Süddeutsche.de Digital

14. Mai 2018, 11:35 Massive Sicherheitslücke

Verschlüsselte E-Mails sind nicht sicher

- Sicherheitsforscher haben die Verschlüsselung von E-Mails ausgehebelt.
- Die beiden verbreitetsten Verfahren PGP und S/Mime weisen schwerwiegende Lücken auf.
- Bislang galten verschlüsselte E-Mails als sicher, selbst die NSA konnte die Verschlüsselung nicht umgehen.

Von Anja Bröker, Svea Eckert und Hakan Tanriverdi

Juraj Somorovsky verschickt eine verschlüsselte E-Mail. Normalerweise könnte genau eine Person diese Botschaft lesen: der Empfänger. Doch das, was Somorovsky Anfang April im Raum B113 am Fachhochschulzentrum in Münster Reportern von *Süddeutscher Zeitung*, NDR und WDR demonstriert, ist weit entfernt von Normalbedingungen. Fünf Minuten, nachdem er die verschlüsselte Mail verschickt hat, kann sie nicht nur der Empfänger lesen, sondern auch ein unbefugter Dritter. In diesem Fall ist es ein Kollege von Somorovsky, Jens Müller. Der dreht seinen Laptop um und liest vor: "Diese Nachricht ist sehr vertraulich, bitte nicht weitergeben."

Einem Forscherteam der FH Münster, der Ruhr-Universität Bochum und der KU Löwen in Belgien ist es in einem Test gelungen, einen der zentralen Bausteine für sichere Kommunikation im digitalen Zeitalter zu zertrümmern. Das Team hat zwei unterschiedliche Wege gefunden, um die Verschlüsselung von E-Mails auszuhebeln. Bisher galten beide Verfahren als sicher, selbst vor Geheimdiensten.

Sebastian Schinzel, Professor für Angewandte Kryptografie der FH Münster, hat die Forschungen geleitet. SZ, NDR und WDR konnten den Prozess über Monate begleiten und mit unabhängigen IT-Sicherheitsexperten reden, die die Ergebnisse der Forscher bestätigten.

Verschlüsselungstechnologie
Privatsphäre dank Quantenphysik
Google arbeitet daran, die NSA sowieso und auch deutsche Wissenschaftler: Auf Quantenphysik basierende Computer könnten die digitale Kommunikation revolutionieren. Ausgerechnet in Deutschland könnten die Mittel dafür aber knapp werden. Von Robert Gast

"Es ist natürlich eine schlimme Sicherheitslücke", sagt Arne Schönbohm, Chef des für IT-Sicherheit zuständigen Bundesamtes für Sicherheit in der Informationstechnik (BSI). "Gerade wenn Sie Dinge verschlüsseln, wollen Sie, dass es hier einen hohen Grad der Vertraulichkeit gibt und dass der auch gewahrt bleibt. Durch eine falsche Konfiguration, wenn man bestimmte Sicherheitsmaßnahmen nicht trifft, ist die Vertraulichkeit nicht gewahrt."

Es steht also fest: Was die Forscher herausgefunden haben, ist so verheerend, dass das Vertrauen in verschlüsselte Mails zumindest auf absehbare Zeit verloren sein dürfte. "E-Mail ist kein sicheres Kommunikationsmedium mehr", sagt Forscher Schinzel, den Kollegen als sehr umsichtige Person beschreiben, als jemanden, der nicht zu Übertreibungen neigt. Das Schlimme ist: Betroffen sind beide Verfahren, mit denen weltweit E-Mails verschlüsselt werden: S/Mime und PGP. Firmen verwenden in der Regel S/Mime, Aktivisten, Whistleblower und Journalisten hingegen PGP.

Geheimnisse von Konzernen weltweit, aber auch vertrauliche Botschaften, die sich Menschenrechtsaktivisten, Anwälte und Journalisten schicken: Alle diese Nachrichten könnten nun im Nachhinein entschlüsselt werden. Die Electronic Frontier Foundation (EFF), eine Organisation für digitale Bürgerrechte, wird ihre Sicherheitsstufe senken, die PGP-Mails Aktivisten ihrer Einschätzung nach bietet.

Die NSA verzweifelte an PGP-Verschlüsselung

Die Angriffe funktionieren nicht beliebig, sondern nur unter bestimmten Bedingungen. Normale E-Mails betrifft das alles nicht, bei ihnen ist aber ohnehin klar, dass sie grundsätzlich deutlich schlechter geschützt sind. Wenn überhaupt werden sie auf dem Transportweg verschlüsselt, also auf ihrem Weg durch das Internet - von Postfach zu Mailserver, von dort ins Netz, der gleiche Weg zurück ins Empfänger-Postfach. Die Mail selbst liegt auf den Servern jeweils im Klartext vor und kann mitgelesen werden - wie eine Postkarte. Bei einer mit S/Mime oder PGP verschlüsselten Mail geht das nicht. Unbefugte bekommen nur Datenwust zu sehen. Den nennen IT-Sicherheitsexperten Ciphertext.

Denn bei S/Mime und PGP werden pro E-Mail-Adresse zwei Schlüssel erzeugt, die zusammengehören: einer ist privat, einer öffentlich. Die Privatschlüssel liegen nicht auf einem Server, sondern auf dem Laptop der Person, der die Mail-Adresse gehört. Solange der private Schlüssel gut geschützt wird, so dachte man, ist egal, ob jemand die E-Mail abfängt. Und genau so ist es ja auch nachzulesen in den NSA-Dokumenten des Whistleblowers Edward Snowden, die der *Spiegel* Ende 2014 veröffentlichte. Dort heißt es in einer Folie: "No decrypt available for this PGP encrypted message."

Die NSA fing eine E-Mail ab, aber konnte die Verschlüsselung nicht brechen. Der wohl mächtigste Geheimdienst der Welt scheiterte jahrelang an PGP. Snowden

war deshalb überzeugt: "Richtig eingestellte kryptografische Verfahren gehören zu den wenigen Dingen, auf die man sich verlassen kann." Wenn die Forscher ihre Ergebnisse an diesem Freitag auf einer Fachkonferenz in Bochum präsentieren werden, dann dürfte dieser Satz überholt sein.

Im Kern funktioniert das Aushebeln des Mail-Schutzes so: Die Angreifer wollen einen Firmenchef ausspähen. Sie wollen wissen, über welche Themen er in den vergangenen Jahren kommuniziert hat. Die Angreifer besitzen den Ciphertext, also den Datenwust. Diesen präparieren sie und verschicken ihn an den Chef. Der Text der E-Mail kann vollkommen unverfänglich sein, zum Beispiel eine Einladung zum Kaffee. Aber in derselben Mail wird, ohne dass es für das bloße Auge sichtbar wäre, der Datenwust versteckt. Der Computer öffnet die Botschaft, erkennt den Datenwust und stellt fest, dass er den verschlüsselten Text entziffern kann. Schließlich verfügt er über den Privatschlüssel. Aber kaum ist der präparierte Text entziffert, wird er an eine Seite verschickt, die die Angreifer kontrollieren.

Zwei Bedingungen, ein Angriff

Der Angriff der Forscher basiert auf zwei Bedingungen: Erstens, sie besitzen den Ciphertext. Zweitens, im E-Mail-Programm wird HTML erlaubt. Nur dank HTML lassen sich zum Beispiel die Links in einer E-Mail anklicken. Die Mail wird so abgeändert, dass sie Elemente nachlädt, also Webseiten besucht, die die Forscher bestimmen können. Ähnliches passiert, wenn in E-Mail-Signaturen zum Beispiel das Firmenlogo auftauchen soll. Das Logo muss erst einmal nachgeladen werden.

Es gibt zwei unterschiedliche Wege, um an die Mails zu kommen. Die erste Variante funktioniert sowohl für S/Mime als auch für PGP. Der Fehler liegt nicht im Algorithmus, sondern in der Art, wie E-Mail-Programme die Nachrichten verarbeiten. Schinzel sagt, dass diese Variante sehr einfach nachzubauen sei.

E-Mails werden auf technischer Ebene in mehrere Blöcke aufgeteilt. In einen dieser Blöcke - nicht dort, wo der eigentliche Text angezeigt wird - packen die Forscher den Datenwust. Um diesen herum bauen sie einen HTTP-Link. Das E-Mail-Programm entziffert die Mail und denkt, dass es sich um eine Webseite handelt, von der zum Beispiel ein Bild nachgeladen werden soll - und dabei bekommen die Angreifern den Text der Mail zugeschickt.

"Das Ergebnis ist wirklich elegant"

Der zweite Angriff hebelt die Verschlüsselung von S/Mime und PGP aus. Schinzel nimmt als Vergleich einen Briefumschlag mit Sichtfenster. Dort lässt sich bei Briefen die Adresse des Empfängers lesen. Im Fall von S/Mime ist die E-Mail ähnlich und vor allem immer gleich aufgebaut. Das heißt, die Forscher können die Verschlüsselung beeinflussen, weil sie Teile des Inhalts kennen - eben durch das Sichtfenster. Mit diesem Wissen können sie die verschlüsselte E-Mail

umschreiben. Diese wird entziffert - und auch in diesem Fall an die Angreifer geschickt.

Matthew Green ist Professor für Kryptografie an der Johns Hopkins University in Baltimore. Er hat die Arbeit der Forscher gelesen und sagt: "Das Ergebnis ist wirklich elegant." Green sagt, dass er ohnehin nicht empfehlen würde, PGP zu verwenden, da es viele Probleme mit der Verschlüsselung gebe. "Das ist ein weiteres Einschussloch in einem ohnehin durchlöcherten Auto", sagt er.

Die kommenden Wochen werden hart, sagt Green. Zwar haben die Forscher allen beteiligten Firmen und Entwicklern mehrere Monate Zeit gegeben, um die Lücken zu schließen. Aber das erwies sich in vielen Fällen als schwerer als gedacht. Auf der Webseite werden Schinzel und Co. auflisten, welche Anbieter noch betroffen sind. Auf Twitter fügte er hinzu, dass es derzeit keine verlässlichen Wege gibt, die Lücke zu schließen. Hinzu kommt: Betroffen von dem Angriff sind alle Gesprächsteilnehmer. Es reicht also nicht, wenn man selbst das aktuellste System installiert hat. Man muss darauf vertrauen, dass auch der Gesprächspartner auf dem aktuellsten Stand ist, falls dieser denn existiert. Und genau das wollten PGP und S/Mime verhindern: Dass man anderen vertrauen muss.

Whatsapp-Alternative Wire
Dieser Messenger ist privater als Whatsapp und kann mehr als Threema
Braucht es wirklich noch eine Whatsapp-Alternative? Ja, sagen die Entwickler von Wire - und haben dafür gute Argumente. Von Simon Hurtz

URL: https://www.sueddeutsche.de/digital/exklusiv-verschluesselte-e-mails-sind-nicht-sicher-1.3978608

Copyright: Süddeutsche Zeitung Digitale Medien GmbH / Süddeutsche Zeitung GmbH

Quelle: SZ.de/jab/sih

Jegliche Veröffentlichung und nicht-private Nutzung exklusiv über Süddeutsche Zeitung Content. Bitte senden Sie Ihre Nutzungsanfrage an syndication@sueddeutsche.de.