Passphrase-Warnung

Version 1.0, 07.04.2014

Das größte Problem in der Schulung ist die sichere Aufbewahrung des Offline-Hauptschlüssels. Die ist nur in der Art praktikabel, dass er mit einer eigenen, kryptografisch harten Passphrase gesichert wird. Die Sicherheit des Schlüssels steht und fällt also damit, dass diese Passphrase geschützt wird. Das bedeutet vor allem, dass sie **nie** in einem unsicheren System eingegeben wird.

Obwohl das leicht einsichtig ist, wird diese einfache Regel beständig ignoriert (von Leuten über die gesamte Spanne möglicher IT-Kompetenz). Es ist auch völlig egal, was man auf den Zettel druckt, auf dem die Passphrase eingetragen wird. Sobald im Arbeitssystem irgendwas nicht so läuft, wie der Nutzer sich das vorstellt, wird erst mal die Hauptschlüssel-Passphrase rausgeholt. Denn die ist ja offenbar das ganz große Geschütz, vielleicht kriegt die das Problem weggeräumt... Sie wird im Zweifelsfall auch – während der Dozent neben einem steht (aber gerade nicht hinguckt) – aus einem verschlossenen Briefumschlag herausgeholt, der genau das verhindern soll.

Was soll man denn noch machen? Den Briefumschlag mit Stacheldraht sichern? Als letzten Schritt vor dieser Maßnahme soll nun folgendes ausprobiert werden: Die Teilnehmer schreiben nicht nur die Passphrase auf den Zettel, sondern eine deutliche Warnung an sich selber auf die andere Seite. Vielleicht bleibt das besser hängen. Braucht es nur noch einen wirksamen Text; hoffentlich findet sich einer.

Versuch 1

> *Wenn ich die Passphrase auf diesem Zettel an der falschen Stelle eingebe, wird der aufwendig erzeugte Schlüssel unrettbar wertlos. Ungeduld ist der Tod des Schlüssels.*