Teil 5: Sicher kommunizieren - einfach erklärt!

Die Aussagen des Videos treffen natürlich zu, die Lösung des Auswahlproblems, was nutze ich wo, ist nicht ganz so einfach.

Nun, wir sind weiter als im Jahre 2016, aber nicht notwendigerweise viel sicherer. Was nutzt es, wenn meine Daten auf dem Transportweg verschlüssel sind, dann aber auf dem Server des Diensteanbieters offen herumliegen oder, bei Messengern noch während eines Gesprächs auf dem Server des Anbieters mitgeschnitten werden können?

Der Mailverkehr findet noch nach Grundsätzen statt, die stark an das ArpNet erinnern, dem Vorläufer des Internets. Klartext wohin man blickt, kein Schutz vor Verfälschungen, selbst der Absender kann seine wirkliche Herkunft verschleiern. Ich schreibe also keine Briefe, mit erkennbarer Handschrift in verschlossenem Umschlag, sondern Postkarten mit Zeichensätzen die vom Computer des Empfängers entstammen. Als noch Siegelwachs in Gebrauch war, konnten die Absender noch eindeutiger identifiziert werden als oftmals heute. Auch der Inhalt war vor fremden Augen oder gar Verfälschungen besser geschützt.

Für Email und die Verschlüsselung einzelner Dateien:

Für die Email-Verschlüsselung gibt es OpenPGP (Pretty Good Privacy), abgeleitet aus einem ursprünglich von Phil Zimmermann entwickelten Verfahren. Der quelloffene Standard co-existiert in einer schlicht PGP genannten kommerziellen Version sowie in freien und kostenlosen Implementierungen.

Prominentester Vertreter ist **GNU Privacy Guard** (auch GnuPG, https://gnupg.org/) und läuft auf verschiedenen Plattformen. Die Verschlüsselungsverfahren sind weitestgehend kompatibel (interoperabel) und unterscheiden sich allenfalls durch die Unterstützung von im Standard zugelassener optionaler Erweiterungen. Der Mozilla Email-Client Thunderbird lässt sich mit **Enigmail** problemlos zu verschlüsselter Kommunikation überreden. Auch S/MIME, das ähnliche Wurzeln hat, wird in Basisfunktionen unterstützt, ist aber weitgehend inkompatibel. Allerdings bietet der dort erforderliche Vertrauensnachweis (das X.509-Zertifikat) bei privater Nutzung Angriffsflächen, die für ein Unternehmen oder eine Gruppe von Unternehmen keine Rolle spielen.

Die Installation von GnuPG ist eigentlich relativ simpel. Ein gewisses Grundverständnis ist aber empfehlenswert. Ich kann nur appellieren, den Mut zum Ausprobieren aufzubringen.

Deutlich bequemer sind diesbezüglich die überwiegend auf Mobilgeräten genutzten Instant Messenger, haben aber oft den Nachteil, dass sie es mit der Verschlüsselung der privaten Nachrichten und Daten nicht ganz so genau nehmen, hängt doch das Geschäftsmodell der Anbieter ganz vom Handel mit diesen Daten ab. Sicherheit geht einher mit mehr Unbequemlichkeit. Da ich selbst diesbezüglich sehr zurückhaltend bin, werde ich auch keine direkte Empfehlungen aussprechen und verweise lieber auf eine Seite des gemeinnützigen Vereins **digitalcourage** (https://digitalcourage.de/digitale-selbstverteidigung/alternativen-zu-

whatsapp-und-threema-instant-messenger) auf der die einzelnen Möglichkeiten vorgestellt werden.