

Autor: Birk, Dominik/ Gröbert, Felix.

Titel: Web 2.0: Freund oder Feind?

Quelle: Lars Gräßer/ Monika Pohlschmidt (Hg.): Praxis Web 2.0 – Potenziale für die Entwicklung von Medienkompetenz. Schriftenreihe Medienkompetenz des Landes Nordrhein-Westfalen, Band 7. München 2007, S. 35-50.

Verlag: kopaed verlagsgmbh.

Die Veröffentlichung erfolgt mit freundlicher Genehmigung der Autoren und des Verlages. Die Schriftenreihe Medienkompetenz ist entstanden mit Mitteln des Landes NRW.

Dominik Birk/ Felix Gröbert

Web 2.0: Freund oder Feind?

Dieser Beitrag diskutiert Möglichkeiten der Sammlung, der Analyse und des Missbrauchs von Datenbeständen des Web 2.0. Es soll gezeigt werden, dass die Vernetzung der Web 2.0 Benutzerprofile und die Veröffentlichung von persönlichen Daten im Internet Identitätsdiebstahl fördert. Anschliessend wird diskutiert, wie die neue AJAX Technologie bei falscher Anwendung einem Angreifer neue Angriffspunkte im Web 2.0 liefert.

1 Einführung

„Es gibt keine Burg, die so stark ist, dass sie nicht mit Geld erobert werden kann“ sagte einst Marcus Tullius Cicero und er behält auch im Web 2.0 Zeitalter recht. Die Burgen der heutigen Zeit sind die Netzwerke der Web 2.0 Plattformen und die Schätze sind ihre Datenbanken.

100 Euro¹ soll dem Holtzbrinck Verlag der Datensatz eines Mitglieds der Studentenplattform StudiVZ.net wert sein. Mit einem solchen Kauf werden nicht nur potenzielle Kunden adressierbar, sondern auch ein Datenstamm gewonnen, der hilfreich für personalisiertes Marketing sein kann.

¹ Christian Stöcker: „Holtzbrinck schnappt sich StudiVZ“ (Online verfügbar unter: <http://www.spiegel.de/netzwelt/web/0,1518,457536,00.html>, zugegriffen am 12. März 2007).

Die goldenen Datenbanken werden nicht nur zum Marketing genutzt, sondern könnten auch als Informationsvorsprung von Unternehmen genutzt werden, um Arbeitssuchende genauer einzuschätzen und um Konkurrenten gegenüber eine bessere Verhandlungsbasis zu erlangen. Staatliche Dienste sind vor allem im Rahmen der Terrorprävention nach dem 11. September 2001 an Datensätzen und Datenrelationen Sozialer Netzwerke interessiert.

Es verwundert daher nicht, dass Cracker versuchen, die Burgen auch ohne Geld zu erobern und die wertvollen Datensätze zu stehlen. Wenn die Cracker nicht in die Server einbrechen können, kopieren sie die öffentlich verfügbaren Daten der Sozialen Netzwerke im Web 2.0. Sie nutzen den Datenbestand, um personalisierten Spam oder Phishing E-Mails zu versenden. Zudem könnten die Datenbestände an Personen aus dem organisierten Verbrechen verkauft werden, um Identitätsdiebstahl zu betreiben. Als Identitätsdiebstahl wird die missbräuchliche Nutzung personenbezogener Daten einer natürlichen Person durch Dritte bezeichnet.²

Unser Beitrag

Das Web 2.0 bietet vielfach neue Angriffspunkte. Wir klassifizieren im Folgenden den nicht-technischen Impersonifikationsangriff, das Spear Phishing und die Rasterfahndung, und erläutern, wie Web 2.0 Anwendungen anfällig für Cross-Site Scripting und Cross-Site Request Forgery werden können.

2 Nicht-technische Sicherheitsherausforderungen

2.1 Datenschutz in Sozialen Netzwerken

Der Begriff des Sozialen Netzwerkes stammt ursprünglich aus der Ethnosoziologie und beschreibt in Hinsicht auf das Web 2.0 Plattformen, die ihren Anwendern ein „Bekanntschaffennetzwerk“ als virtuelles Interaktionsgeflecht anbieten. Dies bedeutet, dass man als registrierter Benutzer ein Profil erstellen kann, das sowohl persönliche als auch unpersönliche Daten beinhaltet. Je nach Wahl ist das Datenprofil für jeden Benutzer

² „Identitätsdiebstahl“, In: „Wikipedia, Die freie Enzyklopädie“ (Online verfügbar: <http://de.wikipedia.org/wiki/Identit%C3%A4tsdiebstahl>, zugegriffen am 12. März 2007).

oder auch nur einen beschränkten Nutzerkreis zugänglich. Der Zielgruppe entsprechend kann man über die Plattform dann persönliche und geschäftliche Kontakte pflegen.

Soziale Netzwerke im Internet sind daher auch eine Alternative für bereits bestehende Kommunikationsmöglichkeiten wie E-Mail und Instant-Messaging. Positiv festzustellen ist, dass durch Soziale Netzwerke Kontakte hergestellt und gepflegt werden können. Sie bringen jedoch auch negative Aspekte mit sich.

Der Datenschutz in Sozialen Netzwerken und die Veröffentlichung von persönlichen Informationen wird gerade bei der jüngeren Generation oftmals unterschätzt. Daten wie das Geburtsdatum, die politische Gesinnung und der Arbeitgeber werden ohne Skrupel im Internet veröffentlicht. Datenschutztechnisch sind diese Informationen jedoch als kritisch einzustufen. Das Verbrechen Identitätsdiebstahl, das in den USA und weiteren hochtechnisierten Ländern eine der am schnellsten wachsenden Kriminalitätsformen ist³, könnte auch in Deutschland bald zunehmen.

Wie der Kryptograph Bruce Schneier schon sagte⁴, verliere man jedes Mal, wenn Daten auf einem Computer gespeichert würden, eine gewisse Kontrolle über diese Daten. Stelle man sie allerdings ins Internet, verliere man auch das letzte Stück Kontrolle.

Leider ist jedoch festzustellen, dass bei den derzeitigen Web 2.0 Nutzern so gut wie kein Bedürfnis nach Datenschutz zu vermerken ist. Es werden lediglich die Vorteile großer Plattformen gesehen, die Nachteile aber meist aufgrund von Unwissenheit ausgeblendet. Mit den neuen Web 2.0 Plattformen sind wir dem *gläsernen Nutzer* unbewusst einen entscheidenden Schritt näher gekommen. Der Begriff *Datenarmut*, der ursprünglich aus dem Teledienstschutzgesetz (TDDSG) stammt, bezeichnet die Beschränkung von Datenerhebung und -verarbeitung auf das unbedingt notwendige Maß⁵.

Bei dem derzeitigen Web 2.0 Wachstum ist nicht zu vernachlässigen, dass es sich bei falscher Anwendung um eine Dystopie handeln könnte, gegen die andere datenschutzkritische Technologien vergleichsweise unproblematisch sind.

3 FBI: „How to Protect Your Good Name from Identity Theft“ (Online verfügbar unter: <http://www.fbi.gov/page2/oct04/preventid102104.htm>, zuletzt erreicht am 12. März 2007).

4 Bruce Schneier: „Lessons From the Facebook Riots“ (Online verfügbar unter: <http://www.schneier.com/essay-127.html>, zuletzt erreicht am 12. März 2007).

5 Deutscher Bundestag: Drucksache 13/7500 vom 16.04.1997 (Online verfügbar unter: <http://dip.bundestag.de/btd/13/075/1307500.asc>, zuletzt erreicht am 12. März 2007).

Um persönliche Informationen im Netz zu missbrauchen, sind Relationen zwischen den Benutzerprofilen hilfreich, die das Kontaktumfeld des Benutzers beschreiben. Diese Relationen werden bei vielen Web 2.0 Plattformen automatisch mitgeliefert. Die Herausforderung für den Angreifer ist es, die Daten zusammenzutragen und auszuwerten.

2.1.1 Data-Mining Problematik

Michael J.A. Berry und Gordon Lindoff haben den Begriff *Data-Mining* unter anderem in Hinsicht auf die Betriebswirtschaft definiert als „Exploration und Analyse großer Datenmengen mit automatischen oder semiautomatischen Werkzeugen, um bedeutungsvolle Muster und Regeln aufzufinden“⁶. Wir verwenden den Begriff in Bezug auf die Aggregation von Anwenderprofilen in Web 2.0 Plattformen. Zusätzlich wollen wir Muster erkennen, indem wir statistisch-mathematischer Methoden auf den Web 2.0 Datenbestand anwenden.

Viele Benutzerprofile verschiedener Web 2.0 Anwendungen wie Profilverzeichnisse, Persönlichkeitsplattformen und Weblogs sind gewünscht frei verfügbar und für jeden Besucher im Internet oder für registrierte Benutzer der Plattform zugänglich. Ein Angreifer kann somit Programme schreiben, sogenannte *Crawler* (engt. Raupe), die selbstständig und voll automatisiert Profile von Web 2.0 Plattformen sammeln und diese in Datenbanken speichern.

Mit gängigen Data-Mining Analysetechniken wie der Clusteranalyse, dem Klassifikationsverfahren und der Regressionsanalyse gewinnen Unternehmen wichtige Informationen, beispielsweise für das Marketing und die Selektion von Zielgruppen eines neuen Produktes⁷. Studentenplattformen⁸ sind hierbei hochwertige Ziele, da man annehmen kann, dass die Zielgruppe zukünftig ein zahlungskräftiger Kunde sein wird.

6 Michael J.A. Berry and Gordon Lindoff: „Data Mining Techniques for Marketing, Sales and Customer Support“, John Wiley & Sons, 1997.

7 Adomavicius, Tuzhilin: „Using Data Mining Methods to Build Customer Profiles“ (Online verfügbar unter: <http://www.cs.pitt.edu/~mrotaru/comp/rs/Adomavicius%20IEEE%202001pdf>, zuletzt erreicht am 12. März 2007).

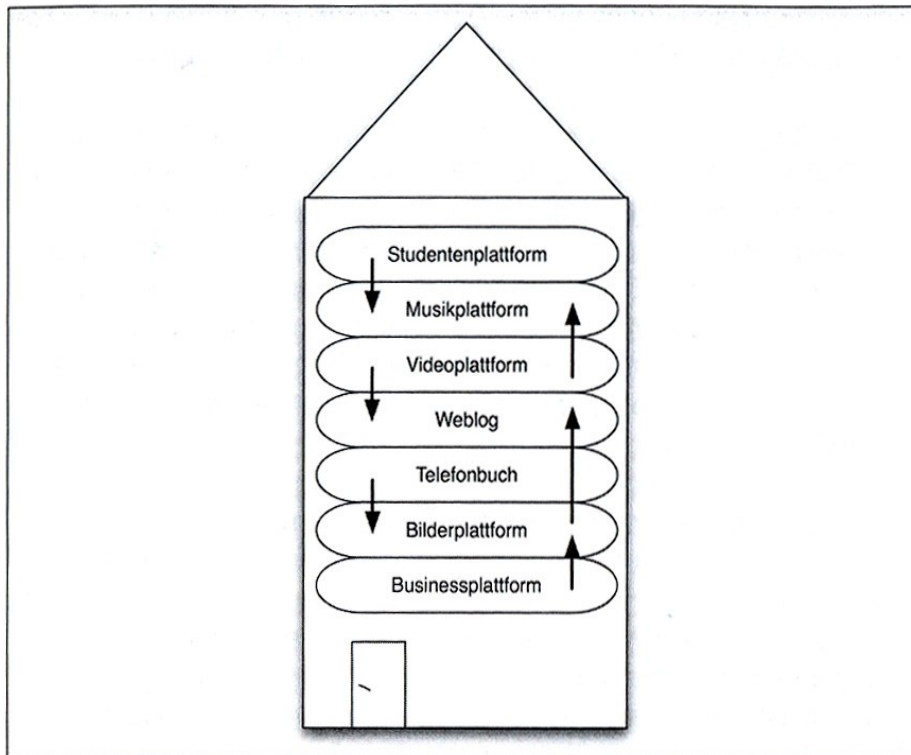
8 „studiVZ - das Studiverzeichnis“ (online verfügbar unter: <http://www.studivz.net>, zuletzt erreicht am 12. März 2007).

Aber nicht nur die Wirtschaft könnte von diesen frei verfügbaren Persönlichkeitsdarstellungen profitieren. Wir sehen im Folgenden zwei Problematiken, die aus dem Besitz eines solchen Datenbestandes hervorgehen könnten. Zum einen lassen sich mit Profilen und den zugehörigen Relationen zwischen Profilen individuell angepasste Phishing-Angriffe realisieren, das sogenannte *Spear Phishing*⁹. Zum anderen lässt sich anhand dieser Profildatenbanken eine Form der Rasterfahndung realisieren, mit der z. B. Arbeitgeber ihre zukünftigen Arbeitnehmer unter die Lupe nehmen können.

Die Frage, wie ein potenzieller Angreifer, Phisher oder Rasterfahnder an die personenbezogenen Daten gelangt, wird nun im Folgenden geklärt. Als erstes werden mit Hilfe der oben genannten Crawler die Datenbestände verschiedener Web 2.0 Anwendungen soweit wie möglich kopiert. Anschließend wird versucht, die einzelnen Profile in den Datenbanken durch Abgleichen mit anderen Datenbanken zu vervollständigen. Dafür muss man sich das Soziale Netzwerk als einen Graphen vorstellen, mittels dessen die einzelnen Teilnehmer durch Knoten und die Relation zwischen diesen Teilnehmern durch Kanten dargestellt werden. Wenn jede kopierte Datenbank einer Web 2.0 Plattform einen Graphen darstellt, kann man sich alle Graphen übereinander als ein Hochhaus vorstellen.

Um nun einzelne Profile einer Person zu vervollständigen, sucht man zu dem zugehörigen Knoten in einer Etage den synonymen Knoten in einer anderen Etage. Unterstützt wird der Angriff von vielen Benutzern, die sich nicht nur auf eine Web 2.0 Plattform beschränken. Auf der einen Plattform pflegt man Kontakte zu Freunden und veröffentlicht ein Profil, auf einer anderen Plattform archiviert man persönliche Bilder und Musik und auf einer weiteren schreibt man in einem Weblog über seine täglichen Erlebnisse. Die Schwierigkeit der Profilvervollständigung liegt darin, für eine Person synonyme Knoten in verschiedenen Etagen zu finden. Ist dies möglich, lässt sich das vollständige Profil eines Menschen mit den Daten, die im Netz über ihn verfügbar sind, wie ein Mosaik zusammensetzen. In den nächsten beiden Kapiteln beleuchten wir Angriffe, die als negative Anwendung der verfügbaren Datenbestände ausgeführt werden können.

9 Microsoft: „Was ist Spear Phishing?“ (Online verfügbar unter: <http://www.microsoft.com/germany/athome/security/email/spear-phishing.mspx>, zuletzt erreicht am 12. März 2007).



2.1.2 Spear Phishing

Eine bisher noch nicht aufgetretene Möglichkeit, durch Profilaggregation von Web 2.0 Anwendungen individuell angepasste Phishing-Angriffe auf die Benutzer zu realisieren, ist das sogenannte *Spear Phishing*. Bei einem Phishing Angriff wird der Internetbenutzer auf eine fingierte Webseite (Phishing-Seite) gelockt, die der Originalseite ähnelt, um private Informationen preiszugeben. Ein Phisher missbraucht diese Daten, um sich illegal Zugang zu den Konten der Opfer zu verschaffen, beispielsweise Online Banking Konten. Im Falle von Spear Phishing mit Web 2.0 Profilinformatoren nutzt der Angreifer die frei verfügbaren Informationen auf Web 2.0 Plattformen um ein Opfer auf eine gefälschte Webseite zu locken.

Durch die in Abschnitt 2.1 beschriebenen Relationen zwischen verschiedenen Profilen, die in Sozialen Netzwerken offengelegt werden, kann der Angreifer nun leicht ausmachen, wem das Opfer vertraut oder bekannt ist. Und welcher Nachricht würde das Opfer mehr vertrauen als der eines guten Freundes oder einer guten Freundin? Genau diese Tatsache macht sich der Angreifer zu Nutze indem er im Relationsgraphen einen Knoten

bzw. ein Opfer mit einem möglichst hohen lokalen Clusterkoeffizienten¹⁰ auswählt. Der lokale Clusterkoeffizient sollte daher möglichst hoch sein, um idealerweise ein Opfer mit vielen Freunden auszuwählen, die sich aber zusätzlich untereinander noch kennen. Sieht man nun diesen Knoten mit benachbarten Freunden als einen Teilgraphen, sind alle Knoten des Teilgraphs potenzielle Opfer des Phishers. Der Angreifer wird versuchen, einen Teilgraphen mit Opfern auszuwählen, der so weit wie möglich einem vollständigen Graphen¹¹ ähnelt.

Um nun die Opfer auf eine gefälschte Webseite zu locken, versucht der Angreifer in der übermittelten Nachricht (z. B. E-Mail, Private Nachricht über Web 2.0 Plattform) eine Vertrauenssituation zu erwecken. Zum Beispiel:

Hallo *Vorname*
hier ist *Freund-B*. *Freund-C* hat mir
folgenden Link von *Freund-D* geschickt.
Schau dir das doch mal an, ist super! Wie
war's beim *Hobby*?

Er schickt Person A eine Nachricht im Namen von Person B und erwähnt darin Personen C und D. Personen B, C und D sind alles Freunde von Person A. Für Person B, wobei hier der Absender Person A ist, verfährt der Angreifer analog, wobei Personen C, D und E ebenfalls erwähnt werden. Nach diesem Prinzip schreibt er nun alle Knoten in einem Teilgraphen an.

Durch die Erwähnung von Freunden versucht der Angreifer Vertrauen zu schaffen und dem Opfer eventuelle Skepsis bezüglich des mitgeschicktem Links zu nehmen. Im Falle einer Übertragung der gefälschten Nachricht per E-Mail kann er leicht den Absender fälschen, da SMTP, das Protokoll zum Versenden von E-Mails, keinerlei Authentifikationsmechanismen für die E-Mail Absenderadresse spezifiziert. Selbst erfahrenere Internetnutzer laufen so Gefahr, Opfer einer Spear Phishing Attacke zu werden. Die Art von Spear Phishing, die wir erläuterten, nutzt also das bereits bekannte Prinzip des Phishing, jedoch mit verfeinerter, opferbezogener Methodik.

¹⁰ Der Begriff lokaler Clusterkoeffizient stammt aus der Graphentheorie und gibt ein Maß für den Grad der Verknüpfung des Knotens in einem Graphen an.

¹¹ In einem vollständigen Graphen ist jeder Knoten mit jedem anderen Knoten über eine Kante verbunden.

Auch personenbezogene Werbung bzw. Spam kann so leicht und effizient erstellt werden. Auf vielen Web 2.0 Profilplattformen werden gerne bevorzugte Freizeitaktivitäten im persönlichen Profil mit angegeben. Diese Informationen können nun genutzt werden, um Spam zu erzeugen, der sich auf die Freizeitaktivität bezieht. Oben wurde bereits eine Möglichkeit beschrieben wie dem Opfer die Skepsis genommen wird auf den manipulierten Link zu klicken (vgl. Kapitel 3.2). Somit kann durch personenbezogenen Spam leicht und effizient versucht werden, ein Produkt zu verkaufen.

2.1.3 Rasterfahndung

Die Rasterfahndung ist ein in den 70er Jahren vom damaligen BKA-Präsidenten Horst Herold entwickeltes Verfahren zur vernetzten Durchsuchung von Datenbeständen. Wir verwenden den Begriff der Rasterfahndung in Zusammenhang mit der individuellen Suche nach Hintergrundinformationen über eine Person. Diese Hintergrundinformationen erhalten wir durch die Datenbestände von Web 2.0 Plattformen.

Anwendung findet dieses Verfahren z. B. bei der Überprüfung eines zukünftigen potenziellen Mitarbeiters durch den Arbeitgeber vor der offiziellen Einstellung. Der Arbeitgeber als Rasterfahnder kann sich im Vorhinein ein Bild über das soziale Umfeld und die Vergangenheit seines künftigen Mitarbeiters machen.

Beginnen kann diese Untersuchung durch das „googlen“ des vollständigen Namens. Dann kann in Sozialen Netzwerken weitergesucht werden und ein vollständiger Profilabgleich in vorhanden Datenbanken durchgeführt werden.

Der gern genutzte Ausdruck „*im Internet geht nichts verloren*“ kann man in diesem Zusammenhang als Nachteil sehen. Denn, was einmal ins Netz gestellt wurde, von einem Crawler erfasst und kopiert wurde, ist unlösbar. So wird zum Beispiel der zukünftige Kandidat für eine Managerposition bei einem renommierten Autohersteller sich in 5 Jahren höchstwahrscheinlich darüber ärgern, dass er während seiner Studienzeit doch so freizügig auf Studentenplattformen Bilder von Wochenend-Exzessen veröffentlichte. Die oben bereits erwähnten Crawler haben auch diesen Datenbestand in Datenbanken kopiert, die überall auf der Welt verteilt plaziert sind.

Auf manchen Plattformen reicht es schon aus, nur ein Profil zu besitzen. Bilder werden dann von anderen Freunden hochgeladen und durch neue Webtechnologien kann im Bild

selbst das Gesicht auf das entsprechende Profil verweisen. So besitzt der Web 2.0 Benutzer nicht einmal mehr die technische Kontrolle darüber, wann und wie Bilder von ihm online gestellt werden.

In Zeiten der präventiven Terrorbekämpfung nach dem 11. September 2001 haben auch Nachrichtendienste Interesse an Sozialen Netzwerken und ihren Datenbeständen bekommen¹²: So investiert die NSA, die sich schon immer ein „relationales, semantisches Internet“ wünschte, in die Aufbereitung von Web 2.0 Datenbeständen zum angeblichen Schutz der nationalen Sicherheit. Es lässt sich aber leicht ableiten, dass der NSA in dieser Hinsicht sicherlich noch ein paar mehr Möglichkeiten offen stehen als den gängigen Crawlern.

In diesem Kontext ist es mehr als wahrscheinlich, dass Unschuldige in das Visier von Fahndungsbehörden kommen, da die Intensität des Kontakts zwischen zwei Personen auf einer Sozialen Netzwerk Plattform nicht klar ersichtlich ist. Es besteht daher die Gefahr, dass eine Person aufgrund ihres möglicherweise großen Umfeldes pauschal verdächtigt wird und somit der Gefahr der Beweislastumkehr ausgesetzt ist. Unter diesen Umständen ist es schwierig zu beweisen, jemanden nur flüchtig oder gar nicht zu kennen.

3 Technische Sicherheitsprobleme

3.1 Input Validation

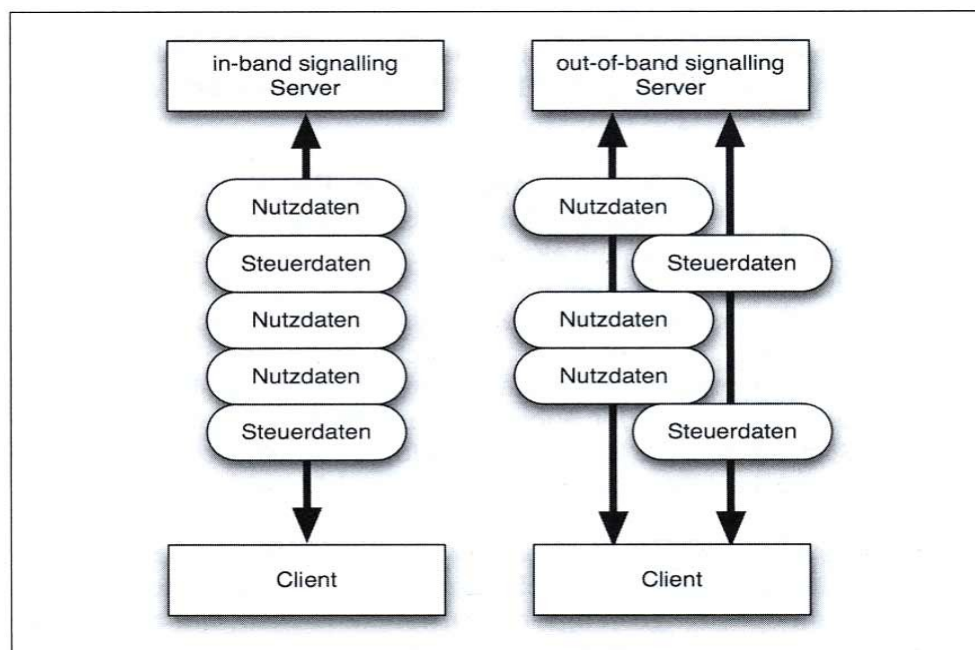
Seitdem 1971 in den USA offiziell bekannt wurde, dass durch das Pfeifen eines 2600 Hertz Tons in ein Telefon Gespräche kostenlos geführt werden können, ziehen sich *input validation* Fehler wie ein roter Faden durch die Geschichte der Computersicherheit. Als man damals mit der Spielzeug-Pfeife aus einer Frühstücksflockenpackung den 2600 Hertz Ton erzeugte¹³, und ein Telefon diesen Ton aufnahm, signalisierte der Ton der Vermittlungsstelle, dass ein neues – kostenfreies – Gespräch initiiert werden soll. Befehle an die Vermittlungsstelle wurden somit über den gleichen Kanal geschickt wie das

12 Paul Marks: „Pentagon sets its sights on social networking websites“ (Online verfügbar unter: <http://www.newscientisttech.com/article/mg19025556.200-pentagon-sets-its-sights-on-social-networking-websites.html>, zuletzt erreicht am 12. März 2007).

13 Gary D. Robson: „The Origins of Phreaking“ (Online verfügbar unter: <http://www.robson.org/gary/writing/phreaking.html>, zuletzt erreicht am 12. März 2007).

Gespräch des Kunden. Diese Technik wird *in-band signalling* genannt und wurde von den Telefonanbietern durch die *out-of-band signalling* Technik abgelöst, die das kostenlose Telefonieren auf die oben genannte Weise schwieriger machte.

Ein *input validation* Fehler tritt auf, wenn Nutzdaten (Telefongespräche) und Steuerdaten (Vermittlungsstellensignale; Wahl einer Nummer) über den gleichen Kanal gesendet werden und keine klare Trennung durch den Empfänger (Vermittlungsstelle; Server) durchgeführt werden kann. Ein Angreifer ist somit in der Lage gezielt manipulierte Nutzdaten zu senden, die von dem Empfänger als Steuerdaten interpretiert werden. Dadurch kann er die Logik des Empfänger-Systems beliebig beeinflussen.



Das Empfänger-System sollte dem Benutzer somit immer misstrauen und alle Benutzereingaben daraufhin überprüfen, dass die Daten keine für das System schadhaften Datenwörter enthalten.

Dass dabei auch die Länge der Eingaben überprüft werden muss, wurde 1988 bekannt, als einer der ersten Internetwürmer, der Morris Wurm, mehrere Schwachstellen in Netzwerkdiensten ausnutzte. Das Charakteristische dieser Schwachstellen war, dass Benutzereingaben zwar angenommen, ihre Länge jedoch nicht überprüft wurde. Somit

war es möglich durch sehr lange Nutzdaten, die am Ende Steuerbefehle enthielten, Teile der Netzwerkanwendung zu überschreiben. Die so genannten *buffer overflow* Fehler werden heute immer noch ausgenutzt und sind das Paradebeispiel für mangelnde Überprüfung der Benutzereingaben.

3.2 Cross-Site Scripting

Cross-site scripting (XSS) Fehler sind die input validation Fehler der heutigen Zeit. Im Jahr 2006 waren 21,5% der gemeldeten Schwachstellen XSS Fehler¹⁴.

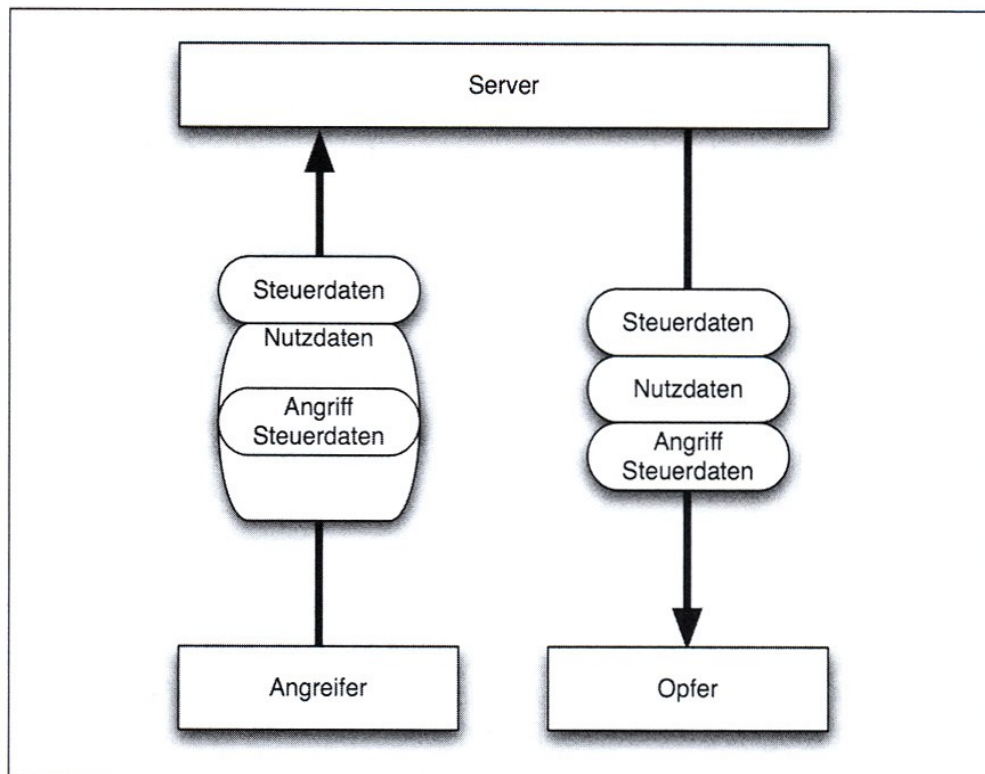
Durch einen XSS Fehler kann der Angreifer zum Beispiel die Darstellung einer Internetseite manipulieren. Die Voraussetzung hierfür ist, dass eine Internetseite Benutzereingaben akzeptiert, zum Beispiel eine Suchanfrage, und daraufhin eine dynamische Seite mit den Suchergebnissen generiert. Falls die Webanwendung die Benutzereingaben nicht ausreichend validiert, kann der Angreifer Steuerbefehle in die Suchanfrage einbetten und somit die Darstellung ändern. Praktisch bedeutet Validieren zum Beispiel, dass HTML Steuerbefehle aus der Suchanfrage entfernt werden müssen, da sonst die Suchantwort, die HTML Steuerbefehle enthält, welche wiederum die Darstellung der Internetseite manipulieren können.

Da die meisten Webanwendungen dynamische Antworten generieren, ist ein Großteil der XSS Fehler nicht persistent, d. h. ein Benutzer muss erst auf einen speziell gefertigten Internetlink klicken, um auf die verfälschte Seite zu gelangen. Ein persistentes XSS hingegen könnte in einem Diskussionsfaden eines Internetforums die Loginfelder so abändern, dass das im Loginfeld eingegebene Passwort an den Angreifer gesendet wird.

Daher sind XSS Fehler gerade für Phisher attraktiv. Ein Internetlink, der auf eine verfälschte Seite einer verwundbaren Bank verweist, funktioniert selbst unter dem als sicher geltenden HTTPS (TLS/SSL) Protokoll, welches die Anwendungsdaten verschlüsselt und authentifiziert überträgt.

Dies eröffnet dem Phisher die Möglichkeit PINs und TANs zu stehlen, obwohl in der Adresszeile des Webbrowsers eine gültige Bank HTTPS URL steht.

¹⁴ Steven M. Christey: „Vulnerability Type Distribution in CVE“ (Online verfügbar unter: <http://www.attrition.org/pipermail/vim/2006-September/001032.html>, zuletzt erreicht am 12. März 2007).



In der jüngeren Vergangenheit war jede große Internetseite betroffen: der Phishmarkt¹⁵ zeigte, dass 33 österreichische und 48 deutsche Banken zwischen Oktober 2006 und Januar 2007 für XSS Angriffe verwundbar waren.

3.3 Cross-Site Request Forgery

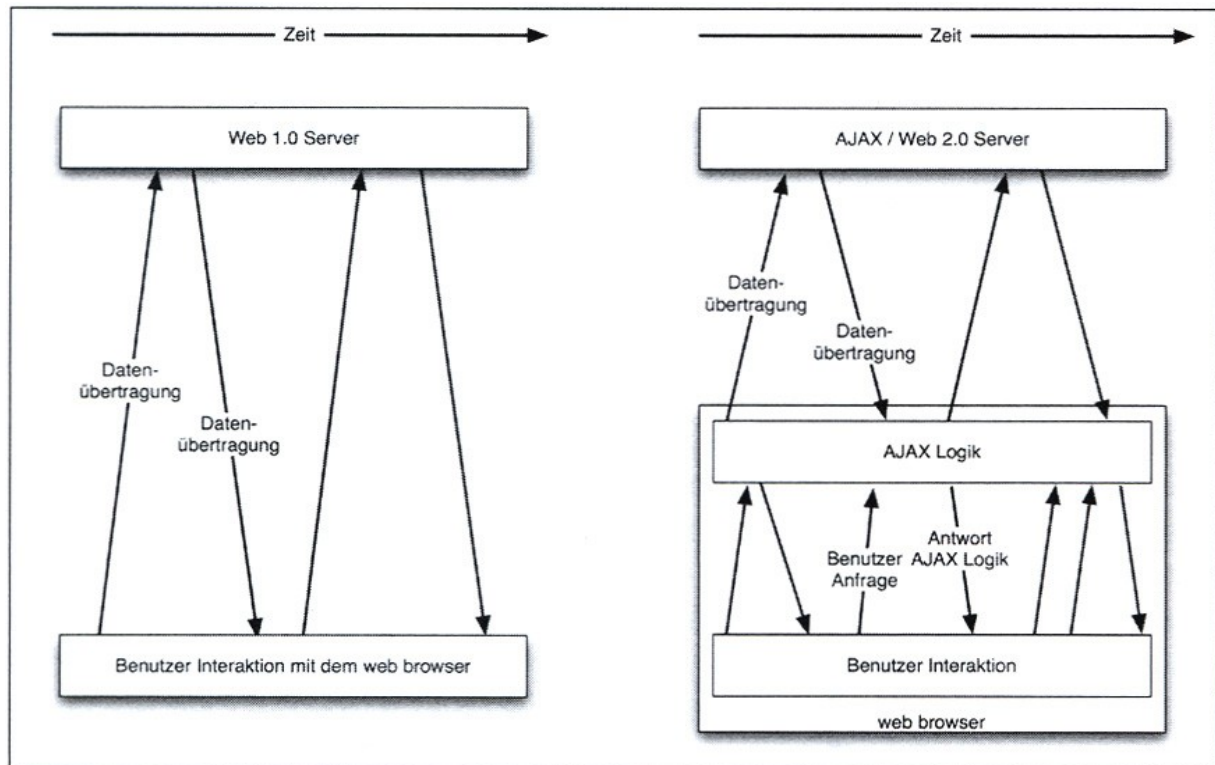
Durch die Web 2.0 Technologie AJAX werden XSS Fehler gefährlicher. Mit AJAX wird eine weitere Ebene eingeführt, die Computer-Logik enthält.

Diese Ebene fungiert als „Mittelsmann“ für Steuerbefehle und Nutzdaten zwischen Server und Browser.

Sollte eine AJAX Webanwendung von einem XSS Fehler betroffen sein, ist es nicht nur möglich, die Darstellung der Internetseite zu manipulieren, sondern auch komplexere Steuerbefehle abzusenden, ohne dass der Benutzer es bemerkt. Diese Steuerbefehle werden dann im Namen des Benutzers abgesendet, der die durch den Angreifer per XSS

¹⁵ SkyOut: „Phishmarkt“ (Online verfügbar unter: <http://baseportal.com/baseportal/phishmarkt/de>, zuletzt erreicht am 12. März 2007).

manipulierte Internetseite betrachtet. Diese Technik wird *cross-site request forgery* (XSRF) genannt.



Steuerbefehle können je nach Webanwendung variieren. Auf einer großen Internetplattform, die Möglichkeiten zur Pflege des Sozialen Netzwerkes und auch zur Veröffentlichung von Musik bietet, kann man zum Beispiel einen Freund zu dem persönlichen Profil hinzufügen oder die persönliche Homepage bearbeiten. Durch diese Aktionen werden Steuerbefehle gesendet. So kam es, dass auf einer großen Musikplattform ein XSS Fehler ausgenutzt wurde, um den schnellsten Virus der Computergeschichte zu schreiben: Der Angreifer veröffentlichte den Virus auf seiner persönlichen Homepage innerhalb der Plattform. Der Virus nutzte den persistenten XSS Fehler aus, um den angemeldeten Besucher der „infizierten“ Homepage schadhafte Steuerbefehle ausführen zu lassen. Durch den XSS Fehler interpretierte der Browser des Besuchers die in der Schadensfunktion enthaltenen Steuerbefehle als legitime Befehle seitens der Musik Plattform. Die Schadensfunktion wurde unbemerkt ausgeführt und enthielt zwei Steuerbefehle:

1. kopiere die Schadensfunktion in die persönliche Homepage des Besuchers
2. füge den Benutzernamen des Angreifers zu der Liste der eigenen Freunde hinzu.

Auf diese Weise verbreitete sich der Virus lawinenartig schnell und innerhalb von 24 Stunden hatte der Benutzername des Angreifers eine Million Freunde¹⁶.

Der Angreifer wollte die Möglichkeiten der Sicherheitslücke humorvoll zeigen; er hätte auch Passwörter stehlen oder einen Angriff auf die Verfügbarkeit (*denial of service*) eines kleineren Internetwettbüros ausüben können.

4 Fazit

Die erweiterte Logik der AJAX Ebene ermöglicht Positives wie auch Negatives. Wenn ein XSS Fehler existiert, kann die Macht der neuen Technik auch vom Angreifer ausgenutzt werden. Mittels der AJAX Logik können Viren geschrieben werden, die unbemerkt den Browser für die Zwecke der Angreifer manipulieren. Hinzu kommt, dass die Geschichte zeigt, dass sich Fehler in den modernen Web 2.0 Plattformen wiederholen. Jedoch ist das Potenzial der Angreifer gestiegen: sie haben den Vorteil, aus vielen verwundbaren Zielen aussuchen zu können und die erbeuteten Daten auf verschiedene Weise zu verwerten. Spam, Phishing und Identitätsdiebstahl sind hier einige Methoden der Kriminellen. Aber die Daten können auch durch Marketing- oder Assessment-Firmen gekauft werden, was ein enormes Datenschutzproblem für unaufgeklärte Benutzer darstellt.

Der Sinn für Datensparsamkeit der Anwender muss daher durch Aufklärung geschärft werden. Der Dienstanbieter, in diesem Fall der Betreiber der Web 2.0 Plattform, muss sich seiner Verantwortung bewusst werden und mit der Aufklärung der Nutzer über Gefahrenpotenziale beginnen. Es müssen Gesetze erlassen werden, die die Betreiber in ihre gesetzliche Schranken weisen.

Allerdings verhält sich der Faktor Spaß mit Web 2.0 Plattformen umgekehrt proportional zur Datensparsamkeit. Es muss daher ein vernünftiger Konsens zwischen der Veröffentlichung von persönlichen Daten und dem Nutzen von Web 2.0 Anwendungen gefunden werden.

¹⁶ Quinn Norton: „Ajax prepares for battle an the dark side“ (Online verfügbar unter: <http://technology.guardian.co.uk/weekly/story/O.,1726234,00.html>, zuletzt erreicht am 12. März 2007).

Leider ist die Akzeptanz von Seiten der Nutzer wie auch von Seiten der Anbieter von Web 2.0 Plattformen für den Datenschutz nicht sehr groß, da sich der Missbrauch auf diesem Gebiet noch in Grenzen hält.

Gestern wurde – heute und morgen wird – der Grundstein für eine Überwachung über das Internet gelegt, die für den durchschnittlichen Benutzer nicht im Bereich des Vorstellbaren liegt. Es muss jetzt gehandelt, der Nutzer aufgeklärt und die grenzenlose Veröffentlichung von persönlichen Daten gestoppt werden. Denn nur solange das Bedürfnis nach Privatsphäre in unserer Gesellschaft noch existiert, können wir der totalen Überwachung entgehen.

Alle Rechte, insbesondere das Recht der Vervielfältigung und Verbreitung sowie der Übersetzung, vorbehalten. Kein Teil des Werkes darf in irgendeiner Form (durch Fotokopie, Mikrofilm oder ein anderes Verfahren) ohne schriftliche Genehmigung des Rechteinhabers reproduziert oder unter Verwendung elektronischer Systeme weiterverarbeitet, vervielfältigt oder verbreitet werden.