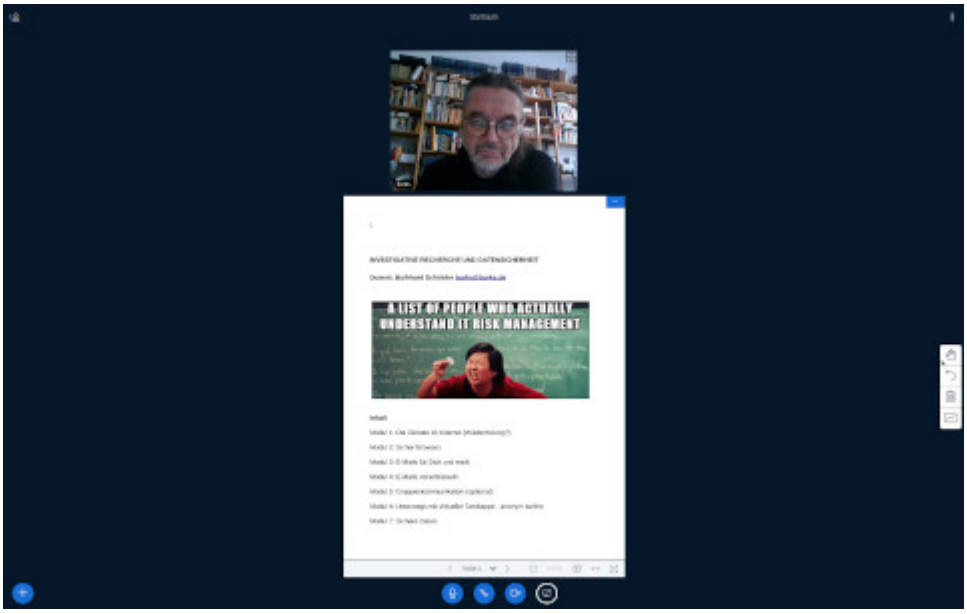
Investigative Recherche und Datensicherheit



Die Berliner Datenschutzbeauftragte empfiehlt BigBluebutton. Ich werde mich natürlich weigern, falls externe Bildungsträger mich anheuern wollten, Zoom zu benutzen – allein schon aus Daffke.

Gestern hat das hier schon angekündigte Seminar „Investigative Recherche und Datensicherheit“ von meinem „Home Office“ aus stattgefunden. Ich war sehr zufrieden.

Ich muss vermutlich das Seminar von fünf auf sechs Stunden ausdehnen, der Stoff ist sehr umfangreich. Am Schluss gerieten wir ein wenig ins Galoppieren. Mir wurde aus anderen Seminaren berichtet, dass die Teilnehmer nie länger als fünf Stunden aushielten. Das glaube ich nicht – es kommt auch auf den Dozenten an. Ich mache ohnehin in jeder Stunde zehn Minuten Pause.

Ich werde in Zukunft auch Einzelunterricht anbieten. Es ist sehr schwierig, schon bei drei Interessenten, einen gemeinsamen Termin zu finden. Wenn jemand nur am Abend Zeit hat, was oft bei Berufstätigen vorkommt, und am Wochenende sich nicht fortbilden will, könnte man die sechs Module des

Seminar in zwei dreistündige Teile splitten und es an zwei Abenden stattfinden lassen.

Ich ärgere mich jedes Mal auf's neue, wie unverständlich Anleitungen zu diesem und jenem sind. Ich werde viel Zeit brauchen, die auf der Website des Vereins German Privacy Fund zu aktualisieren, vor allem für die in den gängigen *manuals* nie erwähnten Fälle, wenn etwas *nicht* funktioniert. Ich habe zum Beispiel vergessen zu erwähnen, dass Thunderbird meckert – versucht man, eine erste verschlüsselte E-Mail zu verschicken -, wenn der verwendete Schlüssel nicht vorher signiert worden ist. ~~Das war früher besser.~~ Das ist ein unsinniges Feature, weil es erschwert, den Teilnehmern zu Testzwecken ein schnelles Erfolgserlebnis zu verschaffen.

Ich habe gerade eine Stunde meiner kostbaren Lebenszeit verwendet, um auf meinem kleinen Laptop, das – zu Demonstrationszwecken – mit Windows läuft, das E-Mail-Programm Claws Mail zu installieren. Witziges und pädagogisch wertvolles Feature: Claws Mail akzeptiert keine Mails in HTML – womit eine zentrale Gefahrenquelle ausgeschaltet ist. Man muss den meisten Leuten erst einmal umständlich erklären, dass sie nicht voraussetzen können, dass HTML im *body* gestattet ist. Die nehmen das als selbstverständlich hin. Mein Linux-Thunderbird ist ebenfalls so konfiguriert, dass HTML in E-Mails *nicht* angezeigt wird.

Ich verzweifele aber daran, mit Claws Mail zu verschlüsseln und zu entschlüsseln. (Ja, GPG4win und Kleopatra sind installiert. Typisch: Wenn man auf der GPG4win-Seite auf „Kleopatra" klickt, kommt error 404 – sehr „ermutigend „für Anfänger!) Braucht man nun ein Plugin oder nicht und welches und wo könnte man es herunterladen? (Auf der Claws-Mail-Plugin-Seite kann man nichts downloaden.) Soll ich PGP/Inline oder PGP/Core nehmen und warum? Es funktioniert einfach nicht.

Wer sich solche Anleitungen antut, ist doch Masochist. In Claws Mail gibt es in den Konteneinstellungen ein Feature, das

sich mit dem Thema beschäftigt, aber nicht verrät, wie vorhandene (!) Schlüsselpaare eingebunden werden können. Das Programm scheint auch weder mit GPG noch mit Kleopatra zu kommunizieren, was sinnvoll wäre. Falls ich das irgendwann hinbekomme, schreibe ich eine verständliche Anleitung auf Deutsch.

In der nächsten Woche wird der Relaunch der Website vermutlich abgeschlossen werden können; auch die Seite zum Seminar erstrahlt dann in neuem Glanz.