Mail-Überwachung ohne Ende

Edward Snowden deckte 2013 auf, dass Geheimdienste Daten mit jedem denkbaren technischen Mittel sammeln. Seit seinen Enthüllungen sind über fünf Jahre vergangen. Doch die grundlegenden Probleme sind immer noch nicht gelöst. Zum Beispiel der Transport von E-Mails: Standardmäßig unverschlüsselt versendet, ist die E-Mail ein ideales Ziel für Lauscher. Mächtigere Angreifer können mit Manipulationen des Internet-Namensdienstes oder -Routings Nachrichten umleiten und dabei mangels Prüfsummen unbemerkt vom Empfänger Inhalte verändern. Ein Albtraum. Die Transportverschlüsselung von E-Mails ist trotzdem noch immer nur optional. STARTTLS gibt es seit dem letzten Jahrhundert, doch es braucht nicht zwingend eine Chinese Firewall, es zu unterdrücken.

2014 hat die IETF die allgegenwärtige Überwachung zu einem realistischen Szenario erklärt. Selbst wenn ein Mailserver dank lokaler Vereinbarungen wie bei „E-Mail Made in Germany“ verpflichtend und authentifiziert verschlüsselt: Die nächste Weiterleitung kann die sichere Insel verlassen und angreifbar sein. Da bleibt bei den Anwendern immer ein ungutes Gefühl.

2015 kam DANE für SMTP. Basierend auf DNSSEC als sicherem Nameservice soll es zuverlässig ermitteln können, ob ein Mailserver die TLS-Verschlüsselung nutzt. Mit DANE wäre sogar eine authentifizierte verschlüsselte Verbindung möglich. Angreifer könnten damit auf dem Transportweg keine Daten mehr mitlesen oder unbemerkt verändern. Trotzdem ist bis heute nur eine Minderheit aller Domains per DNSSEC auflösbar. Selbst große Mailboxprovider nutzen es entweder gar nicht oder nur auf manchen Domains, was zur Unsicherheit der Nutzer beiträgt.

Weitere drei Jahre später wird nun der nächste Standard durch die Newsticker getrieben: Mail Transfer Agent Strict Transport Security, kurz MTA-STS (siehe ix.de/ix1811003). Eine Art DANE ohne DNSSEC, dafür mit einem Trust-on-first-Use-Ansatz. Manche sehen es als Übergangstechnik zu DANE, andere als Symbol des Scheiterns der Branche daran, die E-Mail-Sicherheit auf den heute dringend nötigen Stand zu heben.

Fünf Jahre nach den Snowden-Enthüllungen lässt sich der Stand der Technik also unverändert wie folgt zusammenfassen: Egal, mit welchem Siegel der E-Mail-Anbieter wirbt, Absender und Empfänger können nicht sicher sein, ob die Nachricht nicht doch zwischendurch gelesen oder gar manipuliert wurde. Die Branche hat es bisher nicht einmal geschafft, flächendeckend den Transport zu verschlüsseln, auch wenn der Anteil verschlüsselter Verbindungen zugenommen hat. Und auch die Ende-zu-Ende-Verschlüsselung ist trotz aller Bemühungen weiterhin ein Nischenprodukt.

Vielleicht sollten die Beteiligten die authentifizierte Transportverschlüsselung nicht mehr als optional betrachten, sondern fest in die Protokolle integrieren – auch wenn man dann übergangsweise bei einigen über Altsysteme verschickten Nachrichten einen hässlichen Hinweis anzeigen müsste: Vorsicht, diese Mitteilung könnte gelesen und manipuliert worden sein. Derzeit müsste dieses Etikett an fast jeder E-Mail kleben.

SVEN KROHLAS

ist E-Mail-Spezialist und IT Security Consultant bei der BFK edv-consulting GmbH in Karlsruhe.