Open Source ist Glaubenssache

Berlin, 12. April 2014 – Mit Bekanntwerden von „Heartbleed“, einer der gravierendsten Sichherheitslücken in der Geschichte des Internets, verliert Open-Source seinen Status als „Allheilmittel“.

„Heartbleed“ betrifft OpenSSL. Das heißt, es handelt sich um eine Open-Source-Software, die bislang nicht zuletzt durch die Möglichkeit, den Quellcode einzusehen, für Verlässlichkeit stand. Was nun anlässlich der Sicherheitslücke deutlich wird: Open Source ist keine Garantie für Sicherheit. Viele Anwender (aber auch Hersteller) trösten sich mit dem Stempel "Open Source": "Da wird schon jemand draufgeschaut haben", "Ein Fehler kann nicht lange unentdeckt bleiben" und so weiter. Aber offenbar ist dem nicht so.

Die von Heartbleed betroffene Komponente "OpenSSL" ist ein Projekt von sehr wenigen Personen, die nebenberuflich daran arbeiten. Wollte man besseren, das heißt sichereren Code, müsste man dafür bezahlen. Wenn eine Firma Fehler macht, bezahlt sie mit dem Verlust des Vertrauens in ihre Marke. Wenn Open-Source-Code sich zunehmend als unsicher herausstellt, bezahlen nicht nur gutgläubige Unternehmen, sondern auch diese an sich gute Bewegung als Ganzes. Was fehlt, ist eine seriöse, unabhängige Finanzierung von grundlegender Sicherheitstechnik, wie es OpenSSL eben ist.

Unabhängige Code-Audits sind teuer und passieren nicht von alleine. Während die vielgenutzte Transportverschlüsselung OpenSSL trotz Open Source jahrelang einen fatalen Fehler enthalten konnte, wird die populäre Open-Source-Festplattenverschüsselung TrueCrypt auch zehn Jahre nach dem Erscheinen der ersten Version immer noch genutzt, obwohl keine unahängige Überprüfung des Quellcodes stattgefunden hat – die Tatsache, dass das Programm Open Source ist, reichte als Qualitätssiegel. Erst im Oktober 2013 wurde eine Crowdfunding-Intiative aufgesetzt, um Mittel für eine erste vollständige und unabhängige Überprüfung von Truecrypt zu sammeln. Der Ausgang dieser Überprüfung ist ungewiss.

Open Source ist nicht per se schlecht und kommerzielle Software ohne veröffentlichten Quellcode nicht per se besser. Aber klar ist jetzt auch: Dem Sicherheitsversprechen von Open Source blind zu glauben heisst nicht wissen wollen.