Norbert Pohlmann

Selbstbestimmung und Verschlüsselung

Ob die Nutzer das Internet für sich persönlich nutzen wollen, das können sie selbstbestimmt entscheiden. Die mit der Nichtnutzung verbundenen Nachteile in den Bereichen Zugang zu Informationen (Wikipedia; Online-Medien, wie Spiegel, Zeit, ARD, ZDF, ...), Diensten (Suchmaschinen, E-Mail-Dienste, Shops, Zug- und Flug-Angeboten, Reiseveranstalter, ...) und Sozialen Netzen (Schnelle Info über die Aktivitäten der Freunde, Kinder, Eltern, Kollegen, usw.) müssten sie dann natürlich in Kauf nehmen. Wenn sich die Nutzer im Internet aktiv bewegen, dann sollten sie entscheiden können, auf welchen Webseiten sie Angebote nutzen wollen, z.B. weil diese plausible Kriterien erfüllen oder auf sie vertrauenswürdig wirken. Das Klicken auf Links ist deshalb gefährlich, weil selbst diese Bewertungsmöglichkeiten zunächst fehlen. Je mehr Internet-Kompetenz die Nutzer besitzen, umso besser können sie sich vor darin versteckten Angriffen schützen. Haben die Nutzer gelernt, dass wenn sie die Maus auf einen Link halten, ohne zu klicken, dann in der Statusleiste das Ziel dargestellt wird, dann sind sie in der Lage zu erkennen, wo es hin geht und können entscheiden, ob sie der Adresse vertrauen wollen. Steht auf der Webseite (Link) z.B. Lufthansa und in der Statusseite nur die IP-Adresse oder ein anderer, ähnlich aussehender Link, dann ist das ein Phishing-Angriff, den die Nutzer verhindern können, indem sie den Link nicht anklicken.

Welche Informationen die Nutzer z.B. in ein soziales Netz stellen, wie sie mit E-Mails (Spams, Anhängen, usw.) umgehen, all das können und müssen sie lernen, um sich besser zu schützen.

Weil der Markt zahlreiche Produkte und Dienste anbietet, können die Nutzer selbst darüber entscheiden, ob und wo sie eine Verschlüsselung nutzen wollen. Bei der E-Mail Verschlüsselung können die Nutzer z.B. wählen, ob sie eine SSL-Verschlüsselung der E-Mail-Provider nutzen wollen, wie sie im Rahmen von „E-Mail made in Germany“ von der Telekom und United Internet vermarktet werden. Die Nutzer können aber auch eine sichere End-to-End-Verschlüsselung mit Hilfe von S/MIME oder PGP nutzen. Weitere Möglichkeiten der Verschlüsselung liegen z.B. in den Bereichen: Festplattenverschlüsselung, Dateiverschlüsselung und SSL/TLS-Verschlüsselung zu Webseiten. Allerdings bleibt es schwierig, die tatsächliche Konsequenz dieser Anwendungen auf den Schutz der Privatsphäre und die Sicherheit der zu schützenden Informationen (Werte) zu beurteilen.

Aber auch die richtige Nutzung und Handhabung von Verschlüsselung können die Nutzer lernen. Welche E-Mail sollten

sie verschlüsseln und bei welchen Inhalten ist es nicht notwendig? Welche Dateien sollten immer verschlüsselt sein und wie sieht ein sicheres und vertrauenswürdiges Backup-Konzept aus?

Leider können die Nutzer die richtige und vertrauenswürdige Umsetzung der Verschlüsselung nicht wirklich gut beurteilen. Deshalb müssen sie sich auf die IT-Sicherheitslösungen und -hersteller verlassen können. Wenn die Angaben von Verschlüsselungslösungen stimmen würden, dann könnten sie die genutzten Krypto-Algorithmen auf der Basis von öffentlich verfügbarem Expertenwissen beurteilen.

Die Aufklärungen von Snowden haben uns leider gezeigt, dass die NSA sogar Parameter in Standards manipuliert haben, um verschlüsselte Daten besser entschlüsseln zu können.

Wir haben aber auch gelernt, dass wenn die zugrunde liegenden Krypto-Algorithmen richtig implementiert sind und angemessen lange und gute Schlüssel benutzt werden eine verlässliche Wirkung im Hinblick auf die Datensicherheit erzielt werden kann!

Tatsächlich liegen aber die meisten Angriffe auf die Verschlüsselung auf einer anderen Ebene. Z.B. können die Zufallszahlengeneratoren, mit denen die genutzten Schlüssel für die Verschlüsselung generiert werden, so manipuliert werden, dass die NSA diese leicht aus der Ferne „erraten“ und damit einfach unsere vertraulichen Daten „entschlüsseln“ kann. Auch bei der Speicherung der Schlüssel können sehr viele Fehler „eingebaut“ werden, die den Zugriff der NSA ermöglichen und damit in der Regel auch für alle weiteren kriminellen Organisationen und Business-Spione genutzt werden. Aus diesem Grund ist es bei der Verschlüsselung besonders wichtig, dass wir die Technologien, Produkte und Lösungen von kompetenten und insbesondere vertrauenswürdigen Herstellern nutzen. Angemessene Evaluierungen der IT-Sicherheits-technologien und Qualitätszeiten wie „IT Security Made in Germany“ vom TeleTrust – Bundesverband für IT-Sicherheit – helfen sehr, hier mehr Vertrauenswürdigkeit und IT-Sicherheit für uns umsetzen zu können.

Selbstbestimmung hat im Datenschutzrecht einen hohen Stellenwert, sie auszuüben ist, wie diese Überlegungen zeigen, jedoch nicht trivial. Transparenz zu Datenschutz- und -Sicherheitsqualitäten tut not, und Vertrauenswürdigkeit ist nicht einfach zu erreichen. Aber wir sollten diesen Weg gehen, um Herr über unsere Persönlichkeit und unsere Werte im Internet zu bleiben.