melting-link.com beta

Informationen und grundlegende technische Beschreibung

Inhalt

Einleitung

Was früher von einem Blatt Papier radiert wurde oder einfach im Papierkorb verschwunden ist, bleibt im Fall von digitalen Daten heute dauerhaft der Nachwelt erhalten. Melting-link.com soll helfen, diese Funktionalität auch im Internet wieder bereitzustellen.

Es handelt sich hierbei um eine interaktive Website, die Nutzern eine einfache und sichere Möglichkeit bietet, nicht dauerhaft bestehende Nachrichten zu veröffentlichen und diese Nachrichten auch direkt zur Interaktion zu benutzen.

Für die Probleme, die mit einem nicht-vergessenden Internet einher gehen, kann ein technischer Ansatz natürlich nicht die alleinige Lösung sein. Er soll den Nutzern helfen, sich mit verändernden Situationen auseinander setzen zu können. Erst noch zu schaffende und durchzusetzende gesetzliche Regelungen, oder gar eine Umgestaltung der gesamten Dateninfrastruktur, können hier keine schnell wirksame Hilfe schaffen. Die Funktionalität der Betaversion auf melting-link.com bietet schon jetzt sofortig wirksame Schutzfunktionen, um so einen Beitrag für den verantwortungsvollen Umgang mit Informationen im Web 2.0 zu leisten.

Problemstellung und Motivation

Mit der fortschreitenden Einflussnahme des Internets in viele Lebensbereiche hat sich die Informationskultur vieler Menschen stark verändert. Dienste wie facebook, twitter und ebay bestimmen zunehmend den Alltag und bieten neuartige Kommunikationswege.

Neu hingegen ist auch die Persistenz dieser Kommunikation. Während früher Telefongespräche oder Briefwechsel geführt und alsbald wieder vergessen wurden, bleiben viele Nachrichten heute gespeichert. Gerade die Social-media des Web 2.0 speichern jedes Detail dauerhaft und – was noch deutlich reicher an Konsequenzen ist – machen diese Kommunikation öffentlich sichtbar sowie gezielt such- und auffindbar.

Oftmals ist dies gewünscht, sogar die explizite Aufgabe der genutzten Medien wie tweets bei twitter oder einer öffentlichen Pinnwand bei facebook. Viele Nutzer stellen sich mittlerweile jedoch der Problematik, dass ihnen die Übersicht und Kontrolle über ihre im Netz frei verfügbar zugänglichen und eindeutig ihrer Person zuordenbaren Daten verloren geht. Das Vertrauen gegenüber den entsprechenden Unternehmen hat durch etliche Datenskandale und (unfreiwillige) Einblicke in die Archivierungs- und Auswertungspraxis Schaden genommen. Die meisten Dienste sind nicht mit monetären Aufwendungen verbunden, sondern finanzieren sich durch die immer präziser werdenden Profile der Einzelpersonen und der damit ermöglichten Auswertbarkeit für Zwecke des Marketings. Der so geschaffene „gläserne User“ wird von vielen Anwendern skeptisch betrachtet. Hinzu kommen noch Möglichkeiten des Missbrauchs öffentlich verfügbarer Informationen, vom Bombardement mit Spammails, falls die eigene Emailadresse lesbar für einen Suchbot veröffentlicht wurde, über Kreditkartenbetrug bis zu kompletten Identitätsdiebstählen. Auch die Vorstellung, mit jeder getroffenen Äußerung auch nach Jahren noch konfrontiert werden zu können, führt zu berechtigtem Unbehagen.

Mit einfachsten Mitteln lassen sich umfassende Lebensläufe und ein Bild über private Lebensumstände erstellen, die für die meisten Nutzer erschreckend sind. Ein Beispiel hierfür findet sich in der Ausgabe der Sendung „c’t TV“ vom 25.06.2011[1]. Es reicht oftmals aus, eine Emailadresse in eine Suchmaschine einzugeben, um eine Vielzahl an persönlichen Informationen gewinnen zu können.

Eine einfache Lösung für diese komplexe Problemstellung ist nicht in Aussicht. Technische Hilfsmittel, um eine gezielte nicht-persistente Verbreitung von Informationen zu gewährleisten, lassen sich hingegen schaffen. Bevor der Lösungsvorschlag durch melting-link.com vorgestellt wird, soll ein kurzer Überblick über die bisherige Entwicklung helfen, diesen Ansatz in Kontext zu setzen.

[1] http://www.heise.de/ct-tv/artikel/Video-Die-zerstoerte-Privatsphaere-1258604.html

Der Status quo

Digitale Inhalte sind ständiger Veränderung und Überarbeitung unterworfen. Jeder wird schon einmal einem Link gefolgt sein, dessen ursprüngliches Ziel mittlerweile nicht mehr vorhanden war und so zur typischen „Html: 404 – not found“ Fehlerseite gelangt sein. Webseiten und Foren werden geschlossen, womit viele Inhalte aus dem sichtbaren Bereich der meisten Nutzer verschwinden.

Gleichwohl ist ein Großteil davon immer noch in den Datenbanken großer Suchmaschinen oder Archivierungsanbieter vorhanden und kann mit Mehraufwand noch gefunden werden. Dieser Erosionseffekt führt für die meisten Privatanwender dazu, dass Inhalte zwar nicht endgültig aus dem Internet verschwinden, aber zumindest nicht mehr ohne weiteres sichtbar gemacht werden können.

Hierbei handelt es sich um nicht steuerbare, „natürliche“ Vorgänge, die vom Nutzer individuell nicht beeinflusst werden können. Das einfache Problem, etwas online stellen zu können und nach Bedarf wieder zu entfernen, wird so nicht gelöst. Ein „digitaler Radiergummi“ wäre eine Lösung, auch wenn diese Formulierung eher irreführend ist, da der generelle Ansatz bei Verschlüsselungsverfahren liegt, womit die Daten zwar nicht verschwinden, aber zumindest nicht mehr abrufbar sind.

„Ziel wären ein digitales Radiergummi und ein Verfallsdatum, das ich an meine Daten anbringen kann“

Der ehemalige Bundesinnenminister Thomas de Maizière[2]

Die Idee eines „digitalen Radiergummis“ ist nicht neu, schon mehrfach wurden entsprechende Systeme vorgestellt.

Zwei Beispiele sollen genannt werden:

1) Das Projekt „Vanish – Self-destructing digital data“ der Universität Washington[3], veröffentlicht 2009. Hierbei handelt es sich um ein Cloud-basiertes Verschlüsselungssystem, bei dem Textnachrichten nicht im Klartext gespeichert werden, sondern codiert. Der zugehörige Schlüssel wird in einem Vuze BitTorrent DHT gespeichert und nach Ablauf der eingestellten Laufzeit gelöscht. Das System benötigt zwingend ein proprietäres Zusatzprogramm, das die Anzahl der möglichen Nutzer einschränkt und zeigt Sicherheitsprobleme[4].
2) Die Universität des Saarlandes initiierte die Software „x-pire!“[5] vielbeachtet im Januar 2011. Es handelt sich hierbei um ein Browser-Addon, das Bilder mit einem Verfallsdatum versieht. Hierzu wird das Bild lokal verschlüsselt, das dann anstelle des Originalen hochgeladen wird. Der verwendete

[2] http://www.focus.de/digital/digital-news/internet-innenminister-de-maiziere-will-digitalen-radiergummi_aid_522418.html
[3] http://vanish.cs.washington.edu/index.html
[4] http://z.cs.utexas.edu/users/osa/unvanish/papers/vanish-broken.pdf
[5] http://www.x-pire.de/

Schlüssel wird auf einem Server gespeichert, der diesen nur während der definierten Laufzeit des Bildes an anfragende Clients herausgibt. Nachteilig ist die zwingende Installation des Addons sowie die leichte Umgehbarkeit des Systems durch die Speicherung der verwendeten Schlüssel[6].

Die bisher gebrachten Ansätze basieren auf lokaler Ver- und Entschlüsselung von Daten durch Zusatzprogramme, wobei externe Schlüsselserver die Laufzeiten verwalten.

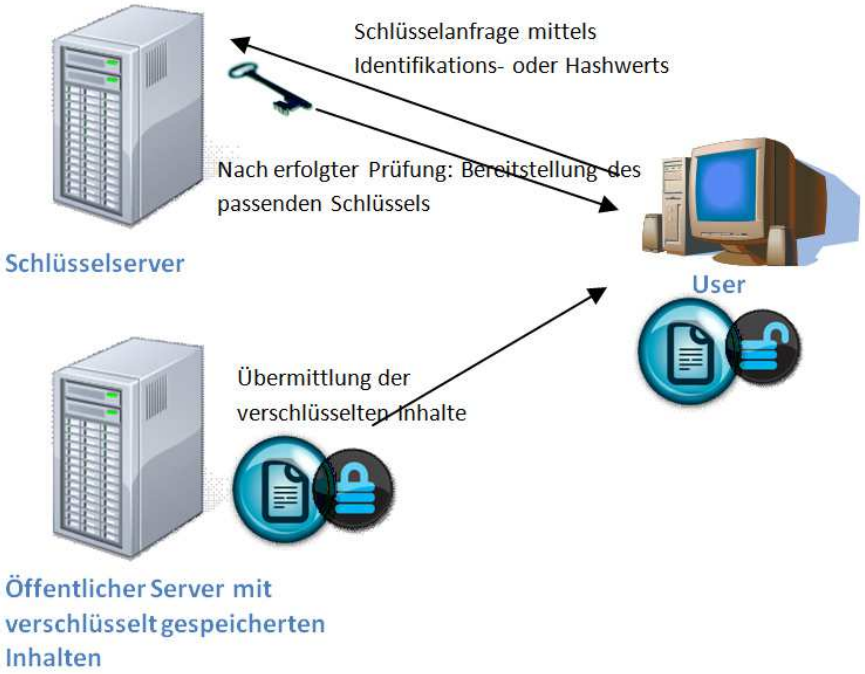

Abbildung 1: Schematische Übersicht eines Abrufvorgangs bei x-pire oder vanish

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

Der öffentliche Server mit den gesicherten Inhalten gibt diese an den Rechner des Users weiter. Diese beinhalten eine eindeutige Kennung oder es wird direkt aus den Ursprungsdaten ein Hashwert erzeugt, womit der Schlüsselserver den passenden Schlüssel (während der zugehörigen Laufzeit) aus seiner Datenbank ermittelt und an den anfragenden Client leitet, der so die ursprünglichen Informationen wieder herstellt.

Nachteile dieses Verfahrens sind die notwendigen Zusatzprogramme, die auf Clientseite installiert sein müssen. Zudem können nur statische Inhalte ohne Interaktionsmöglichkeit verbreitet werden, in den betrachteten Fällen also ein Bild oder eine einzelne Textnachricht.

Diesen Hürden und Einschränkungen möchte ich durch ein alternatives System begegnen, das in wenigen Schritten eine Plattform zum Austausch von Informationen bietet, die jederzeit wieder aus dem Internet verschwinden kann. Die Verwendung der rein browsergestützten Betaversion von melting-link.com ist nahezu überall möglich, ob unter Windows, Mac Os, auf Mobiltelefonen oder Tabletrechnern. Besonderer Wert wurde auf die Sicherheit aller im System befindlichen Daten gelegt, die hierfür verwendeten Verfahren werden noch gesondert erläutert.

Konzeption und Beispielanwendung

Den Ausgangspunkt bildet die Frage, wie mit einfachsten Mitteln eine Information temporär veröffentlicht und bestmöglich vor Missbrauch und ungewollter Archivierung geschützt werden kann. Dies ist kein abstraktes Szenario, jeder Betreiber einer Webseite achtet darauf, im Impressum keine maschinenlesbare Adresse oder Telefonnummer anzugeben und User in Foren versuchen, teils sehr kreativ, eine automatische Auswertung durch deren „Verschlüsselung“ zu verhindern[7]. Dies sind Aufgaben, die durch das Angebot von melting-link.com gelöst werden können.

Um eine Verwendbarkeit für alle Anwender zu gewährleisten, wird das Verfahren rein browsergestützt durchgeführt. Der Anwender veröffentlicht seine Daten nicht direkt, sondern trägt sie in eine Eingabemaske zusammen mit der gewünschten Laufzeit, nach der alle Daten automatisch gelöscht werden sollen, auf melting-link.com ein. Im Anschluss erhält er einen begrenzt gültigen, „schmelzenden“ Link, mit dem die Informationen abrufbar sind.

Dieser „mink“ (=*m*elting l*ink*) kann nun publiziert werden und die Grundlage einer sicheren und nicht persistenten Kommunikation werden. Der mink beinhaltet einen Identifikator, der als Primärschlüssel zum Auffinden des Eintrags in der Datenbank dient, sowie das Passwort, um den zugehörigen Datensatz entschlüsselt ausgeben zu können.

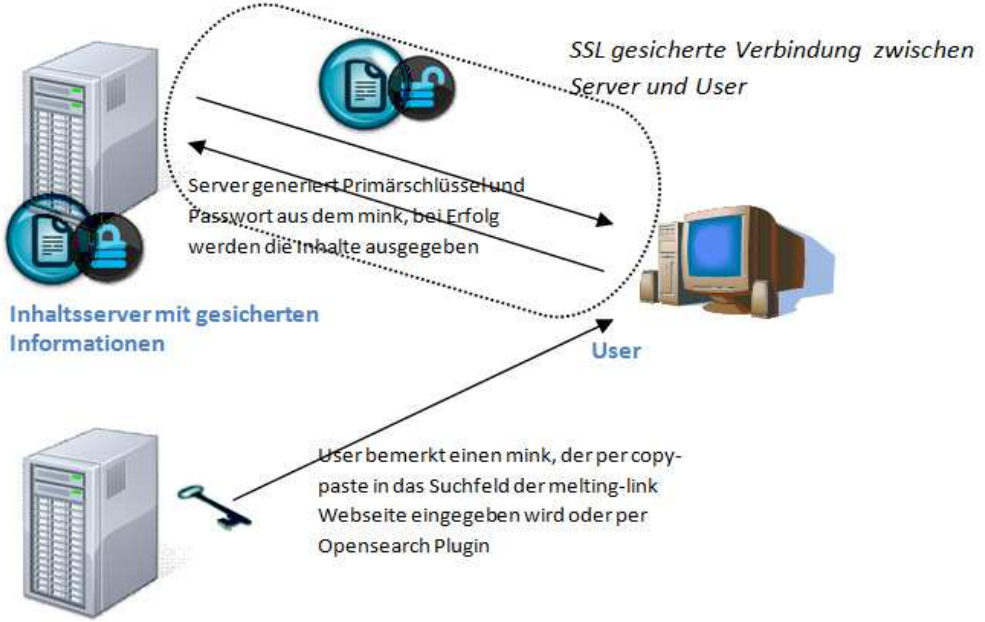

Abbildung 2: Schematische Übersicht eines Abrufvorgangs bei melting-link.com

Als konkretes Beispiel für eine Anwendung soll ein Verkauf eines Wagens auf einer Forenplattform gezeigt werden. Der Verkäufer - nennen wir ihn Herrn Lindemann - möchte potentiellen Interessenten die Möglichkeit bieten, ihn telefonisch oder per Email zu kontaktieren, hat aber keine Lust, dass seine Telefonnummer

[7] als Beispiel sei „dieter punkt jung klammeraffe "buchstabe-nach-f"mail.com“ genannt

dauerhaft online zu lesen ist (andere Nutzer haben geradezu von Telefonterror durch professionelle Händler auch Wochen nach Abschluss des Verkaufs berichtet) und möchte nicht, dass jeder seine Verkaufsaktivitäten auch nach Jahren recherchieren kann.

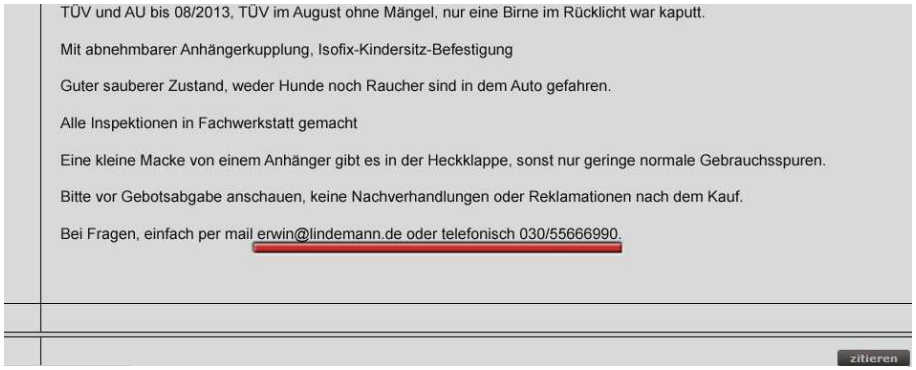

Abbildung 3: Foreneintrag, der dauerhaft lesbar bleibt mit zuordenbaren persönlichen Informationen

Statt diese Daten offen online zu stellen, wird mit wenigen Klicks ein mink erstellt, der nicht nur die gewünschten Informationen enthält, sondern auch Gelegenheit zu direkter Kommunikation bietet. Die Gültigkeitsdauer kann gezielt bestimmt, sowie zwischen verschiedenen Nachrichtentypen ausgewählt werden, in diesem Fall „Chiffre“, womit jeder Leser die Möglichkeit hat, eine Nachricht zu hinterlassen, die nur vom Autor des minks abgerufen werden kann. Nach der gewählten Laufzeit löscht das System alle gespeicherten Daten. Der mink ist zwar noch öffentlich lesbar, die Informationen dahinter jedoch sind endgültig verloren. Übrig bleibt nur ein ungültiger, „geschmolzener“ Link. Natürlich kann ein Leser während der Laufzeit, alle Informationen innerhalb des minks

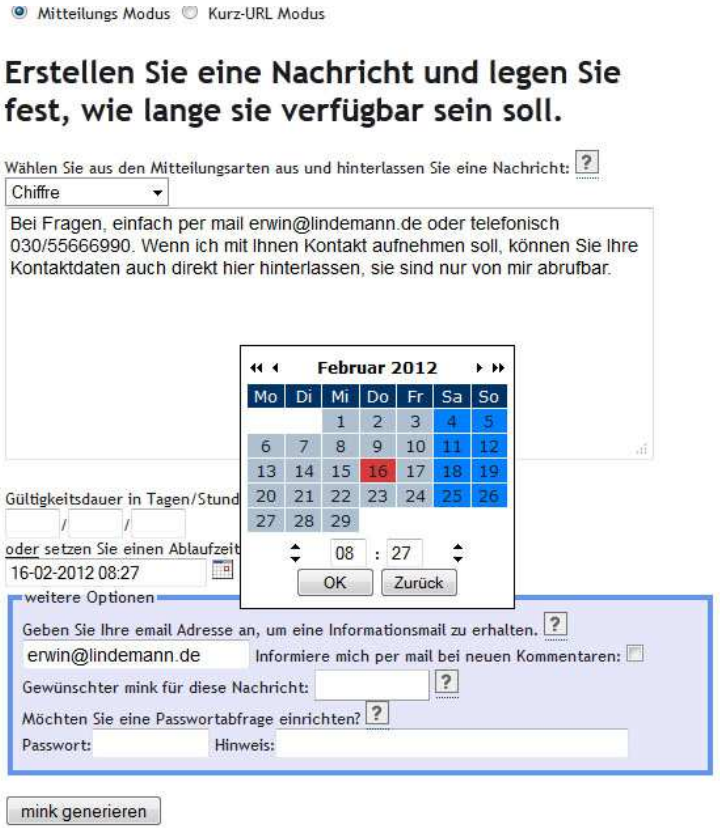

Abbildung 4: Erstellen eines minks

kopieren, im unvermeidbarsten Fall durch ein Kamerabild vom Bildschirm, ein Abruf im Nachhinein, oder eine Suche im Cache von Suchmaschinen, kann so extrem erschwert bis unmöglich gemacht werden.


Ihr mink lautet:

WrCeGpHP6T

Diesen können Sie nun verwenden, um die hinterlegten Informationen während der Gültigkeitsdauer für andere verfügbar zu machen oder eine einfache und sichere Kommunikationsplattform zu erstellen.
Sie können auch direkt darauf verlinken, indem Sie den mink als Direktlink in der Form http://mlnk.de/WrCeGpHP6T angeben, weitere Informationen zu diesem Thema erhalten Sie hier. Sie können zusätzlich einen QR-Code erstellen.
Beachten Sie bitte, daß die Inhalte ohne diesen mink nicht wieder abgerufen werden können!

Die Gültigkeit erlischt am 16.02.12 - 08:27:00.
Sie können Einstellungen und Daten unter folgendem link überprüfen und ändern:
https://www.melting-link.com/minksettings.php?delid=WrCeGpHP6T25e81c020fe4773b
Für Sie abgegebene Nachrichten lassen sich ausschließlich mit diesem Link abrufen.

Eine Informationsmail wird an erwin@lindemann.de versendet.
Zur Startseite

Abbildung 5: Bestätigung nach dem erfolgreichen Erstellen eines minks

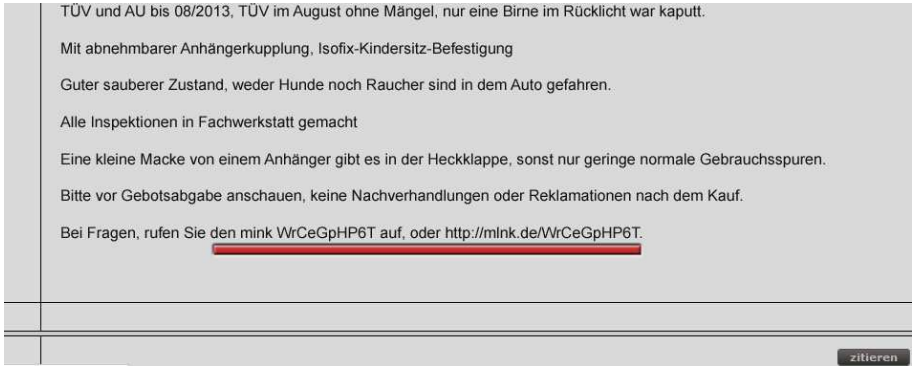

Abbildung 6: So kann der neue Eintrag im Forum aussehen, es wird nur der mink angegeben, oder ggfs. ein (klickbarer) link.

Dies ist natürlich nur ein einfaches Anwendungsbeispiel von vielen, ein mink kann beinahe überall untergebracht werden, ob in einer Email, einer Auktionsbeschreibung, einem Forum oder im Impressum und kann es so ermöglichen, Informationen sicher und gezielt vergessend zu teilen.

Features und Möglichkeiten

Es wird zwischen zwei Haupteinsatzgebieten unterschieden. Der Fokus liegt auf der Verbreitung von nicht persistenten Nachrichten. Zusätzlich wird die Möglichkeit geboten, das System auch als URL-Shortener zu verwenden. Diese Dienste werden in großem Maßstab benutzt und angeboten, um lange URLs auf wenige Zeichen zu verkürzen und sind insbesondere bei twitter sehr beliebt. Diese Funktion leistet auch melting-link.com, so wird der Link
https://www.vergessen-im-internet.de/mitmachen/informationen-fuer-zielgruppen/informationen-fuer-die-wissenschaft.html

durch die Kürzung http://mlnk.de/XsaPN1z2Ih ersetzt und kann von den zusätzlichen Sicherheitseigenschaften profitieren. Links können vertrauliche und sicherheitsrelevante Informationen beinhalten, auch Sessionids und Deeplinks in Firmennetzwerke sind zeitlich begrenzt in den stark verschlüsselten Datenbanken von melting-link.com bestens gesichert. Auch Emailadressen können in diese Form gebracht werden und als Kurz-URL verlinkt werden.

Zusätzlich zu den zeitlichen Begrenzungen kann jeder mink durch ein Passwort geschützt werden. Mit dem optionalen Passworthinweis, können die hinterlegten Informationen gezielt nur einem bestimmten Freundes-/Personenkreis zugänglich gemacht werden. Wer Nachrichten nur mit seinen Freunden teilen möchte, kann für das Passwort „Bello“ etwa den Hinweis „Wie heißt unser Hund?“ wählen und so zusätzliche Privatsphäre schaffen.

Es stehen verschiedene Nachrichtenmodi zur Verfügung:

- „**Normal**“ erstellt eine einfache Nachricht, die ausschließlich während der Gültigkeitsdauer gelesen werden kann.
- „**Einmaliger Abruf**“ erlaubt nur eine einzige Anzeige und löscht dann sofort.
- „**Instantforum**“ erstellt innerhalb eines minks eine Kommunikationsplattform, die in Ihrer Funktionsweise einem öffentlich zugänglichen Forum gleicht. Jeder, dem der entsprechende mink bekannt ist, kann einen Kommentar hinzufügen und so mit anderen Lesern oder dem Ersteller direkt kommunizieren. Eine Benachrichtigungsfunktion informiert auf Wunsch per Email, falls neue Nachrichten im jeweiligen mink geschrieben werden. Diese Benachrichtigungen können jederzeit wieder abbestellt werden. Zudem hat der Ersteller des minks volle Administrationsbefugnisse, kann also unangemessene oder unpassende Kommentare jederzeit editieren oder löschen.
- „**Chiffre**“ bietet eine ähnliche Funktion, wie eine typische Chiffreanzeige in Zeitungen, beispielsweise Stellenanzeigen. Die eingereichten Antworten sind hier lediglich dem Ersteller des minks zugänglich

Es stehen Formatierungsmöglichkeiten, wie Kursivschrift, usw. zur Verfügung, zudem können Videos von youtube.com direkt integriert werden.

Die ausschließlich dem Ersteller zugänglichen administrativen Funktionen erlauben unter anderem eine sofortige Löschung oder Veränderung der Gültigkeitsdauer. Sie sind über einen individuellen Link zugänglich, der nach dem Erstellen angezeigt wird und zusätzlich in der optionalen Informationsmail enthalten ist. Minks können individuell gewählt werden, ansonsten wird ein zufälliger, 10-stelliger Wert ermittelt.

Um die Benutzerführung zu vereinfachen, ist in den Steuerungselementen eine Hilfefunktion integriert, die Informationen zu allen Optionen bereit hält.

Datensicherheit

Der Schutz von Kundeninformationen gehört zu den elementaren Aufgaben jedes Dienstleisters. Wie die erfolg- und folgenreichen Angriffe auf Sony im April 2011 und Stratfor im Dezember 2011 gezeigt haben, stellt diese Aufgabe auch Großkonzerne vor Probleme. Hierbei handelt es sich nur um zwei prominente Beispiele, fast täglich ist in der Presse von entwendeten Kundendaten und gehackten Unternehmensdatenbanken zu lesen. Die hier vorgestellte Anwendung dient explizit der Speicherung sensibler persönlicher Daten und soll diese auch wirkungsvoll schützen. Ein mink soll so sicher sein, dass er auch Konto- und Kreditkartendaten enthalten kann. Diese Sicherheit wird durch die Anwendung eines innovativen Systems der Datenbankverschlüsselung erreicht, das jeden Eintrag individuell sichert und einen Angriff auf enthaltene Daten extrem unwirtschaftlich machen soll.

Die Realisierung erfolgt serverseitig durch PHP und MySQL. Die bereits vorhandenen Schutzmaßnahmen eines Apache Servers sollten im Idealfall einen unberechtigten Zugriff auf den Quellcode sowie die Datenbanken verhindern. Die Erfahrung zeigt aber, dass im Angriffsfall eher ein Worst-Case Szenario vorliegt. Das Sicherheitskonzept muss auch dann wirksam bleiben, wenn der Quelltext (damit auch die Zugriffspasswörter) als auch die kompletten Datenbanken dem Angreifer vorliegen. Um die Sicherheit der Nutzerdaten sicherzustellen, verwendet melting-link.com eine intrinsische und für jeden einzelnen Eintrag separate Reihe von Passwörtern, die dynamisch beim Abspeichern oder Aufrufen erzeugt werden. Weder der Serverbetreiber noch das System hat die Möglichkeit, von sich aus Einträge im Klartext darzustellen.

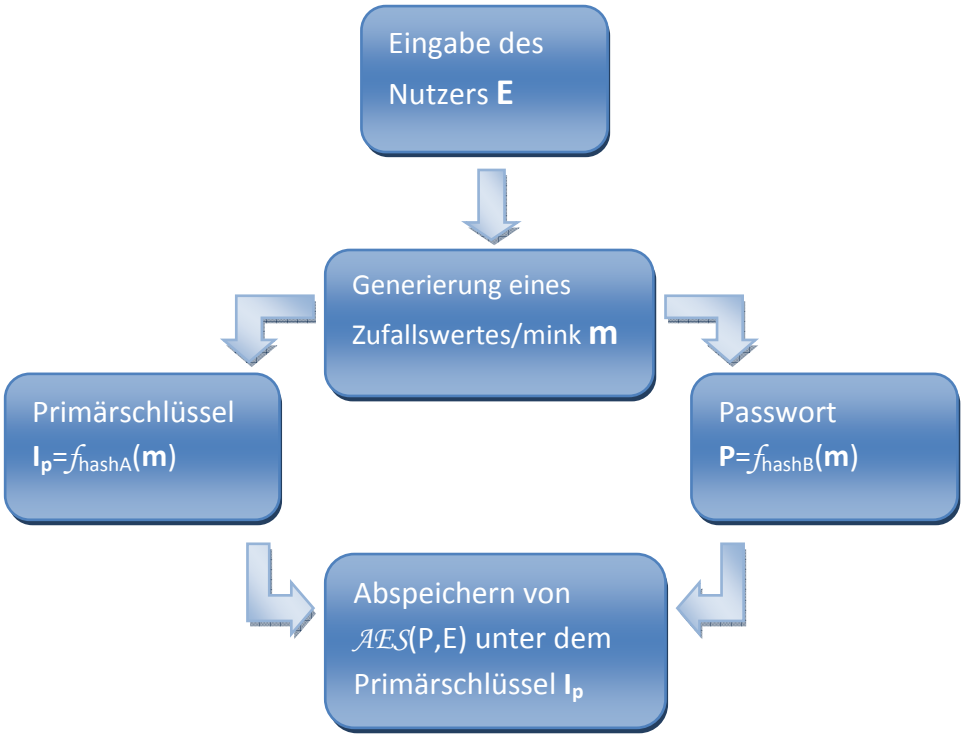

Abbildung 7: Schematische Darstellung der Schlüsselpaarerzeugung bei Neueintrag

Mit jedem neuen Eintrag wird ein 60-bit Zufallswert ermittelt, der den Ausgang für die gesicherte Speicherung bildet, hierbei handelt es sich um den an den Nutzer ausgegebenen mink. Diese Variable wird nach den nötigen Berechnungen vom System sofort verworfen. Für den Eintrag in die Datenbank oder einen Abruf werden zwei voneinander unabhängige Werte benötigt: Der Primärschlüssel, der die Eintragung eindeutig indexiert und wieder auffindbar macht, sowie der Schlüssel, mit dem durch *Rijndael* (AES) die Daten verschlüsselt werden. Generiert werden diese Werte durch kryptographische Hashfunktionen, z.B. MD5 oder SHA-1. Zusätzlich wird mit Salts sowie Key-stretching gearbeitet, um eine höhere Widerstandskraft gegenüber Brute-force Angriffen zu erzielen.[8]

```
function fhashB(mink)
userpw = $_post() ‘optionales Nutzerpasswort
runden = 100000
rundenfunktion = 2^round(log(i))  ‘Beispiel
key = hash(mink+salt)
salt = AAAJxA;AOF/1W;1DtlJytqKbfHlEUQ==mOkO6B
if userpw != null then salt += userpw
for i = 1 to runden do
   key = hash(key+mink+salt+rundenfunktion(i))
next i
return key
```

Erzeugung eines Schlüssels in Pseudocode durch die Funktion $f_{hashB}(m)$

[8] Hintergründe hierzu finden sich z.B. auf http://www.heise.de/security/artikel/Passwoerter-unknackbar-speichern-1253931.html

Um die Unabhängigkeit von Primär- und Codierungsschlüssel zu gewährleisten, können neben verschiedenen Hashfunktionen auch unterschiedliche Salts oder Rundenfunktionen gewählt werden. Mit den so erhaltenen Werten wird ein gesicherter Eintrag in die Datenbanken vorgenommen.

Index value	Encrypted Message	expires
…	…	…
85dd2347aec560680…	…mWu.YT$I1QeaLC…	1365854081
…	…	…

Vereinfachter Auszug aus der von melting-link.com verwendeten Datenbankstruktur

Für eine Suchanfrage wird der fast gleiche Weg gewählt, nur wird anstelle des zu hashenden Zufallswerts die Benutzereingabe verwendet, um die Schlüsselpaare zu erstellen. Kann der so generierte Indexwert $\mathbf{I_p}$ gefunden werden, wird der zugehörige Datensatz „Encrypted Message“ mit **P** entschlüsselt dem Nutzer ausgegeben. Das optional vom Nutzer belegbare Zugriffspasswort ist Bestandteil der Schlüsselerzeugungsroutine $f_{hashB}(\mathbf{m})$ und erhöht so die Verschlüsselungsstärke zusätzlich.

Aber auch ohne Zugriffspasswort ist eine ausreichende Sicherheit gegeben. Ein Angriff mit $1x10^9$ Hashberechnungen pro Sekunde auf einen einzelnen, „normalen“ mink hat einen Erwartungswert von 1,827 Millionen Jahren, bis dieser entschlüsselt dargestellt werden kann. Ohne Kenntnis des minks ist eine Datenausgabe praktisch ausgeschlossen.

Die Internetverbindung von Server zu Computer oder mobilem Endgerät erfolgt standardmäßig über eine zertifizierte SSL-Verbindung.

Obwohl eine 100%ige Sicherheit niemals garantiert werden kann, war es mir wichtig, neben einer Anwendung für ein „vergessendes Internet“ auch die Sicherheit der so gespeicherten Nutzerdaten zu gewährleisten, indem ein Erfolg versprechender Einbruchsversuch in die Datenbank extrem aufwändig und somit teuer wird. Die verwendeten Standardalgorithmen der Hashfunktionen und AES sind sehr gut dokumentiert und gelten bis heute als sicher.

Fazit und Ausblick

Die Weiterentwicklung des gegenwärtigen Web 2.0 ist in vollen Zügen: Die Nutzer gehen immer mehr dazu über, Inhalte nicht nur zu konsumieren, sondern auf den verschiedensten Plattformen selbst zu erstellen und mit anderen zu teilen. Allerdings geschieht dies immer unter fremdem „Hausrecht“ und man verliert jegliche Verfügungsgewalt über die eigenen Daten. Diese werden dauerhaft gespeichert und können auf jede erdenkliche Art und Weise ausgewertet und verknüpft werden. Ein Szenario, dass zwar keine akute Bedrohung beinhaltet, aber doch unabwägbare Konsequenzen bergen kann. Niemand kann heute sagen, was mit über Jahrzehnten gesammelten persönlichen Informationen geschehen wird. Eine Lösung bestünde darin, dass jeder sein eigenes „Social Network“ betreibt oder ausschließlich im eigenen Blog schreibt und so selbst Administrator bleibt.

Es sollte aber auch leichter gehen:

Die bislang vorliegende Version von melting-link.com bietet umfangreiche und sichere Methoden, um Informationen auf jeder Plattform gezielt nicht dauerhaft zu verbreiten. Sie bleiben selbst Herr Ihrer Daten und geben nicht – wie in vielen AGBs festgelegt – Rechte daran an die Betreiber ab. Durch die integrierte Funktion des Instantforums ist noch mehr möglich, als nur Informationen

bereitzustellen. Es bietet eine Basis für schnelle, unkomplizierte und sichere Kommunikation.

Die Betaversion verfügt noch über weitere Ausbaumöglichkeiten, die Integration von Bildern wäre ebenso möglich, wie die Anwendung als Plugin in anderen Diensten. Eine Integration, etwa in das Interface von facebook und angewendet auf Nachrichten und Pinnwandeinträge, wäre ein weiterer Schritt in Richtung einer individuellen, informationellen Selbstbestimmung.

Im Brennpunkt bleibt jedoch nach wie vor der Benutzer selbst, da Datenschutz und Sicherheit nicht automatisch gewährt werden können, sondern immer aktiv betrieben werden müssen.

Melting-link.com will Ihnen ein Werkzeug hierfür zur Verfügung stellen!