Fachhochschule Kaiserslautern
University of Applied Sciences

Informatik und Mikrosystemtechnik
Zweibrücken

Studiengang

Medieninformatik

Studienarbeit

Datenschutzrecht in der Cloud, in Deutschland, der EU und den USA. Eine für Laien verständliche Juristische Gegenüberstellung.

vorgelegt von

Raphael Kiefer 862743

3. Februar 2015

Betreuung: Prof. Adrian Müller, PMP, PSMI

Inhaltsverzeichnis

1. Einleitung....3
2. Datenschutzrecht in Deutschland....5
2.1. Das Deutsche Datenschutzrecht für Laien verständlich erklärt....5
2.2. Unterschiede zum Europäischen Datenschutzrecht....7
2.3. Unterschiede zum Amerikanischen Datenschutzrecht....7
3. Wie kann ich selbst für mehr Datenschutz sorgen?....8
4. Fragestellung „welches Datenschutzrecht greift, beim Ablegen meiner Daten im Ausland?“....12
4.1. Ablegen der Daten bei einem amerikanischem Unternehmen, Server in Deutschland oder Europa....12
4.2. Ablegen der Daten bei einem amerikanischem Unternehmen, Server in Amerika....12
4.3. Ablegen der Daten bei einem deutschen Unternehmen, Server in Deutschland oder der Europäischen Union....12
5. Ausarbeitung der Interviews....13
6. Was ist am aktuellen Datenschutzrecht gut?....14
7. Was muss sich in Zukunft am Datenschutzrecht ändern?....14
8. Einheitliches Datenschutzrecht, sinnvoll und machbar?....15
9. Zusammenfassung....16
10. Fazit....17
11. Literaturverzeichnis....18
12. Anhang....19

1. Einleitung

Gerade nach den Anschlägen in Paris auf die Satirezeitschrift 'Charlie Hebdo' und in dessen Folge nicht nur in Deutschland, sondern auch in ganz Europa die Stimmen nach der Vorratsdatenspeicherung wieder lauter werden, möchte ich meine Studienarbeit mit einem Zitat von Benjamin Franklin beginnen, „Wer die Freiheit aufgibt um Sicherheit zu gewinnen, der wird am Ende beides verlieren.“[1] *[Franklin, B., and A. Wagner., 1818]*

Genau das ist es was meiner Meinung nach passieren wird, wenn wir Vorratsdatenspeicherung zulassen und sogar die Verschlüsselung im Internet abschaffen beziehungsweise Sicherheitsbehörden in die Lage versetzt werden sollen, Verschlüsselung zu entschlüsseln oder zu umgehen, wie es der Britische Premierminister Cameron und mittlerweile auch der US-Präsident Obama oder auch unser Bundesinnenminister de Maizière nach den Anschlägen in Paris fordern.

In meiner Studienarbeit mit dem Thema 'Datenschutzrecht in der Cloud, in Deutschland, der EU und den USA. Eine für Laien verständliche juristische Gegenüberstellung' in der Fachgruppe Cloud, habe ich mich mit dem Datenschutz in Deutschland beschäftigt. Dazu habe ich eine Gegenüberstellung der Datenschutzrechte in Europa und den USA ausgearbeitet.

Während der Ausarbeitung der Interviews und der Literaturrecherche wurde schnell klar, dass dieses Thema ein sehr komplexes Thema ist. Sich zum Beispiel nur mit dem deutschen Datenschutzrecht auszukennen, nützt einem gerade im Hinblick auf die Cloud, die wie das Internet selbst grenzübergreifend und global ist, nicht sehr viel, da nicht nur jeder Staat sondern auch jedes Unternehmen eigene Vorstellungen vom Datenschutz hat. Eine Erklärung dazu folgt in den nächsten Kapiteln.

Als ich mir die Datenschutzrichtlinien der Anbieter, wie Dropbox oder Amazon, genauer angeschaut habe ist mir aufgefallen, dass sich diese doch sehr vom Datenschutzrecht in Deutschland unterscheiden. Auch dazu später mehr.

Wofür ist das Datenschutzrecht denn nun eigentlich gut? Innerhalb von Unternehmen, Hochschulen, Behörden und anderen staatlichen oder nichtstaatlichen Organisationen ist der Datenschutz sicherlich auch gewährleistet. Aber wie sieht es für mich, den einfachen Nutzer aus, für den meist die ganzen Paragraphen mehr verwirrend sind, als dass ich mit ihnen etwas anzufangen wüsste?

Ich denke, man muss selbst das Interesse am Datenschutz finden und sich mit seinen damit verbundenen Rechten auseinandersetzen. Wenn der Datenschutz zum Beispiel von einem Unternehmen wie Dropbox, Facebook, und so weiter nicht ausreichend gewährleistet wird, sollte ich mir als Nutzer überlegen ob ich diese Dienste vielleicht boykottiere oder für meine Rechte sogar auf die Straße gehe. Was wir Deutschen, nebenbei bemerkt, im Vergleich zu anderen Ländern sowieso viel zu selten tun, gerade wenn es um dieses Thema geht. Eigeninitiative ist also gefragt!

1 Zitat von Benjamin Franklin aus dem Jahr 1775, erschienen in *[Franklin, B., and A. Wagner., 1818]*

Große Problem ist oft der Gruppenzwang und das Desinteresse am Thema, gerade wenn man sich zum Beispiel entscheidet, einen bestimmten Dienst aufgrund der mangelnden Einhaltung des Datenschutzes oder mangelnder Verschlüsselung, zu boykottieren. Ich selbst kann dies im engeren Bekannten- und Familienkreis, zu dem auch teilweise Personen mit umfangreichem Wissen im IT-Bereich gehören, immer wieder feststellen. Wenn man zum Wechsel bewegen will oder es um das Thema Sicherheit geht fallen oft die Argumente: 'Aber das nutzen ja meine anderen Freunde nicht!' oder 'Ich habe ja nichts zu verbergen!'.

Wie oben bereits erwähnt fühlte ich mich zu Beginn meiner Studienarbeit von dem ganzen Thema etwas erschlagen und überfordert. Gerade auch weil das Thema Datenschutz, während meiner Recherchen, auch aus aktuellen Anlässen immer wieder in der Fachpresse stark vertreten war und diskutiert wurde. Nach den Recherchen, den Interviews und meinen eigenen Gedanken, die ich mir zum Datenschutz gemacht habe, wurde allerdings mein Interesse für das Thema geweckt. Ich hoffe, dass ich mit dieser Studienarbeit auch das Interesse der Leser für dieses, doch etwas umfangreiche Thema wecken kann.

Im Laufe der Ausarbeitung meiner Studienarbeit habe ich ein paar Änderungen gegenüber dem im Exposè beschriebenen Vorgehen vornehmen müssen. So hat sich das Inhaltsverzeichnis wie Folgt verändert:

- Kapitel 2.4 'Unterschiede zwischen europäischem und amerikanischem Datenschutz' wurde gestrichen, wird in Kapitel 2.3 erklärt
- Kapitel 3 'Vergleich deutsches und amerikanisches Datenschutzrecht' wurde in 'Wie kann ich selbst für mehr Datenschutz sorgen?' umbenannt
- Kapitel 4 an den Unterkapiteln wurden Änderungen vorgenommen.
- Kapitel 5 'Ausarbeitung der Interviews' ist neu hinzu gekommen und enthält die Fragen, die ich den Interviewpartnern gestellt habe. Die Interviews selbst sind in die Studienarbeit eingeflossen, sind aber im Anhang in vollständiger Ausführung zu finden.
  - Dadurch haben sich die anderen Kapitel verschoben
- Kapitel 6 'Ergebnisse der Interviews' wurde in 'Was ist am aktuellen Datenschutzrecht gut' umbenannt und die Unterkapitel, 6.1, 6.2 und 6.3 sind gestrichen worden.

2. Datenschutzrecht in Deutschland

2.1. Das Deutsche Datenschutzrecht für Laien verständlich erklärt

Vor 40 Jahren war das Rheinland-pfälzische Datenschutzrecht erst das dritte Weltweit. Aber was ist Datenschutz überhaupt?

Datenschutz bezieht sich hauptsächlich auf persönliche Daten, wie Name, Alter, Geburtsdatum, Adresse, und so weiter, also personenbezogene Daten. Dabei setzt der Datenschutz direkt auf die Datensicherheit auf.

Verwandte Gebiete zum Datenschutz sind unter Anderem das Persönlichkeitsrecht, wobei auch das Fernmeldegeheimnis eine enge Verwandtschaft zum Datenschutzgesetz aufweist. Gerade beim Thema Cloud, bei dem personenbezogene Daten wie oben beschrieben, personenbeziehbare Daten wie zum Beispiel die IP-Adresse und natürlich auch die Dateien, die in der Cloud gespeichert werden sollen und über das Internet verschickt werden, ist es wichtig, dass diese vom Datenschutzgesetz ausreichend geschützt werden. Auch der Bildnisschutz, Recht am eigenen Bild, ist dadurch, dass Bilder täglich über das Internet verschickt werden, eng mit dem Datenschutzgesetz verwandt und wird durch selbiges erweitert.

Wie macht der Gesetzgeber auf das Thema Datenschutz aufmerksam? In staatlichen und nichtstaatlichen Organisationen, Unternehmen und so weiter, klären die zuständigen Datenschutzbeauftragten über das Thema auf und bieten Schulungen an. Das Problem bei der Öffentlichkeitsarbeit ist, sobald ein aktuelles Datenschutzthema in der Presse aufkommt, dass jeder davon ausgeht er wäre nun ausreichend darüber informiert. Dies stimmt aber nicht! Besser wäre es, wie in Kapitel 3 beschrieben, sich bezüglich des Datenschutzes auf Staatlichen Internetseiten zu informieren. Meist scheitert die Aufklärung allerdings auch an der Grundeinstellung der Nutzer gegenüber dem Datenschutz. Dieses Desinteresse resultiert aus einer Machtlosigkeit der Nutzer, die dadurch bedingt ist, dass die meisten sich von den Datenschutzbestimmungen und Paragraphen eher erschlagen fühlen, als dass sie diese verstehen. Bei der Sensibilisierung und der Aufklärung ist allerdings Interesse und Eigeninitiative sehr wichtig. Die beste Möglichkeit zur Sensibilisierung für Datenschutz ist bei der Ausbildung am Gerät, also bereits in der Schule. Hierfür werden vom Landesdatenschutzbeauftragten auch schon Programme für Schüler angeboten.

Spätestens wenn die Daten dann mal weg sind, sei es durch Diebstahl oder sonstigen Verlust, muss man sich zwangsläufig mit dem Datenschutz auseinandersetzen. Doch an wen wendet man sich, wenn es soweit ist? Als erstes sollte man sich direkt an den Anbieter wenden. Auch die Aufsichtsbehörden sollten informiert werden, wobei dies aber nur im deutschen und europäischen Raum möglich ist. Natürlich kann man sich auch direkt an den Landes- oder Bundesdatenschutzbeauftragten wenden. Allerdings muss man mit langen Antwortzeiten rechnen, da dort sehr viele Anfragen eingehen.

Das deutsche Datenschutzrecht ist im europäischen Vergleich, aber auch im Vergleich zum amerikanischen Recht, sehr viel restriktiver. Zwischen der europäischen Union, und somit auch mit deren Mitgliedsstaaten, und den USA gibt es die Safe Harbour Verträge, die allerdings durch den Patriotact und die NSA Affäre aufgeweicht wurden.

Die Basis für das deutsche Datenschutzrecht ist wie für alle Mitgliedsstaaten der Europäischen Union, die EU-Richtlinie. Allerdings ist das deutsche Datenschutzrecht, wie bereits erwähnt, weitaus strenger.

Es gibt auch von der Bundesregierung finanzierte Cloudprojekte, wie zum Beispiel Tclouds[2] vom ULD[3], das mit 10,5 Millionen Euro gefördert wurde und TrustedCloud[4] vom BMWI,[5] das insgesamt sogar mit 100 Millionen Euro gefördert wird. Man fragt sich natürlich wozu diese Projekte am Ende eingesetzt werden und ob sie mit deutschen Datenschutzstandards auch für deutsche Bürger zugänglich gemacht werden. Allerdings handelt es sich dabei eher um Forschungsprojekte für die Industrie. Sie sind als Lösungsvorschläge zu sehen und werden keine Dienste für die Bürger hervorbringen.

Generell kann man sagen, dass die Gesetzgebung hinter neuen Entwicklungen immer etwa zwischen fünf bis zehn Jahren hinterher hinkt. Was also bedeutet, dass es für eine neue Technologie, sei es eine neue Art der Kommunikation oder Cloud, erst Jahre später, wenn die Technologie quasi schon wieder veraltet ist, eindeutige Gesetze gibt. Das beste Beispiel dafür ist im Zusammenhang mit dem Urheberrecht das Streamen, was immer noch eine Grauzone darstellt, da es noch keine eindeutigen Gesetze dafür gibt.

Aus dem aktuellen Datenschutzbericht des Datenschutzbeauftragten des Landes Rheinland Pfalz von 2014 für 2012/2013 geht hervor, dass gerade im Hinblick auf das Internet, die Nutzung von Smartphones und Cloud Computing, der Datenschutz nicht mehr oder kaum noch gewährleistet werden kann.[6] Genau aus diesem Grund ist es wichtig sich mit dem Thema Datenschutz auseinander zu setzen, denn unsere Daten werden immer mehr zu einer Ware, oder wie der Landesdatenschutzbeauftragte es nennt „zum vierten Produktionsfaktor“, was man im Moment an den geänderten Facebook Datenschutzrichtlinien und AGB am besten sieht.

Wie verworren das Datenschutzrecht ist wird einem klar, wenn man sich einmal anschaut wer alles Datenschutzrichtlinien und -gesetze verabschiedet. Jeder Staat hat sein eigenes Datenschutzrecht. In Europa haben wir wiederum zunächst die EU-Richtlinie, auf die alle anderen Datenschutzrechte der Mitgliedsstaaten aufbauen. Dann hat jeder Mitgliedsstaat noch eigene Regelungen und, wenn wir in Deutschland bleiben, hat auch noch jedes Bundesland wieder eine eigene Gesetzgebung. Nicht zuletzt hat jedes Unternehmen eigene Datenschutzrichtlinien. Da den Überblick zu behalten dürfte selbst einem Juristen ein wenig schwer fallen. Kein Wunder also, dass wir uns als Laien nicht gerne mit dem Thema auseinandersetzen wollen.

Datenschutzrichtlinien und -gesetze regeln den Umgang mit unseren Daten, doch wie so oft liegt es in unserer eigenen Verantwortung, dass die Regeln eingehalten werden beziehungsweise wir unsere Daten schützen. Aber um seine Daten vor unbefugtem Zugriff zu schützen muss man kein Experte für Datenschutzrecht sein. Es genügt für den Anfang ein paar grundlegende Regeln im Umgang mit dem Internet, Smartphones und vor allem der Cloud einzuhalten. In den späteren Kapiteln werde ich erläutern, was man selbst für mehr Schutz seiner Daten tun und wo man sich über Datenschutz informieren kann.

---

2 https://www.datenschutzzentrum.de/projekte/tclouds/
3 Unabhängiges Landeszentrum für Datenschutz, Schleswig-Holstein
4 http://trusted-cloud.de/
5 Bundesministerium für Wirtschaft und Energie
6 *[Datenschutzbeauftragter Rheinland Pfalz, 2014]*

2.2. Unterschiede zum Europäischen Datenschutzrecht

Welche Unterschiede gibt es zwischen dem deutschen und dem europäischen Datenschutzrecht? Dies war auch eine Frage, die ich mir bei der Ausarbeitung meiner Studienarbeit gestellt habe.

Die Datenschutzrichtlinie der Europäischen Union ist noch von 1995, sie wurde vor kurzem angepasst, und lässt Spielräume für die Länder offen. Wichtig ist, dass die zuständigen Behörden für den Datenschutz unabhängig arbeiten, was nicht in allen Ländern der Fall ist.

Im Prinzip gibt es keine Unterschiede zwischen deutschem und europäischem Datenschutzrecht. Vielmehr ist es wie bei der Vererbung in der Informatik. Das Europäische Datenschutzrecht ist eine Richtlinie, von der alle Datenschutzrechte der verschiedenen Mitgliedsstaaten der Europäischen Union abgeleitet werden. Natürlich steht es jedem Land dabei frei, noch weitere Ergänzungen hinzuzufügen. Weggelassen werden kann allerdings nichts.

So ergibt es sich, dass jedes Mitgliedsland der Europäischen Union sein Datenschutzrecht zwar auf den selben Richtlinien aufbaut, es aber trotzdem Unterschiede in der Gesetzgebung gibt. Deutschland zum Beispiel hat in der Europäischen Union die höchsten Datenschutzbestimmungen, wohingegen Irland sich hauptsächlich an der EU-Richtlinie orientiert und somit keine hohen Datenschutzbestimmungen hat, was auch mit einer der Gründe sein dürfte, warum Irland von den großen amerikanischen Unternehmen gerne als Hauptsitz in der Europäischen Union gewählt wird.[7]

2.3. Unterschiede zum Amerikanischen Datenschutzrecht

Gibt es in den USA so etwas wie Datenschutzrecht überhaupt? Natürlich hat jedes Unternehmen auch dort Datenschutzrichtlinien. Nur stellt der Amerikaner den Terrorschutz über alles andere, wodurch Datenschutzrecht in den USA nicht wirklich besteht. Mit der Europäischen Union, und somit auch mit ihren Mitgliedsstaaten, gibt es das Safe Harbour[8] abkommen, das den Datenverkehr zwischen den Vertragspartnern regelt, was aber durch den Patriot- und Freedomact nicht mehr wirklich greift.

Betrachtet man die Datenschutzrichtlinien von Dropbox stellt man fest, dass zwar Dinge darin stehen die vom europäischen oder deutschen Datenschutzrecht gefordert werden, aber nicht so wie es sein sollte.[9] Ein Beispiel dafür ist, dass laut Datenschutzrecht der Anbieter einer Cloudlösung für den Nutzer offen legen muss, wo auf der Welt der Server steht auf dem seine Daten gespeichert werden. In den Datenschutzrichtlinien von Dropbox steht hierzu folgendes: „Weltweit...“[10] Das vermittelt zumindest für mich den Eindruck, und da haben mir die Datenschutzbeauftragten im Interview auch zugestimmt, dass die großen Anbieter eigentlich machen was sie wollen. Einer der Datenschutzbeauftragten ging sogar noch einen Schritt weiter und meinte, ganz getreu dem Motto 'Geld regiert die Welt' würden diese Anbieter auch handeln. Wer also mehr Datenschutz will, muss auch mehr dafür bezahlen. Wer die Dienste günstig oder gar kostenlos nutzt muss dementsprechend mit dem Maß an Datenschutz vorlieb nehmen, das der Anbieter ihm zugesteht.

---

7 *[t3n Magazin 15.11.2014]*
8 *[export.gov safeharbour]*
9 *[Arbeitskreise Technik und Medien der Konferenz der Datenschutzbeauftragten des Bundes und der Länder sowie der Arbeitsgruppe Internationaler Datenverkehr des Düsseldorfer Kreises, Stand: 09.10.2014]*
10 https://www.dropbox.com/privacy

3. Wie kann ich selbst für mehr Datenschutz sorgen?

Eine erste Möglichkeit herauszufinden wie der Anbieter den ich ausgewählt habe mit dem Datenschutz umgeht, ist ein Blick in die AGB und die Datenschutzrichtlinien. Ohne Eigeninitiative geht es leider nicht. Habe ich die AGB beziehungsweise die Datenschutzrichtlinien gelesen, muss ich natürlich für mich selbst entscheiden, ob mir der vom Anbieter versprochene Datenschutzstandard ausreicht. Ein Vergleich der AGB und Datenschutzrichtlinien zwischen verschiedenen Anbietern kann bei der Wahl ebenfalls hilfreich sein. Denn jeder Anbieter hat seine eigenen Richtlinien.

Der Gruppenzwang steht beispielsweise dem Wechsel eines Anbieters meist im Weg. Arbeitskollegen/innen, Kommilitonen/innen oder Freunde und Familie lassen sich meist nur schwer von einem Wechsel überzeugen. Das Argument, 'das nutzen aber alle anderen nicht', überwiegt meist dem Sicherheitsanspruch. Vielleicht auch gerade aus dem Grund der Überforderung oder weil viele den Standpunkt vertreten: 'Warum sollte mich jemand ausspionieren und selbst wenn, ich habe ja nichts zu verbergen.' Doch gerade im Hinblick auf nicht ausreichend gewährleisteten Datenschutz sollte man sich überlegen, ob es einem nicht der Mühe wert ist andere von einem Wechsel zu überzeugen.

Die wohl wichtigste Maßnahme, um seine persönlichen Daten ausreichend zu schützen, ist, sie schon vor dem Hochladen zum Anbieter zu verschlüsseln. Wenn der Anbieter die Verschlüsselung erst bei sich auf dem Server vornimmt, nützt das nicht viel. Sicherer ist es, die Daten selbst vor dem Hochladen zu verschlüsseln oder einen Anbieter zu wählen, der eine solche Methode anbietet. Auch bei der Kommunikation zwischen Server und dem eigenen Computer ist auf Verschlüsselung zu achten. HTTPS[11] ist ein Muss! Um meine Daten also wirklich geschützt zu wissen ist die Verschlüsselung auf meinem PC vor dem Hochladen und die Verschlüsselung der Kommunikation mit dem Server während des Hochladens gleich wichtig.

Eine weitere Sicherheitsmaßnahme besteht darin beim Registrieren weitestgehend Pseudonyme und keine Klarnamen zu verwenden. Dies gewährleistet mir noch ein wenig Anonymität. Sollte es mich allerdings nicht stören, dass der Anbieter weiß, welche Musik ich zum Beispiel gerne höre, kann ich natürlich auch darauf verzichten.

Um meine Daten auch vor Ausfall oder Abhanden kommen zu schützen ist es immer ratsam eine Datensicherung zu machen. Auch der Anbieter einer Cloudlösung kann die Daten verlieren, sei es durch Hackerangriffe, Naturkatastrophen oder weil sie aus Versehen gelöscht wurden, was alles schon vorgekommen ist.

Um immer Herr über meine Daten zu sein und den höchsten Datenschutzstandard zu gewährleisten wäre zum Beispiel eine Private Cloudlösung, die ich auf einem eigenen Webserver oder ausgemusterten Computer zuhause installiere, eine gute Alternative. Die wohl drastischste Art meine Daten hundertprozentig zu schützen wäre, sie natürlich gar nicht erst in der Cloud abzulegen, was aber in der heutigen vernetzen Welt sicherlich auch keine Lösung mehr ist.

In der Richtlinie zur Auslagerung von Daten in die Cloud der Freien Universität Berlin[12] ist zu lesen, dass man anhand von Zertifikaten, wie beispielsweise ISO 27001, diese entspricht BSI 100-1,

11 https://de.wikipedia.org/wiki/Hypertext_Transfer_Protocol_Secure
12 *[Freie Universität Berlin, 2011]*

erkennen kann, wie ernst ein Anbieter die Sicherheit und den Schutz der Kundendaten nimmt.
Wie ich es auch schon in meiner Präsentation angesprochen habe, gibt es noch ein paar mehr Dinge die man selbst für mehr Datenschutz tun kann. Diese erläutere ich nachfolgend.
So gibt es zum Beispiel seit neuestem eine von amerikanischen Wissenschaftlern ins Leben gerufene Website, die Android und bald wahrscheinlich auch IOS und Windows Phone Apps, nach ihren Datenschutzrichtlinien beurteilt. Leider wird dabei kein Wert auf Verschlüsselung gelegt. So kann es vorkommen, dass eine App, die die Datenübertragung nicht verschlüsselt, trotzdem auf einem guten Platz landet, weil sie, wie bereits erwähnt, nur anhand der Datenschutzrichtlinien beurteilt wurde.

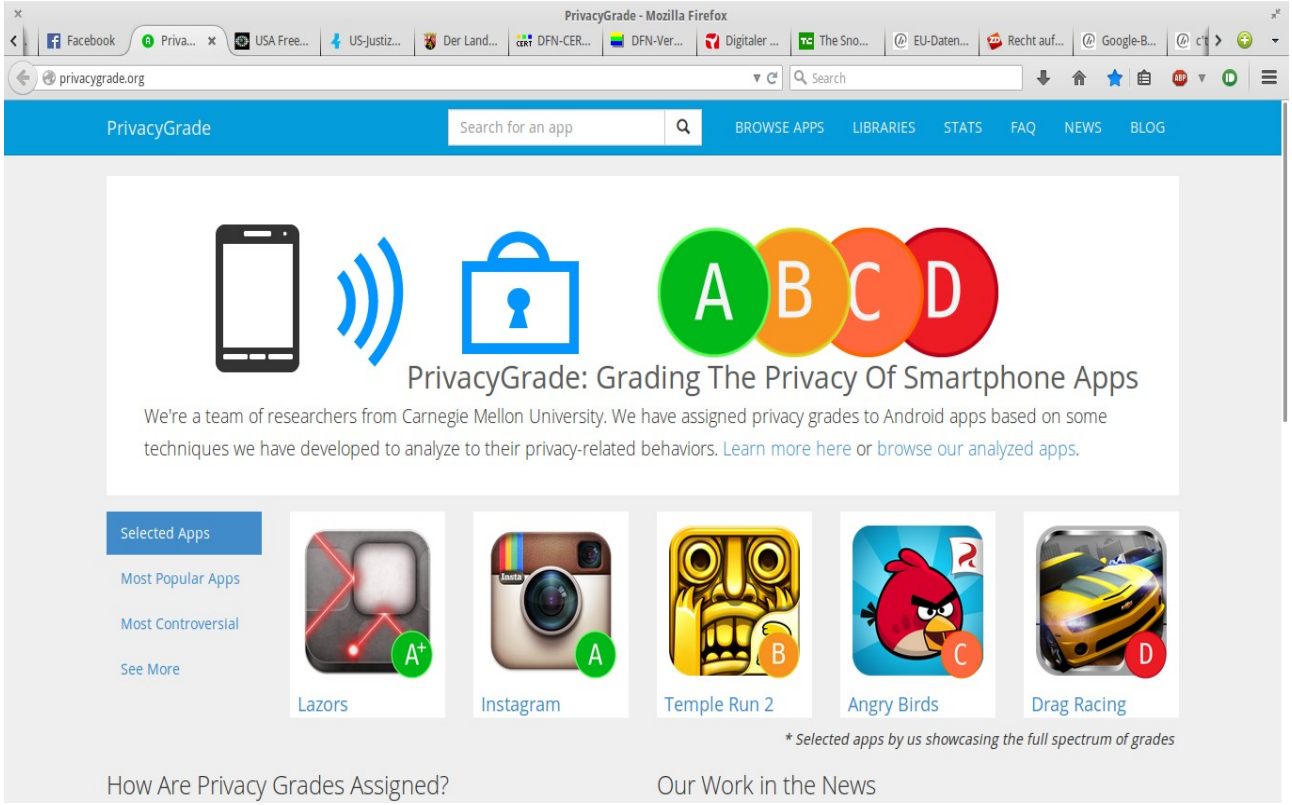

Abbildung 1: Quelle: www.privacygrade.org

Von der US-Bürgerrechtsgruppe Electronic Frontier Foundation (EFF) wurde die folgende Seite ins Leben gerufen, auf der man in Kombination mit der oben genannten Seite schauen könnte:
Erstens, wie gut ist der Datenschutz (Seite oben) und zweitens, wie sicher ist es von den Verschlüsselungsaspekten mit dem Messenger zu kommunizieren (Seite unten).

	Encrypted in transit?	Encrypted so the provider can't read it?	Can you verify contacts' identities?	Are past comms secure if your keys are stolen?	Is the code open to independent review?	Is security design properly documented?	Has the code been audited?
Threema	✓	✓	✓	✓	✗	✓	✗
Viber	✓	✗	✗	✗	✗	✗	✗
Virtru	✓	✗	✗	✗	✗	✓	✓
WhatsApp	✓	✗	✗	✗	✗	✗	✓

Abbildung 2: Quelle: https://www.eff.org/secure-messaging-scorecard

Vom Datenschutzbeauftragten des Landes Rheinland Pfalz wird zur Überprüfung des Passwortes die folgende Seite empfohlen.

Abbildung 3: Quelle: https://checkdeinpasswort.de/

Denn auch ein Sicheres Passwort hilft die eigenen Daten vor fremden Zugriffen zu schützen.

Wie es für Informatik die 'Gesellschaft für Informatik' gibt, so gibt es für den Datenschutz auch die 'Gesellschaft für Datenschutz und Datensicherheit e.V.' kurz GDD, auf deren Internetseite https://www.gdd.de/ man sich auch über Datenschutz informieren kann.

Unter http://www.datenschutz.de/ kann man sich über konkrete Fragen des Datenschutzes informieren oder Probleme melden. Dort findet man auch Infomaterial zum Thema Datenschutz. Somit ist es eine der ersten Anlaufstellen bei Fragen oder Informationsbedarf.

Vom Landesdatenschutzbeauftragten wird http://www.youngdata.de/ betrieben, die sich zwar speziell an Jugendliche richtet aber sicherlich auch für Laien interessant ist. Dort findet man unter anderem ein Datenschutz-quiz und wird umfassend über das Thema Datenschutz informiert, gerade auch was zum Beispiel Kommunikations-Apps, etc. angeht.

Im Zusammenhang mit dem NSA Skandal ist auch oft der Name Edward Snowden gefallen, der mittlerweile fast jedem ein Begriff ist. Er rät von Anbietern wie Dropbox und Google ganz ab und empfiehlt einen Wechsel zu anderen Cloudanbietern. Auf der Seite https://spideroak.com/ kann man sich ein Benutzerkonto mit einem sicheren Cloudspeicher anlegen, die Seite verspricht Verschlüsselung vor dem Hochladen und dass die Nutzung ohne großes Datenschutzwissen genutzt werden kann.[13]

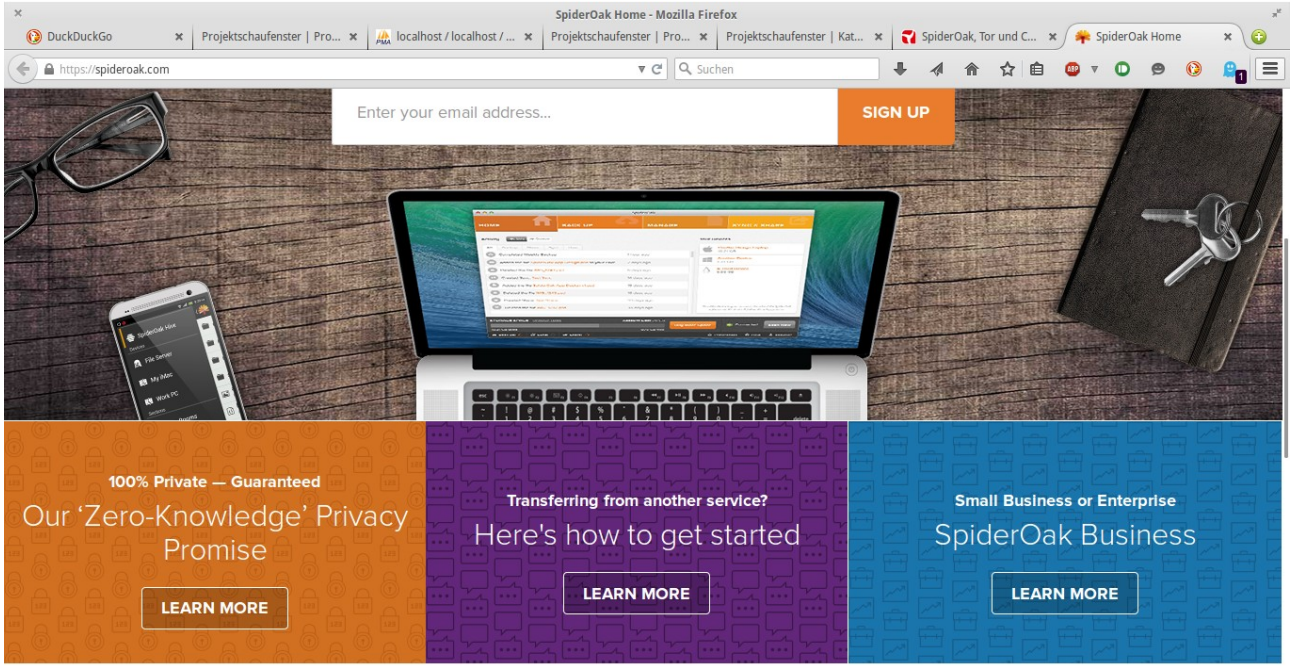

Abbildung 4: Quelle: https://spideroak.com/

Weitere Seiten und Möglichkeiten wurden bereits im Vortrag zu meiner Studienarbeit erwähnt.

13 *[t3n Magazin 03.02.2015]*

4. Fragestellung „Welches Datenschutzrecht greift, beim Ablegen meiner Daten im Ausland?“

Eigentlich würde jeder davon ausgehen, dass das Datenschutzrecht des Landes greift in dem ich mich befinde, beziehungsweise zumindest des Landes, in dem sich der Anbieter befindet. Doch das stimmt nicht ganz. Es gilt das Datenschutzrecht des Landes, in dem sich meine Daten befinden. Aber wie in den vorherigen Kapiteln beschrieben, kann ich meist nicht nachvollziehen wo auf der Welt sich meine Daten befinden. So räumen sich die Anbieter gewisse Freiheiten ein und es ist nicht ganz klar, welches Datenschutzrecht tatsächlich gilt. Wie das dann genau aussehen kann erläutere ich nachfolgend an ein paar Beispielen.

4.1. Ablegen der Daten bei einem amerikanischem Unternehmen, Server in Deutschland oder Europa.

Wie oben schon beschrieben, kommt es nun darauf an ob der Anbieter offenlegt wo meine Daten sich befinden. Liegen sie tatsächlich auf einem deutschen Server, so würde folglich auch deutsches Datenschutzrecht gelten. Da amerikanische Unternehmen, wie schon erwähnt, aber meist ihren Hauptsitz und vermutlich auch ihre Server in Irland haben, würde somit natürlich irisches Datenschutzrecht greifen.

4.2. Ablegen der Daten bei einem amerikanischem Unternehmen, Server in Amerika

Stehen die Server in Amerika und meine Daten liegen nachweislich auch auf diesem Server, so greift amerikanisches und nicht deutsches, beziehungsweise europäisches Recht.

4.3. Ablegen der Daten bei einem deutschen Unternehmen, Server in Deutschland oder der Europäischen Union

Die sicherste Methode seine Daten abzulegen ist, einen Anbieter aus Deutschland oder Europa zu wählen. Selbstverständlich kann es auch dort sein, dass der Server, auf dem sich meine Daten befinden, in einem anderen Land steht. In Deutschland und der Europäischen Union sind die Unternehmen auch an die EU-Richtlinie bzw. deutsches Recht gebunden. Dieses besagt, dass sie genau Auskunft darüber geben müssen, wo sich meine Daten befinden. Also reicht ein Blick in die Datenschutzrichtlinien des Anbieters um sicher zu gehen. In den meisten Fällen kann man davon ausgehen, dass, wenn man seine Daten bei einem deutschen Unternehmen speichert, auch deutsches Datenschutzrecht gilt.

Wie die einzelnen Unternehmen dieses Recht auf Auskunft handhaben, kann bei jedem einzelnen Unternehmen in den AGB beziehungsweise Datenschutzrichtlinien nachgelesen werden und ist folglich auch für alle Unternehmen anders. Hier ist also auch wieder Eigeninitiative gefragt.

Natürlich sollte man sich nicht nur auf die Datenschutzrichtlinien der Unternehmen und das Datenschutzrecht der jeweiligen Staaten verlassen. Wie ich bereits ausführlich beschreiben habe, kann und sollte man noch andere Sicherheitsaspekte beachten und auch selbst für mehr Schutz seiner Daten sorgen.

5. Ausarbeitung der Interviews

1. Deutsches Datenschutzrecht, speziell für Clouds, gut oder ausbaufähig? Ihre Meinung
2. Sind die Rechte der Nutzer zur Zeit ausreichend geschützt?
3. Was ist Ihre Empfehlung, wie ich meine Daten besser schützen kann?
4. Viele Leute wissen nicht wie man seine Daten richtig schützt, wie werden sie auf das Thema Datenschutz aufmerksam gemacht und wie wird es ihnen verständlich erklärt?
5. Wie kann ich herausfinden, wo es „sicher“ ist meine Daten abzulegen? Reicht es die AGB's zu lesen oder kann/muss ich mehr tun um meine Daten ausreichend geschützt zu wissen?
6. An wen wende ich mich, wenn Daten gestohlen wurden, bzw. gegen Datenschutzrecht verstoßen wird?
7. Sollte ich zur Sicherheit meine Daten vor dem Hochladen bei einem Cloudanbieter lieber noch einmal selbst verschlüsseln?
8. AGB's bzw. Datenschutzrichtlinien der Unternehmen lassen meiner Meinung nach viele Fragen offen, bzw. lassen sich die Unternehmen sozusagen eine „Hintertür“ offen um zum Beispiel meine Daten länger zu speichern als nötig, gerade nach dem Löschen. Ist das tatsächlich so?
9. Der Europäische Standort Irland, ist für Ausländische Unternehmen, gerade aus den USA nicht nur wegen den Steuerlichen Vergünstigungen attraktiv, sondern auch gerade wegen den schwachen Datenschutzgesetzen. Ist das wirklich so und was wird in Zukunft dagegen unternommen? Warum greift hier das europäische Datenschutzrecht nicht?
10. Wie gut ist das deutsche Datenschutzrecht, im Vergleich mit den USA, aber auch dem europäischen Datenschutzrecht? Ihre persönliche Meinung
11. Ist es sicherer meine Daten bei einem deutschen oder europäischen Cloudanbieter zu speichern?
12. Was sind die angestrebten oder tatsächlichen Ergebnisse der deutschen Cloudprojekte, Tclouds vom ULD, das mit 10,5 MIO € gefördert wurde und TrustedCloud vom BMWI das insgesamt sogar mit 100 MIO € gefördert wird? Haben nur Wirtschaft und Industrie etwas davon oder wird es eine „deutsche“Cloud auch für private Nutzer geben?
13. Sollte ich generell meine Daten lieber bei Deutschen Unternehmen lagern? Welche Deutschen Unternehmen gibt es und welche ausländischen entsprechen deutschen Datenschutzstandards?
14. Könnte es ein globales, einheitliches Datenschutzrecht geben und wäre dies sinnvoll und machbar? Ihre persönliche Meinung

Die Antworten der Interviewpartner, die Datenschutzbeauftragten der Technischen Universität und der Hochschule Kaiserslautern, Herr Hirsch und Herr Stemler, finden sich im Anhang dieser Studienarbeit.

6. Was ist am aktuellen Datenschutzrecht gut?

Jeder Nutzer hat laut den Regelungen im Datenschutz, Rechte. Wie das Auskunftsrecht, das besagt, dass ich mich jeder Zeit beim Anbieter über die Daten, die er von mir gesammelt hat, informieren kann. Das Recht auf Vergessen, ein sehr neues Gesetz, das dem Anbieter vorschreibt alle meine Daten, die ich dort eingestellt habe oder die er über mich gesammelt hat, unwiderruflich zu löschen. Diese Rechte, die ich als Nutzer habe, können nicht beschränkt werden und der Anbieter muss diese einhalten. Allerdings bedeutet dies nicht automatisch, dass sich die Unternehmen auch wirklich daran halten. Es ist für die Nutzer schwierig nachzuvollziehen, ob die Rechte tatsächlich eingehalten und umgesetzt werden.

Wenn man die Wahl hat, sollte man Anbieter aus Deutschland, oder Anbieter, bei denen die Daten nachvollziehbar auf Servern in Deutschland oder der Europäischen Union gespeichert werden, bevorzugen. Wie schon geschrieben, ist das deutsche Datenschutzgesetz ist eines der strengsten, wenn nicht sogar das strengste der Welt.

7. Was muss sich in Zukunft am Datenschutzrecht ändern?

Gerade bei kostenlosen Diensten sehen die beiden Datenschutzbeauftragten, mit denen ich die Interviews geführt habe, noch Ausbaubedarf. Generell sollte der Nutzer Herr über seine Daten sein, was gerade bei ausländischen Unternehmen, zum Beispiel in den USA, aber auch innerhalb der Europäischen Union nicht unbedingt gewährleistet ist. Hier besteht also noch Nachholbedarf.

Auch müssten die verschiedenen Dienste, die mit der Cloud angeboten werden, stärker im Datenschutz verankert werden. Wenn sich die Unternehmen an die Gesetzgebung halten sind meine Daten auch ausreichend geschützt. Doch bekomme ich darüber genug Informationen vom Anbieter? Dies sollte sich in Zukunft auch ändern.

Sinnvoll wäre es sicherlich, wie im nächsten Kapitel beschrieben, ein einheitliches Datenschutzgesetz, nicht für einzelne Staaten, sondern für das Internet selbst zu entwickeln. Dieser Meinung sind außer mir auch die Datenschutzbeauftragten der Technischen Universität und Fachhochschule Kaiserslautern, mit denen ich gesprochen habe.

Die Gesetzgebung ist immer ein bisschen langsamer als die Entwicklung neuer Technologien. Wenn also ein neues Gesetz für eine bestimmte datenschutzrechtliche Fragestellung erlassen wird kann man davon ausgehen, dass die Technologie schon weiter fortgeschritten und somit das Gesetz vielleicht schon nicht mehr aktuell ist.

Ein einheitliches Datenschutzrecht für Europa wäre auch sinnvoll. Geplant war dies schon, daraus geworden ist die europäische Datenschutzrichtlinie die zwar für alle Mitgliedsstaaten gilt, wobei aber trotzdem jedes Land eigene, unterschiedliche Standards eingeführt hat. Eine Schaffung und Anhebung des europäischen Datenschutzrechts auf deutsches Niveau wäre also sinnvoll.

Wie im vorigen Kapitel beschrieben, muss auch eine stärkere Kontrolle der Anbieter eingeführt werden, sodass sie sich auch wirklich an die Gesetze halten.

8. Einheitliches Datenschutzrecht, sinnvoll und machbar?

Da das Internet und somit auch die Cloud sich nicht auf einen Staat beschränkt, sondern global und grenzübergreifend ist, sollte es auch ein einheitliches Gesetz bzw. eine einheitliche Richtlinie für den Datenschutz geben. Dieser Meinung sind auch die Datenschutzbeauftragten, mit denen ich das Interview geführt habe. Allerdings geben Sie zu bedenken, dass es dann überall die gleiche Messlatte für den Datenschutz geben müsste und sich auch jeder daran halten müsse. Das würde aber nicht reichen, wenn sich in der Europäischen Union alle, US Amerikanische Unternehmen aber nicht daran halten.

Das beste Beispiel dafür, dass ein einheitliches Datenschutzrecht noch in ferner Zukunft liegt, bietet die Europäische Union. Schon hier hat ein einheitliches Datenschutzrecht nicht funktioniert und es wurde nur eine Richtlinie daraus. Deswegen haben nicht alle Mitgliedsstaaten den selben Standard an Datenschutz dadurch erreicht.

Von nichtstaatlichen Organisationen gibt es allerdings gerade Überlegungen, einheitliche Richtlinien festzulegen, die dann aber eher als Verhaltensregeln und nicht als Gesetze zu verstehen sind.[14] An diese Richtlinien werden sich aber wohl die wenigsten halten.

Und auch die Europäische Union denkt wieder darüber nach, doch ein einheitliches Datenschutzrecht für alle Mitgliedsstaaten einzuführen. Dies könnte allerdings zur Folge haben, dass gerade in Deutschland, wo wir einen sehr hohen Standard haben, dieser Standard gesenkt und den anderen angepasst wird. Zu hohe Datenschutzstandards bedeuten unter anderem auch, dass ein europäischer Mitgliedsstaat nicht mehr Interessant für ein Amerikanisches Unternehmen ist. Dem Zufolge wird es wohl nicht so weit kommen, dass das europäische Datenschutzgesetz, welches es dann geben soll, sich deutschen Standards anpasst, sondern umgekehrt.

14 *[t3n Magazin 17.11.2014]*

9. Zusammenfassung

Datenschutz ist aus juristischer Sicht ein sehr komplexes Thema, weshalb wahrscheinlich die meisten Menschen davor zurückschrecken sich intensiv damit auseinander zu setzen. Meist werden Argumente wie 'ich habe ja nichts zu verbergen' vorgebracht, um sich nicht mit dem Thema auseinandersetzen zu müssen. Da alle meine persönlichen Daten gesammelt, gespeichert und benutzt werden und das aus manchmal zweifelhaften Gründen, kann dies nicht der richtige Weg sein.

Jeder sollte sich also mehr mit dem Thema auseinandersetzen, denn schließlich geht es um den Schutz unserer Daten, Informatiker, die für die Einhaltung des Datenschutzes mitverantwortlich sind, aber auch jeden der Dienste wie zum Beispiel Google, Dropbox, Facebook, und so weiter, nutzt.

Das Datenschutzgesetz ist von Land zu Land und von Unternehmen zu Unternehmen unterschiedlich. Selbst in der Europäischen Union hat jeder Mitgliedsstaat ein anderes Datenschutzgesetz. Nicht zuletzt dadurch, sondern auch durch den Umstand, dass die Unternehmen nicht offen legen in welchem Land die Daten der Benutzer abgelegt sind, ist es meist schwer zu bestimmen welches Datenschutzrecht bei Verlust der Daten tatsächlich greift.

In Deutschland haben wir ein sehr starkes Datenschutzgesetz, eines der stärksten, wenn nicht sogar das stärkste der Welt, weshalb es sinnvoll ist deutsche Anbieter gegenüber Anbietern aus dem Ausland zu bevorzugen. Denn solange die Verschlüsselung im Internet, wie in der Einleitung geschrieben, noch nicht abgeschafft ist, sind die Daten innerhalb Deutschlands sehr sicher aufgehoben. Natürlich sollte trotzdem darauf geachtet werden, dass die Daten ordnungsgemäß und vor allem vor dem Hochladen beim Anbieter verschlüsselt werden. Sichere verschlüsselte Kommunikation während des Hochladens ist dabei allerdings genauso wichtig. Auch mit seinen persönlichen Daten, wie Geburtstag, Name, Adresse, und so weiter, sollte man vorsichtig und sparsam umgehen. Generell ist es sinnvoll bei Dropbox und co., Pseudonyme zu verwenden.

Im Moment, gerade durch die Anschläge in Paris, ist das Thema Datenschutz wieder stark diskutiert. Es wurde von einigen Politikern im In- und Ausland sogar gefordert die Verschlüsselung im Internet aufzuheben und zu verbieten, was meiner Meinung nach gegen Terrorismus nicht wirklich etwas bringt.[15] Außerdem hilft die Abschaffung von Verschlüsselung höchst wahrscheinlich mehr den Hackern und anderen, die nichts Gutes mit unseren Daten im Sinn haben, als dass es tatsächlich etwas gegen den Terror bewirken kann. Ich denke nicht, dass Terroristen über Whatsapp, Facebook und co. kommunizieren und sie werden ihre Pläne auch kaum über Clouddienste miteinander teilen. So dient die Überwachung und die Beschneidung des Datenschutzes nur dem Ziel der vermeintlichen Sicherheit und schränkt dabei unsere Freiheit und Anonymität im Internet mehr und mehr ein, wie eingangs mit dem Zitat von Benjamin Franklin unterstrichen.

Jeder sollte sich mit dem Thema Datenschutz auseinandersetzen und sich selbst fragen, ob er Dienste, die eindeutig gegen Datenschutzstandards oder das eigene Verständnis von Datenschutz verstoßen, boykottiert oder sogar für seine Rechte auf die Straße geht.

15 *[c't 4/15 erschienen am 23.01.2015]*

10. Fazit

Mein Fazit zum Thema Datenschutz in der Cloud beziehungsweise auch allgemein zum Datenschutz, muss ich in drei Teile aufteilen. Jeder Teil passt zu einer Phase meiner Studienarbeit und spiegelt somit auch meinen Kenntnisstand bis zu diesem Zeitpunkt wieder.

1. Datenschutz ist ein wichtiges Thema, wir sollten uns alle mehr damit auseinandersetzen.

Zu Beginn meiner Studienarbeit war ich noch der Meinung, dass sich jeder zumindest ein wenig mit dem Thema auseinandersetzen sollte. Jeder sollte wissen wovon die Rede ist und was Änderungen an den Datenschutzrichtlinien von Unternehmen oder Staaten bedeuten. Viele denken, sie wären durch einen Artikel in einer Zeitschrift, Zeitung oder ähnlichem ausreichend über das Thema informiert. Dem ist aber nicht so. Es ist immer noch so, dass man gerade beim Datenschutz viel Eigeninitiative erbringen muss.

2. Datenschutz bringt nur etwas, wenn sich alle daran halten. Was kann ich selbst für mehr Datenschutz tun?

Das ist wohl das größte Problem an der ganzen Sache, dass sich daran gehalten wird. Wie kann es zum Beispiel sein, dass wir in Deutschland eines der stärksten Datenschutzgesetze haben, Facebook aber gerade erst seine Datenschutzrichtlinien geändert hat und diese nicht wirklich mit unserem Datenschutzgesetz konform sind? Dazu fällt mir nur der Spruch 'Geld regiert die Welt' ein. Diese Änderung wurde zwar im Bundestag diskutiert, doch diskutieren bringt, denke ich, bei so etwas nicht viel.

3. Was nützt uns der Datenschutz in Zukunft noch, beziehungsweise wird er vielleicht sogar bald zugunsten einer vermeintlichen Sicherheit ganz abgeschafft?

Was nützt uns also der ganze Datenschutz überhaupt, wenn die Unternehmen ihre eigenen Datenschutzrichtlinien haben und sich überall Hintertüren offen lassen, so wie es auch Dropbox macht? Je mehr aktuelle Entwicklungen und Nachrichten ich zu diesem Thema kurz vor Ende meiner Studienarbeit lese, desto mehr drängt sich mir sogar der Gedanke auf, dass der Datenschutz mehr und mehr zu Gunsten vermeintlicher Sicherheit aufgegeben wird und wir am Ende, beides verlieren werden. Ich hoffe, dass sich mehr Menschen mit dem Thema auseinander setzen und erkennen, dass jeder einzelne die Verantwortung hat dieses Thema ernst zu nehmen und sich für mehr Datenschutz stark zu machen, sei es durch Verschlüsselung, etc. oder in dem man zum Beispiel wirklich auch einmal dagegen demonstriert. Ich für meinen Teil werde in Zukunft mehr auf Anonymität im Internet und die Verschlüsselung meiner Daten, gerade auch in der Cloud, achten. Als Informatiker werde ich auch versuchen auf dieses Thema aufmerksam zu machen und darüber aufklären.

Abschließend möchte ich noch sagen, dass ich es, auch wenn ich in der Studienarbeit doch etwas kritisch dem Thema gegenüber geworden bin, für wichtig halte, dass gerade wir Informatiker uns mit dem Thema auseinandersetzen. Denn wir sind die treibende Kraft wenn es um Datenschutz in der digitalen Welt geht und in unserer Verantwortung und Macht liegt es den Datenschutz für die Nutzer der Software, die wir entwickeln, zu gewährleisten.

11. Literaturverzeichnis

[Franklin, B., and A. Wagner., 1818] Dr. Benjamin Franklin's Nachgelassene Schriften Und Correspondenz: Nebst Seinem Leben. Dr. Benjamin Franklin's Leben : Th. 1., Bd. 3. Landes-Industrie-Comptoir. http://books.google.de/books?id=yeJOAAAAcAAJ.

[Witt, Bernhard C., 2010], Datenschutz kompakt und verständlich: eine praxisorientierte Einführung ; [mit Online-Service]. Vieweg + Teubner, Wiesbaden. ISBN: 978-3834812254

[Patrick Hoerster, Dirk Fox (Hrsg.), 1999] Datenschutz und Datensicherheit: Konzepte, Realisierungen, rechtliche Aspekte, Anwendungen. Braunschweig: Vieweg. ISBN: 3-528-05714-9

[Freie Universität Berlin, 2011], Richtlinie zur Auslagerung von Daten in die Cloud, http://www.mi.fu-berlin.de/wiki/pub/IT/ItProcess/Richtlinie_Cloud-Datenablage_-_1_0.pdf, Zugriff: 17.12.2014

[Datenschutzbeauftragter Rheinland Pfalz, 2014], Datenschutzbericht https://www.datenschutz.rlp.de/downloads/tb/ds_tb24.pdf Zugriff: 01.02.2015

[t3n Magazin 15.11.2014] http://t3n.de/news/google-facebook-twitter-dublin-578339/ Zugriff: 01.02.2015

[export.gov safeharbour] http://export.gov/safeharbor/ Zugriff: 01.02.2015

[Arbeitskreise Technik und Medien der Konferenz der Datenschutzbeauftragten des Bundes und der Länder sowie der Arbeitsgruppe Internationaler Datenverkehr des Düsseldorfer Kreises, Stand: 09.10.2014] Orientierungshilfe – Cloud Computing https://www.datenschutz.rlp.de/downloads/oh/ak_oh_cloudcomputing.pdf Zugriff: 16.01.2015

[t3n Magazin 17.11.2014] http://t3n.de/news/internet-architecture-board-iab-datenschutz-579286/ Zugriff: 01.02.2015

[c't 4/15 erschienen am 23.01.2015] http://www.heise.de/ct/ausgabe/2015-4-Editorial-Nutzlose-Ueberwachung-2520964.html Zugriff: 01.02.2015

http://www.golem.de/news/crypto-wars-2-0-de-maizi-re-und-eu-wollen-recht-auf-entschluesselung-1501-111841.html Zugriff: 01.02.2015
Und dazu auch:
http://www.heise.de/newsticker/meldung/Auch-de-Maiziere-wendet-sich-gegen-Verschluesselung-2523297.html Zugriff: 01.02.2015

[t3n Magazin 02.02.2015] http://t3n.de/news/datenschutz-daten-privacy-591169/?utm_content=buffer86cf2&utm_medium=social&utm_source=facebook.com&utm_campaign=buffer Zugriff: 02.02.2015

[t3n Magazin 03.02.2015] http://t3n.de/news/edward-snowden-tipps-tools-privacy-591562/?utm_content=buffer8e7c8&utm_medium=social&utm_source=facebook.com&utm_campaign=buffer Zugriff: 03.02.2015

12. Anhang

Ehrenwörtliche Erklärung zur Studienarbeit

Auf den nächsten 7 Seiten finden sich die Abschriften der Interviews mit dem Datenschutzbeauftragten der Fachhochschule Kaiserslautern, Standort Kaiserslautern, Herrn Hirsch und der Technischen Universität Kaiserslautern, Herrn Stemler.

Ehrenwörtliche Erklärung

Hiermit erkläre ich, Kiefer Raphael, geboren am 11.04.1988 in Dahn, ehrenwörtlich, dass ich meine Studienarbeit mit dem Titel:

„Datenschutzrecht in der Cloud, in Deutschland, der EU und den USA. Eine für Laien verständliche juristische Gegenüberstellung.“

selbstständig und ohne fremde Hilfe angefertigt und keine anderen als in der Abhandlung angegebenen Hilfen benutzt habe.

Die Übernahme wörtlicher Zitate aus der Literatur sowie die Verwendung der Gedanken anderer Autoren an den entsprechenden Stellen habe ich innerhalb der Arbeit gekennzeichnet.

Ich bin mir bewusst, dass eine falsche Erklärung rechtliche Folgen haben kann.

Zweibrücken, 02.02.15 Raphael Kiefer

Interview mit einem Datenschutzbeauftragten zum Thema:

Datenschutzrecht in der Cloud, in Deutschland, der EU und den USA. Eine für Laien verständliche, juristische Gegenüberstellung.

Interviewpartner: _____Herr Hirsch___ Datum: ___19.11.2014____

1. Deutsches Datenschutzrecht, speziell für Clouds, gut oder ausbaufähig? Ihre Meinung

Da die Dienste des Cloudcomputing immer umfangreicher werden müsste man diese als Problemstellung aufnehmen. Wenn man aber die Auftragsdatenverarbeitung so umsetzt wie der Gesetzgeber das gerne hätte, sind die Daten ausreichend geschützt. Bekomme ich darüber aber genug Informationen vom Anbieter?

2. Sind die Rechte der Nutzer zur Zeit ausreichend geschützt?

Nutzer haben im Datenschutz Rechte, wie das Auskunftsrecht, Recht auf Löschung, Recht auf Sperrung. Diese können nicht beschränkt werden und müssen eingehalten werden. Das heißt aber nicht, dass sich die Firmen auch wirklich daran halten. Es ist schwierig nachzuvollziehen ob die Rechte tatsächlich eingehalten und umgesetzt werden.

3. Was ist Ihre Empfehlung, wie ich meine Daten besser schützen kann?

Pseudonyme verwenden, Daten verschlüsseln, extra Datensicherungen machen.

4. Viele Leute wissen nicht wie man seine Daten richtig schützt, wie werden sie auf das Thema Datenschutz aufmerksam gemacht und wie wird es ihnen verständlich erklärt?

Schulungsveranstaltungen in Unternehmen informieren. Problem: Themen in der Öffentlichkeit aufgegriffen, danach hat jeder das Gefühl ausreichend informiert zu sein.

5. Wie kann ich herausfinden, wo es „sicher“ ist meine Daten abzulegen? Reicht es die AGB's zu lesen oder kann/muss ich mehr tun um meine Daten ausreichend geschützt zu wissen?

Große Anbieter haben ihre eigenen Richtlinien, ich muss entscheiden ob ich mich dem beuge, oder ob ich mir einen „sichereren“ Anbieter suchen. Die wichtigste Frage entsteht beim Gruppenzwang, ist es mir wichtiger, dass alle meine Freunde den Dienst nutzen, kann ich sie vielleicht überzeugen, oder ist mir Sicherheit und Einhaltung meiner Datenschutzrechte wichtiger?

6. An wen wende ich mich, wenn Daten gestohlen wurden, bzw. gegen Datenschutzrecht verstoßen wird?

An die verantwortliche Stelle wenden, als Bürger aber auch immer an den Landesdatenschutzbeauftragten, wobei man dort Wartezeiten in Kauf nehmen muss.

7. Sollte ich zur Sicherheit meine Daten vor dem Hochladen bei einem Cloudanbieter lieber noch einmal selbst verschlüsseln?

Verschlüsselung sehr wichtig, mit gewisser Routine nicht mehr so aufwändig.

8. AGB's bzw. Datenschutzrichtlinien der Unternehmen lassen meiner Meinung nach viele Fragen offen, bzw. lassen sich die Unternehmen sozusagen eine „Hintertür“ offen um z.B. meine Daten länger zu speichern als nötig, gerade nach dem Löschen. Ist das tatsächlich so?

Hintertüren in den AGB's und Datenschutzrichtlinien gibt es. Aus EU Richtlinie leiten sich die Datenschutzrechte der Länder ab. Deutsches Datenschutzrecht ist sehr hart, es gibt in der EU auch schwächere.

9. Der Europäische Standort Irland, ist für Ausländische Unternehmen, gerade aus den USA nicht nur wegen den Steuerlichen Vergünstigungen attraktiv, sondern auch gerade wegen den schwachen Datenschutzgesetzen. Ist das wirklich so und was wird in Zukunft dagegen unternommen? Warum greift hier das europäische Datenschutzrecht nicht?

Europäisches Recht greift nur, wenn auch die Server auf der meine Daten liegen, in der EU stehen. Was aber unter Umständen nicht nachvollziehbar ist → wenn zugesichert wird das die Daten in der EU bleiben, kann ich mich dann darauf auch verlassen? Anbieter lassen sich nicht bzw. ungern in die Karten schauen.

10. Wie gut ist das deutsche Datenschutzrecht, im Vergleich mit den USA, aber auch dem europäischen Datenschutzrecht? Ihre persönliche Meinung

Das Niveau des Deutschen Datenschutzrechts ist höher als US Recht, auch im Europäischen Vergleich ist es höher. Mit den USA gibt es die Safe Harbour Verträge, die aber durch den Patriotact aufgeweicht sind.

11. Ist es sicherer meine Daten bei einem deutschen oder europäischen Cloudanbieter zu speichern?

Deutscher Cloudanbieter gut, Europäische teilweise ca. gleichauf oder drunter aber auch ok, danach USA. Deutsche Cloudanbieter wären eigentlich zu bevorzugen. Die wichtigste Frage ist, welche Daten möchte ich hochladen. Recht auf Löschen, was nicht unbedingt wie gewünscht funktioniert.

12. Sollte ich generell meine Daten lieber bei Deutschen Unternehmen lagern? Welche Deutschen Unternehmen gibt es und welche ausländischen entsprechen Deutschen Datenschutzstandards?

Deutsche Unternehmen sind zu bevorzugen, da ihre eigenen Datenschutzrichtlinien eher mit dem deutschen Datenschutzrecht konform sind als dies bei ausländischen Anbietern der Fall ist.

13. Könnte es ein globales, einheitliches Datenschutzrecht geben und wäre dies sinnvoll und machbar? Ihre persönliche Meinung

Überall gleiche Messlatte, alle müssen sich daran halten, würde aber in der EU nicht reichen, wenn z.B. US Unternehmen sich nicht daran halten. Einheitliches Datenschutzrecht wäre wünschenswert, hat aber schon Europaweit nicht geklappt, es gibt zwar die Richtlinie, aber trotzdem ist es bei jedem Staat unterschiedlich. Man müsste eigentlich wie der Sinn der Cloud auch global denken.

14. Welches Datenschutzrecht greift wenn ich meine Daten im Ausland ablege?

In Europa mit Sitz in Irland, würde Irisches recht gelten. Sitz des Anbieters gilt generell. Es kann aber nicht nachvollzogen werden wo meine Daten liegen, womit sich die Anbieter gewisse Freiheiten einräumen und dadurch nicht klar ist welches Datenschutzrecht greift.

Interview mit einem Datenschutzbeauftragten zum Thema:

Datenschutzrecht in der Cloud, in Deutschland, der EU und den USA. Eine für Laien verständliche, juristische Gegenüberstellung.

Interviewpartner: _____Herr Stemler____ Datum: ___19.11.2014____

1. Deutsches Datenschutzrecht, speziell für Clouds, gut oder ausbaufähig? Ihre Meinung

Für den Geltungsbereich Deutschland ist das Datenschutzrecht gut, Probleme treten im Ausland auf, da z.B. nicht alle EU Mitgliedsstaaten das gleiche Datenschutzrecht haben, wobei die EU Datenschutzrichtlinien für alle EU Mitgliedsstaaten gelten. Ausbaufähig ist es auf jeden Fall noch, gerade bei kostenlosen Diensten ist Ausbaubedarf. Generell sollte der Nutzer Herr über seine Daten sein, was gerade bei Ausländischen Unternehmen, z.B. in den USA oder auch bei anderen EU Mitgliedsstaaten nicht unbedingt gewährleistet ist.

2. Sind die Rechte der Nutzer zur Zeit ausreichend geschützt?

Antwort wie Frage eins, mit der Ergänzung, dass man Anbieter aus Deutschland bevorzugen sollte, wobei auch Anbieter bei denen nachvollziehbar in der EU oder Deutschland gehostet wird ok sind

3. Was ist Ihre Empfehlung, wie ich meine Daten besser schützen kann?

Generell ist immer ein gewisses Risiko beim Ablegen Persönlicher, Personenbezogener und vor allem sensibler Daten im Internet nicht vermeidbar, das ist allerdings Anbieter abhängig, AGB's und Datenschutzrichtlinien des Anbieters lesen! Am besten schützt man seine Daten natürlich wenn man sie garnicht erst in der Cloud speichert und wenn, dann sollte man sie entweder selbst vorher verschlüsseln oder darauf achten, das der Cloudanbieter die Daten vor dem Hochladen in seine Cloud auf dem PC des Nutzers verschlüsselt.

4. Viele Leute wissen nicht wie man seine Daten richtig schützt, wie werden sie auf das Thema Datenschutz aufmerksam gemacht und wie wird es ihnen verständlich erklärt?

Die Aufklärung über den Datenschutz stellt immer noch ein Problem dar, wie soll man es den Menschen näher bringen? Was gerade an der Einstellung der meisten Nutzer scheitert, „ich habe ja nichts zu verbergen“. Dieses Desinteresse resultiert aus einer Machtlosigkeit der Nutzer, die gerade dadurch zustande kommt, dass die meisten mit den Datenschutzbestimmungen und Paragraphen überfordert sind und sich deshalb nicht mit dem Thema auseinandersetzen wollen. Studierende und Mitarbeiter in Unternehmen, werden z.B. durch Veranstaltungen und Schulungen für das Thema sensibilisiert. Allerdings ist bei der Aufklärung natürlich auch Interesse und Eigeninitiative wichtig. Am besten ist eine Sensibilisierung für den Datenschutz schon bei der Ausbildung am Gerät, also in der Schule, wofür es z.B. vom Landesdatenschutzbeauftragten auch schon Programme gibt.

5. Wie kann ich herausfinden, wo es „sicher“ ist meine Daten abzulegen? Reicht es die AGB's zu lesen oder kann/muss ich mehr tun um meine Daten ausreichend geschützt zu wissen?

Hier ist Eigeninitiative gefragt, man muss natürlich auch die verschiedenen Anbieter, ihre AGB's und Datenschutzrichtlinien vergleichen.

6. An wen wende ich mich, wenn Daten gestohlen wurden, bzw. gegen Datenschutzrecht verstoßen wird?

An den Anbieter der Cloud, aber auch Aufsichtsbehörden aber nur im Deutschen und Europäischen Raum möglich. Für Unternehmen → Bundesdatenschutzrecht für Behörden → Landesdatenschutzrecht

7. Sollte ich zur Sicherheit meine Daten vor dem Hochladen bei einem Cloudanbieter lieber noch einmal selbst verschlüsseln?

Auf jeden Fall, immer vorher verschlüsseln, außer der Anbieter bietet selbst eine solche Lösung an. Verschlüsselung nach dem Hochladen bringt nichts! Vorsicht, verschlüsselte Übertragung zum Anbieter z.B. über HTTPS ist nicht gleich Verschlüsselung auf dem Rechner, aber es ist beides gleich wichtig.

8. AGB's bzw. Datenschutzrichtlinien der Unternehmen lassen meiner Meinung nach viele Fragen offen, bzw. lassen sich die Unternehmen sozusagen eine „Hintertür“ offen um z.B. meine Daten länger zu speichern als nötig, gerade nach dem Löschen. Ist das tatsächlich so?

AGB's sind meist nicht durchsichtig, Anbieter mit „nichtssagenden“ AGB's sollten nicht bevorzugt werden. In Deutschland gilt mittlerweile das Recht auf vergessen.

9. Der Europäische Standort Irland, ist für Ausländische Unternehmen, gerade aus den USA nicht nur wegen den Steuerlichen Vergünstigungen attraktiv, sondern auch gerade wegen den schwachen Datenschutzgesetzen. Ist das wirklich so und was wird in Zukunft dagegen unternommen? Warum greift hier das europäische Datenschutzrecht nicht?

Die EU Datenschutzrichtlinie ist noch von 1995 und lässt Spielräume für die Länder offen. Wichtig ist, dass die zuständigen Behörden für den Datenschutz unabhängig arbeiten, was nicht in allen Ländern so ist. Generell kann man das EU Datenschutzrecht nicht direkt mit dem Deutschen vergleichen, eher muss man es sich wie in der Informatik die Vererbung vorstellen. Die EU Datenschutzrichtlinien gelten für alle EU Mitgliedsstaaten, allerdings hat jedes Land die Freiheit es im Datenschutzrecht noch weiter auszubauen.

10. Wie gut ist das deutsche Datenschutzrecht, im Vergleich mit den USA, aber auch dem europäischen Datenschutzrecht? Ihre persönliche Meinung

Die Basis für das deutsche Datenschutzrecht ist wie für alle EU Mitgliedsstaaten die EU Richtlinie, allerdings ist das Deutsche Datenschutzrecht strenger, sogar das strengste in der EU. Wohingegen es in den USA scheinbar kein wirkliches Datenschutzrecht wie bei uns gibt. Es gibt lediglich z.B. das Safe Harbour Abkommen, das allerdings durch die NSA Affäre mehr oder weniger hinfällig geworden sein dürfte.

11. Ist es sicherer meine Daten bei einem deutschen oder europäischen Cloudanbieter zu speichern?

Durch den starken Datenschutz in Deutschland ist es besser seine Daten im Inland zu speichern. Es kommt aber natürlich auch auf die Art der Daten an. Wenn mir egal ist, dass der Cloudanbieter z.B. weiß was mein Musikgeschmack ist, weil ich meine Musiksammlung dort hochlade, ist es ok. Mit Personenbezogenen Daten sollte man allerdings vorsichtiger umgehen. Man sollte z.B. für die Anmeldung Pseudonyme verwenden.

12. Was sind die angestrebten oder tatsächlichen Ergebnisse der deutschen Cloudprojekte, Tclouds vom ULD, das mit 10,5 MIO € gefördert wurde und TrustedCloud vom BMWI das insgesamt sogar mit 100 MIO € gefördert wird? Haben nur Wirtschaft und Industrie etwas davon oder wird es eine „deutsche“Cloud auch für private Nutzer geben?

Dabei handelt es sich wohl eher um Forschungsprojekte für die Industrie. Diese Projekte sind eher als Lösungsvorschläge zu sehen und werden wohl eher keine Dienste für „normale“ Nutzer hervorbringen. Der Staat hängt mit Gesetzgebung und eigenen Projekten/Forschung immer hinter der Industrie her.

13. Sollte ich generell meine Daten lieber bei Deutschen Unternehmen lagern? Welche Deutschen Unternehmen gibt es und welche ausländischen entsprechen Deutschen Datenschutzstandards?

Es gibt z.B. mittlerweile eigene Clouds für Hochschulen, von Hochschulen. Siehe www.dfn.de

14. Könnte es ein globales, einheitliches Datenschutzrecht geben und wäre dies sinnvoll und machbar? Ihre persönliche Meinung

Es gibt von nichtstaatlichen Organisationen wohl gerade Überlegungen darüber einheitliche Richtlinien festzulegen, die dann aber nur als Verhaltensregeln zu verstehen sind. Es wird wohl kein Internationales Recht geben, schön wäre es aber, gerade weil das Internet grenzübergreifend ist.

Vor 40 Jahren war das Datenschutzgesetz in RLP erst das 3. weltweit.