

„Der Einsatz kryptographischer Verfahren ist von außerordentlicher Bedeutung [...]. Dies gilt sowohl für die Gewährleistung der Authentizität und Integrität des Datenverkehrs, wie auch für den Schutz der Vertraulichkeit“ (Bundesregierung 1999/vgl. 2001).

Warum signieren und verschlüsseln?

Briefe, Postkarten und andere Schriftstücke, ja selbst kleine Notizen an den Kollegen, werden mit einer Unterschrift oder einem anderen persönlichen Zeichen versehen; oft hilft auch die Handschrift bei ihrer Zuordnung. Briefe werden zudem vielleicht auf einem Brief- oder Geschäftsbogen geschrieben, gegebenenfalls gestempelt, jedenfalls in einem Umschlag verschlossen und ab und an sogar versiegelt. Dem Empfänger wird so die nötige Sicherheit hinsichtlich der Authentizität und Integrität eines Schriftstücks gegeben, und der Briefumschlag verbirgt dessen Inhalt vor unbefugten Blicken.

Beim Austausch elektronischer Nachrichten und von Dateien ist's mit Briefgeheimnis und Datensicherheit – ohne zusätzliche Maßnahmen – hingegen nicht weit her. Denn zum einen sind ihnen keine zuverlässig ihre Integrität und Authentizität belegende Merkmale zueigen. Die Empfänger können somit nicht prüfen, ob sie tatsächlich vom angegebenen Absender stammen und ob sie beschädigt oder sogar manipuliert wurden. Durch die Signierung („digitale Unterschrift“) seiner elektronischen Nachrichten und Dateien mittels GnuPG oder PGP gibt der Absender den Empfängern die Möglichkeit, die Authentizität und Integrität derselben anhand ihrer jeweiligen Signatur zuverlässig zu prüfen.

Und zum anderen ist keineswegs gewährleistet, daß die elektronischen Nachrichten und Dateien nicht von Dritten gelesen und ausgewertet werden. Problematisch ist etwa der mögliche Zugriff Unbefugter auf einem Computer oder in einem Netzwerk. Nicht weniger problematisch ist z.B auch, daß bereits nur innerhalb Deutschland versendete eMails im Internet über durchschnittlich 15 Knotenpunkte weitergeleitet werden, an denen jeweils ein systematisches Scannen beispielsweise auf bestimmte Stichworte hin und somit eine auf Personen oder eMail-Adressen bezogene Sammlung und Auswertung von Daten sowie ein gezielter Zugriff möglich sind – und auch tatsächlich durchgeführt werden. Ihre Kommunikation via eMail ist also für jeden Interessierten ein „offenes Buch“. Und wenn geeignete Such- und Filteralgorithmen eingesetzt werden, sind Sie ein ebensolches.

Am 23. Juli 2009 berichtete PC-Welt Online, daß „zwei Drittel der Mailserver schlecht gesichert“ seien. Und: „Wirklich sinnvoll ist nur eine End-to-End-Verschlüsselung, etwa durch PGP oder S/MIME“. Den vollständigen Artikel finden sie [hier](#).

Sie meinen trotzdem, „doch nichts zu verbergen“ zu haben, also auf eine Verschlüsselung verzichten zu können? Dennoch sollten Sie dem Empfänger Ihrer Nachricht oder Datei zumindest die Möglichkeit geben zu überprüfen, ob dieselbe tatsächlich von Ihnen stammt und ob sie nicht verändert wurde. Sie sollten Ihre Nachricht oder Datei also wenigstens mittels GnuPG oder PGP signieren.

Quelle: <http://home.arcor.de/rose-indorf>