Auf sich allein gestellt?

Natürlich können Sie Ihre Daten anonymisieren. Alles was Sie dazu tun müssen, ist sich kontinuierlich über Exploits, O-Days, Backdoors, Sockets, Cookies, Fingerprinting, Vulns etc. zu informieren, dazu eine überschaubare Anzahl an Programmen bedienen lernen und Ihre Gewohnheiten, On- wie Offline, ihren individuellen Freiheits- und Sicherheitsbedürfnisen unterzuordnen.

Technik ist die Lösung all Ihrer Probleme, also halten Sie sich ran.

etc.....

FIfF

E-Mailverschlüsselung für alle

Eine E-Mail ist wie eine **Postkarte**, jeder auf dem Weg kann sie lesen und verändern. Bei der E-Mailverschlüsselung werden Nachrichten mathematisch so umgeformt, dass **nur der Empfänger sie lesen kann und nur der Absender sie geschrieben haben kann**. Beide brauchen dafür jeweils ein eigenes Schlüsselpaar aus privatem Schlüssel und öffentlichem Schlüssel. Den öffentlichen Schlüssel kann man sich als **offenes »Schnappschloss«** vorstellen, welches jeder schließen, aber nur der Inhaber des dazugehörigen privaten Schlüssels öffnen kann. Zusätzlich kann man mit einem privaten Schlüssel ein **einzigartiges Muster** erzeugen, das zeigt, dass man das dazugehörige Schnappschloss öffnen könnte; dies dient als **Unterschrift**. Den öffentlichen Schlüssel muss man natürlich den jeweiligen Kommunikationspartnern zukommen lassen.

Will man nun eine verschlüsselte Mail verschicken, braucht man die fertige Mail, den **eigenen privaten Schlüssel** und den **öffentlichen Schlüssel des Empfängers**. Die geschriebene Mail wird nun zusammen mit dem Muster des eigenen privaten Schlüssels (als Unterschrift) durch das

... weiter auf Seite 2 ...

Schnappschloss gesichert und losgeschickt. Nur der Empfänger **kann das Schloss öffnen** und findet so die **Nachricht mit dem Muster**. Passt das Muster zum öffentlichen Schlüssel des behaupteten Absenders, kann sich der Empfänger der verschlüsselten Mail sicher sein, dass die Absenderinformation richtig ist. Zum Glück wird dieser ganze Vorgang von einer Software wie bspw. dem Enigmail-add-on für Thunderbird übernommen.

Einzig die **Überprüfung**, ob man auch den **richtigen öffentlichen Schlüssel des Empfängers bzw. Absenders** hat, muss man selbst übernehmen. Dazu haben öffentliche Schlüssel einen Fingerabdruck, denn man am besten bei einem **persönlichen Treffen abgleicht**, voilà.

Konkrete Schritte an einem Beispiel: Mozilla Thunderbird, Enigmail add-on und GNUpg installieren, Schlüsselpaar erzeugen, den öffentlichen Schlüssel weitergeben und andere öffentliche Schlüssel erhalten, dann Mails schreiben und Verschlüsselung aktivieren. Wenn die Verschlüsselung klappt, wird das auch bei jeder Mail angezeigt.

Workshop im Museum für Kommunikation Berlin

»Möglichkeiten des technischen Computer-Grundschutzes«

Forum InformatikerInnen für Frieden und gesellschaftliche Verantwortung e. V.

Politisch korrekt...

Internet: http://fiff.de
Email: fiff@fiff.de
Mailingliste: fiff-berlin@lists.fiff.de