KERSTIN BLOSSEY &
OLIVER KEMPKENS,
BLOSSEY & PARTNER

Online-Durchsuchungen im Datenschutzfokus

Schwierigkeitsgrad:

Wolfgang Schäuble steht nicht gern im Mittelpunkt. Zu oft wird seine Außendarstellung bemängelt. Zu „knochig“ sei er oder zu „ängstlich“.

Unlängst hörte man Stimmen in einer etablierten (öffentlich-rechtlichen) Radiosendung, die seine „Angst“ und den daraus resultierenden Argwohn als Resultat des Messerattentats 1990 auf ihn schlussfolgern wollten… Nichtsdestoweniger dürfte er nationale Interessen – keine persönlichen Interessen – im Sinn gehabt haben, als er die im Volksmund so genannten *Online-Durchsuchungen* im forcierte. Oder war es am Ende doch eine allzu (un-)menschliche Idee, nach dem Anschlag in derselben Position nochmals dem Volk dienen zu wollen?

Terminus Technicus

Licht ins Dunkel, welchen Inhalt sie genau zum Gegenstand haben und wann *Online-Durchsuchungen* (kursiv gedruckte Begriffe siehe Box *Glossar*) überhaupt stattfinden sollen, hat für viele Bundesbürger erst die Entscheidung des Bundesverfassungsgerichtes vom 27. Februar 2008 zum Gesetz über den Verfassungsschutz in NRW gebracht (*BVerfG, 1 BvR 370/07*). Das Gesetz subsumiert die Online-Durchsuchungen unter den Begriff der *nachrichtendienstlichen Datenerhebung* und ermächtigte eine Landesbehörde mit der Durchführung, sofern auf diese Weise Erkenntnisse über *Verfassungsschutz*-relevante Bestrebungen oder Tätigkeiten oder die zur Erlangung solcher Erkenntnisse erforderlichen Quellen gewonnen werden können.

Doch was genau sind *Online-Durchsuchungen* und weshalb soll es sie überhaupt geben? *Online-Durchsuchungen sollen den Ermittlungsschwierigkeiten Rechnung tragen, die sich ergeben, wenn Straftäter, insbesondere solche aus extremistischen und terroristischen Kreisen, zur Kommunikation sowie zur Planung und Durchführung von Straftaten informationstechnische Mittel und insbesondere das Internet nutzen.* (*BVerfG, 1 BvR 370/07 vom 27.2.2008, Absatz-Nr. 9*), so die Präsidenten des Bundeskriminalamtes und des Bundesamtes für Verfassungsschutz.

Karlsruher Erziehungsauftrag

Fernab strategischer Absprachen beurteilte das Bundesverfassungsgericht die Online-Durchsuchung zu *präventiven* Zwecken – das bedeutet zu Zwecken der Gefahrenabwehr – insofern, als dass die Online-Durchsuchung zunächst sowohl gegen Artikel 10 Grundgesetz (GG) als auch gegen Art. 13 GG verstößt und folglich beide Grundrechte geändert werden müssten. Gleichzeitig erklärten die höchsten deutschen Richter auch, dass dies nicht passieren wird.

Nach ihrer und wohl auch vorherrschender Meinung der Fachliteratur schützt Art. 10 GG nur den laufenden Kommunikationsvorgang. Art. 13 GG widerum bewahrt den Grundrechtsträger nicht in allen Facetten vor einer Online-Durchsuchung. Solange nicht körperlich in die Wohnung eingedrungen wird, z.B. um *Spyware* zu platzieren, oder an das informationstechnische System angeschlossene Geräte wie Kameras oder Mikrofone benutzt werden, um Vorgänge in der Wohnung abzuhören, ist der Eingriff nicht an Art. 13 Abs. 1 GG zu messen. Online-Durchsuchungen könnten also durchaus mit den Art. 10 und 13 GG vereinbar sein, schon allein deshalb, weil sie nicht zwangsläufig in den Gewährleistungsgehalt der erwähnten Grundrechte eingreift. Jedoch ist

IN DIESEM ARTIKEL ERFAHREN SIE…

Die Idee hinter Online-Durchsuchungen

Was der oberste Gerichtshof dazu sagte

Wie der Datenschutz das Thema betrachtet

WAS SIE VORHER WISSEN/KÖNNEN SOLLTEN…

Grundsätzlich sind keine Vorkenntnisse erforderlich, hilfreich ist die Freude an theoretischen Überlegungen zu gesellschaftlichen Brennpunktthemen.

nach Ansicht des Bundesverfassungsgerichts das von ihm so formulierte Grundrecht auf Gewährleistung der *Vertraulichkeit und Integrität* informationstechnischer Systeme durch die Online-Durchsuchung betroffen. Dieses, durch höchstrichterliche Rechtssprechung und Rechtsfortbildung de facto neu ins Leben gerufene Grundrecht, leitet das Gericht aus der Auffangfunktion des *allgemeinen Persönlichkeitsrecht* her, welches seinerseits in Art. 2 Abs. 1 GG i.V.m Art. 1 Abs. 1 GG begründet liegt.

Es bewahrt den persönlichen und privaten Lebensbereich der Grundrechtsträger vor staatlichem Zugriff im Bereich der Informations-

Glossar zum Artikel

- **Allgemeines Persönlichkeitsrecht** – Der Begriff wurde erst nach dem Volkszählungsurteil 1983 (siehe auch *http://www.zv.uni-wuerzburg.de/datenschutz/Urteile/vollksz%C3%A4hlungsgesetz.htm*) richtig gegenständlich und meint den Schutz des Rechts auf freie Entfaltung der Persönlichkeit jedes Bundesbürgers beim Umgang mit seinen Daten und Informationen über ihn oder sie.
- **Antiviren-Software, Router und Firewall** – gängige technische Möglichkeiten, den Kommunikations- und Datenverkehr des Systems und seiner Anwendungen wirksam zu kontrollieren. Diese Mittel sollten auch in privaten Haushalten und Computern zum Einsatz kommen.
- **Ausspionieren** – Sich unbemerkt Zugriff auf Informationen Dritter verschaffen:
- **BverfG** – Bundesverfassungsgericht, oberste deutsche Gerichtsinstanz;
- **Datenerhebung** – im Sinne des Bundesdatenschutzgesetzes (BDSG) handelt es sich dabei um *das Beschaffen von Daten über den Betroffenen.* (§ *3 III BDSG*);
- **Informationelle Selbstbestimmung** – siehe allgemeines Persönlichkeitsrecht;
- **Informationstechnik** – *Oberbegriff für die Informations- und Datenverarbeitung sowie für die dafür benötigte Hard- und Software. Häufig wird die englisch ausgesprochene Abkürzung IT [a ti] verwendet* (Quelle: Wikipedia, *http://de.wikipedia.org/wiki/Informationstechnik*);
- **Keylogger** – Anwendung zum Protokollieren bzw. Erfassen von Tastaturanschlägen;
- **Malware** – *Böse Software*, also auf Deutsch *Schadsoftware*, die Systeme und/oder deren Inhalte aus Sicht des Besitzers unerwünscht beeinflussen, beeinträchtigen bzw. schädigen oder gar unbrauchbar machen soll; Überbegriff für *Spyware*, *Trojaner* etc.;
- **Nachrichtendienstliche Mittel** – Methoden, die Geheimdiensten allgemein zur Verfügung stehen zur Erfüllung ihrer Aufgaben. *Mit dem Begriff Nachrichtendienstliche Mittel werden (geheimdienstliche) Methoden, Gegenstände und Instrumente der heimlichen Informationsbeschaffung bezeichnet (vgl. § 8 Abs.2 Bundesverfassungsschutzgesetz). In den Gesetzen, die die Befugnisse der deutschen Nachrichtendienste regeln, wird dieser generalklauselartige Begriff nicht abschließend definiert, wohl um die sich aus dem Gesetz ergebenden Möglichkeiten der Geheimdienste nicht einzuschränken. Zu den nachrichtendienstlichen Mitteln gehören unter anderem Spione, Observation, geheime Fotografie, Abhören von Funkaktivitäten anderer Staaten, Diebstahl geheimer Unterlagen, Codes brechen, Spionagesatelliten, V-Leute, Tarnmittel und die Überwachung des Brief-, Post- oder Fernmeldeverkehrs. Wichtig bei allen hierdurch erlangten Informationen ist die Verifizierung derselben.* (Quelle: Wikipedia, *http://de.wikipedia.org/wiki/Nachrichtendienstliche_Mittel*);
- **Online-Durchsuchungen** – Zugriff auf Systeme und deren Inhalte über aktuelle Datenübertragungsmedien (z.B. Datenleitung, Schall, Strom) zum Zweck der Überprüfung;
- **präventiv** – bevor ein Ereignis eintritt, in dieser Thematik ist *zu Zwecken der Gefahrenabwehr* gemeint, also das Handeln aufgrund eines Verdachtsmoments.
- **Spyware** – Anwendungen zum Ausspionieren von Systemen und deren Inhalte;
- **Trojaner** – Gemeint ist im Zusammenhang mit Informationstechnik eine Schadsoftware, die oft einen scheinbaren Nutzen bietet, um installiert zu werden. Im Hintergrund wird dann zugleich das System beeinträchtigt, ausspioniert oder gar durch den Urheber bzw. Versender des Trojaners übernommen. Die korrekte Bezeichnung wäre eigentlich *trojanisches Pferd* in Anlehnung an den Mythos der Eroberung Trojas durch die Griechen in der Antike. Sie bauten ein riesiges Holzpferd, in dessen Bauch sie streitfähige Soldaten versteckten und machten dieses den Einwohnern der Stadt Troja, die bis zu dem Zeitpunkt als uneinnehmbar galt, zum Geschenk. Einmal in der Stadt, verließen die Soldaten unbemerkt das Versteck im Holzpferd und sorgten dafür, dass die Tore der Stadt bald sperrangelweit offen standen und der Sieg nur noch eine Frage der Zeit war. Genauso arbeitet auch der *Trojaner.*
- **Verfassungsschutz** – *„Gemäß § 3 Bundesverfassungsschutzgesetz (BVerfSchG) hat das BfV gemeinsam mit den Landesbehörden für Verfassungsschutz (LfV)* **Auskünfte, Nachrichten und sonstige Unterlagen** *zu sammeln und auszuwerten über*

  1. Bestrebungen, die
     - gegen die freiheitliche demokratische Grundordnung oder
     - gegen den Bestand und die Sicherheit des Bundes oder eines Landes gerichtet sind oder
     - durch Anwendung von Gewalt oder darauf gerichtete Vorbereitungshandlungen auswärtige Belange der Bundesrepublik Deutschland gefährden oder
     - gegen den Gedanken der Völkerverständigung (Art. 9 Abs. 2 GG), insbesondere gegen das friedliche Zusammenleben der Völker gerichtet sind,

  2. geheimdienstliche Tätigkeiten für eine fremde Macht (Spionagebekämpfung).

  3. Ferner wirkt das BfV nach § 3 Abs. 2 BVerfSchG beim Geheim- und Sabotageschutz mit.

  Den weitaus größten Teil seiner Informationen gewinnt der Verfassungsschutz aus offenen, allgemein zugänglichen Quellen – also aus Druckerzeugnissen wie Zeitungen, Flugblättern, Programmen und Aufrufen. Mitarbeiter des Bundesamtes besuchen öffentliche Veranstaltungen und sie befragen auch Personen, die sachdienliche Hinweise geben können. Bei diesen Gesprächen auf freiwilliger Basis treten die Mitarbeiter des BfV offen auf. Auch die Sammlung mit nachrichtendienstlichen Mitteln ist unverzichtbar. Dazu gehört das Führen von V-Leuten (angeworbene Personen aus der extremistischen Szene, keine Mitarbeiter der Verfassungsschutzbehörden) in extremistischen Kreisen, die getarnte Observation und ggf. die genehmigungspflichtige und von einem parlamentarischen Gremium kontrollierte Brief- und Telefonüberwachung. Der Verfassungsschutz ist an die Regeln des Rechts und der Verhältnismäßigkeit gebunden". Quelle: *http://www.verfassungsschutz.de/de/das_bfv/waswirtun/was_genau.html* (16.06.08)
- **Vertraulichkeit und Integrität** – Nach dem Grundgesetz, Artikel 2 Abs. 1 in Verbindung mit Artikel 1 Abs. 1 GG, haben alle Bundesbürger ein verbrieftes Recht auf Privatsphäre. Hierzu gehören unter anderem auch ein Recht auf Vertraulichkeit der Informationen, die sie als Person und ihre persönlichen Umstände betreffen, sowie die Integrität ihrer Daten und der Daten erhebenden Stelle. Integrität meint in diesem Zusammenhang die Vollständigkeit und Korrektheit der erfassten Informationen, nicht die Charaktereigenschaft.

technik auch insoweit, als auf das informationstechnische System insgesamt zugegriffen wird und nicht nur auf einzelne Kommunikationsvorgänge oder gespeicherte Daten. (*BVerfG, 1 BvR 370/07 vom 27.2.2008, Absatz-Nr. 201*)

Dies bedeutet jedoch nicht, dass es Schäubles Online-Durchsuchungen nie geben wird, da sie grundsätzlich nicht mit dem Grundgesetz vereinbar sein. Vielmehr gaben die Karlsruher Richter die Lösung mit auf den Weg: die besondere Nähe des neuen *Computer-Grundrechts* zur Menschenwürde impliziert einen besonderen Rechtfertigungsdruck für den Gesetzgeber. Deshalb ist die Online-Durchsuchung im präventiven Bereich nur dann zulässig, wenn sie

- hinreichend klar gesetzlich geregelt ist
- zur Abwehr einer konkreten Gefahr für ein überragend wichtiges Rechtsgut vorgenommen wird und
- durch einen Richter angeordnet wurde.

De Facto reicht eine Regelung innerhalb eines Landesgesetzes also nicht.

Datenschutz vs. Terror

Kurz nach dem Urteil zeigte sich der Bundesinnenminister gesetzeskonform. Von Verbraucherschützern und Reaktionären als *Polizeistaat'ler* stigmatisiert (*Stasi 2.0, Ich habe keine Angst vor bin Laden, ich habe Angst vor Schäuble* – Parolen), erklärte dieser nachdrücklich, dass er sich für das Schaffen einer eindeutigen gesetzlichen Grundlage einsetze und die anfangs geplante Praxis stoppen werde. Wie genau in Zukunft die technische Komponente aussehen wird, ist auch noch nicht vollends klar. Weder Bundeskriminalamt (BKA) noch Bundesnachrichtendienst (BND) nahmen offiziell Stellung. Dennoch reißen die Spekulationen nicht ab: *Keylogger, Malware* oder *Trojaner.* Alles scheint möglich. Gleichzeitig bleibt immer noch die Frage der technisch-praktischen Realisierung offen, ob Online-Durchsuchungen mit den aufgezählten Möglichkeiten überhaupt beim Einsatz handelsüblicher *Antiviren-Software, Routern* und *Firewalls* erfolgsversprechend ist.

Aus datenschutzrechtlicher Sicht stellt sich verstärkt die Frage, ob eine Lockerung der Grundrechte, insbesondere des Rechts auf *informationelle Selbstbestimmung*, die Terrorismusbekämpfung rechtfertigt. Insbesondere ist strittig, ob sich nicht gerade Personengruppen, die intensiv an einem tatsächlichen Anschlag arbeiten, sich nicht gerade gegen Präventivmaßnahmen wie Online-Durchsuchungen präparieren. Gängige Technik vernünftig konfiguriert, ist bereits die halbe Miete – und wer bewußt kriminell arbeitet, weiß in der Regel sehr wohl um die Gefahr der verfrühten *Entdeckung* und der damit verbundenen Erfolglosigkeit eines gesetzten Plans. Er wird daher im Gegenteil alles daran setzen, möglichst so lange unentdeckt zu bleiben, wie es ihm erforderlich scheint. Vor diesem Hintergrund ist es nur schwer zu glauben, dass potentielle Terroristen Dateien á la *Bombenanschag_London_Brainstorming_2008-05-04* systematisch auf ihrem Rechner ablegen. Wäre das der Fall, hätte Strafverfolgungsbehörden wie BKA bzw. Aufklärungsdienste wie der BND sicherlich gute Erfolgsquoten – und damit gute Argumente.

Die Terrorvorbereitungen in Afghanistan und Irak zeigen eher, dass Absprachen, Pläne und Meetings abseits der üblichen messbaren Wege mündlich gefasst und gehalten werden. Analog dazu sind auch die Erfolgsquoten indiskutabel, d.h. im einstelligen Prozentbereich, darf man diversen Zahlen glauben. Bei einer solch niedrigen Aufklärungsquote stellt sich folglich die Frage, ob Online-Durchsuchungen überhaupt notwendig bzw. angemessen sind, um das eingangs genannte Ziel der präventiven Terrorismusbekämpfung zu erreichen. Oder muss hier bei der Abwägung der Interessen des Staates/Volkes gegen das Interesse des grund- und datenschutzgesetzlich zu schützenden Bundesbürgers nicht doch für den Menschen und damit gegen das heimliche Eindringen in heimische bzw. private Systeme entschieden werden? Zudem sieht das BDSG das Prinzip der Datenvermeidung und Datensparksamkeit vor. Es dürfen also nur solche personenbezogene Daten erhoben werden, die für die Erfüllung eines konkreten Geschäftszwecks benötigt werden. Wenn ein vorgesehenes Verfahren nicht den gewünschten Erfolg in anmessenem Umfang bringen kann, ist das Verfahren ungeeignet für den Einsatz und es muss nach anderen Mitteln gesucht werden. Darüber hinaus stellen gesammelte und gespeicherte Daten ein Risikopotential für Datenmissbrauch dar. Immer wieder werden Stimmen und Quellen laut in letzter Zeit, wo neben Banken, Telekommunikationsdiensteanbietern, Reise- und Transportunternehmen, aber auch kommunale Behörde oder staatliche Einrichtungen, nicht nur in Deutschland, auch in England, in der Schweiz und überall sonst auf der Welt, sensible Daten unbefugt erhoben *aus Versehen* ins Netz stellten oder anders veröffentlichten oder verloren.

Ausblick aufs nächste Heft

Private Nutzung von E-Mail- und Internetdiensten am Arbeitsplatz – warum jedes Unternehmen eine eindeutige Regelung haben und was genau geregelt werden sollte.

Ausblick – die Autoren in eigener Sache

Wir denken, dass es wichtig ist, sich über solche Themen, wie die in den letzten Hakin9-Ausgaben erschienenen, Gedanken zu machen. Die Grundvoraussetzung für den vernünftigen Umgang mit seinen eigenen persönlichen Daten ist es, zu wissen, was passieren kann, wenn sie in falsche bzw. unbefugte Hände geraten. Im Datenschutz benutzt man hierfür den Begriff der *Sensibilisierung* und weiß, je aufmerksamer der Einzelne für das Thema gemacht werden konnte, umso leichter fällt es ihm und ihr, sich im Alltag verantwortungsbewußt im Umgang mit eigenen und fremden personenbezogenen Daten umzugehen. Wir denken, wir haben fürs Erste genug Impulse für eine persönliche Auseinandersetzung mit dem Thema Privatsphäre, Persönlichkeitsrecht und Datenschutz-Nutzen gegeben und wollen uns ab dem nächsten Heft den praktischen Themen auf unserer Liste zuwenden. So wird es in der kommenden Ausgabe um die private E-Mail- und Internetnutzung am Arbeitsplatz gehen, warum dies ein heißes Eisen für Personal und Unternehmensführung ist und wie man das Risikopotential wirksam reduzieren kann. Vielleicht gibt es auch schon konkrete Themenwünsche, die wir genauer beleuchten könnten? Wir freuen uns über Ihre Anregungen, nehmen Sie einfach Kontakt mit uns auf.

Kerstin Blossey
Kerstin Blossey ist 1969 in Erlangen geboren, Dipl. Informations-Wirtin (FH) und Gründerin von Blossey & Partner, einem aufstrebenden Unternehmen, das sich auf den deutschen wie internationalen betrieblichen Datenschutz für Medien, Wirtschaft, Gesundheitswesen und die öffentliche Hand spezialisiert hat.

Oliver Kempkens
Oliver Kempkens ist 1983 in Essen geboren, Wirtschaftsmediator (cvm) und studiert Jura an der Ludwigs-Maximilians-Universität in München. Neben seinem Studium arbeitet er freiberuflich im Bereich Datenschutz und Mediation.