PRESSEMITTEILUNG

E-Mail-Verschlüsselung bleibt sicher

Angriff auf PGP- und S/MIME-Verschlüsselung nutzt Schwachstellen in E-Mail-Clients

Berlin, 15.05.2018 - Am 14.05.2018 veröffentlichte ein Team aus Sicherheitsforschern der Fachhochschule Münster, der Ruhr Universität Bochum und der Universität Leuven (Belgien) einen Bericht, der die Sicherheit der Verschlüsselungsstandards PGP und S/MIME in Frage stellt und damit weltweites Aufsehen erregt. Die aufgedeckten Sicherheitslücken (CVE-2017-17688 und CVE-2017-17689) betreffen jedoch nicht die Protokolle selbst, sondern nutzen eine bereits länger bekannte Schwachstelle in E-Mail-Clients, um verschlüsselte E-Mails zu entschlüsseln und dem Angreifer zuzustellen. Die Angriffe sind technisch komplex und benötigen mehrere Schritte zur erfolgreichen Umsetzung.

Erste Voraussetzung für einen erfolgreichen Angriff: Die E-Mail muss bereits in verschlüsselter Form beim Angreifer vorliegen. Hierfür muss er die E-Mails auf dem Transportweg per "Man-in-the-Middle"-Attacke abfangen oder einen Mailserver kompromittiert haben.

Anschließend könnten die Angreifer laut den Autoren des Papers zwei sich ähnelnde Angriffsmethoden anwenden, um E-Mails mit vorhandener PGP- oder S/MIME-Verschlüsselung zu entschlüsseln. Der erste Angriff ist recht simpel auszuführen, dafür aber auf bestimmte Mail-Clients (Apple-Mail, iOS-Mail, Mozilla Thunderbird) und ggf. dort installierte Plugins von Drittanbietern beschränkt. Die zweite Möglichkeit, um PGP- oder S/MIME-verschlüsselte E-Mails auszulesen, besteht aus einer schon länger bekannten Methode zum Extrahieren von Plaintext in Blöcken verschlüsselter Nachrichten. Bei beiden Arten werden die abgefangenen verschlüsselten E-Mails manipuliert.

Wichtig bei diesen beiden Angriffsmethoden ist, dass die Verschlüsselungsmethoden S/MIME und PGP selbst nicht gebrochen werden; vielmehr nutzen sie Schwachstellen in E-Mail-Clients für HTML-Mails aus, um die Verschlüsselungstechniken zu umgehen.

"Die Darstellung, PGP und S/MIME seien nicht mehr sicher, erweist der IT-Sicherheit einen Bärendienst", sagt Oliver Dehning, Leiter der TeleTrusT-AG "Cloud Security" und Geschäftsführer des Cloud-Security-Anbieters Hornetsecurity. "Sie läuft allen Bemühungen zuwider, die Sicherheit des Kommunikationsmittels E-Mail zu erhöhen. Die Empfehlung diverser Sicherheitsforscher nach genereller Deaktivierung von Inhaltsverschlüsselung ist nicht nachvollziehbar. Das Gegenteil ist richtig: E-Mail-Verschlüsselung erhöht die Sicherheit und sollte unbedingt eingesetzt werden."

Auch das Bundesamt für Sicherheit in der Informationstechnik weist darauf hin, dass PGP und S/MIME weiterhin sicher eingesetzt werden können, wenn sie korrekt implementiert und sicher konfiguriert sind.

TeleTrusT - Bundesverband IT-Sicherheit e.V., Dr. Holger Mühlbauer, Geschäftsführer, Chausseestraße 17, 10115 Berlin, Tel.: +49 30 40054310, holger.muehlbauer@teletrust.de
www.teletrust.de