Für sofortige Veröffentlichung freigegeben

Pressemitteilung 3. August 2018

OPEN RHEIN RUHR
Ein Pott voll Software

3. / 4. November
Rheinisches Industrie-museum Oberhausen

www.openrheinruhr.de
presse@openrheinruhr.de

Werner Koch als Keynote Speaker bestätigt

Nicht erst seit Edward Snowdens Enthüllungen werden Aspekte wie Datenschutz und Privatsphäre immer wichtiger. Die Software-Unterstützung für die Realisierung dieser Aspekte stellt damit die Grundlage für diese Anforderungen dar.

Die OpenRheinRuhr freut sich, mit Werner Koch einen der führenden Experten auf dem Gebiet der Software-Unterstützung für Verschlüsselung und damit Datensicherheit und Privatsphäre gewonnen zu haben. Der von ihm entwickelte GNU Privacy Guard (GPG) stellt die Basis für zentrale Sicherheitsaspekte wie Verschlüsselung von E-Mails und anderen Daten dar.

Die OpenRheinRuhr freut sich, mit Werner Koch einen der führenden Experten auf dem Gebiet der Verschlüsselung und Computer-Sicherheit als Keynote Speaker zu bestätigen zu können. Als Initiator und Hauptentwickler von GNU Privacy Guard (GPG) legte er den Grundstein für eine der Software-Infrastrukturen, die Verschlüsselung und damit Datensicherheit und Privatsphäre erst möglich machen. Erweiterungen wie Enigmail für den beliebten Mail-Klienten Thunderbird und Dateiverschlüsselungs-Software wie GPG4win sind durch GPG erst möglich geworden.

Die OpenRheinRuhr hatte im Vorfeld der Konferenz die Möglichkeit, mit Werner Koch ein kurzes Interview zu führen:

OpenRheinRuhr: GPG ist ein führendes Werkzeug zur Verschlüsselung von Daten und stellt damit die Grundlage für Aspekte wie Datenschutz und Privatsphäre dar, die in den letzten Jahren immer mehr Bedeutung erlangt haben. Wie kam es zu der Entwicklung?

Werner Koch: Nach einem Gespräch mit Richard Stallman (Gründer der Free Software Foundation, FSF, Anm. d. Red.), der auf der Suche nach einer Verschlüsselungslösung für das GNU-System war, entschloss ich mich, den Grundstein in Form einer freien Implementierung zu legen. Der Rest ist Geschichte. <Stimmt das? Bitte um Richtigstellung bzw. Ergänzung>

ORR: Wie wichtig ist Datenschutz und Privatsphäre im Zeitalter von sozialen Netzwerken, die ihre Nutzerdaten verkaufen und Großkonzernen, die im großen Stil ähnliche Geschäfte mit den Daten ihrer Kunden machen? Seitdem Inkrafttreten der Datenschutzgrundverordnung (DSGVO) fühlen sich ja viele Benutzer durch Popups auf Webseiten genervt – mal von den hunderten von E-Mails, die eine explizite Einwilligung für die Speicherung und Nutzung von persönlichen Daten fordern. Siehst Du einen Trend hin zur Ermüdung von Nutzern, was Themen wie Privatsphäre und Datenschutz angeht?

WK: Im Gegenteil – nicht erst seit den Enthüllungen zur Abhörtätigkeiten des BND, der NSA und des GCHQ wird der Schutz von privaten Daten immer wichtiger. Firmen, wie auch Benutzer, müssen heutzutage immer genauer hinschauen, welche Daten sie wem wann in welcher Form und wie zur Verfügung stellen. Dabei spielt die Übermittlung der Daten eine zentrale Rolle – ohne sichere Datenverschlüsselung ist hiermit Missbrauch Tür und Tor geöffnet. Werkzeuge die auf GnuPG (auch als GPG bekannt) basieren, helfen Benutzern hierbei, online und offline sicher zu bleiben und so ihre Daten und Privatsphäre zu schützen..

ORR: GPG unterliegt der GNU General Public License (GNU GPL) und ist damit freie Software. Was waren Deine Gründe für die Offenlegung des Quellcodes?

Für sofortige Veröffentlichung freigegeben

WK: Nicht nur grundlegende Software wie GPG sollte frei sein. Freie und damit quelloffene Software stellt einen wichtigen Baustein für sämtliche Aspekte des modernen Lebens dar. Ob wir unser Smartphone auf Android-Basis zum Lesen von E-Mail benutzen, Firefox oder Chrome zum Surfen verwenden oder Software wie GPG zur Sicherung der Privatsphäre nutzen – immer kommen damit freie Software zum Einsatz. Insbesondere die GNU GPL und deren Varianten stellen, die mit der Verbreitung der Software auch zur Weitergabe des Quelltextes verpflichten, leisten einen wichtige Beitrag zur Software-Qualität und Innovation. Dadurch das der Quellcode frei zugänglich ist, kann jeder potentielle Fehler analysieren und durch geeignete Korrektur des Quellcodes diese beheben und somit zur Optimierung der Sicherheit von dieser Software beitragen. Desweiteren wird hierdurch auch eine Abhängigkeit von nur einem Hersteller verhindert. Niemand würden ein Auto kaufen, welches nur in einer Vertragsverkstatt repariert werden darf. Allerdings birgt quelloffene Software auch Herausforderungen.

ORR: Was genau meinst Du damit?

WK: Nicht erst seit der Schaffung der GNU GPL ist ein Ökosystem an freier Software entstanden, die von Millionen Entwicklern tagtäglich eingesetzt wird. Aber mit Nutzung von quelloffener Software bzw. an deren Mitarbeit geht ebenfalls Verantwortung einher.

ORR: Das klingt abstrakt.

WK: Zwei Beispiele: Sehr viel quelloffene Software ist exzellent dokumentiert. Leider wird diese Dokumentation oft nur flüchtig gelesen, wie man u. a. an den Fragen zu vielen Themengebieten auf Plattformen wie z. B. Stackoverflow erkennen kann. Wie oft sehe ich Kommentare zu Fragen, die vorschlagen, doch erst einmal die jeweiligen Manual-Pages oder Online-Dokumentation zu Rate zu ziehen, anstatt direkt eine Frage auf dem jeweiligen Portal zu stellen?

ORR: Das klingt vertraut....

WK: Ein anderer Aspekt ist die suboptimale Implementierungs-Qualität von einigen quelloffenen Software-Pakete. Ein Beispiel aus jüngerer Vergangenheit hierfür ist die EFAIL-Sicherheitslücke. Diese Angriffsmöglichkeit erlaubt es, verschlüsselte E-Mails unter gewissen Umständen unautorisiert zu entziffern. Zwar ist die Konstruktion des Angriffsvektors (also die Art und Weise, wie ein System hierbei angegriffen wird), ein wenig aufwendiger, aber sobald diese Hürde überwunden ist, kann eine eigentliche verschlüsselte E-Mail mit wenig weiterem Aufwand gelesen werden. Ein wenig mehr Sorgfalt bei der Implementierung der grundsätzlichen Mechanismen bei den verwendeten Komponenten (S/MIME bzw. OpenPGP, Anm. d. Red.) in Verbindung mit sicheren Standard-Konfiguration der jeweiligen E-Mail Software hätte hier Wunder gewirkt.

ORR: Aber trotzdem wurde diese Lücke nach Bekanntwerden relativ schnell geschlossen...

WK: Die Community steht in der Regel zeitnah mit Rat und Tat zur Seite. Nach der initialen Analyse gibt es sehr schnell Abhilfe in Form von Anleitungen zur Rekonfiguration von E-Mail Klienten und anderen Möglichkeiten die Angriffe ins Leere laufen zu lassen. In dem besagten Fall hatten die Autoren der Studie es allerdings versäumt, die verantwortlichen Mitglieder rechtzeitig und vollständig zu informieren. Sie hatten von großen Herstellern, die wirklich relevant von dem Problem betroffen sind (S/MIME in Outlook), die Antwort erhalten, es würde sich lediglich um ein theoretisches Problem handeln und keiner Abhilfe bedürfen. Die Community um die freie Software hat es dagegen sofort als ernstes Problem erkannt und Lösungen geschaffen die schnell verfügbar waren (für S/MIME und OpenPGP). Auf der proprietären Seite ist S/MIME immer noch leicht angreifbar.

Werner Koch ist der Initiator und Hauptautor des GNU Privacy Guard (GPG), einer freien Software zur Verschlüsselung und digitalen Signatur nach den OpenPGP und S/MIME Standards. Seit über 30 Jahren entwickelt er Software wie Gerätetreiber, Fakturierung- und Finanzberatungssysteme, Datenkonvertierungen und seit 1997 eben auch kryptographische Anwendungen. Er ist Vorsitzender des GnuPG e.V., Mitgründer der FSFE sowie Geschäftsführer der g10 Code GmbH, die technische Lösungen gegen Überwachung entwickelt.

Pressekontakt: OpenRheinRuhr e. V., presse@openrheinruhr.de, Tel.: 0208-675240