Hannes Federrath, Karl-Peter Fuchs, Dominik Herrmann, Daniel Maier, Florian Scheuer, Kai Wagner

Grenzen des „digitalen Radiergummis“

Der Beitrag zeigt die prinzipiellen und technischen Untauglichkeiten der Durchsetzung des Konzepts eines „digitalen Radiergummis“ auf, mit dem Inhalte im Internet mit einem Verfallsdatum versehen und somit zeitlich begrenzt zugänglich gemacht werden sollen.

1 Einleitung

In den letzten Jahren hat die Verbreitung von persönlichen Informationen über das Internet vor allem dank „sozialer Netzwerke“ wie StudiVZ und Facebook stark zugenommen. Vor allem Jugendliche nutzen solche Plattformen ausgiebig, um private Daten und Bilder dem Bekanntenkreis und teilweise auch der Öffentlichkeit zugänglich zu machen. Datenschützer beobachten diese digitale Freizügigkeit mit Sorge und ermahnen die Nutzer immer wieder zu Zurückhaltung. Eine häufig ausgesprochene Warnung lautet: „das Netz vergisst nie“. Einmal ins Internet gestellte Informationen können später nicht oder nur sehr schwer wieder entfernt werden.

Im Juni 2010 forderte der deutsche Bundesinnenminister Thomas de Maizière in einer Grundsatzrede zur Netzpolitik unter anderem, dass sich Internet-Nutzer „gegen die Datenmacht Dritter selbst zur Wehr“ setzen sollten [1]. Konkret formulierte er: „Ziel wären ein digitales Radiergummi und ein Verfallsdatum, das ich an meine Daten anbringen kann“. Als eine Form des Selbst-Datenschutzes solle das Internet mittels künstlicher Alterung von Daten „das Vergessen lernen“.

Der Minister schlägt damit in dieselbe Kerbe wie schon 2007 Mayer-Schönberger mit seinem Vorschlag, einen Wechsel in der Philosophie des Umgangs mit sensiblen Daten zu vollziehen [2]. Mayer-Schönberger argumentiert, dass in der analogen Welt das Vergessen und Verbleichen von Daten ein natürlicher Prozess ist. Auch wenn eine Information noch vorhanden ist, besteht immer die Herausforderung, sie in Archiven oder bei Zeitzeugen aufzufinden und zu verarbeiten. Mit der Digitalisierung hat sich dies geändert. Verarbeiten und Speichern von digitalen Daten sind nicht nur drastisch einfacher, sondern auch billiger.

Das Internet hat zudem das Suchen und Auffinden von weltweit verteilten Daten revolutioniert. Mayer-Schönberger zeigt an Beispielen wie Kreditauskunfteien, Flugdatensammlungen der Reiseveranstalter und biometrischen Datenbanken öffentlicher Stellen, dass das Aufbewahren aller Arten von Daten zum Standard geworden ist, wo früher das „Vergessen“ über die Zeit meist gegeben war [3]. Missbrauch von Daten und das Auftauchen von Information zu einem Zeitpunkt, an dem sie dem Urheber Schwierigkeiten bereiten könnten (zum Beispiel das kompromittierende Party-Foto, das der Personalchef nach dem Vorstellungsgespräch in Facebook entdeckt), werden folglich zunehmend zum Problem.

Lawrence Lessig [4] argumentiert, dass eine rein juristische Regulierung der Datenverarbeitung keinen effektiven Schutz der Betroffenen bieten kann. Ebenso wenig kann man sich in der unpersönlichen Umgebung des Internets auf ausreichende soziale Kontrollmechanismen gegen Datenmissbrauch verlassen. Ein Schutz durch technische Maßnahmen, die den juristischen Rahmen unterstützen, erscheint erforderlich.

Das Konzept eines „digitalen Radiergummis“ erscheint in den Augen vieler technischer Laien äußerst vielversprechend. Dementsprechend hoch gesteckt waren die Erwartungen, als mit dem im Januar 2011 vorgestellte X-pire! eine „innovative Software, die Ihre Bilder mit einem digitalen Verfallsdatum versieht“[1] angekündigt wurde. Umso größer war die Ernüchterung, als die erste Beta-Version des Plug-ins zum Download bereitgestellt und Details zur Funktionsweise bekannt wurden. Medien und Weblogs berichteten kritisch und identifizierten zahlreiche Unzulänglichkeiten und Schwächen der Lösung. Bevor wir eine konkrete Umsetzung betrachten, untersuchen wir die allgemeinen Anforderungen, die an ein solches System gestellt werden.

2 Prinzip eines „digitalen Radiergummis“

Der durch Medien und Politik geprägte Begriff „digitaler Radiergummi“ ist irreführend, da die damit bezeichnete Technologie nicht dazu dienen soll, um nachträglich Inhalte aus dem Netz zu entfernen, sondern um sie vor dem Einstellen mit einem Verfallsdatum zu versehen, nach dessen Ablauf sie nicht mehr genutzt werden können. Daher sollte – wie es auch von den Entwicklern von X-pire! gemacht wird – zutreffender von einem „digitalen Verfallsdatum“ gesprochen werden.

Für die zufriedenstellende Funktionsweise eines solchen auf Techniken des Digital Rights Management (DRM) basierenden Systems lassen sich vier allgemeine Anforderungen identifizieren:

1. **Plattformunabhängigkeit:** Die geschützten Inhalte sollen auf jeder relevanten Plattform Browser- und Betriebssystemunabhängig zur Verfügung gestellt werden können.
2. **Formatsunabhängigkeit:** Es soll möglich sein, Inhalte beliebigen Formats (Bilder, Texte, Audio, Video usw.) mit dieser Technik zu schützen.
3. **Betreiberunabhängigkeit:** Es ist wünschenswert, nicht von einem einzelnen Anbieter dieses Dienstes abhängig zu sein, sondern vielmehr das durch das

Universität Hamburg
Fachbereich Informatik
Arbeitsbereich Sicherheit in Verteilten Systemen
www.informatik.uni-hamburg.de/SVS/

1 vgl. http://www.x-pire.de/

Internet verbreitete Paradigma der Verteiltheit zu nutzen.

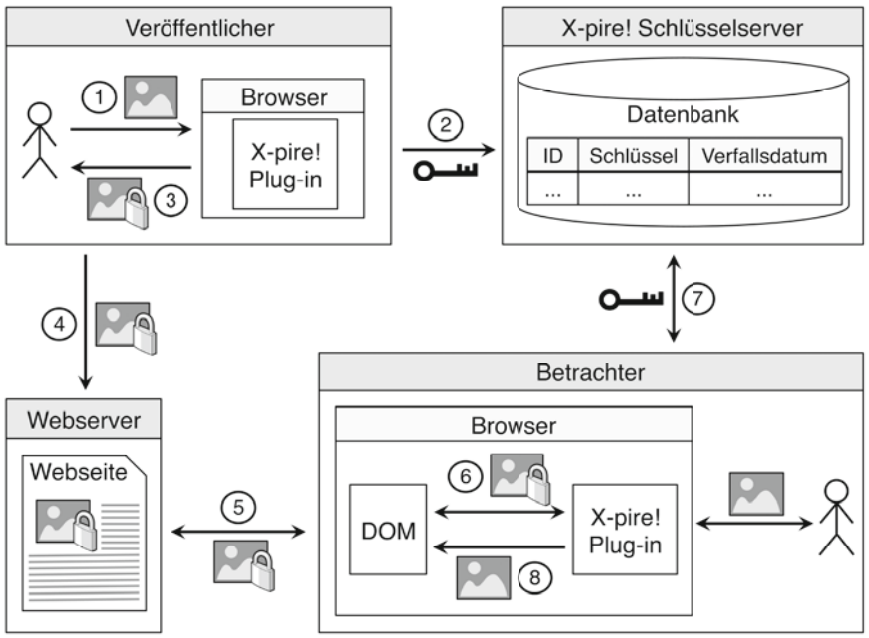
4. **Effektivität:** Der Schutz der Inhalte muss wirkungsvoll sein, d. h. es muss sichergestellt werden, dass der Angreifer die geschützten Inhalte nur im Rahmen der vorgegebenen Restriktionen (hier das Verfallsdatum) nutzen und nur in geschütztem Zustand kopieren kann.

Zum Schutz der Inhalte lassen sich unterschiedlich aufwändige Techniken einsetzen.

1. Die einfachste Möglichkeit ist die **Verwendung von Software im Vertrauensbereich des Nutzers**, mit deren Hilfe die Inhalte verfügbar gemacht werden. Der erreichbare Schutz ist jedoch gering: Die Daten können noch digital innerhalb des Systems problemlos kopiert werden, zum Beispiel durch das Abspeichern von angezeigten Inhalten oder die Verwendung von Screenshot-Werkzeugen. Wir sprechen in diesem Zusammenhang von der „digitalen Lücke".
2. Auch der Einsatz eines **vertrauenswürdigen Hardware-Moduls im PC des Nutzers** bietet wenig mehr Schutz, da die Inhalte wiederum ungeschützt dem System zur Ausgabe zur Verfügung gestellt werden. Die aus dem Trusted Computing bekannte Idee, dass während der Wiedergabe eines geschützten Mediums nur zertifizierte Software auf dem Rechner laufen darf, erschwert das digitale Kopieren deutlich, ist aber vermutlich für einen digitalen Radiergummi aufgrund der Einschränkungen in der Benutzbarkeit des Rechners unpraktikabel.
3. Effektiven Schutz bieten **komplett abgeschottete Systeme**, wie sie beispielsweise bei HDCP[2] umgesetzt werden. Dabei wird die Übertragung bis hin zur analogen Ausgabe auf einem Monitor abgesichert und die digitalen Daten können nicht mehr leicht unerlaubt abgezweigt werden. Der Nutzer muss also über zertifizierte Hardware verfügen, um die Inhalte nutzen zu können. Dennoch existiert selbst hier eine **„analoge Lücke"**, da keine Technik verhindern kann, dass ein Bildschirm mit einer Digitalkamera abfotografiert wird.

Diese Betrachtungen zeigen bereits, wie schwierig es ist, ein brauchbares digitales Verfallsdatum zu realisieren. Im Folgenden betrachten wir die konkrete Implementierung von X-pire!, die für großes mediales Aufsehen gesorgt hat.

Abbildung 1 | Funktionsweise von X-pire!



3 Funktionsweise von X-pire!

X-pire! ist ein Plug-in für den Browser Firefox, das im Wesentlichen zwei Funktionen bereitstellt.

1. **Anbieter (Einsteller) eines Inhalts:** Es wird die Verschlüsselung eines Bildes vor dem Hochladen ermöglicht und an ein Verfallsdatum geknüpft. Die so aufbereiteten Bilder sollen im Internet – insbesondere bei sozialen Netzwerken wie Facebook, wer-kennt-wen oder Flickr – veröffentlicht werden können, ohne dass diese nach Ablauf des Verfallsdatums noch anzeigbar sind.
2. **Betrachter des Inhalts:** Zum anderen soll das Plug-in Nutzer in die Lage versetzen, entsprechend aufbereitete Bilder zu entschlüsseln und darstellen zu können, so lange deren Verfallsdatum noch nicht erreicht ist.

Beide Funktionen sind in Abbildung 1 schematisch dargestellt. Nach dem Herunterladen und Installieren des Plug-ins steht dem Nutzer eine Oberfläche zur Verfügung, in der er seine zur Veröffentlichung vorgesehenen Bilder öffnet, die entsprechende Verfallszeit angibt und eine symmetrische Verschlüsselung (AES-128 mit CBC) der Bilder durchführt (Schritt 1). Zur Verschlüsselung wird durch X-pire! ein zufälliger Schlüssel generiert und zusammen mit dem gewählten Verfallsdatum und einem bildspezifischen Identifier (ID), bestehend aus einem Hashwert des Bildes und einer Zufallszahl, an einen als vertrauenswürdig angesehenen Schlüsselserver geschickt (Schritt 2). Im Auslieferungszustand des Plug-ins ist hierfür der Server keyserver.x-pire.net voreingestellt.

Die Kommunikation zwischen Plug-in und Schlüsselserver wird mittels TLS (Transport Layer Security) abgesichert. Das verschlüsselte Bild wird von X-pire! um Meta-Informationen (unter anderem eine Kennzeichnung als mit X-pire! aufbereitetes Bild) angereichert und auf der Festplatte des Einstellers abgespeichert (Schritt 3), von wo aus es dieser im Internet veröffentlichen kann (Schritt 4). Für kryptographische Operationen wird auf die Bibliothek OpenSSL zurückgegriffen.

Möchte ein Besucher einer Webseite das so veröffentlichte Bild ohne X-pire!-Plug-in betrachten, wird lediglich eine schwarze Fläche mit dem Hinweis dargestellt, dass eine Betrachtung ohne entsprechendes Plug-in nicht möglich ist. Ist das Plug-in hingegen installiert, sucht es nach dem Laden einer Webseite im Dokumentbaum (Document Object Model, DOM) nach verschlüsselten Bildern, die es anhand der eingebetteten Kennzeichnung erkennt (Schritt 6). Wurde ein verschlüsseltes Bild gefunden, ermittelt das Plug-in die eindeutige ID des Bildes und fordert beim Schlüsselserver den zur Entschlüs-

2 High-bandwidth Digital Content Protection

selung nötigen Schlüssel an. Ist das Verfallsdatum noch nicht erreicht, antwortet der Server mit dem zugehörigen Schlüssel (Schritt 7). Nach der Entschlüsselung des Bildes durch das Plug-in wird die schwarze Fläche mit dem Hinweistext durch das eigentliche Bild ersetzt (Schritt 8). Der gesamte Vorgang läuft für den Nutzer transparent (im Hintergrund unbemerkt) ab.

Ist das Verfallsdatum für ein Bild erreicht, beantwortet der Schlüsselserver die Anforderung des Schlüssels mit einer Fehlermeldung. Das Plug-in hat somit ab diesem Moment keine Möglichkeit mehr, das Bild darzustellen und der Nutzer bekommt einen Hinweis eingeblendet, dass das Verfallsdatum des Bildes erreicht ist.

Der Einsteller kann beim Verschlüsseln und Veröffentlichen eines Bildes festlegen, dass der Schlüsselserver den Schlüssel in Schritt 7 nur zurückliefert, falls der Betrachter ein CAPTCHA[3] korrekt gelöst hat. Während CAPTCHAs von Menschen relativ leicht gelöst werden können, fällt dies Computerprogrammen vergleichsweise schwer. Diese Hürde soll verhindern, dass zum Beispiel der Betreiber des Webservers bzw. des sozialen Netzwerks automatisiert die Schlüssel für eine Vielzahl von verschlüsselten Bildern vor deren Verfallsdatum ermitteln und abspeichern kann. Mit einer solchen Schlüsselsammlung könnte er die Bilder auch nach Verstreichen des Verfallsdatums automatisiert entschlüsseln und zur Verfügung stellen.

X-pire! hat im Januar 2011 den kommerziellen Dienst aufgenommen. Wer Bilder verschlüsseln möchte, muss eine Lizenz erwerben. Eine 90-tägige Privatnutzung kostet derzeit 6,99 Euro (Stand: 08.03.2011). Dies könnte gerade bei der jungen Generation, die es gewohnt ist, Internetdienste kostenfrei zu konsumieren, zu Akzeptanzproblemen führen. Empirische Studien, u. a. von Acquisti et al. [5], deuten zudem darauf hin, dass viele Privatnutzer derzeit nicht dazu bereit sind, für Datenschutz zu bezahlen. Dies wurde offenbar erkannt, denn in naher Zukunft soll die private Nutzung nach Aussagen von Prof. Backes kostenlos werden. Unternehmensabonnements und Lizenzen für den Betrieb eines eigenen Schlüsselservers sind individuell zu verhandeln. Die Nutzung des Plug-ins zur Darstellung von Bildern ist kostenlos. Zunächst ist X-pire! nur für den Schutz von Bildern und nur für Nutzer von Mozilla Firefox 3.5 oder höher erhältlich, soll nach Angaben der Hersteller jedoch um Unterstützung für andere Browser und Anwendungen (z. B. PDF-Dateien) erweitert werden. Grundsätzlich ist das Arbeitsprinzip auf beliebigen Datentypen anwendbar.

4 Bewertung

X-pire! ist nicht plattformunabhängig. Es setzt den Einsatz von Firefox voraus, der nicht für alle Systeme (wie mobile Endgeräte) verfügbar ist. Zudem könnten aktuell nur Bilder bestimmter Formate mit einem Verfallsdatum versehen werden. Ebenso ist man an einen einzigen Betreiber gebunden; eine verteilte Architektur von Schlüsselservern ist nicht vorgesehen.

Einschränkungen der Benutzbarkeit ergeben sich aus der Technik, mit der X-pire! versucht, die verschlüsselten Bilder gegen nachträgliches Umkodieren und Skalieren, das auf vielen Webseiten praktiziert wird, resistent zu machen. Würde man ein Bild, das mit einem symmetrischen Algorithmus verschlüsselt wurde, ohne entsprechende Vorkehrungen hochladen, würde die nachträgliche JPEG-Kompression auf dem Webserver auf das Chiffrat angewandt und dieses zerstören. Ein späteres Entschlüsseln würde fehlschlagen. X-pire! begegnet dieser Herausforderung, indem es das Chiffrat des Bildes in einen Bereich der JPEG-Datei einbettet, der nachträgliches Umkodieren weitgehend unbeschadet übersteht. Zusätzlich werden fehlerkorrigierende Codes eingesetzt. In der Praxis zeigt sich jedoch, dass die fehlertolerante Verschlüsselung nicht bei allen Internetangeboten funktioniert, beispielsweise nicht bei TwitPic[4]. Beim Verschlüsseln gehen zudem alle Meta-Daten (EXIF-Header, Erstellungsdatum, usw.) in den Bildern verloren, die gerade in auf Fotografie spezialisierten Communities einen großen Stellenwert einnehmen.

Neben den genannten Problemen weist das System einige fundamentale konzeptionelle Schwächen bezüglich der Effektivität auf, die wir im Folgenden ausführen.

Aus Sicherheitssicht fällt zunächst ein Verfügbarkeitsproblem auf. Alle Schlüssel liegen auf einem zentralen Schlüsselserver. Dieser Server ist ein Single-Point-of-Failure – ist er nicht (mehr) erreichbar, kann kein einziges Bild mehr angezeigt werden. Solche Insellösungen stehen im Widerspruch zur verteilten Architektur des Internets. Die Lösung ist zwar hinsichtlich der Verfügbarkeit „Fail-Safe", d.h. wenn der Schlüsselserver Offline ist, entsteht auch kein Vertraulichkeitsproblem, allerdings könnte dies den Nutzer dazu bewegen, sich nach anderen Möglichkeiten umzusehen, um an die von ihnen gewünschten Inhalte zu gelangen.

Ein zentraler Schlüsselserver ist auch aus Sicht der Vertraulichkeit problematisch, da die Datenbank aller Schlüssel ein lukratives Angriffsziel darstellt und der Betreiber des Schlüsselservers alle Zugriffe auf die Schlüssel zur Profilierung seiner Nutzer protokollieren kann. Weiterhin müssen die Nutzer darauf vertrauen, dass der Schlüssel auf dem Schlüsselserver nach dem Verfallsdatum wirklich gelöscht wird und nicht – etwa für spätere Zugriffe durch „berechtigte Stellen" – darüber hinaus aufbewahrt wird.

Prinzipiell wäre X-pire! auch ohne einen solchen zentralen Schlüsselserver realisierbar. In der Forschung existieren vergleichbare Ansätze, die kein Vertrauen in einen einzelnen Anbieter voraussetzen und den Schlüssel stattdessen z. B. mit Shamir's Secret-Sharing-Verfahren auf mehrere Server verteilen. Ein solches Verfahren ist in dem Firefox-Plug-in „Vanish" umgesetzt, das als Prototyp zur Verfügung steht [6]. Solche verteilten Lösungen verbessern somit die Vertraulichkeit und Verfügbarkeit gegenüber einem zentralen Schlüsselserver.

Techniken wie Vanish und X-pire! können jedoch auch dann keinen perfekten Schutz gewährleisten. Bilder, die im Browser angezeigt werden, können grundsätzlich vom Nutzer kopiert oder abgespeichert werden (siehe Abschnitt 2).

Das erneute Hochladen einmal entschlüsselter Bilder kann ein digitaler Radiergummi ebenfalls nicht verhindern. Den Entwicklern sind diese prinzipbedingten Umgehungsmöglichkeiten und die Grenzen ihrer Technik bewusst.[5] Schutzmaßnahmen gegen digitale Kopien haben sie daher erst gar nicht implementiert.

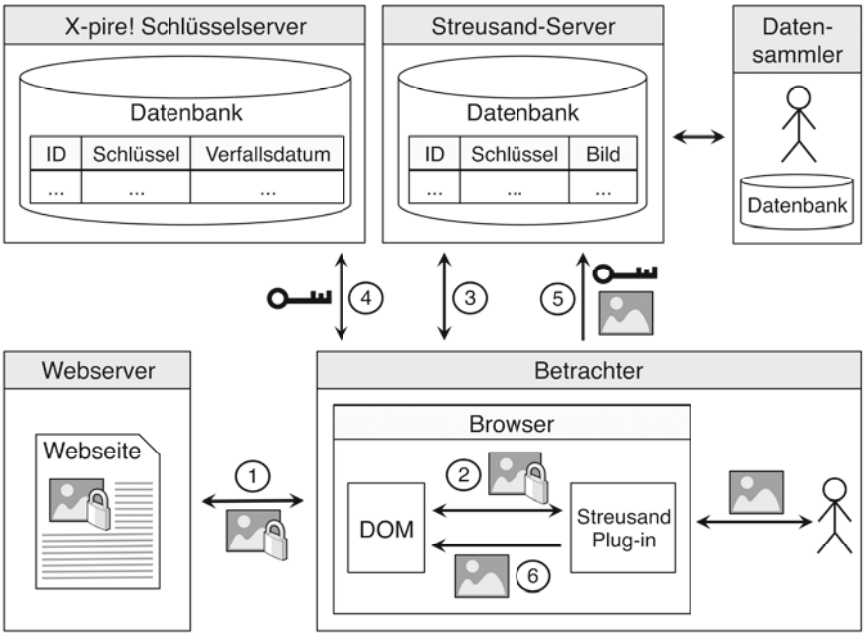
Das manuelle Kopieren und Abspeichern der Bilder ist für den Nutzer vergleichsweise aufwändig und kaum im großen Stil durchführbar. Das Verfallsdatum kann jedoch durchaus auch einfacher um-

3 Completely Automated Public Turing test to tell Computers and Humans Apart

4 http://www.twitpic.com/

5 http://www.x-pire.de/index.php?id=93

Abbildung 2 | Funktionsweise der Streusand-Erweiterung



gangen werden, etwa indem die Schlüssel aller vor ihrem Verfallsdatum betrachteten Bilder vom Browser dauerhaft aufbewahrt werden. Damit kann ein Nutzer ein Bild, das er erstmals vor dem Verfallsdatum angesehen hat, auch danach noch unbegrenzt betrachten. Das Schweizer Unternehmen scip AG hat demonstriert, dass eine entsprechende Anpassung des X-pire!-Plug-ins nur geringen Aufwand verursacht.[6]

Ein automatisiertes Sammeln von Schlüsseln vor dem Verfallsdatum durch Crawler soll in X-pire! durch den Einsatz der CAPTCHAs unterbunden werden. Ein manuelles Zusammentragen einer großen Menge von Schlüsseln ist daher auf den ersten Blick nicht praktikabel.

CAPTCHAs bieten jedoch keine absolute Sicherheit, da zum einen immer leistungsfähigere Bilderkennungsverfahren entwickelt werden, die auch stark verzerrte Texte aus den CAPTCHAs auslesen können, und zum anderen spezialisierte Dienstleister preisgünstig das Lösen von CAPTCHAs anbieten [7]. Gegen den Betreiber eines sozialen Netzwerks oder einer Online-Plattform bieten CAPTCHAs ohnehin nur geringen Schutz: Dieser könnte als Man-in-the-Middle auftreten und jedes CAPTCHA, das ihm der X-pire!-Schlüsselserver präsentiert, im Rahmen seines eigenen Dienstes nutzen, z. B. beim Anlegen eines neuen Profils oder vor dem Hochladen eines Bildes. Mit den CAPTCHA-Lösungen seiner Nutzer könnte er sich dann beim X-pire!-Schlüsselserver Zugriff auf die Verschlüsselungsschlüssel verschaffen.

Zusammenfassend lässt sich feststellen, dass X-pire! die verschlüsselten Bilder nur vor neugierigen Augen schützen kann, die nach dem Verfallsdatum darauf aufmerksam werden. Erkennt ein Angreifer schon frühzeitig das Potenzial eines geschützten Bildes, bleibt das System wirkungslos.

5 Streusand-Erweiterung

Die persistente Speicherung der Schlüssel bereits betrachteter Bilder beim Nutzer, wie im zuvor genannten Plug-in der scip AG realisiert, erhöht das Risiko einer Weiterverbreitung der zu schützenden Bilder nur geringfügig: Die Bilder sind damit zwar noch nach dem vorgesehenen Verfallsdatum darstellbar, allerdings nur für Nutzer, die die Bilder auch vor diesem Verfallsdatum abgerufen haben.

Wesentlich problematischer wird die Situation, wenn die Schlüssel nicht mehr lokal, sondern öffentlich zugänglich auf einem „Piratenserver“[7] gespeichert werden. In diesem Fall können Nutzer auch solche Bilder entschlüsseln, die sie vor dem Verfallsdatum nicht selbst abgerufen haben. Werden neben den Schlüsseln aber auch die entschlüsselten Bilder öffentlich zugänglich gespeichert, bietet selbst das Löschen der verschlüsselten Bilder aus dem Internet keinen Schutz.

Schlimmer noch: Die entstehende öffentlich zugängliche Sammlung dieser Bilder führt den Grundgedanken des Selbstdatenschutzes eines digitalen Radiergummis ad absurdum: Bilder, die als besonders schützenswert angesehen werden, sind im Ergebnis an besonders exponierter Stelle dauerhaft im Internet frei verfügbar und gesammelt herunterladbar.

Der Versuch, die Weiterverbreitung der Bilder zu unterdrücken führt also genau zum Gegenteil. Die Bilder werden besonders bekannt und leicht zugänglich, was als „Streisand-Effekt“ bezeichnet wird [8].

Zur Demonstration der Umsetzbarkeit dieser Idee haben wir ein zu X-pire! kompatibles Firefox-Plug-in „Streusand“ entwickelt, dessen Funktionsweise in Abbildung 2 dargestellt ist. Streusand wird anstelle von X-pire! im Browser installiert. Ruft ein Nutzer des Streusand-Plug-ins eine Webseite mit einem durch X-pire! geschützten Bild auf (Schritt 1), wird dieses, wie auch im Fall des Original-Plug-ins, aus dem Dokumentbaum des Browsers geladen (Schritt 2). Die wesentliche Erweiterung zeigt sich in Schritt 3: Anstatt mit dem X-pire!-Schlüsselserver Kontakt aufzunehmen, wird die Anfrage nach dem Schlüssel zunächst an den „Streusand-Server“ geschickt. Kennt dieser den angeforderten Schlüssel, gibt er ihn direkt und unabhängig vom Verfallsdatum an das Streusand-Plug-in weiter, wo der Schlüssel zur Entschlüsselung des scheinbar geschützten Bildes verwendet wird (Schritt 6).

Kennt der Streusand-Server den passenden Schlüssel hingegen nicht und ist das Verfallsdatum des Bildes noch nicht überschritten, bezieht das Streusand-Plug-in den Schlüssel über den X-pire!-Schlüsselserver (Schritt 4), entschlüsselt das Bild und lädt es zusammen mit dem Schlüssel auf den Streusand-Server (Schritt 5) hoch. Ab diesem Zeitpunkt ist das Bild in der öffentlich einsehbaren Streusand-Galerie frei verfügbar und der Schlüssel kann anderen Nutzern ohne jegliche zeitliche Restriktionen zur Verfügung gestellt werden.

Im Ergebnis können Bilder nur dann nicht mehr nach ihrem Verfallsdatum entschlüsselt werden, wenn sie vor dem Verfallsdatum von keinem einzigen Streusand-Nutzer abgerufen worden sind.

6 http://www.scip.ch/?labs.20110131

7 http://tinyurl.com/6jfk4d3

Da beim Einsatz des Streusand-Plugins im Vergleich zu X-pire! die von vielen Nutzern als störend empfundenen CAPTCHAs viel seltener angezeigt werden – nämlich nur beim allerersten Betrachten durch irgendeinen Nutzer – entsteht zudem ein Anreiz zur Nutzung von Streusand anstelle des X-pire!-Plug-ins. Der „Nutzwert" von Streusand steigt also direkt proportional mit seiner Verbreitung.

Derzeit ist aus ethischen und urheberrechtlichen Gründen nicht geplant, die Streusand-Erweiterung öffentlich zugänglich zu machen. Es handelt sich jedoch um ein voll funktionsfähiges Plug-in, das als Proof-of-Concept entwickelt wurde.

6 Fazit

In diesem Beitrag haben wir am Beispiel des Firefox-Plug-ins „Streusand" gezeigt, dass das von Politikern geforderte „digitale Vergessen" mit technischen Mitteln nicht zuverlässig realisiert werden kann. Die Entwickler von X-pire!, auf dem Streusand basiert, machen daraus auch kein Geheimnis: „Es geht nicht darum, den perfekten Schutz zu bekommen. Das ist technisch unmöglich", stellt Backes klar und ergänzt: „das Verfallsdatum funktioniert nur, wenn niemand Böses will und die Bilder nicht kopiert werden." [9] X-pire! ist demnach eine Selbstdatenschutz-Technik, die nur dann schützt, wenn sie nicht angegriffen wird. Die hohen Erwartungen, die Politiker mit dem Begriff des „digitalen Radiergummis" bei den Bürgern geweckt haben, lassen sich damit nicht erfüllen.

Ein wirksames digitales Verfallsdatum wäre aus technischer Sicht nur dann realisierbar, wenn Kopien der zu schützenden Inhalte zuverlässig verhindert werden könnten. Mit genau dieser Herausforderung sieht sich seit einigen Jahren auch die Medien-Industrie konfrontiert, die das Ziel verfolgt, Kopien urheberrechtlich geschützter Werke zu unterbinden. Im Laufe der Jahre wurden hierfür zahlreiche Kopierschutz-Techniken bzw. Digital-Rights-Management (DRM) Systeme entwickelt.

Bis heute ist jedoch keine DRM-Technik bekannt, die die Inhalte zuverlässig schützt. Zudem ist es der Industrie nicht gelungen, eine breite Akzeptanz dieser Techniken bei ihren Kunden zu erreichen. Deswegen gehen die großen Anbieter wie iTunes, Musicload oder Amazon Musik inzwischen dazu über, ihre Inhalte wieder ohne Kopierschutz auszuliefern. Einige Marktbeobachter sprechen daher bereits davon, dass DRM gescheitert ist [10].

Offenbar sind die Unzulänglichkeiten einer technischen Lösung eines digitalen Verfallsdatums inzwischen auch in der politischen Diskussion angekommen. Am Rande der Tagung „Safer Internet Day" am 8. Februar 2011 bezeichnete Verbraucherschutzministerin Ilse Aigner einen digitalen Radiergummi zum Löschen von Daten im Internet als „Wunschvorstellung" [11].

Wenn schon Selbstdatenschutz-Techniken wie X-pire! keinen zufriedenstellenden Schutz bieten können, sollte darüber nachgedacht werden, die Anbieter von sozialen Netzwerken und populären Internet-Portalen in die Pflicht zu nehmen. Diese könnten von ihren Nutzern beim Einstellen von Inhalten ein Verfallsdatum abfragen und hochgeladene Inhalte automatisch nach einer beliebigen Zeitspanne wieder entfernen. Dadurch ließe sich schon heute ein mit X-pire! vergleichbares Schutzniveau erreichen, ohne dessen Einschränkungen in Kauf nehmen zu müssen.

Danksagung

Wir danken Dirk Fox für wesentliche Hinweise zur Verbesserung dieses Beitrages.

Literatur

[1] FOCUS Online: Innenminister de Maizière will „digitalen Radiergummi", 22.06.2010. http://www.focus.de/digital/digital-news/internet-innenminister-de-maiziere-will-digitalen-radiergummi_aid_522418.html

[2] Viktor Mayer-Schoenberger: Useful Void: *The Art of Forgetting in the Age of Ubiquitous Computing*. Working Paper, John F. Kennedy School of Government, Harvard University, 2007.

[3] Viktor Mayer-Schoenberger: *Delete: die Tugend des Vergessens in digitalen Zeiten*. Berlin University Press, 2010.

[4] Lawrence Lessig: *Code: And Other Laws of Cyberspace*. Version 2.0, New York, Basic Books, 2006.

[5] Alessandro Acquisti, Leslie John, George Loewenstein: *What is privacy worth?* In: Privacy Papers for Policy Makers, 2009, S. 5-7.

[6] Roxana Geambasu, Tadayoshi Kohno, Amit A. Levy, Henry M. Levy: *Vanish: Increasing Data Privacy with Self-Destructing Data*. In: Proceedings of the USENIX Security Symposium, Berkeley, USENIX Association, 2009, S. 299-316.

[7] Carlos Javier Hernandez-Castro, Arturo Ribagorda: *Remotely Telling Humans and Computers Apart: An Unsolved Problem*. In: iNetSec 2009 – Open Research Problems in Network Security, IFIP AICT 309, Berlin, Springer, 2009, S. 9-26.

[8] Bradley T. Tennis: *Privacy and Identity in a Networked World*. In: Personal Data Privacy and Protection in a Surveillance Era: Technologies and Practices, Hershey, IGI Global, 2011, S. 1-18.

[9] Peter Welchering: *Was im Netz steht, bleibt – verschlüsselt oder nicht*. In: Frankfurter Allgemeine Zeitung, 18.01.2011, Nr. 14, S. T1.

[10] Willms Buhse, Dirk Günnewig: *Digital Rights Management*. In: Ökonomie der Musikindustrie, 2. Auflage, Wiesbaden, Deutscher Universitätsverlag, 2008, S. 215-228.

[11] Varinia Bernau: *Dolmetscher Digitaler Radiergummi*. In: Süddeutsche Zeitung, 09.02.2011, S. 24.