Original-URL des Artikels: https://www.golem.de/news/e-mail-verschluesselung-pgp-und-s-mime-abschalten-1805-134359.html **Veröffentlicht:** 14.05.2018 09:41 **Kurz-URL:** https://glm.io/134359

E-Mail-Verschlüsselung

PGP und S/MIME abschalten

Ein fundamentales Sicherheitsproblem untergräbt die Sicherheit von verschlüsselten E-Mails, betroffen sind sowohl PGP als auch S/MIME. Die Details wurden noch nicht veröffentlicht. Die Electronic Frontier Foundation empfiehlt die Abschaltung im Mailprogramm.

Ein Forscherteam kündigt an, am Dienstag Details über ein Sicherheitsproblem in den Mailverschlüsselungsstandards OpenPGP und S/MIME zu veröffentlichen. Die Lücke könnte, so Sebastian Schinzel von der Fachhochschule Münster auf Twitter, dazu genutzt werden, bereits verschickte E-Mails zu entschlüsseln.

Die US-Bürgerrechtsorganisation Electronic Frontier Foundation (EFF) warnt in einem Blogeintrag vor der Lücke. *"Unser Ratschlag, der auch von den Forschern geteilt wird, ist es, umgehend Tools zu deaktivieren oder zu entfernen, die automatisch PGP-verschlüsselte Mails entschlüsseln"*, heißt es von der EFF. *"Bis die Fehler, die in dem Paper beschrieben sind, besser verstanden und behoben sind, sollten Nutzer alternative Ende-zu-Ende-verschlüsselte Kanäle nutzen, wie beispielsweise Signal, und vorläufig aufhören, PGP-verschlüsselte Mails zu verschicken und insbesondere zu lesen."*

Die Verschlüsselung von E-Mails - egal ob mit dem OpenPGP- oder mit dem konkurrierenden S/MIME-Standard - hat sich nie in größerem Maße durchgesetzt, was vor allem an der schlechten Usability lag. Doch bislang galt die Verschlüsselung zumindest dann, wenn man sie richtig anwendet, als relativ sicher. (hab)

Verwandte Artikel:
Linux: Hardware soll Schlüssel der Kernel-Entwickler schützen
(06.04.2018, https://glm.io/133710)
E-Mail-Verschlüsselung: EU-Kommission hat Angst vor verschlüsseltem Spam
(22.06.2016, https://glm.io/121638)
Schleuder: Wie verschlüsselt man eine Mailingliste?
(10.09.2016, https://glm.io/123206)
Kryptographie: Der Debian-Bug im OpenSSL-Zufallszahlengenerator
(14.05.2018, https://glm.io/134355)
Microsoft: Viel Neues rund um den Kalender und die App von Outlook
(02.05.2018, https://glm.io/134170)