HORNETSECURITY®

PRESSEMITTEILUNG 15.05.2018

E-Mail-Verschlüsselung bleibt sicher

Angriff auf PGP- und S/MIME-Verschlüsselung läuft über E-Mail Clients

Hannover, den 15. Mai 2018 – Am gestrigen Montag veröffentlichte ein Team aus Sicherheitsforschern der Fachhochschule Münster, der Ruhr Universität Bochum und der Universität Leuven (Belgien) ein Paper, das die Sicherheit der Verschlüsselungsstandards PGP und S/MIME infrage 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, um verschlüsselte E-Mails durch den Mail-Client zu entschlüsseln und dem Angreifer zuzustellen. Die Angriffe sind technisch komplex und benötigen etliche Schritte.

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 (MidM) 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 relativ einfach auszuführen, dafür aber auf bestimmte Mail-Clients (Apple-Mail, iOS-Mail, Mozilla Thunderbird) und ggf. dort installierte Plugins von Drittanbietern beschränkt. Hierbei fügt der Angreifer einer verschlüsselten E-Mail weitere Teile hinzu und stellt diese dem Empfänger zu. Die dort entschlüsselten Inhalte werden anschließend automatisch an eine bestimmte Website übertragen.

Die zweite Weg zum Auslesen PGP- oder S/MIME-verschlüsselte E-Mails nutzt eine schon länger bekannte Methode zum Extrahieren von Plaintext in Blöcken verschlüsselter Nachrichten. Hierbei werden bekannte Textanteile in verschlüsselten Nachrichten erkannt und sich anschließende Inhaltsblöcke überschrieben. Dabei kommt das bereits in der ersten Methode erwähnte Verfahren zum Einsatz, so dass beim Empfänger die verschlüsselte E-Mail entschlüsselt und an den Angreifer übertragen wird.

Bei beiden Angriffsmethoden werden jedoch die Verschlüsselungen via S/MIME und PGP selbst nicht gebrochen; vielmehr werden Schwachstellen in E-Mail-Clients für HTML-Mails ausgenutzt, um durch die Clients berechtigt entschlüsselte Nachrichten an die Angreifer weiterzuleiten und dadurch die Verschlüsselung zu umgehen.

„Die gestern verbreitete Darstellung, PGP und S/MIME seien nicht mehr sicher, ist barer Unsinn“, sagt Daniel Hofmann, Geschäftsführer bei Hornetsecurity. „Sie führt zur Verunsicherung der Anwender und läuft dadurch allen Bemühungen zuwider, die IT-Sicherheit durch konsequenten

Einsatz von Verschlüsselung zu verbessern. Die Empfehlung diverser Sicherheitsforscher nach genereller Deaktivierung von Inhaltsverschlüsselung kann ich nicht nachvollziehen.“

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.

Die von Hornetsecurity verschlüsselten E-Mails sind per Design vor Angriffen dieser Art geschützt, da Hornetsecurity die für den Angriff vorausgesetzten unterschiedlichen Content-Types (Multipart/Mixed) gar nicht erst zulässt. Zudem benötigt der Verschlüsselungsservice keinerlei Client-Plugins: Die Ver- und Entschlüsselung erfolgt vollautomatisiert durch Hornetsecurity in der Cloud – es sind keine Installation, Wartung oder Nutzerinteraktion erforderlich – einfach sicher!

Über Hornetsecurity:
Der führende deutsche Cloud-Security-Provider Hornetsecurity schützt die IT-Infrastruktur, Kommunikation und Daten von Unternehmen und Organisationen jeglicher Größenordnung. Seine Dienste erbringt der Sicherheits-Spezialist aus Hannover über redundante, gesicherte Rechenzentren in Deutschland und nach deutschem Datenschutzrecht. Das Lösungsportfolio beinhaltet Services in den Bereichen Mail Security, Web Security und File Security. Alle Services des Unternehmens sind in kurzer Zeit implementierbar und rund um die Uhr verfügbar. Bis Anfang 2015 firmierte Hornetsecurity unter dem Namen antispameurope. Zu den Kunden von Hornetsecurity zählen unter anderem KONICA MINOLTA, Bitburger Braugruppe, LVM Versicherung, DEKRA, Melitta und Otto Group.

Mehr Informationen finden Sie unter www.hornetsecurity.com.

Pressekontakt:
Hornetsecurity
Christoph Maier
Am Listholze 78
30177 Hannover
Tel.: +49 (511) 515 464-901
E-Mail: presse@hornetsecurity.com