

# 50 Days of Lulz : Welche informationsethischen Fragen warf die Hackergruppe LulzSec mit ihren Aktivitäten auf?

Karsten Schuldt

Im Mai und Juni 2011 operierte eine Gruppe von Hackern unter dem Namen LulzSec relativ offensiv und mit starker medialer Begleitung. Die Gruppe verkündete, sich vor allem über die schwache Sicherheit von Servern und Homepages lustig zu machen und hauptsächlich nach dem Prinzip zu operieren, selber Spaß zu haben. Als Methoden ihrer Angriffe benutzte die Gruppe vor allem DDoS-Attacken, offenbar ausgeführt von einem eigens aufgebauten Bot-Netz, sowie das Auslesen von Daten mittels SQL Injections. Beide Methoden wurden von anderen Hackern als relativ simpel bezeichnet, obgleich LulzSec immer wieder betonte, weitere Methoden zu benutzen. Dennoch erregt die Gruppe großes Aufsehen, zum einen da sie relativ viele Daten, zu denen sie Zugang gefunden hatte, veröffentlichte und sehr großen Organisationen – unter anderem das FBI – als Ziel ihrer Angriffe aussuchte, zum anderen durch die Angewohnheit, die Öffentlichkeit beständig über ihre Angriffe zu informieren.

Die Gruppe wurde von einigen auf Internetthemen spezialisierten Medien als „Grey Hat Hackers“ bezeichnet, da sie Elemente des Hackens, welches sich moralisch oder politisch motiviert und des Crackens, welches explizit Zerstörung in Daten und Servern anrichten oder einen finanziellen Gewinn aus den Onlineaktivitäten ziehen will, in sich vereinte.

Am 26.06.2011 Mitteleuropäische Zeit, beziehungsweise kurz vor dem Ende des 25.06.2011 in den nordamerikanischen Zeitzonen, verkündete LulzSec, sich nach 50 Tagen Aktivität selber aufzulösen. Über die Gründe für diese Auflösung wurde sofort spekuliert, wobei mehrere Stimmen davon ausgingen, dass die bislang anonym agierende Gruppe befürchten musste, kurz vor der Ent-Anonymisierung durch andere Hackergruppen oder aber durch Strafverfolgungsbehörden zu stehen. LulzSec selber verkündete, dass sie ihre Aktivitäten von vornherein auf diese 50 Tage angelegt hätte.

Die Existenz und die Aktivitäten dieser Gruppe sowie die Reaktionen auf diese von Seiten anderer Hackergruppen, spezialisierter Medien, der unterschiedlichen Internet- und Spiele-Communities und der von den Angriffen betroffenen Firmen und Organisationen werfen eine Reihe von ethischen Fragen im Bezug auf Informationsnutzung, Datenschutz, Verantwortung, Hackerethik und Netzaktivismus auf. Es ist leicht ersichtlich, dass sich diese ethischen Fragen nicht nur für die Subkultur des Hackens, sondern für alle Einrichtungen und Individuen stellen, die sich mit dem Internet befassen, insbesondere aber für Initiativen, die sich dem Netzaktivismus verschrieben haben. Angesichts dessen, dass diese Gruppe mit ihrem – unter Umständen auch vorläufigen – Ende eine klare Zäsur gesetzt hat, bietet sich dieses Beispiel für eine Übersicht zu den ethischen Fragen des Internetzeitalters an.<sup>1</sup> Im Folgenden sollen anhand von LulzSec diese Fragen kurz diskutiert werden.

Im ersten Teil dieses Textes werden die Aktivitäten von LulzSec und die Reaktionen darauf dargestellt, im zweiten Teil die informationsethischen Fragestellungen, die sich aus diesen Aktivitäten ergeben. Im dritten Teil soll ein, selbstverständlich vollkommen unvollständiger,

---

1 Weiterhin existieren ähnliche Gruppen unterschiedlicher Struktur, wobei durch LulzSec offenbar auch wieder kleinere Gruppen neben der bekannten Anonymous beziehungsweise AnonOps beachtet zu werden scheinen. Ein aktuelles Beispiel in Deutschland ist die „no name crew“, die im Mai 2011 Homepages der NPD hackte und im Juli 2011 Daten veröffentlichte, die sie bei einem Hack der Bundespolizei erhalten haben will.

Versuch unternommen werden, die Relevanz dieser Frage für Informationseinrichtungen und Bibliotheken auszuloten.

## Teil I: LulzSec

LulzSec stellte, um dies vorweg zu nehmen, keine explizit kriminelle Gruppe dar, welche sich mit ihrem Hacken einen persönlichen Vorteil, und sei er rein finanzieller Art, hätte sichern wollen. Dennoch verstieß die Gruppe mehrfach gegen geltende Gesetze oder zumindest gegen das weithin vertretende Rechtsverständnis.

Wertet man die Tweets der Gruppe selber sowie die Medienberichte über sie aus, so ergibt sich, bezogen auf die sichtbarsten ihrer Aktionen, folgende Zeittafel.<sup>2</sup>

Datum	Form der Aktion	Aktion
07.05.2011:	Hack / Leak	Hack und Leak: Fox.com, „X Factor“ (Unter anderem wurde die Datenbank von X Factor, einer Sendung ähnlich „Deutschland sucht den Superstar“, inklusive der Ergebnisse der noch unausgestrahlten Sendungen, veröffentlicht.)
10.05.2011:	Hack / Leak	Hack und Leak: private Daten von Angestellten von Fox.com werden veröffentlicht
11.05.2011:	Hack	„Minihack“, persönliche Daten aus ATM-Maschinen (Geldautomaten)
12.05.2011:	Leak	„Random-Leaks“, Fox.com-Leak II
13.05.2011:	Leak	Fox.com-Leak III
16.05.2011:	Leak	„Pointless“ ATM-Hack
24.05.2011:	Hack	Hack: Sony Japan und andere <sup>3</sup>
30.05.2011:	Hack	Hack: PBS (Fernsehstation, platzieren unter anderem die Nachricht, das Tupac Shakur und Notorious B.I.G. (ermordet 1996 und 1997) in Neu Seeland leben würden)
31.05.2011:	DDoS	DDoS: 2600.net (Hacker-Magazin)
02.06.2011:		Eigene Homepage ( <a href="http://lulzsecurity.com/">http://lulzsecurity.com/</a> <sup>4</sup> ) freigeschaltet
02.06.2011:	Hack	Hack: Sony Pictures, Playstation Network
03.06.2011:	Leak	Serverkonfiguration von Nintendo.com veröffentlicht
03.06.2011:	Ankündigung	FuckFBIFriday
03.06.2011:	Hack, Leak	Hack und Veröffentlichung von Daten: Infragard (Private-Public-Sicherheitskoalition unter der Führung des FBI)
05.06.2011:	Hack	Hack: Sony Pictures Russland
10.06.2011:	Leak	Veröffentlichung der Nutzerdaten von pron.com (Pornoseite)
10.06.2011:	Hack	Hack: Endgame Systeme (Internetsicherheit Unternehmen)
11.06.2011:	Hack	Behauptet, eine „Jihad-Seite“ (islamitische Homepage) vom Netz genommen zu haben
11.06.2011:	Leak	Hilft NHS (National Health Service, UK), indem auf Sicherheitsprobleme in der Datenbank hingewiesen wird, ohne diese zu veröffentlichen
11.06.2011:		Eigene Telefonnummer von LulzSec eingerichtet, wird in den nächsten Tagen zeitweise als Telefon-DDoS genutzt (Umleitung auf andere Nummern)
12.06.2011:		Beginn der Auseinandersetzung mit Anonymous beziehungsweise 4chan
13.06.2011:	Hack	Hack: Bethesda Softworks (Spielefirma, unter anderem jetziger Produzent der „Fallout“-Reihe)
13.06.2011:	Hack	Hack: Homepage US-amerikanischer Senat

<sup>2</sup> Vgl. <http://www.twitter.com/lulzsec> sowie Anhang I und II dieses Textes.

<sup>3</sup> Sony war im April und Mai 2011 Ziel zahlreicher Hacks und DDoS-Attacken, bei denen die Hintergründe bislang nicht vollständig klar geworden sind. Zumindest in einer späten Phase scheinen diese Attacken von verschiedenen Hackergruppen vor allem durchgeführt worden zu sein, weil Sony in den ersten Hacks als angreifbares Ziel mit zahlreichen Sicherheitslücken bekannt wurde.

<sup>4</sup> Die Homepage ist weiterhin einsehbar. Allerdings ist vor dem Besuch zu einigen Vorsichtsmaßnahmen, zumindest dem Einsatz eines oder mehrerer Proxyservers und die Überwachung des Netzverkehrs, zu raten.

14.06.2011:	DDoS	Angriff auf escapistmagazine.com (Zeitschrift für Computerspiele und Webthemen)
14.06.2011:	Hack	Hack: Eve Online (Spielservers)
14.06.2011:	DDoS	DDoS: Minecraft (Spielservers)
14.06.2011:	DDoS	DDoS: League of Legends (Spielservers)
15.06.2011:	DDoS	DDoS: cia.gov
16.06.2011:	Spam	LulzSec kündigt an, das Imageboard /b/ mit Spam zu vermüllen. Dies wird teilweise umgesetzt
16.06.2011:	Leak	Interne Mails von HBGary (Internetsicherheitsfirma) veröffentlicht
17.06.2011:	DDoS	DDoS: tribalwars.net (Spielservers)
17.06.2011:	DDoS	DDoS: hackforums.net
17.06.2011:		Offener Brief von Lulzsec, in dem die Gruppe ihre Aktivitäten begründet
18.06.2011:		Web Ninjas (Hackergruppe) treten auf und behaupteten, LulzSec enttarnen zu wollen ( <a href="http://lulzsecexposed.blogspot.com/">http://lulzsecexposed.blogspot.com/</a> )
19.06.2011:	Hack	Hack: Recol.org (Internet-Hosting)
19.06.2011:	Hack	Hack: Infragard-ct.org (Infragard Connecticut, Sicherheitsfirma für staatliche Einrichtungen)
19.06.2011:		Web Ninjas behaupteten, erste Mitglieder von LulzSec enttarnt zu haben
20.06.2011:		LulzSec ruft dazu auf, an Operation #antisecc (Natzaktivismus gegen Überwachung durch staatliche Stellen) teilzunehmen
20.06.2011:	(Leak)	Die gesamten Daten der britischen Volkszählung werden veröffentlicht. Behauptung, dass es LulzSec war. LulzSec bestreitet dies.
20.06.2011:	DDoS	DDoS: Serious Organized Crime Agency, Sondereinheit der Polizei in Großbritannien (soca.gov.uk)
21.06.2011:		Verhaftung eines 19-jährigen in Großbritannien, der zur Gruppe gehören soll (laut Polizei). LulzSec bestreitet seine Mitgliedschaft.
22.06.2011:	DDoS	DDoS: brasil.gov.br und presidencia.gov.br (brasilianische Regierung)
24.06.2011:	Leak	Daten der Polizei in Arizona werden veröffentlicht
26.06.2011:		LulzSec gibt Auflösung bekannt. "Die Hackergruppe „The A-Team“ behauptet, alle Mitglieder von Lulzsec enttarnt zu haben.

Tabelle 1: Aktionen von LulzSec, Mai und Juni 2011

## Exkurs: Begriffe

Im folgenden Exkurs werden kurz die Begrifflichkeiten des Hackens, soweit sie für die Darstellung der Aktivitäten von LulzSec benötigt werden, dargestellt, da leider nicht davon ausgegangen werden kann, dass diese allgemein bekannt wären.

**Hack:** Mit einem Hack ist wird im Regelfall jeder nicht vorgesehene Zugriff auf einen Rechner bezeichnet, wobei unvorhergesehen nicht unbedingt unrechtmäßig bedeuten muss. Bei einem Hack werden offene Schnittstellen ebenso wie Sicherheitslücken benutzt, um auf einen Rechner – zumeist von einem anderen Rechner aus – zuzugreifen, auf diesem Daten abzufragen oder auch zu verändern. Hack als Oberbegriff lässt sich selbstverständlich weiter differenzieren.

**DDoS:** Distributed Denial of Service-Attacs zielen darauf ab, einen Server, der eine oder mehrere Homepages hostet, zu überlasten. Technisch funktioniert dies, indem der Server beziehungsweise die Homepages schnell hintereinander so oft aufgerufen werden, dass diese Anfragen nicht mehr vom jeweiligen Server zu verarbeiten sind. Dies kann erreicht werden, indem äußerst viele Menschen zur gleichen Zeit eine Homepage aufrufen, was teilweise als Form des politischen Protestes angewandt wird; oder aber durch ein automatisiertes Abrufen der angegriffenen Homepages von verschiedenen Rechnern aus, zumeist aus Botnetzen. Der Angriff auf die Homepages oder Server erfolgt beim DDoS äußerlich. Ein Eingriff in den Server oder gar eine Veränderung von Daten findet nicht statt.

*SQL Injection:* SQL Injections gelten als eine der einfachsten Formen des Hackens. Hierbei werden einem Datenbanksystem von außen Befehle untergeschoben, zumeist durch das Hinzufügen dieser Befehle bei normalen Zugriffen auf die jeweilige Seite, beispielsweise den Suchabfragen. Aufgrund der technischen Einfachheit dieses Angriffs ist er eigentlich sehr einfach durch die Administratoren und Administratorinnen der jeweiligen Homepages abzufangen. Dennoch funktioniert er, wie unter anderem LulzSec zeigte, erstaunlich oft bei Systemen, die Datenbanken einsetzen. Gleichzeitig rufen erfolgreiche Angriffe per SQL Injection in der Hacker-Szene wenig Reputation hervor, da sie als Mittel von Anfängerinnen und Anfängern gelten.

*Leak:* Mit einem Leak wird die Veröffentlichung zuvor geheimer Daten, zumeist in großer Menge, bezeichnet. Weithin bekannt geworden ist der Begriff bei den Auseinandersetzungen um Wikileaks Anfang 2011. Im Falle von LulzSec bezeichnet ein Leak zumeist die Veröffentlichung von „erbeuteten“ Datenbeständen.

*Spam:* Spam bezeichnet nicht nur im Email-Verkehr die Auslieferung zahlloser inhaltlich sinnloser Nachrichten. Als Taktik lässt sich das Spammen auch einsetzen, um die Diskussion in Foren oder auf Imageboards mittels zahlreicher irrelevanter Beiträge absichtlich zu verunmöglichen.

*4chan, /b/:* 4chan ist eine Sammlung von Imageboards, die unter anderen als Heimstätte von Anonymous aber auch anderen Gruppen von Hackern und Internet-Aktivistinnen und -Aktivisten angesehen wird. /b/ ist ein Imageboard auf 4chan (welches auch auf anderen Imageboard existiert), auf welchem sich angeblich ein Großteil dieser Gruppen finden und miteinander kommunizieren würde.

*Anonymous:* Anonymous gilt als diejenige Hackergruppe, die sich auf 4chan gefunden und dort eine Internetkultur entwickelt haben soll, zu der auch das beständige „raiden“ von anderen Homepages und Computerspielen gehört. Anfang 2008 begann Anonymous ein Kampagne gegen die Scientology-Organisation, bei der die Gruppe ihren Netzaktivismus unter anderem durch Demonstrationen vor den Gebäuden der Sekte unterstützte. Seitdem gehen von Anonymous immer wieder neue Aufrufe zu ähnlichen Kampagnen aus, die allerdings unterschiedlich durchgeführt und unterstützt werden. Während sich die Kampagne gegen Scientology zu einer kontinuierlichen Bewegung entwickelte, die mit anderen Kritikerinnen und Kritikern der Sekte zusammenarbeitet, wurden andere Kampagnen nur kurz durchgeführt. Gleichzeitig orientierten sich viele Teilnehmende dieses losen Zusammenhangs weiterhin aus eher subkulturellen Interessen an den Imageboards. Heute existieren zahlreiche Gruppen, die unter dem Namen Anonymous operieren, gleichzeitig gilt dieser Zusammenhang auch als Ort, an welchen sich andere Hackergruppen wie LulzSec grundsätzlich zusammengefunden hätten. Anonymous beziehungsweise die Untergruppe AnonOps scheinen diesen kleineren Hackergruppen immer wieder als Bezugspunkt zu gelten, von dem sich zumeist abgegrenzt werden muss. Gleichzeitig ist wichtig darauf zu verweisen, dass sich Anonymous in der gleichen rechtlichen Grauzone bewegt, wie LulzSec. Es werden immer wieder einmal Gesetze übertreten oder zumindest der rechtliche Rahmen stark ausgenutzt, gleichzeitig geschieht das nicht zum persönlichen Vorteil, wie dies bei kriminellen Vereinigungen der Fall ist, sondern als Freizeitaktivität oder als gesellschaftliches Engagement.

## **Aktivitäten von LulzSec**

Das Vorgehen von LulzSec zeichnete sich durch drei Eigenschaften aus:

- Obgleich LulzSec immer wieder betonte, weiter Aktionen durchzuführen, die sie geheim halten würden, war die Gruppe bei den Aktionen, die bekannt wurden, relativ offensiv im Bezug auf die Öffentlichkeit. Nicht nur, dass ein Twitteraccount und eine Homepage betrieben wurden, es wurden zudem regelmäßige Erklärungen veröffentlicht und sich auch auf anderem Weg bemerkbar gemacht. Gleich ignorierte die Gruppe viele Interviewanfragen und versuchte, ihre öffentliches Bild selber zu bestimmen.
- Die Aktionen der Gruppe folgten keiner einheitlichen Linie. Einige von ihnen schienen einen gesellschaftspolitischen Hintergrund zu haben und deshalb im Zusammenhang mit dem

Netzaktivismus der letzten Jahre zu stehen, andere Aktionen schienen einzig dem Interesse der Gruppe zu folgen.<sup>5</sup> Sowohl die Ziele der Attacken als auch deren Form waren eigentlich nicht vorherzusagen.

- LulzSec trat immer mit einem überheblichen Gestus auf und verortete sich gleichzeitig in der Internetkultur. Insbesondere in ihren Tweets und Erklärungen beleidigte LulzSec regelmäßig die Opfer ihrer Attacken und diejenigen Personen, die sich offenbar gegen die Gruppe stellten. Gleichzeitig zeigte sich LulzSec immer wieder begeistert, erklärte beispielsweise, dass sie den National Health Service in Großbritannien nicht angreifen, sondern ihm helfen würden, weil sie dessen Arbeit wichtig fänden. Ebenso erklärte sie, bestimmte Firmen nicht angreifen zu wollen, weil sie deren Spiel oder Spielkonsolen lieben würde. Allerdings überwogen die Beleidigungen. Gleichzeitig zitierte die Gruppe beständig die Internet-Kultur, wählte Darstellungsformen, die mit Internetmemes und ASCII-Art agierten und benutzte die von den Imageboards bekannten Sprachformen und -bilder.

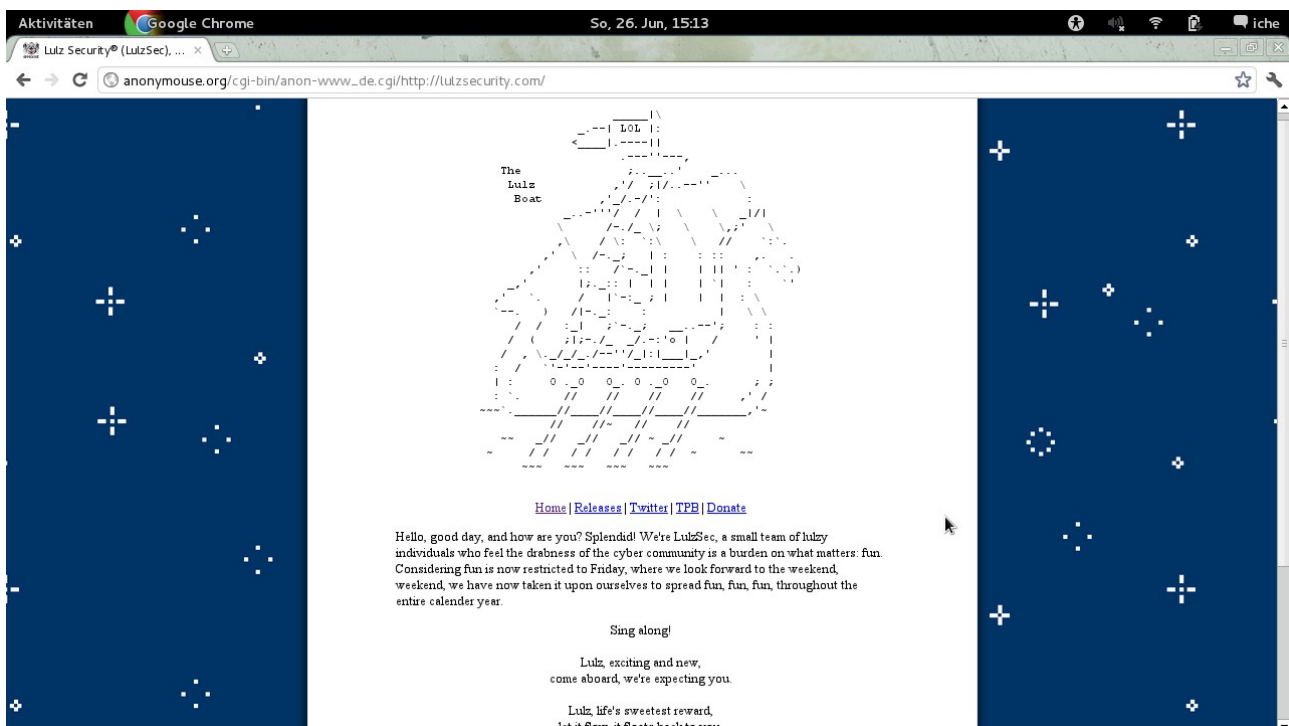


Abbildung 1: Homepage von LulzSec am Tag der Auflösung. Im Zentrum das sogenannte "LulzBoat", ein in ASCII-Art gestaltetes Boot, welches auch in den Erklärungen der Gruppe beständig benutzt wurde.

5 Andere Hackergruppen, beispielsweise die Web Ninjas, behaupteten, dass LulzSec die Ziele auch danach aussuchte, ob diese angreifbar wären. Wenn die Sicherheitsvorkehrungen einer Homepage hoch und diese ordentlich gepflegt war, sei es für LulzSec nicht möglich gewesen, diese anzugreifen. Insoweit hätten sie die Ziele danach gerichtet, ob Seiten angreifbar waren. (Vgl. <http://lulzsecexposed.blogspot.com/2011/07/whos-who.html>: „They randomly check websites for known vulnerabilities to hack them. If given a specific target which is fully patched, they would fail.“)



justice, which we might well be. But you know, we just don't give a living fuck at this point - you'll forget about us in 3 months' time when there's a new scandal to gawk at, or a new shiny thing to click on via your 2D light-filled rectangle. People who can make things work better within this rectangle have power over others; the whitehats who charge \$10,000 for something we could teach you how to do over the course of a weekend, providing you aren't mentally disabled.

This is the Internet, where we screw each other over for a jolt of satisfaction. There are peons and lulz lizards; trolls and victims. There's losers that post shit they think matters, and other losers telling them their shit does not matter. In this situation, we are both of these parties, because we're fully aware that every single person that reached this final sentence just wasted a few moments of their time.<sup>6</sup>

Gleichzeitig bekannte sich LulzSec zur Tradition der Raids, einer Form des Amüsemments für Hacker und andere Nutzerinnen und Nutzer der Imageboards, bei denen sich ein gemeinsames Ziel – zumeist ein Forum, eine Spieleplattform oder ähnliche Onlinetreffpunkte – auserkoren wird, welches mit einer jeweils speziellen Form des Spammens für eine gewisse Zeit gestört wird. Dabei werden die meisten Raids ohne weitere Begründung durchgeführt: Für einen Tag wird dann beispielsweise in einem Forums in jedem Beitrag ein und die selbe Reaktion gepostet und registriert, wie in diesem Forum darauf reagiert wird. Dennoch gibt es auch beständig Vorschläge, bestimmte Raids inhaltlich zu begründen, wobei diese Begründungen sehr unterschiedliche Qualitäten aufweisen. Einige beschränken sich auf persönliche Beleidigungen, während andere politische oder moralische Gründe (insbesondere bei den Raids gegen die Scientology-Organisation oder staatlichen und quasi-staatlichen Einrichtungen, denen Pläne zur Überwachung und Zensur vorgeworfen werden) vorbringen.

LulzSec scheint mit diesen Eigenheiten gespielt zu haben. Teilweise wurden Organisationen ihr Ziel, bei denen sich ein Vorgehen politisch begründen ließ, teilweise wurden Seiten angegriffen, die dem vollständig unverdächtig sind. Insbesondere die DDoS-Attacken gegen mehrere Spieleserver, die dazu führten, dass einige von diesen für eine längere Zeit nicht benutzt werden konnten, schienen einer nachvollziehbaren Begründung außer den Lulz für LulzSec selber, entzogen zu sein. Gleichzeitig begründet LulzSec, warum sie bestimmte Seiten nicht angreifen würden, mit persönlichen Motivationen.

## **Reaktionen auf LulzSec**

Mit ihren beständigen Provokationen rief LulzSec – vielleicht auch gewollt – einige Reaktionen hervor. Während angegriffene Firmen und Behörden sich zumeist in erwartbarer Weise äußerten – also entweder schwiegen oder die Strafverfolgungsbehörden aufforderten, einzugreifen – traten spätestens ab Ende Mai 2011 andere Hackergruppen auf den Plan, die sich mit der moralischen Begründung, dass LulzSec zu weit gegangen und ihre Aktionen unbegründet seien, gegen die Gruppe wandten. Diese Gruppen – allen voran die „Web Ninjas“, „The A-Team“, „Th3j35t3r“ und „TeaMp0isoN“ – versuchten vor allem, die Anonymität der Mitglieder von LulzSec aufzudecken. Sie veröffentlichten Chatlogs (Aufzeichnungen von Onlinechats), die vorgeblich Gespräche von LulzSec darstellten. Insbesondere zielten sie dabei auf den Chatchannel pureElite ab. Gleichzeitig veröffentlichten sie persönliche Daten von Personen, denen sie unterstellten, Mitglieder bei LulzSec zu sein.

Am Tag, an dem LulzSec die Selbstauflösung bekanntgab, tauchte eine Datensammlung von „The A-Team“ auf, in dem angeblich alle Mitglieder von LulzSec enthalten sein sollen, gleichzeitig wird dort versucht, eine kurze Geschichte von LulzSec darzustellen.<sup>7</sup>

Interessant war allerdings, dass es keine einhellige Meinung gab, die dieses Vorgehen oder das von LulzSec unterstützt oder abgelehnt hätte. Sowohl die Fachpresse und deren Foren, als auch die publizierten Meinungen, die beispielsweise auf Twitter und Identi.ca nachvollzogen werden

<sup>6</sup> Vgl. <http://pastebin.com/HZtH523f>.

<sup>7</sup> Vgl. <http://pastebin.com/iVujX4TR>.

können,<sup>8</sup> benutzen zwar oft die für diese Internetkultur typischen Übertreibungen, fanden aber für alle Beteiligten sowohl positive als auch negative Gründe. Sowohl das Vorgehen von LulzSec als auch gegen LulzSec wurde von anderen verteidigt. LulzSec selber betonte, dass sie immer wieder moralische Unterstützung bekommen hätte.

## Teil II: Informationsethische Fragen

Fernab der rein rechtlichen Fragen, welche sich beim international angelegten Vorgehen von LulzSec stellen, warfen die Aktionen und vor allem die Reaktion auf diese, einige ethische Fragen auf. Obgleich sich, allen Voraussagen zum Trotz,<sup>9</sup> bislang keine Debatte um Informationsethik entwickelt hat, lassen sich doch aus den wenigen zu dieser Bereichsethik im deutschen Sprachraum wahrgenommen Texten, einige Grundaussagen referieren, die sich auf die Aktionen von LulzSec beziehen lassen.

Rainer Kuhlen entwickelte vor allem an Fragen des Rechts auf Information und Kommunikation, des Copyrights beziehungsweise der rechtlichen Verfassung elektronischer Räume und der Nachhaltigkeit von Informationen – und damit merklich nicht zu Fragen des Hackens – Grundlagen der Informationsethik.<sup>10</sup> Für ihn stellt diese Ethik

„das Ensemble offener Aussagen über normatives Verhalten, das sich in fortschreitend telemedialisierten Lebenswelten und in der Auseinandersetzung mit den in bisherigen Lebenswelten gültigen Welten und normativen Verhaltensweisen entwickelt [dar].“<sup>11</sup>

An dieser Eingrenzung anschließend, lässt sich am Verhalten von LulzSec und den Reaktionen auf die Gruppe die Frage stellen, welche ethischen Normen offenbar auf- oder angegriffen wurden. Dabei soll die Informationsethik im Anschluss an Kuhlen und Wiegering (vgl. Wiegerling, 1998) als deskriptive verstanden werden, die beschreibt, welche Normen sich entwickeln und gerade nicht normative Forderungen für das richtigen Verhalten aufzustellen sucht.

Kuhlen und Wiegering verwiesen beide darauf, dass sich Bereichsethiken wie die Informationsethik nicht unabhängig von gesamtgesellschaftlich geteilten ethischen Grundlagen entwickeln – es also keine Sonderethik gäbe, die beispielsweise durch den Status der Expertinnen und Experten den handelnden Subjekten Rechte einräumte, die vollkommen gegen die gesellschaftlich geteilten Normen stehen würden –, gleichzeitig aber doch besondere Ausformungen zulassen. Des Weiteren erinnern beide Autoren daran, dass es sich bei Informationsethik nicht um eine Ethik handeln würde, die sich aus der Technik ergeben würde. Die Hard- und Software ermöglicht zwar ein bestimmtes Handeln, beispielsweise überhaupt die Existenz elektronischer Räume als Kommunikationsort oder das Kopieren großer Datenmengen. Aus diesen Eigenschaften lassen sich allerdings keine ethischen Grundsätze ableiten. Vielmehr ist auch die Informationsethik durch menschliches Handeln determiniert. Die technische Möglichkeit, Dinge zu tun, ergibt beispielsweise noch kein Recht dazu. Gleichwohl lässt sich auch kein Verbot direkt aus technischen Möglichkeiten ableiten.

### ***Ist ein Hack immer gerechtfertigt?***

Eine erste ethische Frage, die sich an den Aktionen von LulzSec orientierte, ist die nach der Bewertung von Hacks und Leaks. Insbesondere Anonymous hat in den letzten Jahren durch ihre Methode, Hacks und Online-Attacken moralisch zu begründen, dazu beigetragen, dass auch in der kritischen Öffentlichkeit eine Differenzierung vorgenommen wird. Im Gegensatz zu einigen Medien, die alle Hacks mit kriminellen Aktivitäten – die im Allgemeinen als Cracks abgegrenzt werden –

---

8 Vgl. <http://www.twitter.com/searches?q=lulzsec>, <http://identi.ca/search/notice?q=lulzsec.s>

9 Auffällig ist, dass fast alle Veröffentlichungen zur Informationsethik seit den 1990er Jahren konstatieren, dass es ein steigendes Interesse an diesem Thema gäbe, ohne dass seitdem die Anzahl der Debattenbeiträge gestiegen wäre. Vielmehr scheint das Thema immer wieder neu eingeführt zu werden.

10 Überhaupt ist festzuhalten, dass sich die meisten Texte zur Informationsethik auf Fragen des Copyrights beziehen und dabei andere Bereiche des Verhaltens in elektronischen Räumen kaum besprechen.

11 Kuhlen (2004), S. 23.

identifizieren, wird immer mehr die Frage gestellt, zu welchem Zweck ein bestimmter Hack durchgeführt wird.

Beispielsweise gab es während der Auseinandersetzung um Wikileaks Anfang des Jahres 2011 immer wieder Online-Aktionen, die in der kritischen Presse, aber auch der Öffentlichkeit Verständnis hervorriefen, teilweise auch Zustimmung. Die Erklärung der damaligen Aktivistinnen und Aktivisten, dass sie beispielsweise Amazon mit DDoS-Attacken angreifen würden, weil die Firma sich dem Druck der US-amerikanischen Behörden gebeugt und deshalb die Inhalte von Wikileaks auf ihren Servern gelöscht hätte, wurden teilweise als berechtigter Protest gegen vorgebliche Zensurvorhaben begriffen.

Die Reaktionen auf LulzSec zeigten vor allem, dass eine solche Differenzierung vorgenommen wird. Die ersten Aktionen der Gruppe erheischten weithin Zustimmung, da insbesondere der Angriff auf Fox.com als politische Aktion verstanden werden konnte. Gleichwohl schlug die Stimmung mit der Zeit dahingehend um, dass bei weiteren Angriffen ein solcher politischer Grund nicht immer ersichtlich war. Gleichwohl war auffällig, dass zumindest ein Teil der Internetöffentlichkeit jeden Angriff gesondert bewerten wollte. So wurde der Leak von Daten der Polizei in Arizona auch von solchen Menschen positiv bewertet, welche Angriffe auf Spieleserver ablehnten.

Interessant war, dass immer wieder implizit eine Erklärung für die Hacks eingefordert wurde. Offensichtlich gehört zur gelebten Ethik in elektronischen Räumen, dass Hacks und Angriffe auf Homepages, wenn sie begründet erfolgen, als gerechtfertigt angesehen werden. Es ist vielleicht möglich, in dieser Frage eine Parallele zu politischen Aktivitäten zu ziehen, bei denen die Öffentlichkeit für bestimmte Demonstrationsformen, zum Teil auch radikalen, Verständnis zeigt, wenn sie den Grund für diese berechtigt findet, während sie gleiche Aktionen ohne erkennbaren Grund massiv ablehnt. Beispielsweise kann eine Beeinträchtigung des Straßenverkehrs durch Protestierende gegen Aufmärsche von neofaschistischen Gruppen mit mehr Verständnis rechnen, als andere Eingriffe in den Straßenverkehr. Eine ähnliche Differenzierung, die Aktion und Hintergrund gemeinsam bewertet, hat sich offenbar im Internet etabliert.

## ***Wer ist schuld, wenn eine Homepage gehackt wird?***

Der Vorwurf anderer Hackergruppen an LulzSec, bei ihren Angriffen nur einfache Sicherheitslücken auszunutzen und gerade keine schwierigen Hacks durchgeführt zu haben, enthält unter anderem eine implizite ethische Frage, nämlich danach, wer dafür zu verurteilen ist, wenn Sicherheitsvorkehrung relativ einfach umgangen werden können. Sowohl LulzSec selber als auch die Gruppen, welche sich zur Aufgabe gemacht haben, LulzSec zu enttarnen, wiesen immer wieder darauf hin, dass bestimmte Sicherheitsvorkehrungen sehr einfach zu treffen seien. So sollten Server und Datenbanken regelmäßig geupdatet und niemals die gleichen Passwörter für unterschiedliche Zugänge verwendet werden. So kam es zum Beispiel vor, dass Lulzsec die Zugangsdaten vom privaten Nutzerinnen und Nutzern zum Sony-Netzwerk veröffentlichte und sich andere Menschen erfolgreich darin versuchten, mit diesen Passwörtern und Nutzernamen auf Accounts bei Maildiensten, Facebook und so weiter zuzugreifen, was tatsächlich des Öfteren funktionierte.

Während das Benutzen gleicher Passwörter als Nachlässigkeit von einzelnen Individuen angesehen werden kann, stellt sich die Frage bei nicht geupdateten Servern und Datenbanken anders. Die Firmen, welche die Datenbanken verwalten, sind offenbar nicht ihrer Verpflichtung nachgekommen, private Daten, die sie gesammelt hatten, bestmöglich zu schützen. In den Diskussionen, die sich an die Leaks von LulzSec anschlossen, wurden diese Firmen sichtbar wenig in Schutz genommen. Selbst, wenn sich darüber beschwert wurde, dass LulzSec einzelne Spieleserver angegriffen hätte, wurden nur die betroffenen Nutzerinnen und Nutzer in Schutz genommen. Die Firmen, deren Daten geleakt wurden, hatten eher mit weiterer Kritik zu rechnen.

Ganz offensichtlich herrscht die Vorstellung vor, dass insbesondere große Firmen, die viele persönliche Daten sammeln, die Verpflichtung hätten, diese Daten bestmöglich zu schützen. Insbesondere wenn diese Daten durch solche einfachen Angriffe wie SQL Injections ausgelesen

werden können – zudem in unverschlüsseltem Klartext –, würden sie ihrer Verpflichtung nicht nachkommen. Dies war auch ein Grund dafür, dass die Angriffe auf Sony, die schon vor dem Auftauchen von LulzSec angefangen hatten, weithin nicht kritisiert wurden. Sony hatte sich als eine Firma erwiesen, die offenbar nicht in der Lage war, die geforderten Sicherheitsvorkehrungen zu treffen und deshalb – so zumindest die Ansicht – nicht zu Unrecht Opfer von Angriffen wurde.

Interessant ist, dass es trotz dieser verbreiteten Haltung Kritik am Vorgehen von LulzSec gab. Mehrfach wurde darauf verwiesen, dass er für Hackergruppen vollkommen berechtigt wäre, Sicherheitslücken aufzudecken und auszunutzen, aber nicht, diese Lücken weithin zu veröffentlichen oder gar Daten in großen Mengen zu leaken. Vielmehr sei es die Aufgabe, nachdem man die Sicherheitslücke entdeckt hätte, die Betreiber und Betreiberinnen darauf persönlich hinzuweisen und ihnen zumindest eine gewisse Zeit zu geben, um die Lücken zu schließen.

Nicht unwichtig scheint, dass bei den Veröffentlichungen von LulzSec und den anderen Hackergruppen, die implizite Forderung erhoben wurde, dass Individuen immerhin soweit für ihre eigene Sicherheit im Netz zuständig wären, nicht beständig die gleichen Passworte für unterschiedliche Accounts zu benutzen. Die Hacks, die sich dadurch ergaben, dass diese Regel missachtet wurde, wurden offenbar als berechtigt angesehen.

### ***Ist die Netiquette aktuell?***

Dieser letzte Verweis auf das richtige Verhalten von Hackern und Hackerinnen rekrutierte auf die Netiquette und Hackerethik, die sich vor allem in den 1980er und 1990er Jahren ausgeprägt und seitdem immer wieder betont wird. So unterschiedliche Personen und Initiativen wie der Richard Stallman und Linus Torvalds, der Chaos Computer Club, die GNU/Linux und die Mozilla-Community, 2600.net und Heise.de berufen sich auf diese Vorgaben, nach denen beispielsweise persönliche Angriffe zwar Beleidigungen, aber keine körperlichen Attacken oder über das Netz hinausgehende Rufschädigungen beinhalten dürften. Bestandteil dieser zum Teil verschriftlichten, zum Teil tradierten Richtlinien ist der Schutz persönlicher Daten und die Offenlegung anderer Daten.

Es gab auch in den letzten Jahren mehrfach Hinweise darauf, dass diese Etikette in den elektronischen Räumen in den 1980er Jahren – die geprägt waren durch relativ wenige Personen, die sich zudem oft persönlich kannten und zumeist einen universitären Hintergrund hatten – relevant war, aber nicht mehr für elektronische Räume gelten könne, an denen zumindest in den westlichen Staaten ein Großteil der Bevölkerung partizipiert.

LulzSec setzte sich mit seinem Handeln oft über diese Netiquette hinweg, ohne überhaupt auf sie zu referieren. Für die Gruppe schien vor allem die persönliche Motivation, dass ihnen eine bestimmte Aktion zusagen würde, ausreichend, um diese Aktion auch durchzuführen. Weit mehr noch verwies sie darauf, dass auch andere Menschen daran Spass hätten. Gleichwohl wurde die Aktivitäten der Gruppe immer wieder mit impliziten und expliziten Rückgriff auf die hergebrachte Netiquette bewertet. Offensichtlich wurde hier auch ein Deutungskampf ausgetragen, der vielleicht auch auf einen Generationenkonflikt innerhalb der Hackercommunity hindeutet. Klar wurde dabei, dass die Netiquette nicht mehr allgemein geteilt wird, gleichzeitig aber immer noch für eine Anzahl von Personen eine relevante Richtlinie zum Handeln in elektronischen Räumen darstellt.

### ***Ist der persönliche Spaß ein ausreichender Grund?***

Die Betonung von „Lulz“ bei einem Großteil der Aktionen von LulzSec lässt auch auf die Frage zurückschließen, ob diese Lulz alleine eine Aktion rechtfertigen können. Dabei sollte nicht vergessen werden, dass gerade solche nicht weiter begründeten Lulz auch die Rechtfertigung für andere Aktionen darstellen, beispielsweise die bekannten Flashraids in Groß- und Mittelstädten oder der massenhafte Besuch von eigentlich nicht-öffentlichen Veranstaltungen, die versehentlich bekannt werden, wie dies zu Beginn des Sommers 2011 in der deutschsprachigen Presse unter dem Begriff „Facebookparty“ thematisiert wurde.

Es ist auffällig, dass der Grund selber in der Diskussion nicht bestritten wurde. Nachdem LulzSec über die Angriffe auf fox.com hinausgegangen war und es klar wurde, dass ihre Ziele zumindest sehr unterschiedlich waren und keine reinen politischen Hintergrund hatten, wurde weithin akzeptiert, dass die Gruppe am persönlichen Spaß interessiert war. Die Diskussionen bezogen sich darauf, ob diese Lulz bestimmte Grenzen haben müssten und ob diese Grenzen überschritten wären. Eine oft vertretende Position berief sich, wie schon gezeigt, auf den Grundsatz, dass private Daten zu schützen wären, während die Offenlegung anderer Daten berechtigt wären. Gleichwohl etablierte sich keine eindeutige Position. Vielmehr scheinen die Aktionen von LulzSec dazu geführt zu haben, dass die unterschiedlichen Positionen zur in der Internet-Community verbreiteten Position „We did it for the Lulz“ offensichtlich wurden. Die gleiche Position war schon seit 2008 bei den Aktionen von Anonymous gegen die Scientology-Organisation vorgebracht worden, war dort aber – offenbar auch wegen der als unmoralisch angesehenen Zielsetzungen und Verhaltensweisen von Scientology selber – auf keine Kritik gestoßen.

Hingegen riefen die Aktionen von LulzSec immer wieder den Kommentar hervor, dass die Gruppe mit bestimmten Aktionen zu weit gegangen wäre. Auffällig war dabei, dass zum Beispiel der Angriff auf fox.com, auf Sicherheitsfirmen oder auf PBS nicht wirklich wegen solcher überschrittenen Grenzen kritisiert wurde, die Angriffe auf Spieleserver und die Veröffentlichung von privaten Daten von Nutzerinnen und Nutzern dieser Server schon. Offensichtlich wird diese Frage nach den Grenzen der Position, etwas vor allem deshalb zu tun, weil es Spass macht, auch in elektronischen Räumen in Zukunft weiter verhandelt werden müssen.

## Teil III: Schlussfolgerungen

Kuhlen, Wieglerling, Capurro und andere Autorinnen und Autoren postulieren, dass die von ihnen insbesondere bei Fragen des Copyrights und der Nutzung elektronischer Daten ausgemachte Informationsethik auch für Bibliotheken, Informationseinrichtungen sowie die Bibliotheks- und Informationswissenschaft relevant wären. Wenn der Umgang mit Daten auf ethischen Richtlinien beruht, die gesellschaftlich ausgehandelt werden, dann müssen sich auch Einrichtungen und die Wissenschaft, die sich mit diesen Daten beschäftigen, für diese Richtlinien interessieren. Diese Grundthese lässt sich auch auf Hacks und Netzaktivismus über die Fragen des Urheberrechts hinaus erweitern.

Die Aktionen von LulzSec und die Diskussionen über diese haben gezeigt, dass es offensichtlich ein ausreichend große Öffentlichkeit gibt, die – wenn auch nicht unbedingt reflektiert – Richtlinien entwickelt hat, die Angriffe und Leaks in elektronischen Räumen weit differenzierter bewertet, als mit einfacher Zustimmung oder Ablehnung. Offensichtlich haben sich Bewertungskriterien und -anforderungen etabliert, um Hacks als legitim oder nicht legitim zu bewerten. Gleichzeitig zeigten die Aktionen von LulzSec auch, dass diese Bewertungskriterien nicht allgemein geteilt werden – auch nicht von „schweigenden Mehrheiten“ – und sich sehr schnell wandeln können. Von besonderem Interesse sollte sein, dass LulzSec immer wieder für bestimmte Aktionen politische oder moralische Gründe angab, während sie im Allgemeinen den eigenen Spass als Hauptgrund verteidigten. Eine Durchsicht der Erklärungen von LulzSec selber vermittelt den Eindruck, dass das Stiften von Verwirrung Teil der Strategie der Gruppe war.

Sichtbar ist an diesen Auseinandersetzungen aber auch, dass Einrichtungen, die wie Bibliotheken den Anspruch erheben, Fähigkeiten für den Umgang in elektronischen Räumen zu vermitteln, sich nicht allein auf Recherchefähigkeiten konzentrieren dürfen. Die unterschiedliche Bewertung von Aktionen und die immer wieder erhobene Forderung nach Begründungen für diese Aktionen verweist darauf, dass die Öffentlichkeit eine sehr differenzierte Unterscheidung von Hacks und Leaks vorzunehmen bereit ist. So wird nach der Verhältnismäßigkeit und auch bestehenden Forderungen gefragt. Diese gesellschaftspolitisch motivierten Anfragen an Netzaktivismus wäre von Bibliotheken und Informationseinrichtungen zu unterstützen. Die Fragestellung, wer für welche Sicherheitslücken Verantwortung trägt, bedarf beispielsweise eines Grundlagenwissens über verschiedene Formen von Sicherheitslücken, Möglichkeiten zur Verhinderung derselben aber auch unterschiedliche technische Formen des Hackens. So äußerten sich in den Diskussionen um die

Aktionen immer wieder Teilnehmende irritiert davon, wenn DDoS-Attacken in der Presse als Hacks bezeichnet wurden, obgleich diese Attacken sich gerade dadurch auszeichnen, nicht auf die Daten der angegriffenen Server zuzugreifen. Ein solches Wissen zu erarbeiten und zu verbreiten könnte als Aufgabe von für die Öffentlichkeit zuständigen Einrichtungen wie Bibliotheken bezeichnet werden.

Gleichzeitig zeigten die Debatten um die Aktionen von LulzSec auch, dass zumindest von einem Teil der Öffentlichkeit das Handeln in elektronischen Räumen als Teil gesellschaftlich zu bewertender Kommunikation verstanden wird. Dies impliziert selbstverständlich die Aufgabe für die Bibliotheks- und Informationswissenschaft, auch dieses Bewertungen in die eigene Forschung mit einzubeziehen.

## Literatur

- Capurro, Rafael ; Wieglering, Klaus ; Brellocks, Andreas (Hrsg.) / Informationsethik (Schriften zur Informationswissenschaft ; 18). – Konstanz: Universitätsverlag Konstanz, 1995
- Kuhlen, Rainer / Informationsethik : Umgang mit Wissen und Information in elektronischen Räumen (UTB ; 2454). – Konstanz: Universitätsverlag Konstanz, 2004
- Kuhlen, Rainer / Erfolgreiches Scheitern – eine Götterdämmerung des Urheberrechts? (Schriften zur Informationswissenschaft ; 48). – Boizenburg: Verlag Werner Hülsbusch, 2008
- Spinner, Helmut F. ; Nagenborg, Michael ; Weber, Karsten / Bausteine zu einer neuen Informationsethik. – Berlin: Philo, 2001
- Wieglering, Klaus / Medienethik (Sammlung Metzler ; 314). – Stuttgart ; Weimar: Metzler, 1998

## Anhang I (Presstexte zu LulzSec)

Anmerkung: Die folgenden Artikel zu LulzSec aus Onlinemedien enthalten allesamt Diskussionsmöglichkeiten, die zur aktiven Zeit von LulzSec rege genutzt wurden. Diese Kommunikation wurde für den vorliegenden Text ausgewertet. Der letzte Zugriff zu allen in diesem Text angegebenen elektronischen Dokumenten fand am 10.07.2011 statt.

- Anderson, Nate / LulzSec manifesto: "We screw each other over for a jolt of satisfaction". – Arstechnica.com, 18.06.2011, <http://arstechnica.com/tech-policy/news/2011/06/lulzsec-heres-why-we-hack-you-bitches.ars>
- Ars Staff / Lulz? Sony hackers deny responsibility for misuse of leaked data. – Arstechnica.com, Juni 2011, <http://arstechnica.com/tech-policy/news/2011/06/lulz-sony-hackers-deny-responsibility-for-misuse-of-leaked-data.ars>
- Ars Staff / Week in tech: full speed ahead on the LulzBoat. – Arstechnica.com, 19.06.2011, <http://arstechnica.com/tech-policy/news/2011/06/week-in-tech-full-speed-ahead-on-the-lulzboat.ars>
- Bachfeld, Daniel / Einbruch in Online-Buch-Shop der NATO. – Heise.de, 24.06.2011, <http://www.heise.de/security/meldung/Einbruch-in-Online-Buch-Shop-der-NATO-1267139.html>
- Bright, Peter / Titanic Takeover Tuesday: LulzSec's busy day of hacking escapades. – Arstechnica.com, 15.06.2011, <http://arstechnica.com/tech-policy/news/2011/06/titanic-takeover-tuesday-lulzsecs-busy-day-of-hacking-escapades.ars>
- Bright, Peter / LulzSec rampage continues: 62k e-mails and passwords, CIA attacked. – Arstechnica.com, 23.06.2011, <http://arstechnica.com/security/news/2011/06/lulzsec-rampage-continues-62k-e-mails-and-passwords-cia-under-attack.ars>
- Bright, Peter / Dox everywhere: LulzSec under attack from hackers, law enforcement. – Arstechnica.com, 24.06.2011, <http://arstechnica.com/security/news/2011/06/dox-everywhere-lulzsec-under-attack-from-hackers-law-enforcement.ars>
- Bright, Peter / LulzSec's first Operation Anti-Security release: Arizona DPS. – Arstechnica.com, 25.06.2011, <http://arstechnica.com/security/news/2011/06/lulzsecs-first-operation-anti-security-release-arizona-dps.ars>

- Bright, Peter / LulzSec calls it quits, claims 50 days of mayhem was all it wanted. – Arstechnica.com, 26.06.2011, <http://arstechnica.com/security/news/2011/06/lulzsec-calls-it-quits-claims-50-days-of-mayhem-was-all-it-wanted.ars>
- Bright, Peter / LulzSec blamed for UK census theft, hacker arrest; LulzSec denies everything, 22.06.2011, <http://arstechnica.com/security/news/2011/06/lulzsec-blamed-for-uk-census-theft-hacker-arrest-lulzsec-denies-everything.ars>
- Bright, Peter / Lulz Security takes on Nintendo, FBI, Sony; FBI fights back?. – Arstechnica.com, Juni 2011, <http://arstechnica.com/security/news/2011/06/lulz-security-takes-on-nintendo-fbi-sony-fbi-fights-back.ars>
- Chen, Adrian / LulzSec Hacker Says He's Never Felt Safer. – Wired.com, 23.06.2011, <http://www.wired.com/threatlevel/2011/06/topiary/>
- Eikenberg, Ronald / LulzSec legt sich mit der CIA an. – Heise.de, 16.06.2011, <http://www.heise.de/security/meldung/LulzSec-legt-sich-mit-der-CIA-an-1261257.html>
- Eikenberg, Ronald / LulzSec außer Rand und Band : Eine Hackergruppe hinterlässt eine Spur der Verwüstung. – Heise.de, 16.06.2011, <http://www.heise.de/security/artikel/LulzSec-ausser-Rand-und-Band-1261669.html>
- Eikenberg, Ronald / Hacktivist knacken Datenbank von Sony Pictures. – Heise.de, 03.06.2011, <http://www.heise.de/security/meldung/Hacktivist-knacken-Datenbank-von-Sony-Pictures-1254485.html>
- Eikenberg, Ronald / US-Sender wegen WikiLeaks-Bericht gehackt. – Heise.de, 31.05.2011, <http://www.heise.de/security/meldung/US-Sender-wegen-WikiLeaks-Bericht-gehackt-1252676.html>
- Grüner, Sebastian / Angriff auf PBS nach Wikileaks-Doku. – Golem.de, 31.05.2011, <http://www.golem.de/1105/83862.html>
- Himmelein, Gerald / LulzSec hackt FBI-Liaison und Sicherheitsunternehmen. – Heise.de, 04.06.2011, <http://www.heise.de/security/meldung/LulzSec-hackt-FBI-Liaison-und-Sicherheitsunternehmen-1255276.html>
- Ihlenfeld, Jens / Lulzsec hört auf. – Golem.de, 26.06.2011, <http://www.golem.de/1106/84484.html>
- Ihlenfeld, Jens / Lulzsec veröffentlicht Polizeidokumente. – Golem, 24.06.2011, <http://www.golem.de/1106/84453.html>
- Ihlenfeld, Jens / Streit, Verrat und neue Kampfansagen. – Golem.de, 22.06.2011, <http://www.golem.de/1106/84381.html>
- Ihlenfeld, Jens / Mutmaßliches Lulzsec-Mitglied verhaftet. – Golem.de, 21.06.2011, <http://www.golem.de/1106/84359.html>
- Ihlenfeld, Jens / Lulzsec angeblich enttarnt. – Golem.de, 20.06.2011, <http://www.golem.de/1106/84311.html>
- Ihlenfeld, Jens / Lulzsec hackt FBI-Vermittler. – Golem.de, 05.06.2011, <http://www.golem.de/1106/83971.html>
- Ihlenfeld, Jens / Sony bestätigt Lulzsec-Hack. – Golem.de, 04.06.2011, <http://www.golem.de/1106/83967.html>
- Jurran, Nico / Hackergruppe LulzSec löst sich auf. – Heise.de, 26.06.2011, <http://www.heise.de/security/meldung/Hackergruppe-LulzSec-loest-sich-auf-1268063.html>
- Klaß, Christian / "Nyan-nyan-nyan-nyan, oder so...". – Golem.de, 17.06.2011, <http://www.golem.de/1106/84299.html>
- Klaß, Christian / Lulzsec nimmt sich Community vor. – Golem.de, 16.06.2011, <http://www.golem.de/1106/84264.html>
- Klaß, Christian / Lulzsec nervt. – Golem.de, 15.06.2011, <http://www.golem.de/1106/84219.html>
- Klaß, Christian / Lulzsec greift Eve Online, Minecraft und weitere Ziele an. – Golem.de, 14.06.2011, <http://www.golem.de/1106/84195.html>
- Klaß, Christian / Bethesda Softworks empfiehlt sofortigen Passwortwechsel. – Golem.de, 13.06.2011, <http://www.golem.de/1106/84160.html>
- Klaß, Christian / Sexwebseite gehackt und Nutzer bloßgestellt. – Golem.de, 13.06.2011, <http://www.golem.de/1106/84156.html>
- Klaß, Christian / Sony Pictures gehackt. – Golem.de, 03.06.2011, <http://www.golem.de/1106/83932.html>
- Klaß, Christian / Sonys nicht endender Alptraum. – Golem.de, 24.05.2011, <http://www.golem.de/1105/83688.html>
- Kravets, David / LulzSec Claims Another Sony Hack. – Wired.com, 06.06.2011, <http://www.wired.com/threatlevel/2011/06/lulzsec-sony-again/>

- Kuchera, Ben / LulzSec hackers demand hats, threaten release of Brink user data. – Arstechnica.com, 14.06.2011, <http://arstechnica.com/gaming/news/2011/06/hacker-group-lulzsec-demands-hats-threatens-release-of-brink-user-data.ars>
- Pluta, Werner / Teenager wird wegen DDoS-Attacken angeklagt. - Golem.de, 23.06.2011, <http://www.golem.de/1106/84431.html>
- Pluta, Werner / Lulzsec legt CIA lahm. – Golem.de, 16.06.2011, <http://www.golem.de/1106/84248.html>
- Pluta, Werner / Lulzsec hackt Website des US-Senats. – Golem.de, 14.06.2011, <http://www.golem.de/1106/84184.html>
- Poulsen, Kevin / LulzSec Releases Arizona Police Documents. – Wired.com, 24.06.2011, <http://www.wired.com/threatlevel/2011/06/lulzsec-arizona/>
- Poulsen, Kevin / British Police Swoop In on Possible LulzSec Suspect. – Wired.com, 21.06.2011, [http://www.wired.com/threatlevel/2011/06/lulzsec\\_bust/](http://www.wired.com/threatlevel/2011/06/lulzsec_bust/)
- Poulsen, Kevin / Sony Hit Yet Again; Consumer Passwords Exposed. – Wired.com, 02.06.2011, <http://www.wired.com/threatlevel/2011/06/sony-lulzsec/>
- Poulsen, Kevin / Hacktivists Scorch PBS in Retaliation for WikiLeaks Documentary. – Wired.com, 30.05.2011, <http://www.wired.com/threatlevel/2011/05/lulzsec/>
- Rötzer, Florian / Panikmache gegen Hacktivisten : Anonymous hat mit einem DDoS-Angriff die Website des französischen Atomkonzerns EDF kurzfristig lahmgelegt. – Telepolis, 06.06.2011, <http://www.heise.de/tp/artikel/34/34884/1.html>
- Steinlechner, Peter / Nintendo war im Visier der Hacker. – Golem.de, 05.06.2011, <http://www.golem.de/1106/83973.html>
- Wilkins, Andreas / Scotland Yard verhaftet mutmaßlichen Hacktivisten. – Heise.de, 21.06.2011, <http://www.heise.de/security/meldung/Scotland-Yard-verhaftet-mutmasslichen-Hacktivisten-1264601.html>
- Wilkins, Andreas / Hacker-Gruppen verbünden sich. – Heise.de, 21.06.2011, <http://www.heise.de/security/meldung/Hacker-Gruppen-verbueden-sich-1264215.html>
- Wilkins, Andreas / LulzSec hackt Website des US-Senats. – Heise.de, 14.06.2011, <http://www.heise.de/security/meldung/LulzSec-hackt-Website-des-US-Senats-1259601.html>

## Anhang II (Erklärungen von und zu LulzSec)

- LulzSec: Fox.com-Hack und Erklärung, 10.05.2011, <http://mirror.anapnea.net/lulzsec-fox.txt>
- LulzSec: Beschreibung des Hacks bei PBC, 30.05.2011, <http://pastebin.com/0YULt1ZG>
- LulzSec: Ankündigung des FuckFBIFriday, 03.06.2011, <http://pastebin.com/MQG0a130>
- LulzSec: Erklärung zu Karim und FBI, 04.06.2011, <http://pastebin.com/AjVd0L9E>
- LulzSec: Erklärung, dass PureElite nicht Teil von LuzSec sei, 06.06.2011, <http://pastebin.com/yut4P6qN>
- LulzSec: Erklärung zu Hack von Bethesda-Software und Senate.gov, 13.06.2011, <http://pastebin.com/i5M0LB58>
- LulzSec: Erklärung zum 1000. Tweet. 17.06.2011, <http://pastebin.com/HZtH523f>
- LulzSec: Erklärung zum Beitritt zur Operation antisecc, 19.06.2011, <http://pastebin.com/9KyA0E5v>
- LulzSec: Erklärung zum Ende von LulzSec, 26.06.2011, <http://t.co/GbAD070>
- The A-Team: Erklärung zu LulzSec, angeblich mit den Daten aller Mitglieder, 26.06.2011. <http://pastebin.com/iVujX4TR>