Verschlüsselt Johnny jetzt endlich seine Mails?

Neue Impulse fördern Akzeptanz und Umsetzung der E-Mail-Verschlüsselung

Trotz aller Sicherheitsvorfälle verschlüsseln nach wie vor nur wenige Nutzer ihre E-Mails. Dank neuer gesetzlicher Vorschriften soll sich dies nun ändern. Damit es funktioniert, muss der Anwender der Verschlüsselungslösung mehr als bisher im Vordergrund stehen, insbesondere bei der Benutzerfreundlichkeit.

Der Forschungsaufsatz „Why Johnny Can't Encrypt" ist zwar schon 20 Jahre alt, doch viele Experten halten ihn immer noch für aktuell. In dieser Arbeit von Alma Whitten und J. D. Tygar geht es um die Frage, wie ein Durchschnittsanwender („Johnny") im praxisnahen Test das Verschlüsseln von E-Mails bewältigt. Das Ergebnis ist ernüchternd. Bezeichnenderweise hat „Why Johnny Can't Encrypt" 2015 den USENIX Test of Time Award erhalten. Dieser wird für Forschungsarbeiten vergeben, die auch nach mindestens einem Jahrzehnt noch aktuell sind.

Mehr Bewusstsein und neue Gesetze

Dabei wäre mehr E-Mail-Verschlüsselung (momentan sind nur etwa 0,1 Prozent aller Mails auf diese Weise gesichert) wichtiger denn je. Man denke nur an die zahlreichen E-Mail-Sicherheitsvorfälle, die regelmäßig durch die Presse gehen. Und spätestens seit den Enthüllungen von Edward Snowden hat sich herumgesprochen, dass die NSA und andere Geheimdienste im großen Stil mitlesen.

Weniger beachtet wird bisher, dass die Snowden-Affäre die Notwendigkeit von E-Mail-Verschlüsselung auch auf eine andere Weise deutlich gemacht hat. Erstaunlich ist nämlich, dass Snowden an 1,7 Millionen NSA-Dateien herankam, obwohl die NSA zweifellos eines der am besten geschützten Computer-Netze der Welt betreibt. Die Erklärung dafür ist äußerst banal: Snowden hatte als Administrator legalen Zugriff auf die von ihm geleakten Dokumente und musste daher keine größeren Sicherheitsvorkehrungen aushebeln. Die Affäre bestätigt daher die – keineswegs neue – Erkenntnis, dass Insider-Angriffe eine große Gefahr sind.

Um das Verschlüsseln von E-Mails endlich populärer zu machen, hat sich inzwischen der Gesetzgeber eingeschaltet. Am bekanntesten ist in diesem Zusammenhang die Datenschutz-Grundverordnung (DSGVO) der EU, die in einigen Bereichen nur durch das Verschlüsseln von E-Mails zu erfüllen ist. Eine Verschlüsselungspflicht gibt es außerdem für Berufsgeheimnisträger wie Rechtsanwälte, Patentanwälte, Notare, Wirtschaftsprüfer und Steuerberater – gemäß dem 2017 neu gefassten § 203 des Strafgesetzbuchs. Die Details werden derzeit erarbeitet, wobei vor allem die DATEV (der IT-Dienstleister der Steuerberater, Wirtschaftsprüfer und Rechtsanwälte) eine wichtige Rolle spielt. Von Bedeutung sind außerdem das IT-Sicherheitsgesetz mit der zugehörigen Kritisverordnung des Bundesamts für Sicherheit in der Informationstechnik (BSI), das E-Government-Gesetz und das für das Gesundheitswesen bedeutsame E-Health-Gesetz. Sie alle fordern – direkt oder indirekt – das Verschlüsseln von E-Mails.

Ein gestiegenes Bewusstsein und gesetzliche Vorschriften sind die eine Seite, wenn E-Mail-Verschlüsselung populärer werden soll. Die andere ist der Anwender. Wenn Johnny seine E-Mails endlich verschlüsseln soll, dann muss er dies erst einmal können und wollen. „Anwender-zentrierte IT-Sicherheit" heißt das Stichwort. Zu den weltweit führenden Expertinnen in diesem Segment gehört die deutsche Professorin Angela Sasse von der Ruhruniversität Bochum.

Zusammen mit vier Kollegen hat Sasse beispielsweise den Umgang mit E-Mail-Clients untersucht. Viele Anwender hatten schon bei der Installation und Konfiguration ihre Probleme. Bis zur Verschlüsselung der ersten Mail vergingen im Schnitt über 40 Minuten. Im Rahmen eines neuen Forschungsprojekts namens Casa (Cyber-Sicherheit im Zeitalter großskaliger Angreifer) untersucht Sasse derzeit Aspekte wie Nutzer-Akzeptanz und Benutzerfreundlichkeit in der IT-Sicherheit unter anderem gemeinsam mit Psychologen, wobei auch die E-Mail-Verschlüsselung eine wichtige Rolle spielt.

Johnny muss in den Mittelpunkt

Damit Johnny endlich seine Mails verschlüsselt, hält Sasse es zunächst für notwendig, die Anwender zu sensibilisieren. „So mancher E-Mail-Nutzer denkt immer noch, Verschlüsselung bringe nichts, denn man kann das sowieso knacken", berichtet sie. „Diese Einschätzung ist jedoch komplett falsch, denn heutige Krypto-Algorithmen gelten als äußerst sicher."

Bekannt ist allerdings, dass auch heute noch so manche Lösung zur E-Mail-Verschlüsselung diverse Kinderkrankheiten aufweist. Sasses Arbeit berichtet beispielsweise von Bugs in den untersuchten Clients, die zur Nichtverfügbarkeit von Funktionen, Abstürzen und unerwünschten Nebenwirkungen führen. Darüber hinaus sieht Sasse noch Verbesserungsmöglichkeiten in der Benutzerfreundlichkeit. Ein Mail-Client sollte beispielsweise die Kommunikation mit der Zertifizierungsstelle übernehmen und dabei für eine reibungslose Registrierung und Zertifikatserneuerung sorgen, die ohne größere Interaktion des Anwenders abläuft.

Geheimschutz als Vorbild

Eine Vorreiterrolle in Sachen E-Mail-Verschlüsselung könnten demnächst Behörden und Unternehmen übernehmen, die Geheimschutzanforderungen erfüllen müssen. Diese dürfen Daten bis zur Geheimhaltungsstufe „Verschlusssache – Nur für den Dienstgebrauch" (VS-NfD)

verschlüsselt per Mail verschicken, sofern die dazu genutzte Lösung entsprechend zugelassen ist. Die von Outlook oder Notes bereitgestellten Verschlüsselungsfunktionen verfügen nicht über eine solche Zulassung (es ist auch kaum zu erwarten, dass der Geheimschutz in Deutschland in die Hände von US-Herstellern gelegt wird), doch es gibt inzwischen VS-NfD-zugelassene Add-ins.

Viele Organisationen nutzen für den VS-NfD-Datenaustausch jedoch keine Mail-Verschlüsselung, sondern die Software Chiasmus. Chiasmus ist kein Tool für das Verschlüsseln von E-Mails, sondern dient der Datei-Verschlüsselung und ist vor allem für das stationäre Sichern von Daten gedacht. Ein Anwender kann damit jedoch Daten sicher übertragen, indem er eine verschlüsselte Datei über ein geteiltes Verzeichnis zugänglich macht oder als Mail-Anhang verschickt. Allerdings muss der Schlüssel hierbei manuell übergeben werden, da Chiasmus keine asymmetrische Kryptografie unterstützt. Da es sich um symmetrische Schlüssel handelt ist das Verfahren stark reglementiert und weder flexibel noch benutzerfreundlich.

Neuere Entwicklungen steigern die Benutzerfreundlichkeit, indem sie E-Mail-Verschlüsselung und Datei-Verschlüsselung als eine Einheit betrachten. Der Anwender kann hierbei beispielweise eine verschlüsselte Datei als Mail verschicken, wobei der Client des Empfängers diese als verschlüsselte Mail erkennt. Umgekehrt kann der Anwender eine verschlüsselte Mail abspeichern und später mit der Datei-Verschlüsselungslösung entschlüsseln. Der zugrunde liegende Standard der dies ermöglicht ist S/MIME. Das Schlüssel-Management erfolgt über digitale Zertifikate. Eine Lösung, die so arbeitet und VS-NfD-zugelassen ist, ist z. B. GreenShield von cryptovision.

Oft lässt sich E-Mail-Verschlüsselung im Geheimschutzbereich benutzerfreundlicher umsetzen als in anderen Umgebungen. So ist in VS-NfD-Kommunikation das hierarchisch ausgelegte S/MIME-Format deutlich weiter verbreitet als das oft nur provisorisch genutzte PGP – Johnny muss sich also nicht mit zwei inkompatiblen Formaten herumschlagen. Die digitalen Zertifikate kommen von einer VS-NfD-konformen Zertifizierungsstelle, die der Betreiber festlegt und die im Normalfall von allen Beteiligten anerkannt wird – die Flut an Zertifizierungsstellen, mit denen sich ein Anwender herumschlagen muss, wird dadurch eingedämmt.

Fazit

Es könnte also durchaus sein, dass sich E-Mail-Verschlüsselung zumindest im Geheimschutzsegment durchsetzen wird. Es bleibt zu hoffen, dass diese Entwicklung auch auf andere Bereiche überspringt. Wer weiß, vielleicht erscheint demnächst eine Forschungsarbeit, in der die erfolgreiche Umsetzung von E-Mail-Verschlüsselung bei einer Organisation mit Geheimschutzanforderung beschrieben wird („Why Johnny Finally Can Encrypt")? Und vielleicht wird diese Arbeit dann zehn Jahre später den USENIX Test of Time Award gewinnen.

Klaus Schmeh
cv cryptovision GmbH