Wem gehören die Daten?

Ich möchte in diesem Vortrag der Frage „Wem gehören die Daten?“ einmal aus Hacker-sicht nachgehen. Da stellt sich für Sie natürlich zuerst die Frage, über welche Art von *Hacker*[1] ich hier eigentlich rede, denn es gibt verschiedene Spezies:

Hacker-Spezies

Hacker unterscheiden sich dabei nicht so sehr in dem *was* sie tun, sondern mehr im *wie* und *warum* sie es tun.

Als erstes hätten wir den „black hat“, der so etwas wie die dunkle Seite der Macht repräsentiert. Es sind in der Regel von kriminellen Motiven getriebene Hacker, die ihr Wissen auf dem schwarzen Markt verkaufen oder – was seltener vorkommt – auch selbst ausnutzen, um sich zu bereichern. Auf jedem Fall teilen sie ihr Wissen nicht mit jedermann.

Interessanterweise gibt es eine Hacker-Konferenz gleichen Namens, nämlich die „Black Hat“. Die Veranstaltung wird seit 1997 in den USA, heute auch in Europa, Asien und im Vorderen Orient durchgeführt. Sie ist die Schwesterveranstaltung der DEFCON, einem anderen Hacker-Event in den USA. Das der Name „Black Hat“ wohl ironischerweise gewählt wurde und das die Veranstaltung heute zu den etablierten *Security Events* gehört, zeigt schon die Tatsache, dass Jeff Moss – der Initiator der „Black Hat“ und der „DEFCON“ – mittlerweile im Beraterstab des DHS (Departement of Homeland Security) sitzt und Sicherheitsverantwortlicher[2] bei der ICANN ist.

Die zweite Spezies der Hacker sind die „white hats“ - die Harmlosen. Sie arbeiten in der Regel für Sicherheitsfirmen und verdienen ihr Geld unter anderem durch Testen der IT-Infrastruktur (Penetrationstests) – „Hacken als Job“ sozusagen.

Die Aufteilung in „black hats“ und „white hats“ kommt übrigens aus den Westernfilmen des

1 http://de.wikipedia.org/wiki/Hacker

2 http://www.heise.de/newsticker/meldung/Sicherheitsfachmann-wird-ICANN-Vizepraesident-1235249.html

frühen letzten Jahrhunderts: Die Bösen trugen immer schwarze Hüte, die Gutem immer weisse Hüte – damit man sie besser auseinander halten kann...

Die dritte und letzte Spezies sind die „gray hats“, die als politische Hacktivisten agieren. Sie sind nicht kommerziell interessiert und lehnen Auftrags-Hacks ab. Statt dessen verwenden sie ihr Wissen, um auch politische Ziele zu erreichen oder um das Bewusstsein der breiteren Öffentlichkeit für bestimmte (Fehl-)Entwicklungen in der digitalen Welt wie Internetzensur oder Vorratsdatenspeicherung zu wecken. Ihr Handeln wird durch selbst-definierte ethische Grundsätze bestimmt.

Hackerethik

Dass es so etwas wie eine *Hackerethik* gibt, in der Hacker ihre Vorstellung von „gut“ und „böse“ in der digitalen Welt festgeschrieben haben, verwundert Leute immer wieder – vor allem diejenigen, die nicht wissen, dass es vom Chaos Computer Club auch eine *Hackerbibel* [3] gibt. Der erste Band – sozusagen das „alte Testament“ – erschien 1985[4], drei Jahre später erschien dann die Fortsetzung als „neues Testament“.[5] Die Druckausgaben sind mittlerweile (fast) komplett vergriffen; allerdings gibt es unter „http://www.offiziere.ch/trust-us“ die digitalisierten Bände zum Online-Lesen – ganz für umsonst.

Die Hackerethik des CCC basiert auf den Grundsätzen, die Steven Levy 1984 in seinem Buch „Hackers: Heroes of a Computer Revolution“[6] zusammen gestellt hat:

- **Der Zugang zu Computern und allem, was einem zeigen kann, wie diese Welt funktioniert, sollte unbegrenzt und vollständig sein.**

  Wer sich bei diesem Satz ein bisschen an Wikipedia erinnert fühlt, hat nicht ganz Unrecht – WP ist ein in diesem Sinne ein Werkzeug, freies Wissen zu sammeln, zu bewerten, zu redigieren und für alle kostenlos zugänglich zu publizieren. Damit

3 http://de.wikipedia.org/wiki/Hackerbibel
4 Die Hackerbibel – „Kabelsalat ist gesund“, Herausgeber: Werner Pieper, Grüner Zweig 98, Grüne Kraft, ISBN 3922708986
5 Die Hackerbibel – „Das neue Testament“, Herausgeber: Werner Pieper, Grüner Zweig 124, Grüne Kraft, ISBN 3925817247
6 Steven Levy: „Hackers: Heroes of the Computer Revolution“, Anchor Press/Doubleday, ISBN 0385191952

steht WP auch in der Tradition eines Diderot und d'Alembert, die um 1750 die erste echte Enzyklopädie editierten und druckten – und so, wie Wikipedia die zugrunde liegende MediaWiki-Software unter einer OpenSource-Lizenz gestellt hat, beginnt die Enzyklopädie von Diderot und d'Alembert mit einer Anleitung zum Bau einer Druckmaschine, mit der das Werk dupliziert werden kann. Copyright in unserem heutigen restriktiven Sinne war damals noch unbekannt: statt dessen war Wissen eine digitale Allmende – ganz im Sinne der Aufklärung.

Kurze historische Randnotiz: Die Enzyklopädie von Diderot und d'Alembert war kaum gedruckt, da stand sie auch schon auf dem *Index der verbotenen Bücher* des Vatikans, oder genauer gesagt der *Inquisition*. Dieses päpstliche Wissens-Verbot war sozusagen das mittelalterliche Äquivalent einer Websperre – und genauso effektiv. Das heute einige Staaten versuchen, aus den gleichen Motiven den Zugang zu Wikipedia zu verbieten und zu filtern, kann glücklicherweise nicht auf Dauer von Erfolg gekrönt sein.

- **Alle Informationen müssen frei sein.**

  Eigentlich heisst der ganze Abschnitt bei Stewart Brand: „Information möchte frei sein. Information möchte aber auch wertvoll sein. Information will frei sein, weil es billig ist, sie zu verteilen, zu kopieren und wieder zu verwenden – zu billig, um überhaupt noch in Geld gemessen werden zu können. Auf der anderen Seite möchte Information wertvoll sein, weil sie einen unermesslich grossen Wert für ihren Empfänger haben kann. Und diese Spannung wird nicht vergehen...“

  Mit diesem Thema sind wir wieder mitten drin in der Copyright- und Patent-Problematik – oder anderes ausgedrückt: bei der Sinnhaftigkeit des Eigentums-begriffes bei immateriellen Gütern überhaupt. Dass Hacker diesbezüglich ihre eigene Weltanschauung haben, dürfte jedem klar sein, der schon mal von „OpenSource“ und „Creative Commons“ gehört hat.

Die Konnotationen, die sich auch unter dem Stichwort „Informationsfreiheit“ finden, werde ich im letzten Punkt der Hackerethik noch mal ansprechen.

- **Mißtraue Autoritäten - fördere Dezentralisierung**

  Das gilt natürlich auch für die eigene Autorität – und deshalb hat sich die deutsche Hackerbewegung selbst getreu dieses Mottos „dezentralisiert“. Neben den CCC-Hochburgen Hamburg und Berln gibt es mittlerweile in vielen Orten in Deutschland und der umliegenden Länder Erfa-Kreise (Erfahrungsaustausch-Kreise) und Chaostreffs – und jede Menge Hackerspaces, in denen Hacker und kompatible Zeitgenossen sich auch direkt treffen und zusammen arbeiten, spielen und diskutieren können.

- **Beurteile einen Hacker nach dem, was er tut und nicht nach üblichen Kriterien wie Aussehen, Alter, Rasse, Geschlecht oder gesellschaftlicher Stellung**

- **Man kann mit einem Computer Kunst und Schönheit schaffen**

  Besuchern des Chaos Communication Congresses (zwischen Weihnachten und Neujahr in Berlin) oder des Chaos Communication Camps (alle vier Jahre, dieses Jahr wieder im August) ist schon aufgefallen, dass es immer eine Abteilung „Art & Beauty“ gibt – Hacker sind durchaus keine Kulturbanausen, vor allem nicht, wenn es um digitale Kunst in allen Formen geht.

  Bekannter geworden ist auch das Projekt „Blinkenlights“ mit Installationen in Deutschland, Frankreich und Kanada.

- **Computer können dein Leben zum Besseren verändern**

- ***Mülle nicht in den Daten anderer Leute***

  Dieser Punkt ist noch ein Überbleibsel der Netikette aus der Frühzeit der Vernetzung und des CCC – als es noch kein Internet gab und das Surfen in Hackerkreisen unter dem Namen „Datenreisen“ bekannt war (die „Datenschleuder“, die gedruckte

Magazin des CCC, heisst heute noch im Untertitel „Wissenschaftliches Fachblatt für Datenreisende“). Man empfand noch Respekt für die Personen auf der anderen Seite des Modemkabels und es galt eben bei Zugriff auf fremde Daten der Grundsatz: „Nur angucken, nicht anfassen.“

- ***Öffentliche Daten nützen, private Daten schützen***

  Dieser CCC-spezifische Zusatz zu den Punkten der Levy'schen Hackerethik ist einer der wesentlichen Eckpfeiler des politischen Engagements der Hacker in Deutschland. Er spricht zwei grundsätzliche Herzensangelegenheiten der Hacker-gemeinde an:

  - **Informationelle Selbstbestimmung**
  - **Informationsfreiheit**

  Diese Punkte waren auch die Grundlage, auf der sich 1992 Leute im Netz zur einer Gruppe namens *Cypherpunks*[7] zusammen gefunden haben – Cyberpunks mit speziellem Interesse an Kryptographie. In der Presse oft als „Krypto-Anarchisten“ verschrieen, war diese Gruppe unter anderem an der Verbreitung von PGP mass-geblich beteiligt und verkündete zudem die frohe Botschaft, das Verschlüsselungs-technik als libertäres Werkzeug unerlässlich ist. Und das zu Zeiten, in denen die Weitergabe von Verschlüsselungstechnik noch als eine Form des illegalen Waffenexports unter Strafe stand (CoCom) oder in denen staatliche Stellen überall in der Welt den privaten Einsatz von Verschlüsselung verbieten (Russland, Frankreich), kontrollieren (Key Escrow) oder kompromittieren (Backdoor) wollten...

  Informationelle Selbstbestimmung ist – zumindest in Deutschland – ein vom BVG im Vorfeld der Volkszählung '87 in einem Urteil erklärtes Grundrecht, dass jede Person „die Herrschaft über die eigenen Daten hat“. In diesem Zusammenhang ist Verschlüsselung natürlich ein effektives Werkzeug, diese Herrschaft faktisch auch

7 Steven Levy: „Crypto. How the code rebels beat the government. Saving privacy in the digital age“. Viking, New York NY 2001, ISBN 0-670-85950-8

wirklich ausüben zu können.

Für viele Politiker ist starke Verschlüsselung sogar zu effektiv, weil im Gegensatz zu einem verbrieften Recht, das durch richterliche Anordnung jederzeit auch wieder individuell und befristet ausser Kraft gesetzt werden kann, ist eine verschlüsselte Email eben verschlüsselt – Richter hin oder her.

Damit war Krypto auf einmal nicht nur mehr technisch, sondern auch politisch. Auf der Mailingliste der Cypherpunks wurden somit nicht nur technische Diskussionen über Verschlüsselungsprogramme geführt, sondern auch die politischen und allgemein-gesellschaftlichen Implikationen von informationeller Selbstbestimmung und Informationsfreiheit ausgelotet.

Informationsfreiheit in diesem Zusammenhang bezieht sich vor allem auf Informationen und Daten, die im öffentlichen Bereich anfallen und die deshalb auch der Öffentlichkeit zugänglich gemacht werden müssen. Ähnlich dem „Freedom of Information Act (USA 1974)“ wurde auch in Europa eine ähnliche Regelung gefordert; in Deutschland dauerte es noch bis 1998, bis ein Informationsfreiheitsgesetz verabschiedet wurde, dass an vielen Stellen Akteneinsicht und Zugriff auf Dokumente erlaubt – allerdings mit Gebührenbremse und enormen Zeitaufwand. In den USA ist man da zumindest gedanklich schon wieder etwas weiter, als die Obama-Administration das Konzept des „Open Government“ einführt – ein Projekt, das übrigens wegen einiger fehlender Budget-Millionen gerade auf der Kippe steht, während gleichzeitig jeden Monat Milliarden für zweifelhafte Militäraktionen ausgegeben werden.

Im politischen Kontext gehören zum Bereich Informationsfreiheit auch Themen wie Zensur, Umgehung von Internet-Zensur und Anonymität im Netz, die von den Hackern und Cypherpunks gerne und ausgiebig diskutiert werden.

Genauso wie die Forderung nach freier und ungehinderter Kommunikation weltweit

– etwas, was sogar direkt in der Satzung des CCC verankert ist. Auch wenn die damalige „*Deutsche Bundespost*“ - von den Hackern oft respektlos als der *Gilb* bezeichnet und als Kommunikations-Monopolist gefürchtet – als so etwas wie der natürliche Feind des Hackers empfunden wurde, so gab es doch Respekt für eine Traditionslinie, die eng mit dem Name Heinrich von Stephan verbunden ist. Von Stephan war Generalpostdirektor des deutschen Reiches und einer der Begründer des Weltpostvereins, der durch internationale Verträge dafür sorgte, dass selbst Länder, die sich miteinander im Krieg befanden, noch geregelten Postverkehr aufrecht erhielten – ungehinderte Kommunikation also.

Nicht so sehr können sich Hacker mit einer zweiten Traditionslinie in der Postwelt anfreunden, die auf Leonhard von Taxis zurückgeht, der sich vom Kaiser das Postregalamt für viel Geld erkaufte, damit dieser seine Hurerei und Völlerei bezahlen konnte. Das Taxis danach gleich einmal schwarze Kammern einrichtete, die den Postverkehr im Reich mitlas und direkt dem Kaiser rapportierte, macht ihn aus Hackersicht nicht gerade sympathischer.

Anspruch vs. Realität

Das Spannungsfeld zwischen der gesellschaftlichen Realität und den Zielen aus der Hackerethik ist klar definiert: Während Hacker und andere Cypherpunks sich eine Welt wünschen, in der jeder seine Daten verschlüsseln kann, aber der öffentliche Sektor alle Informationen offenlegen muss, sah die Realität – damals wie heute – genau anderes herum aus: Der Staat versteckt die Informationen vor seinen Bürgern, während diese alle Daten beim Staat abgeben müssen.

Dieser Zustand hat sich in den letzten 20 Jahren nicht grundlegend geändert. In einigen Bereichen hat es sich graduell verbessert (Informationsfreiheitsgesetz), in den meisten anderen hat es sich sogar eher verschlimmert. So sind es heute nicht mehr nur die öffentlichen Einrichtungen, die als Datenkraken überall mit ihren Tentakeln unsere

Privatsphäre abtasten – diesen Rang haben ihnen die privaten Internet-Unternehmen schon lange abgelaufen.

Realitätsabgleich – Informationelle Selbstbestimmung

- **Daten-Exhibitionsmus**: Allerdings scheint es auch eine neue Generation von Internet-Usern zu geben, die auf Web 2.0-Plattformen wie Facebook oder ähnlichem völlig freiwillig und ungeniert einen Daten-Exibitionismus betreibt, den sich Datenschützer mit ihrem Leitmotiv der Datensparsamkeit nur schwer vorstellen können. Aber wer die Hoheit über seine eigenen Daten hat, kann auf dieses Recht natürlich auch von sich aus verzichten. Ob dabei allen klar ist, dass das Konsequenzen haben kann, die man selbst tragen muss – das wage ich mal zu bezweifeln. Es wird schon einen Grund haben, warum HR-Manager das Internet so lieben...

- **Tauschgeschäft**: Da wo die Freiwilligkeit zur Datenabgabe nicht gegeben ist, werden Leute mit vermeintlichen Vorteilen und kostenlosen Angeboten zur Preisgabe von privaten Informationen animiert. Ob der kostenlose Email-Account bei Google, die passende Buchempfehlung bei amazon oder die Rabattpunkte bei Discounter-Bonuskarten: sie alle haben nur einen Zweck: dem Unternehmen den Zugang zu persönlichen Daten zu ermöglichen, die dieses dann gewinnbringend einsetzen kann – z.B. durch Verkauf qualifizierter Adressdaten.

- **Zwangsbeichte**: Während private Unternehmen noch Anreize für eine freiwillige Datenabgabe verwenden müssen, werden im Kontext der öffentlichen Hand vorzugsweise entsprechende Gesetze geschmiedet, um an die gewünschten Daten zu gelangen. Überwachung des öffentlichen – und teilweise sogar des privaten Raumes – werden durch Projekte wie INDECT staaten-übergreifend organisiert und legitimiert.

- **Daten-Diebstahl**: Wer sein Recht auf Datenhoheit abgibt – nicht mein Problem.

Mein Problem fängt immer da an, wo Daten über mich gesammelt habe, über die ich nicht selbst bestimmen kann. Von Glück kann man dabei fast schon reden, wenn man wenigstens im Nachhinein erfährt, *das* Daten gesammelt wurden; richtig übel sind aber die Fälle, wo ich es noch nicht einmal erfahre, dass Daten erfasst und an Dritte weitergeben werden. Dies ist aus meiner Sicht einem Diebstahl gleichzusetzen...

Zwei Beispiele aus der letzten Zeit mögen dies verdeutlichen: Da ist zum einen Sony, denen etwa 100 Millionen von persönlichen Kundendaten – inklusive Kreditkarten-Daten – abhanden gekommen sind. Wenn ich also meine privaten Informationen an Unternehmen weitergebe, dann kann ich mich nicht auf Datenschutz-Gesetze verlassen, damit meine Daten nicht in dritte Hände fallen können.

Das zweite Beispiel ist die Standort-Protokollierung auf Apple iPhones. Die damit mögliche Erstellung von Bewegungsprofilen ist nun echt kein Spass mehr, sondern ein massiver Eingriff in die Privatsphäre, wenn diese Daten von Zweiten eingesehen werden können. Traurig an diesem Fall ist vor allem aus meiner Sicht die Tatsache, dass die Protokollierung wahrscheinlich wirklich nur eine Unachtsamkeit eines Programmieres und keine geplante Spionageaktion von Apple war. Aber nicht der Wille zählt, sondern nur die Tat – und tatsächlich sind diese Daten angefallen und wurden ziemlich sicher auch ohne Zustimmung der Betroffenen verwendet.

Allerdings muss man aufpassen, dass die Empörung über den Zwischenfall nicht heuchlerisch wird; schliesslich werden bei der Vorratsdatenspeicherung noch mehr Informationen sogar über einen längeren Zeitraum aufbewahrt. Wer nämlich glaubt, dass der Zugriff auf diese Verbindungsdaten – zumindest in Deutschland – nur nach rechtmässigen und richterlichen Verfügungen erfolgen kann, sollte sich mal damit befassen, wie die polizeiliche Nutzung der Autobahn-Mautdaten oder der direkte Zugriff

auf die Bankdaten durch die Bafin mal gedacht und dem Bürger verkauft worden ist und wie es heute wirklich gehandhabt wird...

Leseempfehlung: Das Buch „Die Datenfresser“, geschrieben von zwei Pressesprechern des Chaos Computer Clubs

Realitätsabgleich – Informationsfreiheit

Auch der Realitätsabgleich im Bereich Informationsfreiheit fällt nicht so viel besser aus. Offenheit der öffentlichen Hand gegenüber dem Bürger ist noch immer selten. Informationsfreiheitsgesetze werden – so sie denn überhaupt existieren – noch immer gerne restriktiv von der Bürokratie gehandhabt. Gerade in einer direkten Demokratie wie der Schweiz muss aber der mündige Bürger, der am politischen Entscheidungsprozess partizipieren will, durch den einfachen Zugang zu öffentlichen Informationen im Internet auch dazu in die Lage versetzt werden.

Auch sollten wir an dieser Stelle – und alle reden ja von einer globalisierten Welt – nicht die vielen Ländern vergessen, in denen die Bevölkerung keinen freien Zugang zum Internet überhaupt hat und in denen die Zensur von Gedanken noch an der Tagesordnung ist.

WikiLeaks

Einer der *Cypherpunks*, die neben der reinen Krypto-Technik speziell auch an dieser politischen Ausrichtung des Themas *Informationsfreiheit* interessiert waren, ist heute ein berühmter Mann: *Julian Assange*, einer der Gründer und der heutige Kopf von *WikiLeaks*.

Wer sich schon immer gefragt hat, wessen geistiges Kind *WikiLeaks* ist, hat hier eine Antwort: Die Hacker und Cypherpunks haben mit der Hackerethik und ihren Diskussionen zur politischen Gesellschaftsgestaltung den philosophischen Unterbau beigetragen, ohne den Plattformen wie *WikiLeaks* gar nicht existieren würden.

Ablauf

Wie arbeitet WikiLeaks? WikiLeaks ist eine Plattform, die es einem Whistleblower erlaubt, brisante Dokumente elektronisch zu publizieren, ohne dabei selbst in Erscheinung zu treten. Es gibt von WL dafür entsprechende Anleitungen, mit ein Whistleblower seine Anonymität erhöhen kann; WL selbst stellt zusätzlich durch seine Infrastruktur sicher, dass Einsender später nicht mehr identifiziert werden können (keine Logdateien, Verwendung von „Mixin-Kaskaden“).

In einem ersten Schritt werden die Metadaten aus dem Dokument entfernt, weil diese später eventuell noch die Herkunft und die Identität des Whistleblowers verraten könnten. Diese Anonymisierung findet immer und für jedes Dokumentenformat statt.

In einem weiteren Schritt wird die Authentizität und Relevanz eines Dokumentes bewertet; Entlarvte Fälschungen werden als solche gekennzeichnet.

Der letzte Schritt ist die Veröffentlichung der Dokumente, die in einer verteilten Infrastruktur (Mirroring) erfolgt. Nur wenn absolut notwendig werden Dokumente vor der Veröffentlichung redigiert – zum Beispiel, wenn erkennbar Gefahr für Leib und Leben von im Dokument erwähnten Personen besteht.

Geschichte

WikiLeaks beginnt seine Arbeit gegen Ende 2006 und geht mit der Plattform im Dezember 2006 online. Das erste geleakte Dokument dokumentiert den unterschriebenen Auftrag zur Ermordung von Regierungsmitarbeitern durch den somalischen Diktator Hassan Dahir Aweys. Im darauffolgenden Jahr wurde das „*Standard Operating Procedures for Camp Delta“*, also das Handbuch von Guantanamo veröffentlicht. 2008 folgte die Veröffentlichung von internen Dokumenten der Scientologen, die Internet-Sperrlisten verschiedener Staaten sowie die komplette Mitgliederliste der britischen BNP, die WikiLeaks immer mehr in das Blickfeld einer breiteren Öffentlichkeit brachten.

Bank Julius Bär / Streisand-Effekt

Die erste grössere öffentliche Aufmerksamkeit erhielt WikiLeaks Anfang 2008 durch Veröffentlichung von Unterlagen der Bank Julius Bär auf den Cayman Islands. Die zugespielten Dokumente belegten das dubiose Geschäftsgebaren der Bank Julius Bär, die Beihilfe bei Geldwäsche und Steuerhinterziehung im Offshore-Steuerparadies tätigte.

Gleich nach Veröffentlichung ging die Bank Julius Bär juristisch gegen WikiLeaks vor; sie erwirkte eine einstweilige Verfügung gegen WikiLeaks und Dynadot (den Registrar) auf Sperrung der Internet-Domain „wikileaks.org“ und reichte Klage in Kalifornien ein.

Durch den sogenannten „Streisand-Effekt“ erzeugt die Klage der Bank erst für die Aufmerksamkeit auf die Dokumente, die sie eigentlich zu vermeiden suchte. Fast zwei Dutzend Personen und Institutionen – davon die Hälte etablierte Medienorganisationen – legte Einspruch gegen die Klage ein; die *New York Times* druckte die numerische IP-Adresse von WikiLeaks in ihrem Artikel ab und umging somit die richterliche Verfügung der Domain-Sperrung.

Die Klage wurde von der Bank Julius Bär nach etwa zwei Monaten still und leise zurück gezogen.

Kaupting-Bank

Ein mittleres Erdbeben löste WikiLeaks in Island mit der Veröffentlichung von Dokumenten zum Untergang der Kaupting-Bank aus. Die Dokumente belegten, wie die Manager die Bank kurz vor dem Kollaps regelrecht plünderten, indem sie Kredite zwischen 45 Millionen und 1.25 Milliarden Euros an die Shareholder ausgaben. WikiLeaks wurde so zu einem Kristallisationspunkt für isländische Politiker, die als Resultat der Finanzkrise und des Handlings des resultierenden Kollateralschadens begannen, über eine neue Politik Islands in der digitalen Welt nachzudenken – die Geburtsstunde der IMMI (Islandic Modern Media Initiative, die Island zu einem Datenfreihafen machen will).

Spendenaktion der WHS

Mitte des Jahres 2009 – direkt nach der Aktion auf Island – war klar geworden, dass der Betrieb von WikiLeaks auf eine neue, professionellere Ebene gehoben werden muss. Bisher finanzierte sich WikiLeaks wesentlich aus den Eigenmitteln der Macher, die so die technische Infrastruktur aufrecht erhielten. Der Zufluss von Dokumenten nahm aber so stark zu, dass es Vollzeit-Aktivisten brauchte, um die Abarbeitung zu ermöglichen. Der finanzielle Jahresbedarf von WikiLeaks wurde auf 200'000 bis 600'000 Dollar veranschlagt, je nachdem ob Aufwandsvergütungen gezahlt werden oder nicht.

So kam es, dass eine offizielle Anfrage bei der Wau-Holland-Stiftung einging, ob man nicht WikiLeaks als Spendenprojekt finanzieren könnte. Nach Absprache im Vorstand wurde dem zugestimmt – immerhin entspricht WikiLeaks dem Stiftungsziel, die Informationsfreiheit zu fordern und zu fördern. Seit September 2009 wurden deshalb Spenden für das Projekt „Enduring freedom of information“ der Stiftung gesammelt.

Von Ende 2009 an war WikiLeaks nicht mehr direkt erreichbar; der Betrieb wurde eingestellt, bis die Finanzierung über Spenden sichergestellt werden konnte. Zu den letzten Veröffentlichungen vor der Deaktivierung zählt eine Sammlung der 570'000 Pager-Nachrichten, die am Tage des 11.Septembers 2001 in New York verschickt und empfangen worden waren und der komplette Toll-Collect-Vertrag aus Deutschland, der bisher sogar Parlamentariern vorenthalten worden war.

Der Betrieb wurde Ende des 1.Quartals 2010 wieder aufgenommen.

Aktionen 2010

„**Collateral Murder**“: Die Ermordung von Zivilisten, darunter zwei Journalisten von Reuters, im Iraq 2007 durch Apache-Militärhubschrauber der US-Armee. Reuters hatte jahrelang versucht, Aufklärung von der Armee zu erhalten – ohne Erfolg.

„**War Diary: Afghanistan War Logs**“: Veröffentlichung von 75'000 militärischen Nachrichten aus dem Afghanistan-Krieg; von den ursprünglich 90'000 Nachrichten werden

15'000 zurück gehalten, weil nach Einschätzung von WikiLeaks diese Veröffentlichung Leib und Leben von erwähnten Personen zur Folge haben könnte.

Nach der Veröffentlichung wird WikiLeaks von verschiedenen Seiten (Pentagon, Jimmy Wales u.a.) vorgeworfen, durch die Veröffentlichung Menschenleben gefährdet zu haben, da die veröffentlichten Dokumente nicht redigiert (geschwärzt) worden waren. Tatsächlich wurde aber bisher kein einzelner Fall bekannt, in dem dies passiert wäre – die Einschätzung von WL bei den 75'000 Nachrichten war also soweit richtig.

Fazit: Es zeigte sich schnell, dass die Nachrichten als Rohmaterial für eine breite Öffentlichkeit nicht verständlich waren – sie benötigten eine journalistische Aufarbeitung und mussten in einen grösseren Kontext gestellt werden. Auch militärische Fachkenntnisse (jedes zweite Wort ein Akronym) waren für die Einordnung notwendig. Deshalb begann man bei WikiLeaks, über eine engere Kooperation mit etablierten Printmedien nachzudenken.

„War Diary: Iraq War Logs“: Fast 390'000 militärische Nachrichten aus dem Iraq-Krieg sind die grösste Veröffentlichung von Kriegsdokumenten, die jemals stattgefunden hat. Die Probleme, die mit dem viel kleineren „Afghanistan War Logs“ schon aufgetreten waren, erhielten noch einmal eine neue Dimension. Als Folge wurde die nächste Veröffentlichung in Zusammenarbeit mit fünf Medienpartnern (Guardian, NYT, Spiegel, Le Monde und El Pais) geplant.

„Cablegate“: Insgesamt 250'000 US-Botschaftsdepeschen sind bei WikiLeaks eingelaufen; bis heute wurden davon etwa 8'000 veröffentlicht – das sind mal gerade etwas über drei Prozent. Damit wäre noch genug Stoff für die nächsten 15 Jahre vorhanden, allerdings hat das Interesse doch schon stark abgenommen.

Eskalation

Cablegate hat die USA tief im Mark getroffen – sehr viel mehr als die Militärnachrichten, von denen man eigentlich erwartet hatten, das sie zu „Verstimmungen“ zwischen

WikiLeaks und den USA führen würden. Dass amerikanische Journalisten und Politiker – allen voran die Teetrinkerin Sarah Palin – sogar so weit gehen, ungeniert die Ermordung von Julian Assange zu fordern, das hatte allerdings kaum einer erwartet. Aber direkt nach der Veröffentlichung der ersten *Cables* passierten verschiedene Dinge, die offensichtlich alle nur ein Ziel hatten: *WikiLeaks* ab- und auszuschalten, indem der Geldhahn zugedreht wird.

Am 4.Dezember kündigte *PayPal* das Spendenkonto der *Wau-Holland-Stiftung* mit der Begründung, das über das Konto „illegale Aktivitäten gefördert werden“ und fror das Rest-Guthaben (mehrere 10'000 Euro) auf dem Konto ein. Erst nach Einleitung juristischer Schritte konnte *PayPal* bewegt werden, wenigstens das Geld vom Konto zu uns zu transferieren.

Am 6.Dezember kündigte *Mastercard* an, keine Buchungen mehr auf WikiLeaks-Konten auszuführen – mit ähnlicher Begründung wie PayPal. Ebenfalls an diesem Tag kündigte die PostFinance das Konto von Julian Assange, weil dieser bei der Kontoeröffnung falsche Angaben zum Wohnsitz gemacht haben soll. Da dies normalerweise kein Problem darstellt, berief man sich zusätzlich auf das Postgesetz, das es der PF erlaubt, „Geschäftsbeziehungen zu beenden, die dem öffentlichen und sittlichen Empfinden zuwider laufen“. Das Problem mit diesem Gesetzestext war nur, dass dieser Artikel erst eine Woche vorher vom Ständerat eingereicht und noch gar nicht vom Nationalrat verabschieden worden war – mithin also noch gar nicht gültig war.

Am 7.Dezember folgte Visa der Ankündgung von Mastercard; eine Woche später gab die *Bank Of America* bekannt, jedwede Transfers von oder zu WikiLeaks und WHS-Konten unterbinden zu wollen.

Da wundert es nicht, das die *BoA* das erste Ziel einer bis dahin unbekannten Bewegung wurde: *Anonymous*. Vernetzt durch das Internet haben Leute zusammen gefunden, die über das Vorgehen gegen Wikileaks so frustriert waren, dass sie ihren Unmut durch

digitale Formen des zivilen Ungehorsams ausdrücken wollten. Mit einem frei auf dem Netz verfügbaren Werkzeug (LOIC = *Low Orbit Ion Cannon*) kann jeder – auch ohne technisches Vorwissen – seinem Rechner einem DDoS (Distributed Denial of Service) zur Verfügung zu stellen und so an einer digitale Sitzblockade vor den Webseiten von Firmen teilzunehmen. Das war sehr erfolgreich: Alle Blockaden führten dazu, dass betroffene Webseiten tagelang nicht oder nur sehr sporadisch zu erreichen waren.

Hat es funktioniert, den Geldhahn zuzumachen: Wie beim Streisand-Effekt ist genau das Gegenteil eingetreten: Etwa ein Drittel des gesamten Spendenvolumens 2010 ging nach dem 7.Dezember 2010 als Banküberweisung auf dem deutschen Stiftungskonto ein. Insgesamt weist der Transparenzbericht der WHS für das Jahr 2010 einen Spendeneingang von rund 1.8 Millionen CHF auf; davon wurden rund 560'000 an WikiLeaks wieder ausgezahlt. Selbst wenn ab heute keine Spenden mehr eingehen würden – was aber nicht der Fall ist – kann die Stiftung WikiLeaks weitere zwei Jahre vollständig finanzieren.

Das wirkliche Wichtige aus meiner Sicht ist aber, dass heute immer mehr Plattformen wie WikiLeaks entstehen, die sich dem Ideal der Informationsfreiheit verbunden fühlen...

IT-Security Hype: DLP

In den Manager-Etagen und bei IT-Entscheidern hat *WikiLeaks* vor allem auch dazu beigetragen, noch mehr über den Abfluss von vertraulichen Dokumenten aus einem Unternehmen nachzudenken – die Schweiz hat ja mit den Steuer-CDs zusätzlich einen ganz besonderen Anreiz.

Software-Hersteller haben schnell reagiert und mit DLP (*Data Loss Prevention* bzw. *Data Leakage Prevention*) ein neues Sicherungswerkzeug auf den Markt geworfen. Ist das das Ende von *WikiLeaks* und allen anderen Plattformen?

Ich habe als *Security Architect* in einem Projekt für eine schweizerische Grossbank die Möglichkeit gehabt, mir alle am Markt gängigen DLP-Lösungen sehr genau anzusehen

und bin heute beruhigt – keines der DLP-Systeme, die nach *Gartner* zu den besten ihres Fachs gehören, ist in der Lage, gewollte und absichtliche Leaks zu verhindern – bestenfalls Unachtsamkeit und Fahrlässigkeit beim Umgang mit vertraulichen Daten.

Die hohen Erwartungen, die das Management an eine DLP-Lösung hat, werden meiner Ansicht nach nicht erfüllt; keines der Systeme ist uneingeschränkt Enterprise-fähig. Neben viel Vorarbeit zur Klassifikation von Daten in einem Unternehmen und im Rechtemanagement der Anwender ist auch das organisatorische Umfeld eines DLP-Einsatzes nicht zu unterschätzen. Leaks werden uns also auch in Zukunft erhalten bleiben.