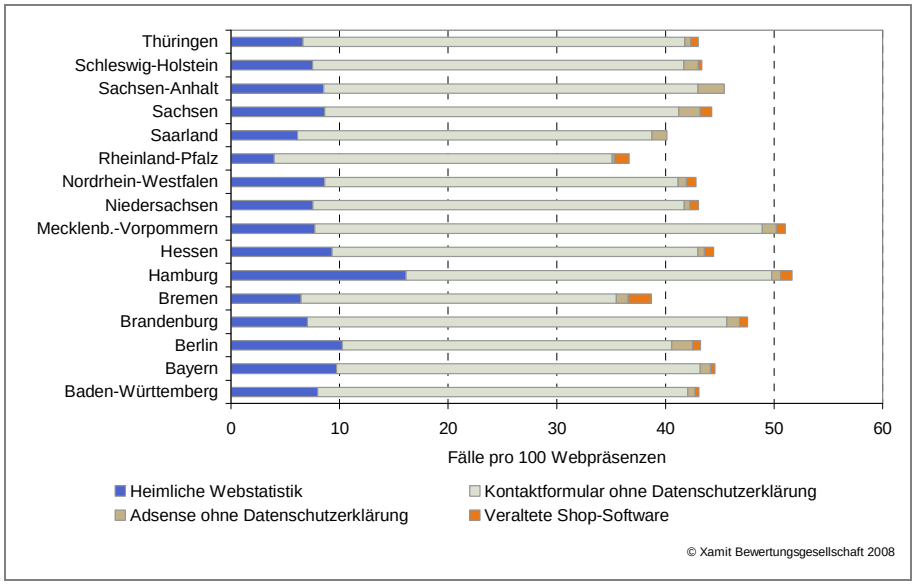


Abbildung 8: Verstöße und Beanstandungen nach Bundesländern

6 Fazit

Das Vertrauen von Kunden und Bürgern wird auch weiterhin aufs Spiel gesetzt und zunehmend zerstört

Auch ein Jahr nach Veröffentlichung der alarmierenden Studie über verheimlichtes Webtracking und trotz anhaltender Meldungen über spektakuläre Sicherheitsvorfälle zeigt das Xamit Datenschutzbarometer 2008 deutlich auf, dass ein spürbares Umdenken in Sachen Datenschutz im Internet bis heute ausgeblieben ist. Ob Webstatistik, Webshop, Kontaktformular oder Werbung – die überwiegende Mehrheit der Unternehmen und Institutionen hierzulande lässt die Besucher Ihrer Internetseiten im Unklaren darüber, was mit online generierten Nutzerdaten geschieht. Das Vertrauen von Kunden und Bürgern in sichere und zuverlässige Geschäftsvorgänge im Internet wird nicht nur weiterhin fahrlässig aufs Spiel gesetzt, sondern mit jedem neuen bekannt werdenden Vorfall massiv erschüttert.

Über die Hintergründe dieser nachweislich Schaden verursachenden Haltung der Webseiten-Anbieter kann an dieser Stelle nur spekuliert werden. Die gesammelten Erfahrungswerte legen allerdings den folgenden Verdacht nahe: Profiteure der unsicheren Internet-Kommunikation wehren sich standhaft gegen den längst überfälligen Paradigmenwechsel, während sich Webseitenanbieter und die Mehrzahl der Behörden ahnungslos geben oder die Augen vor der Realität verschließen.

Xamit Datenschutz-Barometer wird die weitere Entwicklung dokumentieren

Nicht zuletzt vor diesem Hintergrund hat Xamit das Projekt Datenschutzbarometer ins Leben gerufen. Es soll Anbietern wie Nutzern eine realistische Bestandsaufnahme des Internet Datenschutz-Niveaus in Deutschland ermöglichen und somit der längst überfälligen Verbesserung von Sicherheitsstandards den Weg ebnen.

7 Anhang

Im Rahmen dieses Kapitels sind sowohl ergänzende Hintergrundinformationen zum Datenschutzbarometer 2008 als auch die aus den Ergebnissen resultierenden Handlungsempfehlungen zusammengefasst.

7.1 Datenschutz als Basis für Vertrauen

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 äußert sich im Geschäftsleben in vielfältigen Formen, insbesondere:

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

Im Internet tritt ein weiteres Vertrauen neben die bisher bekannten: 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.

Vertrauen bedeutet nicht nur, dass der Betreiber die Daten nicht „zweckentfremdet“, sondern auch, dass er sie sicher aufbewahrt. Gerade Webshops erhalten nicht nur Adressdaten sondern oft auch Konto- oder Kreditkartendaten. Weil Webshops diese wertvollen Daten in größere Menge online verfügbar vorhalten, sind sie besonderen Gefahren ausgesetzt. Eine wichtige Sicherheitsmaßnahme ist, aktuelle Softwareversionen einzusetzen. Deshalb untersuchen wir auch, ob bei Webshops aktuelle Software-Versionen verwendet werden.

Spektakuläre Diebstähle persönlicher Daten wühlen die Öffentlichkeit auf:

- Süddeutsche Klassenlotterie (SKL): Datensätze von bis zu 17.000 Personen illegal im Umlauf[19]
- PricewaterhouseCoopers: Bewerberdaten gestohlen und für Betrug verwendet[20]
- Beate Uhse: E-Mail-Adressen von tausenden Interessenten ungewollt veröffentlicht und von Suchmaschine indiziert[21]

[19] Heise Online (2008): Verbraucherzentrale: Massenhafter Missbrauch von Bankkonten-Daten. URL: http://www.heise.de/newsticker/Verbraucherzentrale-Massenhafter-Missbrauch-von-Bankkonten-Daten-2-Update--/meldung/114124. Letzter Zugriff: 2008-11-05.

[20] Heise Online (2008): Gestohlene PwC-Datensätze für Missbrauch von Click&Buy benutzt. URL: http://www.heise.de/newsticker/Gestohlene-PwC-Datensaetze-fuer-Missbrauch-von-Click-Buy-benutzt-Update--/meldung/115621. Letzter zugriff: 2008-11-05.

Dabei zeigen diese Beispiele nur die Spitze des Eisbergs auf. In den USA kamen nach öffentlich zugänglichen Quellen allein im Jahr 2008 bislang gut 22 Mio. Kundendatensätze abhanden.[22] Die Dunkelziffer dürfte erheblich höher liegen, so dass die durch Datenmissbrauch verursachten Schäden und Verluste vermutlich ein Vielfaches des offiziell angenommenen Ausmaßes betragen.

Ist der Diebstahl von Adressdaten bereits hochgradig ärgerlich, so bieten illegal ausgespähte Kreditkarten- oder Kontodaten Kriminellen die Möglichkeit, zusätzlich Geld von den betroffenen Kunden zu stehlen. Konto- und Kreditkartendaten sind der Schlüssel zum Onlinehandel. Webshops beispielsweise bieten häufig Kreditkartenzahlungen zusätzlich oder anstelle von Vorkasse oder Nachnahme an. Damit sind Webshops in besonderem Maße gefordert und verpflichtet, für eine sichere Aufbewahrung ihrer Kundendaten zu sorgen.

7.2 Was ist zu tun?

Ein Verzicht auf Kontaktformulare, Werbung oder Webstatistiken ist keine zielführende Option. Deshalb geben wir Betreibern von Webseiten einige Anregungen, wie sie Vertrauen schaffen können. Ob die Anstrengungen von ehrlichen Betreibern zu deutlich mehr Vertrauen im Internet führt, hängt maßgeblich von den Rahmenbedingungen ab, die Politik und Aufsichtsbehörden schaffen. Besucher können ehrliche Betreiber unterstützen und sich auch selber schützen.

7.2.1 Politik und Aufsichtsbehörden

Die Hauptlast, Vertrauen zu schaffen, liegt beim Betreiber. Er 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, die den Umgang mit Daten nachlässig oder bösartig gestalten, schaden dem Ruf einer Branche bis hin zur gesamten Internetwirtschaft. Dies ist die gegenwärtige Situation, in der 54% der deutschen Internet-Nutzer fürchten, dass ihre persönlichen Daten im Internet nicht geschützt sind.[23]

Eine ähnliche Situation zeigt sich im Straßenverkehr. Sicher an das 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-Plicht eingehalten wird, ist Gegenstand polizeilicher Kon-

[21] Heise Online (2008): Beate Uhse: Tausende E-Mail-Adressen veröffentlicht. URL: http://www.heise.de/newsticker/Beate-Uhse-Tausende-E-Mail-Adressen-veroeffentlicht-Update--/meldung/115260. Letzter Zugriff: 2008-11-05.

[22] Heise Online (2008): Verlustfälle bei Kundendaten nehmen zu. URL: http://www.heise.de/newsticker/meldung/114893. Letzter Zugriff: 26.08.2008.

[23] Institut für Demoskopie Allensbach (2007): Sicher im Netz? Mehr Internetaktivität trotz wachsender Bedenken zur Datensicherheit. allensbacher berichte Nr. 17.

trollen. Autofahrer können darauf *vertrauen*, dass alle Autos TÜV-geprüft sind. Deshalb braucht kein Autofahrer den Wagen seines Nachbarn zu untersuchen und diesen bei Mängeln abzumahnen! Der TÜV (und seine Wettbewerber) in Kombination mit der *durchgesetzten* TÜV-Pflicht schaffen Vertrauen in die Verkehrssicherheit. Dieses Vertrauen nützt allen Autofahrern.

Im Web fehlen sowohl der „TÜV“, wie auch eine durchsetzungsfähige Kontrollinstanz. Als Folge kann der bereits mehrfach herangezogene Max Mustermann nicht blind vertrauen, sondern muss bei jedem Betreiber aufmerksam die – meist nicht vorhandene – Datenschutzerklärung studieren. Er fragt sich oft, ob mit seinen Daten auch trotz Datenschutzerklärung Missbrauch getrieben wird. Einen Missbrauch kann Max Mustermann jedoch selten aufdecken. Und selbst wenn er ihn entdeckt, bleibt der Missbrauch meistens ohne negative Konsequenzen für den Betreiber. Max Mustermann bleibt indes auf dem (finanziellen) Schaden sitzen.

Allgemeine Standards wie Inhalt und Platzierung von Datenschutzerklärung, sind typische Themen für Industrie- und Branchenverbände. Für die Kontrolle ist der Staat – wie im Straßenverkehr – in der Pflicht. Eine Kontrolle, ob Gesetze eingehalten werden, gehört zu den konstituierenden Kernaufgaben eines Staates. Erst eine wirksame Kontrolle verhilft Gesetzen zu ihrer Wirkung – wie das TÜV-Beispiel zeigt.

Die existierenden Aufsichtsbehörden für den Datenschutz sind offensichtlich für diese Aufgabe personell nicht gerüstet. In Schleswig-Holstein stehen bspw. 26 Stellen zur Verfügung[24] und in NRW 50 Personen[25], um landesweit die Einhaltung des Datenschutzes zu kontrollieren. Zwei Zahlen zeigen die Dimension der personellen Unterbesetzung auf:

- NRW beschäftigt rund 50.000 Polizisten.[26]
- Bundesweit sind 3,5 Mio. Unternehmen registriert.[27]

Der Gesetzgeber sieht die Einrichtung von Aufsichtsbehörden im Bundesdatenschutzgesetz (§ 38) explizit vor. Er geht also auch davon aus, dass erst die Kontrolle wirksamen Schutz bietet. Warum werden die Aufsichtsbehörden nicht adäquat ausgestattet? Ein möglicher Grund ist, dass der Staat auch selber Daten sammelt. Wer will schon die eigene Aufsicht stärken…

Die Ergebnisse des Datenschutzbarometers wie auch die aktuell in der Presse berichteten Datendiebstähle und Datenmissbräuche zeigen, dass ohne wirksame Kontrollen Internetnutzer, Konsumenten

[24] https://www.datenschutzzentrum.de/presse/20080125-rechnungshof.htm
[25] https://www.ldi.nrw.de/mainmenu_Ueberuns/index.php
[26] http://www.polizei-nrw.de/im/Wir_ueber_uns/. Letzter Zugriff: 2008-11-05.
[27] Statistisches Bundesamt (2008): Unternehmen und Betriebe im Unternehmensregister. Stand: 2005. URL: http://www.destatis.de/jetspeed/portal/cms/Sites/destatis/Internet/DE/Navigation/Statistiken/UnternehmenGewerbeInsolvenzen/Unternehmensregister/Unternehmensregister.psml;jsessionid=6FD5F32408A4C0A6B9B29D80D2E2E1B5.internet. Letzter Zugriff: 2008-11-05.

und Bürger weiter fürchten müssen, dass ihre Daten gestohlen und zu ihrem Schaden verwendet werden. Der hiermit einhergehende Vertrauensverlust bedeutet weniger Umsatz und gefährdet Arbeitsplätze für die Online agierenden Branchen. Ein hoher Preis für Politikversagen.

7.2.2 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.

Weiterführende Informationen zu Webstatistiken und Kontaktformularen finden Sie in unseren Studien:[28]

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

- „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“

7.2.3 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 akzeptable Datenschutzerklärung meiden.
- Dateneingaben auf das erkennbare Minimum reduzieren und Pflichtfelder im Zweifel mit sinnlosen Eingaben zufriedenstellen.
- Schwarze Schafe bei der zuständigen Aufsichtsbehörde[29] oder den Verbraucherzentralen[30] anzeigen.

Einige Webseiten bieten Downloads an, falls vorher eine gültige E-Mail-Adresse angegeben wird. Typischerweise wird der Downloadlink wenig später per E-Mail an die angegebene E-Mail-Adresse zugesandt. Deshalb muss diese gültig sein. Um die eigene E-Mail-Adresse zu schützen, helfen kostenlose Mail-Adressen oder Wegwerfadressen weiter, die bspw. sechs Stunden lang gültig sind. Während dieser Zeit kann man wie gewohnt E-Mails abrufen. Anschließend sind die Adressen ungültig und die Postfächer werden gelöscht. Für die Anmeldung werden keine persönlichen Angaben benötigt. Die Browsererweiterung „Temporary Inbox“[31] erlaubt komfortabel eine Wegwerfadresse einzurichten und das Postfach abzurufen. Im auf den Browser Firefox aufbauenden JonDoFox[32] ist die Erweiterung bereits enthalten.

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:

---

[29] 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

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

[31] Erhältlich für den Mozilla Firefox, Internet Explorer und Opera. URL: https://www.temporaryinbox.com/?l=de. Letzter Zugriff: 2008-03-12

[32] URL: https://www.jondos.de/de/jondofox. Letzter Zugriff: 2008-03-12

- Browser so einstellen, dass Cookies höchstens für die aktuelle Sitzung angenommen werden[33]
- Bei sensiblen Themen einen Anonymisierungsdienst verwenden[34]
- Bei Nutzung von Firefox Scripte selektiv mit der Firefox-Erweiterung „noscript“ [35] steuern, so dass Cookies von Google und Co. gar nicht erst gesetzt werden können. Ein vergleichbares 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.[36]

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

[34] 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.

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

[36] 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

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 Erfolg.**
  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 (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