# Leserbrief c’t Security II

Lieber Kollege Holger Bleich,

in der aktuellen c’t Security schreiben Sie (S. 11), man solle die „Möglichkeiten der Ermittler“ nicht unterschätzen. So weit, so gut und nachvollziehbar. „Seit 2010 ist bekannt, dass hierzulande auch die sogenannte ‚Quellen-TKÜV‘ zum Einsatz kommt, also das Belauschen von Verdächtigen direkt an ihrem Endgerät. Auf diese Weise haben Behörden bereits verschlüsselte Skype-Telefonate mitgehört und Mails nach der Entschlüsselung am PC abgfangen.“

Gestatten Sie, dass ich „der Kaiser ist nackt!“ rufe. Der Begriff „Quellen-TKÜV“ stammt aus dem Propaganda-Fundus des Innenministeriums und suggeriert, dass Behörden sich ohne Wissen eines Verdächtigen „von fern“ einen Remote-Access-Zugriff auf dessen Rechner verschaffen können. Das ist Unfug, wenn dieser Verdächtige sich einigermaßen vernünftig verhält und zum Beispiel Meldungen wie „cipav.exe is an unknown application. Install anyway?“ ignoriert.

Skype kann abgehört werden. Das Programm kann sogar andere Malware heimlich nachladen. Wer aber das Programm installiert, hat diese Features mit einer freien Willensentscheidung a priori akzeptiert und darf sich über die Folgen dann nicht wundern. Und wie sollen Behörden diese Spionage-Software ohne physikalischen Zugriff auf den (geöffneten!) Rechner installieren können? Dürfte ich auf Ihrem Laptop einfach so Programme installieren? Mir ist nicht bekannt, dass Skype zwangweise installiert werden könnte, ohne dass der Nutzer des jeweiligen Rechners das mitbekommt.

Thesen wie „Online-Durchsuchung: LKA installiert Spionage-Software bei Flughafenkontrollen“ würde ich gern zunächst auf Fakten überprüfen. Die Behörden können mir also Programme auf meinen Laptop installieren, ohne dass ich das merke? Da wüsste

ich doch gern mehr über die Details (Ich nutze Windows und Linux und denke mitnichten daran, die BIOS- und Truecrypt-Passworte auf einem Zettel bei mir zu tragen).

Mails nach der Entschlüsselung am PC abgefangen? Ist Ihnen irgendeine technisch nachvollziehbare Möglichkeit bekannt, gezielt (!) verschlüsselte Mails „von fern“ zu lesen, wenn der Verdächtige KEINE Mal- und Spionagesoftware vorher selbst installiert hat? Ich halte das, mit Verlaub, für eine Verschwörungstheorie, die aber so „sexy“ ist, dass sie gern wiederholt wird. „Seit 2010 ist bekannt“ bedeutet nur, dass das irgendwo in der Zeitung stand. Damit wird es nicht richtig. Die Methode „Stille Post“ ist aber für journalistische Standards kein gültiges Referenzsystem.

Kopie an Jürgen Kuri, der – wie ich – zu der leider nur kleinen Gemeinde der Ungläubigen und Zweifler gehört.

Mit freundlichen Grüßen
Burkhard Schröder
(Autor des Buches „Die Online-Durchsuchung“, Telepolis)