SICHERHEIT UND DATENSCHUTZ MIT "MANITOU4U"

- www.manitou4u.com -

Infostand: 20.02.2014 14:29:00

aracube e.V.
Händelstraße 7a
09120 Chemnitz

Tel.: +49 371 / 4020133
Mobil: +49 171 / 9320133
www.aracube.de
Dirk Liesch: manitou4u@web.de

INHALTSVERZEICHNIS:

1 EINLEITUNG UND ÜBERSICHT 2

2 FRAGMENTIERUNG MEINER DATEN ÜBER VERTEILTE QUELLEN 3

3 VERSCHLÜSSELUNG MEINER DATEN 3

4 PEER-2-PEER (P2P) ÜBERTRAGUNG 4

5 CLIENT-SICHERHEIT (OPEN SOURCE) 4

6 100% SICHERHEIT WIRD ES NICHT GEBEN 5

7 WAS ERREICHE ICH MIT MANITOU4U AN ZUSÄTZLICHER SICHERHEIT UND DATENSCHUTZ? WIE WÜRDEN TYPISCHE STUFEN EINEN ANGRIFFS AUF MEINEN DATENSCHUTZ AUSSEHEN? 6

8 WARUM BENÖTIGE ICH DATENSCHUTZ, FRAGTE MICH MEIN KLEINER SOHN? 7

9 WEITERE NÜTZLICHE UNABHÄNGIGE INFORMATIONEN ZUM THEMA- SICHERHEIT, DATENSCHUTZ UND ÜBERWACHUNG: 7

1 Einleitung und Übersicht

In 2010 entschieden wir erstmals im aracube e.V., dass der Weg der serverseitigen Zusammenführung persönlicher Daten (so wie heutige soziale Netzwerke und Unternehmensportale funktionieren) aus Sicherheits- und Datenschutzaspekten der falsche Weg ist. U. E. führt dies zu Monopolen und quasi einer Versklavung der Nutzer, da die Abhängigkeit von einzelnen Anbietern zu hoch wird und zu viele kritische sensible Daten an einer Stelle (außerhalb der Kontrolle des Nutzers) zusammengeführt werden.

So entstand die Idee einer Lösung welche mit vielen verteilten Daten, Verschlüsselungen und Übertragungswegen umgehen kann und die Informationen erst auf dem Endgerät des Nutzers im vollständigen Kontext zusammenführt. Nach zahlreichen Diskussionen mit IT-Experten zur Sicherheit der technischen Machbarkeit und zur Strategie mit der höchsten Erfolgswahrscheinlichkeit einer Realisierung, startete im Frühjahr 2012 offiziell das „manitou4u"-Projekt zu einer persönlichen Wissensumgebung, welche dieses Konzept umsetzt.

Obwohl dieses Konzept damals hautsächlich die übermäßige Abhängigkeit von großen Internet-Konzernen (Wirtschaft) reduzieren sollte, taugt es nun genauso gut, für einen besseren Schutz gegen den Datenmissbrauch durch Geheimdienste. Es schützt sowohl die Privatsphäre von Nutzern, als auch die Daten von Unternehmen, wenn deren Mitarbeiter „manitou4u" nutzen würden.

Was sind Vision und Ziele des manitou4u-Projektes:

"manitou4u" verändert das Internet zu einem „Sicheren Sozialen Netz" in dem konsequent der Nutzer und seine Interessen, sein Datenschutz und seine Unabhängigkeit im Mittelpunkt stehen, in dem:

- Menschen wieder die Hoheit über ihre persönlichen Daten erlangen und diese selbst kontrollieren
- Nutzer frei entscheiden können welchen Dienst mit welchen Geschäfts- und Datenschutzbedingungen sie nutzen möchten, weil sie reale Auswahlmöglichkeiten haben.
- Freunde und Kontakte aus unterschiedlichen sozialen Netzwerken von überall auf der Welt (auch von privaten Rechnern) zusammen führen
- Schüler, Studenten und andere Lernende nur eine Bedienoberfläche nutzen um an allen Universitäten, Schulen und in Weiterbildungseinrichtungen (inkl. Unternehmen) online zu lernen (wobei "Lernen" nur ein Beispiel von vielen "Wissensbereichen" ist)
- Wir all unser persönliches Wissen zusammenführen, nur einmal, ohne Duplikate, was vielleicht aus hunderten Qellen und Diensten kommt, zusammengeführt nur persönlich für uns, erst und nur bei uns, wo wir es kontrollieren können ... und nicht Dritte.

Bis Ende 2014 soll die Finanzierung und das Partnernetzwerk stehen, mit dem die erste Version des Open Source Projektes „manitou4u" realisiert wird. Dabei sind wir als gemeinnütziger Verein auf eine starke Unterstützer - Community angewiesen.

Dazu hilft uns auch IHRE Unterstützung.

Wie hilft der „matitou4u"-Ansatz konkret, den Datenschutz und die Sicherheit der Nutzer mittelfristig zu verbessern? Auf die Hauptkomponenten gehen die nächsten Abschnitte ein:

- Fragmentierung meiner Daten über verteilte Quellen
- Verschlüsselung meiner Daten
- Peer-2-Peer (P2P) Übertragung
- Client-Sicherheit (Open Source).

Antworten auf typische Fragen im Umfeld des Datenschutzes und der Sicherheit sollen in den folgenden Abschnitten die relativ umfassende Betrachtung zum Thema abrunden:

- 100% Sicherheit wird es nicht geben
- Was erreiche ich mit manitou4u an zusätzlicher Sicherheit und Datenschutz? Wie würden typische Stufen einen Angriffs auf meinen Datenschutz aussehen?
- Warum benötige ich Datenschutz, fragte mich mein kleiner Sohn?
- Weitere nützliche unabhängige Informationen zum Thema- Sicherheit, Datenschutz und Überwachung.

Als Reaktion auf die Enthüllungen von E. Snowden und die daraus folgende NSA Affäre, hat sich das manitou4u-Projektteam auf Basis seiner dreijährigen Vorarbeit die Frage gestellt:

- Wie könnte eine grundlegende, übergeordnete und vorwärtsgerichtete Strategie der Bundesregierung aussehen?

Als Ergebnis ist der „Offener Brief an die Bundesregierung“ des manitou4u-Projektteams vom 22.7.2013 entstanden, der eine mögliche sinnvolle Strategie umreißt. Das Projektteam würde sich sehr freuen, an einer Ausgestaltung, Weiterentwicklung und Umsetzung dieses Strategie-Vorschlages aktiv mitzuarbeiten.

2 Fragmentierung meiner Daten über verteilte Quellen

Wenn meine persönlichen Daten bruchstückhaft über viele Dienste verstreut sind, z. B. über viele "soziale Netzwerk"-Anbieter und Cloud-Services, dann besitz jeder Anbieter z.B. nur ein Puzzleteil eines 1000teiligen Puzzles. Daraus ist es sehr schwer (für den einzelnen Anbieter unmöglich) das Gesamtbild zusammen zu setzen. Befinden sich die Dienste auch noch auf Servern und Rechnern unterschiedlicher "Gesellschaftssysteme" ist das Einsammeln aller Puzzleteile auch für mächtige Organisationen schwierig, also für einen "Normalbürger" als Ziel wahrscheinlich zu aufwändig. Habe ich Teile meiner Daten mit Freunden nur so geteilt, dass diese nur bei diesen, auf deren Endgeräten liegen, wird das Einsammeln für jene Organisationen noch aufwendiger. Das zentrale Ergebnis von "manitou4u" ist, dass so ein verteiltes Netzwerk von Puzzlestücken entstehen kann, ohne Mehraufwand oder kompliziertere Bedienung für den Nutzer selbst.

3 Verschlüsselung meiner Daten

Wenn ich meine Daten "sicher" verschlüsseln kann, so dass nur der berechtigte Empfänger diese wieder entschlüsseln (lesen, sehen, hören, schmecken, fühlen ;-) kann, so ist die unberechtigte Nutzung dieser Informationen nur noch durch die Hacker / Organisationen möglich, welche entweder den eigenen Computer (Smartphone etc.) oder den des Kommunikationspartners gekapert (gehackt) haben. Dazu ist jedoch eine ununterbrochene Verschlüsselung zwischen Sender und Empfänger (Ende zu Ende Verschlüsselung) erforderlich. Oft erfolgt die Verschlüsselung derzeit (auch bei Diensten, die mit Sicherheit werben) nur auf dem Übertragungsweg, von Ihrem Rechner bis zum Server des

Dienstanbieters. Zum Beispiel auf dem Server von Facebook, Google o. a. liegt z. B. Ihr Foto unverschlüsselt. Jeder, der also Zugriff auf die Festplatten bei diesem Anbieter hat, kann ihr Foto lesen, kopieren und nach seinen Wünschen verwenden (ob nun rechtlich erlaubt o. verboten). Sie müssen sich also Anbieter wählen, die es auch gestatten, dass Ihre Inhalte auf dem Server (des Anbieters) verschlüsselt bleiben und nur die von Ihnen zugelassenen Personen diese Infos erst auf ihren privaten Rechnern (Endgeräten) entschlüsselt bekommen und sehen können. Die gilt ganz besonders für Dienste, welche Sie zum synchronisieren Ihrer Daten über verschiedene Ihrer Endgeräte (z.B. Computer, Smartphone) nutzen.

Ein weiterer Aspekt hier ist die Wahl eines geeigneten Verschlüsselungsverfahrens. Es gibt verschiedene Verfahren, von denen einige durch die NSA mitentwickelt wurden und unterstützt werden. Diese könnten zumindest Geheimdiensten einen unverschlüsselten Zugang ermöglichen. Je nach aktuellem Entwicklungsstand sollten jeweils die Verschlüsselungsverfahren eingesetzt werden, die als recht sicher gelten. Derzeit könnten dies auf GnuPG beruhende Verschlüsselungen sein.

Das "manitou4u"-Projekt unterstützt die Einbindung unterschiedlichster Verschlüsselungsverfahren, die dann sehr einfach und weitgehend transparent durch die Nutzer eingesetzt werden können. Dies geht natürlich nur über Dienste, die auch den Austausch verschlüsselter Daten zwischen ihren Nutzern gestatten.

4 Peer-2-Peer (P2P) Übertragung

Wenn Sie Ihre Daten direkt von Ihrem Rechner auf das Endgerät des berechtigten Empfängers übertragen, also z. B. direkt von Ihrem Rechner auf das Smartphone Ihrer Tochter, dann spricht man von einer "peer-to-peer" Übertragung (Verbindung). Die Daten werden dabei auf keinem Server eines Anbieters (z. B. Facebook) zwischengespeichert. Diese Übertragung ist auch verschlüsselt möglich. Achtung: Es gibt auch P2P-Modelle bei denen die Daten zuerst auf einem Server zwischengespeichert werden. Diese sind hier nicht gemeint. Da bei der direkten Übertragung an den Rechner des Empfängers keine Datei bei einem Anbieter abgelegt wird, können diese dort auch nicht von Dritten abgegriffen / genutzt werden. Dadurch bieten "peer-to-peer" Lösungen systembedingt ein besseres Datenschutz-Potential. P2P hat deshalb natürlich auch den Nachteil, dass die Übertragung der Daten nur zu einem Zeitpunkt möglich ist, an dem beide Geräte (Sender und Empfänger) gleichzeitig online sind.

Eine typische heute verwendete Lösung zur P2P Übertragung ist BitTorrent (vor allem zum Austausch größerer Dateien verwendet).

Das "manitou4u"-Projekt unterstützt von Anfang an den P2P - Datenaustausch zwischen Nutzern, so dass Freunde Daten austauschen können, ohne dass dies ein "Anbieter" mitbekommt.

5 Client-Sicherheit (Open Source)

Wenn eine Software als "Open Source Software" (OSS) entwickelt wird, ist der gesamte Quellcode (der durch Menschen erstellte, lesbare und hoffentlich verständliche Programmcode) frei zugänglich. Computer- und Sicherheitsexperten können daraus viel einfacher erkennen, ob eine Software sicher ist und vor allem auch, ob sie Hintertüren (Backdoors) für Angreifer hat. Auch Programmierfehler (Bugs) sind wesentlich einfacher zu erkennen und können direkt durch die offene Community behoben werden. Damit ist es möglich transparent nach Außen nachzuweisen, dass eine Software sicher ist, oder welche Sicherheitslücken zu beheben sind. Dadurch ist nicht nur Vertrauen in die Lösung

möglich (frei von Hintertüren), sondern auch die schnellstmögliche Beseitigung von erkannten Schwächen. Deshalb ist Open Source Software eher geeignet, Vertrauen zu schaffen, als eine geschlossenen Software, bei der evtl. die Sicherheitsdienste des Landes des Herstellers die Hände mit im Spiel haben könnten.

"manitou4u" soll als Open Source Projekt in einer offenen Community entwickelt werden.

6 100% Sicherheit wird es nicht geben

Wir werden keine 100%ige Sicherheit der persönlichen Daten erreichen können. Wieso? Ein Beispiel für den Anfang:

Im Betriebssystem "Windows" wurde entdeckt, dass es in der zentralen Verschlüsselungsbibliothek seit der Version "Win95" einen "NSAKey" gibt. Es ist u. a. deshalb sehr wahrscheinlich, dass die NSA seit dieser Version jeden Windows-Rechner "kapern" kann (sich wahrscheinlich direkt darauf einloggen, sobald dieser Rechner online ist). Danach könnte alles was auf dem Rechner passiert, alles, was eingegeben oder angezeigt wird, mitgeschnitten werden. Dagegen hilft auch "manitou4u" nicht. Es ist wahrscheinlich, dass noch viele andere amerikanische Softwarekonzerne solche "Backdoors" in ihre Lösungen einbauen mussten. Unabhängig von diesen extra bereitgestellten Hintertüren, gibt es natürlich noch Sicherheitslücken die zufällig in komplexer Software enthalten sind und welche ausgenutzt werden können. Davor sind auch Open Source Systeme wie "Linux" nicht gefeit. Außerdem nutzen alle komplexen Lösungen bestehende Entwicklungsplattformen (z. B. Java = Oracle, früher Sun Microsystems) oder Datenbanklösungen. In diesen Lösungen sind ebenfalls sicherheitsrelevante Bugs und eingebaute Hintertüren möglich. Nicht zuletzt ist "manitou4u" selbst eine komplexe Lösung, die nie 100% bugfrei sein kann.

Nach dem großen Aufschrei (und Strafverfolgung) der US-Sicherheitsbehörden, dass der sichere Verschlüsselungs-Algorhythmus PGP (public key Verschlüsselung, Pretty Good Privacy) die USA verlassen hat, wurde in Zusammenarbeit mit der NSA das AES - Verschlüsselungsverfahren entwickelt und dessen weltweite Durchsetzung sehr gefördert. Es hält sich seitdem das Gerücht, dass es dafür einen Generalschlüssel gibt, um alle damit verschlüsselten Daten lesen zu können. Das bedeutet, dass wir selbst bei verschlüsselten Daten nicht sicher sein können, dass diese einigermaßen sicher sind, ganz unabhängig davon, wie lang der Verschlüsselungs-Key ist, mit dem immer geworben wird.

Das oft größte Risiko kommt zudem von uns als Anwendern selbst, wenn ich z. B. Daten von nicht vertrauenswürdigen WWW-Sites auf meinen Rechner / Smartphon lade, wenn ich Apps installiere, die ggf. auch ohne meine Zustimmung alle Infos vom Smartphone, inkl. evtl. aller Eingaben und Ausgaben aufzeichnen und weiterleiten. Wenn ich nicht sorgsam mit Passworten, Zugängen und Schlüsseln umgehe, usw. Hier als Anwender das Meiste richtig zu machen, erfordert Disziplin und Bewusstsein für die Risiken und Lösungsmöglichkeiten. Dies ist schwer, kontinuierlich durchzuhalten.

7 Was erreiche ich mit manitou4u an zusätzlicher Sicherheit und Datenschutz? Wie würden typische Stufen einen Angriffs auf meinen Datenschutz aussehen?

Wenn wie heute alle persönlichen Daten meines sozialen Netzwerks bei einem Anbieter liegen, und ich dort sein muss, weil es quasi ein Monopol hat, dann bestimmt dieser Anbieter seine allgemeinen Geschäftsbedingungen nach seinem kommerziellen Interesse. Er wird mich und meine Daten hierdurch mit maximalem Profit verkaufen. Ich habe keine Wahl und mein gesamtes privates (und ggf. berufliches) Leben wird für diesen Anbieter und seine Kunden (inkl. Geheimdienste) transparent, ganz einfach und ohne großen Aufwand. Der "gläserne Mensch" ist Realität.

Erfolgt nur die einfache Fragmentierung der Daten über eine möglichst große Zahl von Anbietern und Wettbewerbern, wie mit dem "manitou4u"-Projekt angestrebt, erhält jeder Anbieter nur ein Puzzle-Teil. Nur dieses Teil von uns, wird dann bei diesem Anbieter transparent. Das zusammensammeln dieser Teile ist deutlich erschwert, vor allem, wenn die Anbieter Wettbewerber sind und in unterschiedlichen Staaten und Gesellschaftssystemen zu Hause sind.

Wenn ich meine Daten jetzt noch mit "manitou4u" auf dem Gesamtweg vom Sender zum Empfänger verschlüssele, dann sind selbst diese Puzzleteile nicht mehr für den Anbieter transparent und selbst für Geheimdienste kann es schwierig sein, diese zu entschlüsseln, selbst bei Zugriff auf die Server des Anbieters. Nutze ich dann noch die "peer-to-peer" Funktionalität über "manitou4u", kommen diese verschlüsselten Puzzleteile gar nicht mehr zum Anbieter auf den Server. Einem Geheimdienst bleibt dann nur noch das Abfangen der Pakete an den Datenleitungen. Werden hierzu durch die "peer-to-peer" Lösung unterschiedliche Übertragungswege gewählt, muss der "Angreifer" alle genutzten Wege kontrollieren, was noch einmal deutlich schwieriger ist. Die Folge wäre die Strategie des "Angreifers" Ihr Endgerät (Rechner, Smartphone etc.) zu kapern, wie Sie dies heute über Trojaner und Vieren kennen. Seit Stuxnet und Bundestrojaner wissen wir, dass dies auch an allen Virenscannern vorbei möglich ist, aber es ist aufwändig, heute noch zum Teil auch durch Behörden illegal und wird wahrscheinlich zumindest für private Firmen illegal bleiben.

Eine Verteidigung gegen das Kapern des eigenen Rechners liegt außerhalb der Möglichkeiten von "manitou4u". Teilweise können hier andere Strategien helfen: Zum einen könnte man sich jeweils auf einem "komplett platt gemachten" Endgerät (Computer, Smartphone) ein als sicher geltendes Betriebssystem in einer als sicher geltenden Konfiguration neu einrichten (z. B. Linux, wohl eher nicht Windows oder MacOS). Die Einrichtung sollte so erfolgen, dass alle angeschlossenen Datenträger,auf denen man seine Dateien/Daten speichert, möglichst sicher verschlüsselt sind. Danach legt man sich davon ein Backup (Image) an, auf einem nur 1x beschreibbaren Medium (z.B. DVD). Idealerweise spielt man dieses System-Backup (Image) jede Nacht erneut auf seinen Rechner, so dass ein Trojaner dabei mit hoher Wahrscheinlichkeit platt gemacht wird. Notfalls reicht dies auch 1x pro Woche bzw. nachdem man sein Notebook zum Sicherheitscheck auf dem Flughafen kurz abgeben musste ;-). 100% sicher ist dieses Vorgehen auch nicht und zudem recht aufwändig und derzeit für "Normalbürger" sehr schwierig.

8 Warum benötige ich Datenschutz, fragte mich mein kleiner Sohn?

Wieso brauche ich Datenschutz, wenn ich nichts zu verbergen habe und nur ein kleiner unbedeutender Bürger oder Schüler bin?

Natürlich konnte ich es meinem Sohn nicht mit der Werbung inoffizieller Mitarbeiter durch die Stasi oder entsprechende Veröffentlichungen zur Informanten-Gewinnung durch die NSA (von Edward Snowden) erklären. Auch dass er vielleicht keine Krankenversicherung mehr bekommt, wenn er einmal nach seinem Hobby "Klettern" im Internet gesucht hat, kann er in der Konsequenz noch nicht ganz verstehen. Er versteht auch nicht, dass es für eine funktionierende Demokratie ungünstig ist, wenn Atomkraftgegner schon aus dem Verkehr gezogen werden, ehe sie auch nur den Antrag auf eine Demonstration stellen können. Also habe ich es so versucht:

" Hast Du schon einmal mit einem Freund ein Spiel getauscht, dass ihr beide nicht bezahlt habt oder Euch einen Login für ein Spiel geteilt, dass ihr nicht teilen durftet? Hast Du schon einmal Musik von einem Freund bekommen, oder einen Film geschaut, den ihr nicht bezahlt habt?

Stell Dir nun einmal vor, Du wirst auf der Straße von einer lieben Frau angesprochen, die Dich bittet, Ihr aus dem Leben Deines Freundes oder Deiner Eltern zu erzählen. Wenn Du es nicht tust, sagt Sie, kommen Deine Eltern ins Gefängnis, weil sie für Dich verantwortlich sind, da Du illegal z. B. Filme angesehen oder Musik getauscht hast. Würdest Du dann Deine Eltern ins Gefängnis gehen lassen, oder sie ausspionieren?"

Ich hatte das Gefühl, er hat verstanden, warum es ungünstig ist, wenn alles was man tut durch eine autoritäre Macht gegen einen verwendet werden kann, selbst wenn man ein kleines Licht ist.

Die aktuellen E.Snowden Veröffentlichungen und die Reaktion unserer westlichen Demokratien darauf, zeigen, dass diese Gefahren für jeden Einzelnen und die Gesellschaft wie wir sie heute kennen, ganz real sind und nicht die Theorien von Verschwörungstheoretikern.

9 Weitere nützliche unabhängige Informationen zum Thema-Sicherheit, Datenschutz und Überwachung:

"Der Überwachung entgehen? Das macht richtig viel Arbeit" (faz, 3.7.2013, Felix von Leitner)

Wer schon heute etwas für sich selber tun oder sich mehr informieren möchte, dem hilft vielleicht die "Sicherheits"-Reihe in Spiegel-Online:

- "Tor-Router zum Selberbauen: Internet -Tarnkappe für 65 Euro"
- "Schutz gegen Internet - Spione: So verschlüsseln Sie Ihre eMails"
- "Cryptopartys: Verschlüsseln gegen Staat und Schurken"

oder der Artikel in der Zeit-online:

"Die Massen sollen Verschlüsseln lernen"(8.7.2013, zeit-online, P.Beuth)

Eigentlich sollte Bürgern in Deutschland auch das BSI (Bundesamt für Sicherheit in der Informationstechnik) helfen. Einige nützliche Informationen und Hinweise finden sich auch dort. Ob aber auch hier Verbindungen zur NSA bestehen und bestimmte "Hintertüren" gedeckt werden, ist seit den E. Snowden Veröffentlichungen und fehlenden Stellungnahmen des BSI schwer einzuschätzen. Die Frage für die Zukunft ist, hilft das BSI zukünftig aktiv mit Lösungsempfehlungen und Projektunterstützungen die Bürger und Unternehmen gegen bekannte Bedrohungen auch durch Geheimdienste und gegen öffentlichen Missbrauch zu schützen.

Eine gute und bisher neutrale Informationsquelle auch für diese Themen ist der "Chaos Computer Club" (CCC).

Autor: Dirk Liesch (8.7.2013, einige kleinere aktuelle Ergänzungen: Jan/Feb 2014)