Felix Freiling

Was ist eine Quellentelekommunikationsüberwachung?

Im Verfahren des Bundesverfassungsgerichts zur Online-Durchsuchung im Jahr 2007 interessierten sich die Richter sehr für die tatsächlichen Möglichkeiten und Methoden, mit denen informationstechnische Systeme durch Ermittlungsbehörden infiltriert werden können. Die technischen Gutachter, zu denen auch der Autor zählte, waren damals gezwungen, allgemeine Erkenntnisse aus dem Bereich der Cyberkriminalität auf den Bereich staatlicher Eingriffe zu übertragen. Im vergangenen Jahr bot sich jedoch erstmals die Gelegenheit, die damaligen Annahmen anhand eines konkreten Falles staatlicher Infiltration zu überprüfen.

TKÜ und Quellen-TKÜ

Hoch entwickelte Gesellschaften sind sehr viel mehr auf sichere Informationstechnik angewiesen als die organisierte Kriminalität. Darum ist die Einführung von starker Kryptographie in allen Bereichen des Cyberspace aus gesellschaftlicher Sicht uneingeschränkt zu befürworten. Natürlich ergeben sich neue Probleme aus der zunehmenden Tendenz, Daten standardmäßig Ende-zu-Ende-verschlüsselt auszutauschen,

Ein bekanntes Problemfeld entsteht aus dem Wunsch staatlicher Ermittlungsbehörden, laufende Telekommunikation zu überwachen (TKÜ), da auch die Hilfe des Telekommunikationsdiensteanbieters bei entsprechender Verschlüsselung nicht mehr ausreicht. Ein möglicher Lösungsweg besteht im Einbringen einer Software an der *Quelle* der Verschlüsselung, also an der Stelle, wo beispielsweise die Sprachinformationen aufgenommen werden. Dies wird häufig mit dem Begriff *Quellentelekommunikationsüberwachung* (Quellen-TKÜ) bezeichnet. So sehr sich dieser Begriff an die *normale* Telekommunikationsüberwachung anlehnt, so unterschiedlich sind doch die Mechanismen, mit denen gearbeitet wird. Es stellt sich die Frage, unter welchen Bedingungen eine Quellen-TKÜ mit einer klassischen, netzbasierten TKÜ vergleichbar wäre.

Untersuchung von BckR2D2

Im Sommer 2011 wurde uns durch den Rechtsanwalt Patrick Schladt die Kopie der Festplatte eines seiner Mandanten zur Verfügung gestellt. Aus dem Kontext des Ermittlungsverfahrens heraus bestand die Vermutung, dass eine auf dem Rechner installierte Software Daten an die Polizeibehörden ausgeleitet hatte. Wir fanden auf dieser Festplatte ein Programm, das sich als Variante der Schadsoftware herausstellte, deren Analyse der Chaos Computer Club im Oktober 2011 medienwirksam veröffentlichte [2]. Die Umstände des Fundes und die öffentlichen Reaktionen der Behörden legen nahe, dass es sich in der Tat um eine Software handelt, die auch zur Durchführung einer Quellen-TKÜ in das System eingebracht wurde.

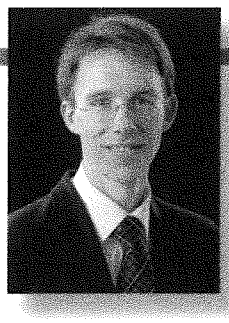
Uns liegen mittlerweile zwei Varianten dieser Software vor, die inzwischen meist als BckR2D2-I und II bezeichnet werden. Die Ergebnisse unserer Analysen [1] decken sich im Wesentlichen mit denen des CCC [2] und anderer. Bemerkenswert erscheinen uns dabei zwei Punkte.

Der erste Punkt bezieht sich auf die mangelhafte Qualität der durch die verschiedenen Varianten der Software implementierten Datensicherheitsmechanismen. So beruhten der Authentifikationsmechanismus und die Verschlüsselung auf fest codierten Werten, die leicht aus der Software extrahierbar waren. Außerdem wurden sämtliche Parameter, die an den aufgefundenen Kernel-Level-Treiber übermittelt wurden, nicht überprüft. Durch den unbeschränkten Zugriff auf das Dateisystem war es dadurch für Dritte sehr leicht, das System in beliebiger Weise auch ohne Administratorrechte zu manipulieren.

Der zweite Punkt bezieht sich auf die durch die Software implementierte Überwachungsfunktionalität. In der Variante BckR2D2-I wurde offenbar die Schadsoftware in alle startenden Prozesse injiziert und aktivierte sich, wenn der Prozessname in einer Applikations-Whitelist enthalten war. Diese enthielt in Version BckR2D2-I sechs Programmnamen, darunter die VoIP-Programme Skype und XLite. In Version II wurden jedoch bereits 14 Programme auf ähnliche Weise überwacht, darunter auch einige Instant-Messenger-Anwendungen. Zusätzlich erlaubte die Software, Bildschirmfotos sowohl aktiver Fenster von Internetbrowsern als auch des gesamten Desktops anzufertigen.

Was ist eine Quellen-TKÜ?

Im Lichte der Analyseergebnisse ist fraglich, ob die Überwachungsmöglichkeiten, die die untersuchte Software erlaubte, noch in irgendeiner Form mit einer klassischen Telekommunika-



Felix Freiling

Felix Freiling ist Inhaber des Lehrstuhls für IT-Sicherheitsinfrastrukturen an der Friedrich-Alexander-Universität Erlangen-Nürnberg. Schwerpunkte seiner Arbeitsgruppe in Forschung und Lehre sind offensive Methoden der IT-Sicherheit, technische Aspekte der Cyberkriminalität sowie digitale Forensik (IT-Beweismittelsicherung und -analyse). In den Verfahren zur Online-Durchsuchung und zur Vorratsdatenspeicherung vor dem Bundesverfassungsgericht diente Felix Freiling als sachverständige Auskunftsperson.

tionsüberwachung vergleichbar sind. Es scheint deshalb geboten, die Anforderungen an eine Quellen-TKÜ sowohl technisch als auch juristisch präziser zu definieren und von einer klassischen netzbasierten TKÜ abzugrenzen.

Als erstes muss gefordert werden, dass Datensicherheitsstandards nach dem Stand der Technik eingehalten werden. Dies betrifft sowohl die Verschlüsselung und (individuelle) Authentifikation der Netzwerkkommunikation als auch die sichere Implementierung aller Softwarekomponenten. Die Risiken, die durch die Überwachungssoftware entstehen, müssen nach dem Stand der Technik minimiert werden. Im Vergleich zu BckR2D2 erscheinen aktuelle Banking-Trojaner als geradezu vorbildhaft.

Beschränkung auf „laufende Telekommunikation"

Nimmt man den Vergleich zur klassischen TKÜ ernst, so darf auch die Quellen-TKÜ ausschließlich „laufende Telekommunikation" ausleiten. Die Software ist aber gezwungen, Daten bereits vor der Ausleitung (nämlich vor der Verschlüsselung) abzufangen und zu speichern. Ausgeleitet werden dürfen sie jedoch nur, wenn das entsprechende Chiffrat über das Netz verschickt wird.

Technisch könnte man das wie folgt definieren: Wenn ein gegebenes Kommunikationssystem (etwa ein Computer mit VoIP-Software) keine Verschlüsselung benutzt, dann ist „laufende Telekommunikation" das, was über das Netz verschickt wird. Wenn wir allerdings ein Kommunikationssystem K1 haben, das Verschlüsselung benutzt, dann kann man sich gedanklich ein hypothetisches Kommunikationssystem K2 konstruieren, was genau das gleiche macht wie K1, ohne allerdings Verschlüsselung zu benutzen. (Technisch würde man einfach die Aufrufe der Verschlüsselung weglassen.) Was dann bei K1 mitgeschnitten werden darf, sind alle Daten, die K2 versenden oder empfangen würde.

Selbstverständlich muss die Verschlüsselung in unmittelbarem (funktionalem und auch zeitlichen) Zusammenhang mit dem Versand passieren. Andernfalls könnte man die Definition auf jede Art von Verschlüsselung anwenden. Die Definition passt also auf typische VoIP-Programme, SSL-verschlüsselten Datenverkehr und verschlüsselte E-Mails, die unmittelbar vom Mailprogramm chiffriert werden (beispielsweise via S/MIME). Die Definition träfe nicht zu auf Dateien, die zu einem Zeitpunkt händisch verschlüsselt und dann später als Anhang verschickt werden. Dies ist auch sinnvoll, denn bei einer weiter gefassten Definition wäre es möglich, beliebige Dateien (quasi prophylaktisch) beim Verschlüsseln abzufangen, auch wenn nicht klar ist, ob diese überhaupt jemals verschickt werden. Das wäre auch bei wohlwollender Interpretation des Begriffs keine Telekommunikationsüberwachung.

Fazit

Die Schwierigkeiten, eine Quellen-TKÜ im Sinne einer klassischen TKÜ zu definieren, zeigen auf, wie unterschiedlich diese beiden Konzepte eigentlich sind. Darauf hat auch das Bundesverfassungsgericht in seinem Urteil zur Online-Durchsuchung deutlich hingewiesen: Mit der Infiltration eines Systems sei „die entscheidende Hürde genommen, um das System insgesamt auszuspähen." [3, Absatz-Nr. 188] Diese Einsicht ist aber vielerorts noch nicht im Bewusstsein von Richtern und Gesetzgebern angekommen. Das neue BKA-Gesetz regelt beispielsweise in einem eigenen Paragraphen die Quellen-TKÜ (§20l, Absatz 2, BKAG), jedoch wird (1) der Begriff der „laufenden Telekommunikation" nicht näher definiert, und es werden (2) keine spezifischen Anforderungen an die eingesetzte Software formuliert. Im Lichte der Erkenntnisse über die Software BckR2D2 sollte jedoch klar sein, dass es neben präzisen technischen und juristischen Definitionen auch eine unabhängige Kontrolle der Überwachungssoftware geben muss, etwa in Form einer Zertifizierung durch das Bundesamt für die Sicherheit in der Informationstechnik [4, S. 144].

Danksagung

Der Autor dankt Matthias Bäcker für hilfreiche Diskussionen.

Anmerkungen

[1] *Andreas Dewald, Felix C. Freiling, Thomas Schreck, Michael Spreitzenbarth, Johannes Stüttgen, Stefan Vömel, Carsten Willems: Analyse und Vergleich von BckR2D2-I und II. Friedrich-Alexander-Universität Erlangen-Nürnberg, Department Informatik, Technischer Bericht CS-2011-08, Dezember 2011.*

[2] *Chaos Computer Club: Analyse einer Regierungs-Malware. http://www.ccc.de/system/uploads/76/original/staatstrojaner-report23.pdf, 8. Oktober 2011.*

[3] *BVerfG, 1 BvR 370/07 vom 27.2.2008.*

[4] *Dominik Brodowski, Felix C. Freiling: Cyberkriminalität, Computerstrafrecht und die digitale Schattenwirtschaft. Forschungsforum öffentliche Sicherheit, Schriftenreihe Sicherheit Nr. 4, März 2011.*

Foto: Dagmar Boedicker