Online-Durchsuchung

Liebe Leserinen und Leser,

ganz aktuell ist das „Gesetz zur effektiveren und praxistauglicheren Ausgestaltung des Strafverfahrens", Bundesgesetzblatt, 23. August 2017, S. 3202. Es klingt wie ein Schritt zum Bürokratieabbau, ist aber im Kern ein tiefer Einschnitt in die Glaubwürdigkeit von Sicherheitsversprechen für Daten und Kommunikation im Netz. Es geht um den schon lange schwelenden Konflikt zwischen Straftatverfolgung und -prävention auf der einen Seite und Datenschutz und -sicherheit andererseits. Durch die inzwischen leicht verfüg- und implementierbare starke Verschlüsselung hat sich dieser Konflikt weiter verschärft. Beschädigt wird durch den im Eilverfahren durchgesetzten Gesetzgebungsakt vor allem das Sicherheitsversprechen der Kryptographie.

Die Apologeten einer beweisbar sicheren Kryptographieanwendung setzen dafür hohe Maßstäbe. Mit großer Beharrlichkeit wird den Internetnutzern klargemacht, dass nur eine Ende-zu-Ende Verschlüsselung zielführend sein kann. Sie hegen dabei keinen Zweifel daran, dass der Anwender die damit in ihn gesetzten Anforderungen sorgfältig erfüllen will und kann. Die Anwender sollen dabei immer umfangreicher werdende Awarenessvorschriften befolgen. Oft unausgesprochene Voraussetzungen für das Vertrauen in die Sicherheit einer Ende-zu-Ende Verschlüsselung sind die Integrität der Anwendungsumgebung der Nutzer (Bundesverfassungsgericht, Urteil zur Online-Durchsuchung vom 27. Februar 2008 – 1 BvR 370/07, 1 BvR 595/07, BVerfGE 120, 274, „Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme") sowie vertrauenswürdige Kommunikations- und Sicherheitsinfrastrukturen. Beide Voraussetzungen sind heute im Netz nicht gegeben und wären auch auf Nutzerebene nicht überprüfbar.

Zwei Faktoren sind maßgeblich daran beteiligt, dass tendenziell die Sicherheitsrisiken weiter zunehmen:

1. Die IT-Systeme werden immer komplexer, insbesondere weist die Software regelmäßig Schwachstellen auf, die Lücken für Angriffe durch Schadprogramme bieten;
2. die Entwicklung und Anwendung von Schadsoftware wird zunehmend „kommerzialisiert". Die damit verbundenen Geschäftsmodelle sind tatsächlich auch für Cyberkriminelle und Hacker erfolgreich.

Vor diesem Hintergrund ist nüchtern festzustellen, Sicherheit und Vertrauenswürdigkeit im Internet bleiben noch immer Visionen.

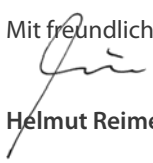
Eine positive Ausnahme stellt – für sich genommen – die in den letzten Jahrzehnten erreichten Optimierungen von Kryptoverfahren und -anwendungen dar. Immerhin mit dem Ergebnis, dass nun deren Implementierung so sicher ist, dass auch mit großen Ressourcen – wie sie Staaten und ihren Diensten zur Verfügung stehen – die Entschlüsselung von Nachrichten nahezu unmöglich geworden ist. Die „traditionelle" Telekommunikationsüberwachung (TKÜ) durch Abhören läuft ins Leere.

Für Datenschutz und Informationssicherheit im strengen Sinne ein erfreuliches Ergebnis, für Strafverfolgung oder -prävention ein Dilemma.

Dass diese Situation durch die gesetzliche Zulassung von Online Durchsuchungen mit Schadsoftware (z.B. Bundestrojaner für Quellen-TKÜ) beantwortet wird, ist ein folgenreicher Schritt gegen die Vertrauenswürdigkeit kryprographischer Anwendungen im Internet. Die Fachwelt weiß, dass hierzu vergleichbare Angriffsmethoden erforderlich sind, wie sie von Hackern und Internetkriminellen benutzt werden. Es ist aber nicht zu verantworten, deren Instrumentarium indirekt aufzuwerten, zu nutzen oder zu ergänzen. Im Sinne einer vertrauenswürdigen Internet-Sicherheit wäre dagegen allein die kompromisslose Aufdeckung und Beseitigung von Schwachstellen aller Art – die letztlich das Eindringen in IT-Systeme ermöglichen – ein glaubwürdiger Weg in die Zukunft.

Lesen Sie mehr über die Hintergründe in der Rubrik Forum in diesem Heft der DuD ab S. 37.

Mit freundlichen Grüßen, Ihr



Helmut Reimer