2018/22 Networld

https://www.jungle.world/artikel/2018/22/cryptowars-cypherpunks-und-ein-fehlalarm

Das Thema Verschlüsselung wird in der Datenschutzdebatte zu wenig thematisiert

Cryptowars, Cypherpunks und ein Fehlalarm

Von **Enno Park**

Vermeintliche Sicherheitslücken in Verschlüsselungssystemen für E-Mails haben im vergangenen Monat für Verwirrung gesorgt. Doch die Krypto-Verfahren selbst sind überhaupt nicht betroffen.

Mitte Mai brachte ein Tweet der Electronic Frontier Foundation viele Menschen weltweit dazu, ihre E-Mail-Verschlüsselung abzuschalten. Die US-Bürgerrechtsorganisation behauptete, einen schwerwiegenden Fehler im Kryptographiesystem GNU Privacy Guard gefunden zu haben, der die Computer, auf denen das System eingesetzt wird, angreifbar mache. Sie empfahl, entsprechende Plug-ins für E-Mail-Programme zu entfernen. Wer das tat, konnte anschließend keine verschlüsselten Mails mehr senden oder empfangen. Alte verschlüsselte Mails ließen sich nur noch mit Mühe lesen. Dabei war die Warnung völlig unnötig.

Innerhalb kurzer Zeit stellte sich heraus, dass die Sicherheitslücke gar nicht die Verschlüsselungssoftware selbst betraf, sondern die E-Mail-Programme. Für den Fall, dass ein Angreifer in der Lage ist, E-Mails vor der Zustellung abzufangen und zu manipulieren, könnte etwas eingeschleuster HTML-Code das E-Mail-Programm dazu bringen, den entschlüsselten Inhalt an einen Server im Internet zu schicken. Das ist eine peinliche Lücke für die Programmierer von Software wie Microsoft Outlook oder Apple Mail. Die eigentliche Verschlüsselung wurde dabei aber nicht geknackt und auch private Schlüssel des Programms kamen nicht abhanden. Wer sich gegen den unwahrscheinlichen Angriff schützen möchte, sollte die Anzeige von HTML-Mails abschalten – eine Einstellung, die aus Sicherheitsgründen in jedem E-Mail-Programm vorgenommen sein sollte.

Völlig unklar ist, was die Electronic Frontier Foundation mit dieser Warnung bezweckt hat, die viele Nutzerinnen und Nutzer verunsichert hat. Schließlich sollte sie kein Interesse daran haben, dass weniger Menschen verschlüsseln. Allgemein ist es üblich, beim Auffinden von Sicherheitslücken zunächst die Hersteller der betroffenen Software zu

informieren und mit dem Veröffentlichen drei Monate zu warten, um Sicherheitsupdates zu ermöglichen, bevor Angreifer die Lücken ausnutzen können.

Vielen Menschen ist das Thema Verschlüsselung unangenehm. Sie reagieren mit schlechtem Gewissen, weil sie nie dazu kommen, sich um Verschlüsselung zu kümmern. Bei E-Mails wird neben dem Industriestandard S/MIME immer noch vor allem der GNU Privacy Guard eingesetzt. Wer ihn nutzen will, muss zunächst einen privaten und einen öffentlichen Schlüssel generieren. Der öffentliche Schlüssel wird an Freunde und Kollegen weitergegeben, während der private streng gehütet werden muss. Wer jemandem eine Mail schreiben möchte, verschlüsselt diese Mail mit dem öffentlichen Schlüssel des Adressaten. Der Empfänger hat den dazu passenden privaten Schlüssel und kann die E-Mail entschlüsseln und lesen. Das Ganze funktioniert nur, wenn alle Beteiligten ihre Schlüssel pflegen und tauschen und dabei aufpassen, nichts zu verwechseln. Die zugehörige Software ist zwar recht einfach und komfortabel zu bedienen, stellt aber für weniger computeraffine Menschen dennoch eine Hürde dar. Wer Verschlüsselungssoftware einsetzt, hat selten mehr als eine Handvoll Kommunikationspartner, mit denen das klappt. Der weitaus größte Teil des weltweiten E-Mail-Verkehrs bleibt unverschlüsselt.

> Für Ermittlungsbehörden ist es lästig, wenn Menschen in größerem Umfang ihre Geräte und Kommunikation verschlüsseln.

Dass es auch einfacher geht, zeigen Messenger-Dienste. Das zu Facebook gehörige Whatsapp verschlüsselt die Botschaften mittlerweile standardmäßig. Wer Facebook, dem Eigentümer von Whatsapp, nicht über den Weg traut, verwendet alternativ den ebenfalls kostenlosen Messenger-Dienst Signal. Es gibt weitere Alternativen wie Threema und Telegram, die allerdings aus verschiedenen Gründen kritisiert werden. Alle haben gemeinsam, dass sie ohne den Aufwand der E-Mail-Verschlüsselung auskommen und einfach funktionieren. Für E-Mails gibt es weiterhin nichts Vergleichbares.

Das will nun eine Genossenschaft namens Pep Coop ändern. Dahinter stehen Programmierer, Juristen und Bürgerrechtsaktivisten, darunter auch Sibylle Berg und Juli Zeh. Ziel der Genossenschaft ist es, die Privatsphäre in der digitalen Welt mit technischen Mitteln schützen. Das heißt unter anderem, bessere Verschlüsselungssoftware zu entwickeln. Die Genossenschaft soll sich aus Spendengeldern, Mitgliedsbeiträgen und Anteilsscheinen finanzieren. Wer Genosse wird, darf mitbestimmen, was für Software entwickelt werden soll. Verschlüsselungssoftware soll auch von Menschen ohne Vorwissen einfach benutzt werden können. Pep Coop wurde erst im Mai gegründet. Anwendbare Software wird also noch etwas auf sich warten lassen.

Einfach zu bedienende Verschlüsselung für alle – das gefällt längst nicht jedem. Besonders Polizeibehörden und Geheimdienste haben Interesse daran, die Kommunikation der Bevölkerung zu überwachen. Mit Prism hat der US-amerikanische Geheimdienst NSA ein Programm entwickelt, mit dem große Teile des weltweiten Internetverkehrs mitgelesen und analysiert werden können.

Hierzulande erlaubt der sogenannte Bayern-Trojaner den bayerischen Behörden, Schadsoftware auf den Rechnern von Verdächtigen zu installieren, um diese zu überwachen. Immer wieder kommt es zum Beispiel im Zusammenhang mit Demonstrationen zu Zwischenfällen, bei denen die Polizei Smartphones konfisziert und die Inhaber auffordert, sie zu entsperren, um den Inhalt des Telefons prüfen zu können. Das geht eigentlich nur mittels richterlicher Anordnung, aber die Polizei tut es trotzdem. Das Ende Mai verabschiedete neue bayerische Polizeiaufgabengesetz (Jungle World 21/2018) wird dieses Vorgehehen künftig legalisieren.

Für Ermittlungsbehörden ist es lästig, wenn Menschen in größerem Umfang ihre Geräte und Kommunikation verschlüsseln. Deshalb fordern Politiker einen digitalen Dietrich. Zuletzt ist Ende 2017 ein entsprechender Entwurf des Innenministeriums bekannt geworden, der dann aber ausgerechnet auf Twitter dementiert wurde. Apple wehrt sich in den USA regelmäßig gegen Forderungen von FBI und CIA nach Hintertüren und in Moskau stehen die Entwickler des Messenger-Dienstes Telegram vor Gericht, weil sie den russischen Behörden keinen Einblick in die Kommunikation ihrer Nutzer geben möchten.

Das sind nur die neusten Episoden einer langen Geschichte, die unter dem Namen Cryptowars bekannt wurde. Diese Kryptographie-Kriege begannen, als Banken und Konzerne in den sechziger Jahren anfingen, ihre Daten zu verschlüsseln. Damals wollte die US-Regierung noch verhindern, dass die Verschlüsselungssoftware ins Ausland gelangt, und erlegte der Software-Industrie Exportbeschränkungen auf. Das führte unter anderem dazu, dass der Netscape-Browser aus den frühen Zeiten des WWW außerhalb der USA nur mit künstlich geschwächter, leicht umgehbarer Verschlüsselung ausgeliefert werden durfte.

Mit wachsender Verbreitung von internetfähigen PCs entstand unter Hackern eine Subkultur innerhalb der Subkultur. Die Cypherpunks setzen sich für freie Verschlüsselungssoftware ein, entwickeln diese weiter, erklären und verbreiten sie auf Kryptopartys und engagieren sich als Graswurzelbewegung gegen die Überwachung durch Staaten und Konzerne. Politisch schwanken die Sympathien der Bewegung zwischen anarchistischen und rechtslibertären Gruppen, deren Anhängerschaft und Programmatik sich überschneiden. Bekannte Vertreter sind John Gilmore, der die Electronic Frontier Foundation gegründet hat, und Julian Assange, der Gründer und Leiter der Whistleblower-Platform Wikileaks berühmt wurde. Ebenfalls aus dem Milieu der Cypherpunks stammt auch der Versuch, eine staatlich nicht kontrollierte Währung auf der Basis von Verschlüsselungstechnik zu etablieren: die Kryptowährung Bitcoin.

Verschlüsselung alleine reicht allerdings nicht aus, um die Kommunikation zu schützen. Der Inhalt von Nachrichten ist für Ermittlungsbehörden oftmals nicht so interessant wie die zugehörigen Metadaten: wann wo eine Nachricht von wem an wen verschickt wurde. Diese Daten lassen sich nicht verschlüsseln und entstehen zwangsläufig, anders kann digitale Kommunikation nicht funktionieren. Für den Schutz der Metadaten gibt es keine technische Lösung, aber eine rechtlich-politische: Datenschutzgesetze. Bei denen erlaubt sich der Staat aber zahlreiche Ausnahmen für die eigenen Zwecke.