Universität Konstanz

#efail -- Was ist da mit eMail und Verschlüsselung kaputt?

In den letzten Tagen haben viele von Ihnen sicher in den Medien von diesem Problem gehört oder gelesen: verschlüsselte eMails sind nicht mehr sicher!? Was ist da los?

Problem 1:
Die meisten Mail-Clients (Programme, mit denen wir eMails lesen) interpretieren "aktive" Inhalte von Mails, indem sie z.B. html-formatierten Mail-Text "schön aufbereitet" anzeigen, dabei auch als Link eingebettete Bilder nachladen u.Ä. Auch das automatische Entschlüsseln von verschlüsselt zugesandten Mailtexten gehört zu diesen "Komfort-Funktionen", die nun zum Problem geworden sind.

Problem 2:
Der sogenannte MIME-Standard (Multi-purpose Internet Mail Extensions), der z.B. das Anhängen von Attachments an Mailtexte erlaubt, veranlasst Mail-Clients ebenfalls dazu, bestimmte Aktionen auf dem Inhalt einer Mail auszulösen.

Problem 3:
Zwar gelten die grundlegenden kryptographischen Algorithmen, die bei der verschlüsselten Mail-Übertragung verwendet werden, nach wie vor als sicher, jedoch werden sie bei der Behandlung von eMail so eingesetzt, dass der verschlüsselte Text (verhältnismäßig) einfach unberechtigt und unbemerkt modifiziert werden kann. Ein "Man-in-the-middle" Angriff auf dem Transportweg kann so unbemerkt bleiben. (Sowohl S/MIME- wie auch PGP/GPG-Verschlüsselung von
eMails haben hier ein Problem, auch wenn es bei S/MIME deutlich ausgeprägter ist.)

Die Kombination dieser drei Probleme erlaubt nun mehr oder weniger einfache Angriffe auf verschlüsselte eMails, die z.B. das unberechtigte Mitlesen verschlüsselter Mails ermöglichen. Im einfachsten Fall bedient sich ein Angreifer, der auf dem Transportweg einer verschlüsselten Mail diese unbemerkt modifizieren kann (Problem 3), des MIME-Standards (Problem 2), und "verpackt" den verschlüsselten Inhalt so, dass der Mail-Client des Empfängers nach dem automatischen Entschlüsseln der eMail (Problem 1) ein "Bild" beim Angreifer nachladen will (Problem 1) und dabei den gesamten entschlüsselten Mailtext als "Parameter" beim Aufruf zum Bild-Nachladen mit sendet. So hat der Angreifer den entschlüsselten Mail-Inhalt erhalten, ohne dazu selbst die Verschlüsselung "knacken" zu müssen, denn das hat ja freundlicherweise der Mail-Client des Empfängers für ihn übernommen.

Was kann/muss man tun?

1. Wenn Sie hin und wieder oder häufig verschlüsselte Mails empfangen, dann sollten Sie reagieren:

a) Schalten Sie aktives Interpretieren von Mail-Inhalten in Ihrem Mail-Client ab.
In Thunderbird beispielsweise setzen Sie das Häkchen bei "Externe Inhalte in Nachrichten erlauben" nicht und lassen die "Externen Inhalte" auch nachträglich nicht anzeigen.

Etwa, indem Sie Mails immer als "reinen Text" anzeigen lassen oder, wo möglich, auf "einfaches html" (z.B. in Thunderbird) einschränken. Automatisches Nachladen von Bildern kann man in den meisten Mail-Clients abschalten. (Das ist unabhängig von #efail ohnehin eine gute Idee, weil Absender sonst auch eine Menge ungewollter Informationen über die Empfänger sammeln können!)

b) Sie können auch das automatische Entschlüsseln von verschlüsselten Mailinhalten abschalten (im Zweifelsfall durch Deinstallieren entsprechender Plug-ins oder Schlüsselpaare). Dann sind Sie gegen solche Angriffe geschützt, müssen aber den verschlüsselten Mailinhalt in einem separaten Tool/Fenster "von Hand" entschlüsseln lassen (und dort natürlich dafür sorgen, dass keine "aktiven Inhalte" ausgeführt werden).

2. Wenn Sie nie/selten verschlüsselte Mails erhalten, dann sind Sie auch nicht/kaum gefährdet.

3. Wenn Sie nur SOGo verwenden, dann sind Sie nicht betroffen, können ja aber ohnehin keine verschlüsselten Mails entschlüsseln.

4. Die Mail-Clients und die Standards müssen angepasst werden. Das wird aber dauern.

Weitere Hinweise:

- Verwenden Sie gerne verschlüsselte Mails auch weiterhin, wenn Sie das bisher getan haben. Das ist immer noch besser als die unverschlüsselte Übertragung, bei der jeder "Man-in-the-middle" gleich Klartext mitlesen kann.

- Versenden Sie am besten auch keine html-formatierten Mails, eMail war nie für die Übertragung von formatierten Inhalten gedacht, daher wundert es auch nicht, dass immer wieder html-formatierte Mails Probleme bereiten.

- Halten Sie Ihre Software immer auf dem aktuellen Stand. Einige Mail-Clients und/oder Verschlüsselungswerkzeuge sind bereits/werden hoffentlich bald zumindest gegen die einfacheren Formen der #efail-Angriffe geschützt (so auch enigmail für Thunderbird).