Efail: Und ewig grüßt das Murmeltier

Die Nachricht verbreitete sich wie ein Lauffeuer. PGP und S/MIME, die beiden gängigen Formate für verschlüsselte E-Mails, seien gehackt, hieß es am 14. Mai 2018. Ein Angreifer könne sich eine verschlüsselte Mail von deren Absender oder Empfänger unbemerkt entschlüsseln lassen – gleichsam wie ein Kuckuck, der sein Ei von einem anderen Vogel ausbrüten lässt. Das hatten Forscher der FH Münster, der Ruhr-Universität Bochum und der KU Leuven (Belgien) herausgefunden.

Die Hiobsbotschaft traf gerade einen Tag vor *iX*-Redaktionschluss ein, und so war das Ausmaß der Katastrophe beim Abfassen dieser Zeilen noch gar nicht abzusehen. Immerhin: Die volkswirtschaftlichen Folgen dürften sich in Grenzen halten, denn die meisten E-Mail-Nutzer verschlüsseln ohnehin nicht. Oder um es etwas zynischer zu formulieren: Die von Spiegel Online per Überschrift verbreitete Empfehlung „Experten raten vorerst von E-Mail-Verschlüsselung ab“ wird von den meisten Usern schon seit zwei Jahrzehnten konsequent befolgt. Hacker und Geheimdienste können daher meist auch ohne Sicherheitslücke mitlesen.

Die wohl größte Gefahr von Efail liegt daher eher in der Signalwirkung. Seit Jahren versuchen Sicherheitsexperten, das Verschlüsseln von E-Mails zu etablieren. Und jetzt das.

Beim Blick auf die Ursachen fällt auf: Efail funktioniert ziemlich ähnlich wie gefühlt Hunderte anderer Lücken in der Verschlüsselungstechnik. So liegt der Knackpunkt, wie nahezu immer, nicht in den verwendeten Verschlüsselungsverfahren (vor allem RSA und AES) selbst. Die betroffenen Formate S/MIME und OpenPGP haben dagegen mit einigen kleineren Mängel durchaus zu Efail beigetragen, auch wenn man sie nicht als grob fehlerhaft bezeichnen kann.

Wie in den allermeisten Fällen liegt das Hauptproblem von Efail dagegen in der Implementierung. Hierbei zeigt sich einmal mehr: Komplexität ist der Feind der Sicherheit. Und nicht zum ersten Mal hat ein Feature die Sicherheit zum Kollabieren gebracht (in diesem Fall das Einbinden externer Inhalte in eine Mail), das eher in die Rubrik „nice to have“ fällt.

Und schließlich ist auch die Anatomie von Efail nicht gerade neu. Es geht wieder einmal darum, dass Daten unterschiedlichen Typs nicht sauber voneinander abgegrenzt sind, was eine gefährliche Falschinterpretation erlaubt. Das kennen wir beispielsweise vom Heartbleed-Bug, Spectre, Meltdown und unzähligen Buffer-Overflow-Fehlern.

Man sieht also: Mit Efail grüßt ein allzu bekanntes Murmeltier, nur eben dieses Mal besonders laut. Die Frage, wie sich so etwas zukünftig vermeiden lässt, ist damit fast schon beantwortet: Weniger Komplexität in Sicherheitslösungen und gleichzeitig mehr Sorgfalt in der Entwicklung lautet die Devise. Dummerweise sind diese Ursachen nicht nur längst bekannt, sondern auch kaum aus der Welt zu schaffen. Sicher ist daher immerhin eines: Der nächste Gruß des Murmeltiers wird nicht lange auf sich warten lassen. (ur@ix.de)

KLAUS SCHMEH

Quelle: Christina Förster

Klaus Schmeh arbeitet für die Gelsenkirchener Firma cryptovision. Er ist Kryptologie-Experte und Blogger (www.schmeh.org).