Standardisierende Leistungsbeschreibung

(Stand 2. Oktober 2012)

Die „Standardisierende Leistungsbeschreibung“ (SLB) verfolgt den Zweck, den in Deutschland zur Quellen-Telekommunikationsüberwachung (Quellen-TKÜ) berechtigten Stellen Mindeststandards an die Hand zu geben, um den Einsatz der Quellen-TKÜ in Deutschland auf einem vergleichbaren Stand sicherzustellen. Sie dient der Festlegung insbesondere technischer Vorgaben, die eine Software[1] für die Quellen-TKÜ erfüllen muss, um die verfassungsrechtlichen und gesetzlichen Vorgaben für Quellen-TKÜ-Maßnahmen zu erfüllen. Dies ist grundsätzlich der Fall, wenn:

1. der Eingriff in das informationstechnische System zwingend notwendig ist, um die Überwachung und Aufzeichnung der Telekommunikation insbesondere in unverschlüsselter Form zu ermöglichen und
2. durch Maßnahmen nach dem Stand der Technik sichergestellt ist, dass ausschließlich laufende Telekommunikation überwacht und aufgezeichnet wird.

Im Unterschied zu herkömmlichen TKÜ-Maßnahmen, bei denen die Telekommunikation den berechtigten Stellen[2] im Regelfall durch Ausleitung einer Überwachungskopie durch die Telekommunikationsdienstleister zur Verfügung gestellt wird, werden bei einer Quellen-TKÜ die Kommunikationsdaten durch ein von der berechtigten Stelle auf dem zu überwachenden System installiertes Programm[3] erhoben und eine Kopie dieser Daten an die berechtigte Stelle ausgeleitet. Insofern unterscheidet sich die Online-Durchsuchung von der Quellen-TKÜ, bei der ausschließlich auf Daten eines laufenden Kommunikationsvorgangs zugegriffen werden darf. Die SLB konzentriert sich auf die von der herkömmlichen TKÜ abweichenden technischen Verfahren und legt technische Sicherungsmaßnahmen als Mindeststandards fest. Sie ist damit keine Leistungsbeschreibung im Sinne einer Vergabeunterlage.

<u>Prinzipieller Aufbau der Quellen-TKÜ-Software und -Infrastruktur:</u>

Das Ziel der Quellen-TKÜ ist die Erfassung von Kommunikation, bevor diese verschlüsselt wird oder nachdem diese entschlüsselt wurde, da Kommunikation in verschlüsselter Form für eine Auswertung nicht zugänglich ist. Aus technischen Grün-

[1] Software wird in diesem Dokument als Oberbegriff für die zur Aufgabenerfüllung erforderlichen Programme, den zugehörigen Quellcode und sonstige für die Ausführung der Programme benötigten Ressourcen verwendet.

[2] Gemäß § 2 Nr. 3 TKÜV die nach § 100b Abs. 3 Satz 1 der Strafprozessordnung, § 1 Abs. 1 Nr. 1 des Artikel 10-Gesetzes, § 23a Abs. 1 Satz 1 des Zollfahndungsdienstgesetzes oder nach Landesrecht auf Grund der jeweiligen Anordnung zur Überwachung und Aufzeichnung der Telekommunikation berechtigte Stelle.

[3] Ein Computerprogramm oder kurz Programm ist eine Folge von Anweisungen, die auf einem informationstechnischem Systemausgeführt werden können, um damit eine bestimmte Funktionalität zur Verfügung zu stellen.

den besteht die Software zur Quellen-TKÜ i. d. R. aus einem Programm, das die Daten vor der Verschlüsselung bzw. nach der Entschlüsselung auf dem zu überwachenden informationstechnischen System erfasst und ausleitet (Überwachungsprogramm), sowie einem weiteren Programm, das von den berechtigten Stellen genutzt wird, um das Überwachungsprogramm zu steuern und die ausgeleiteten Daten aufzuzeichnen (Aufzeichnungs- und Steuerungseinheit). Die Programme werden daher auf getrennten informationstechnischen Systemen eingesetzt. Hinzu kommt i. d. R. eine Netzwerkverbindung, über die die Steuerdaten und die mit der Maßnahme überwachten bzw. ausgeleiteten Inhalte gesichert übertragen werden (üblicherweise das Internet). Dieser Struktur folgt auch die Gliederung dieser SLB.

Während sich das IT-System zur Steuerung des Überwachungsprogramms und Aufzeichnung der Telekommunikationsdaten einschließlich der darauf genutzten Programme in der gesicherten Hand der berechtigten Stellen befindet, erfordert die Kontrolle des Überwachungsprogramms erhöhte Schutzmaßnahmen, da es sich auf dem zu überwachenden, von einem Dritten kontrollierten IT-System (Zielsystem) befindet. Da der wesentliche technische Unterschied zwischen herkömmlicher TKÜ und Quellen-TKÜ darin besteht, dass eine Überwachungssoftware auf das Zielsystem aufgespielt werden muss, beschränkt sich die SLB im Weiteren auf die Beschreibung der Sicherungsmaßnahmen für das Überwachungsprogramm sowie des Übertragungsweges zur Datenausleitung und Steuerung. Im Hinblick auf das Aufzeichnungs- und Steuersystem wird soweit wie möglich auf Lösungen im Rahmen der bestehenden Technik der herkömmlichen TKÜ verwiesen.

Aufgrund der kurzen Innovationszyklen der für Telekommunikation genutzten technischen Geräte und deren Software sowie des technischen Fortschritts ist die SLB regelmäßig auf Aktualisierungsbedarf zu prüfen, und ggf. sind die erforderlichen Schritte zur Fortschreibung zu initiieren.

1 Allgemeine Anforderungen

1.1 Hersteller und Anbieter von Software

Hersteller und Anbieter von Software zur Quellen-TKÜ sind sorgfältig im Hinblick auf ihre Fachkompetenz und Vertrauenswürdigkeit auszuwählen. Aufgrund der Vertraulichkeit der Funktionsdetails der Quellen-TKÜ-Software ist die Geheimschutzbetreuung der Hersteller und Anbieter durch das BMWi anzustreben. Diese Betreuung und die damit verbundene Sicherheitsüberprüfung nach dem Gesetz über die Voraussetzungen und das Verfahren von Sicherheitsüberprüfungen des Bundes (SÜG) der Beschäftigten des Anbieters gewährleisten ein hohes Maß an personeller Sicherheit, das auch in anderen sicherheitssensiblen Bereichen als Mindeststandard angesehen

wird. Für Anbieter aus dem Ausland ist ein diesem Standard entsprechendes Verfahren anzuwenden.

1.2 Quellcodetransparenz und Quellcodeprüfung

Quellcodetransparenz

Die Hersteller und Anbieter von Software zur Durchführung von Quellen-TKÜ, die am Beschaffungsverfahren einer Quellen-TKÜ-Software teilnehmen, verpflichten sich, den ausreichend kommentierten Quellcode und andere zur Prüfung der Funktionalität der Software relevante Informationen (z.B. Dokumentation der gesamten Architektur und des Designs einzelner Software-Komponenten und -Module) offenzulegen. Die Offenlegung kann gegenüber der beauftragenden Stelle oder einer von dieser beauftragten dritten Stelle erfolgen. Die prüfenden Stellen müssen in die Lage versetzt werden, den Erstellungsvorgang aller gelieferten Quellen-TKÜ-Programme aus dem Quellcode vollständig und exakt nachzuvollziehen.

Auch der Quellcode und die Details des Erstellungsvorgangs (Kompilation etc.) der vom BKA selbst zu entwickelnden Software zur Durchführung von Quellen-TKÜ (Eigenentwicklung) muss neben den anderen zur Prüfung der Funktionalität relevanten Informationen den einsetzenden Stellen offengelegt werden.

Die Möglichkeit zur Prüfung des Quellcodes durch die für die beauftragende Stelle jeweilige datenschutzrechtlich zuständige Stelle ist zu gewährleisten.

Quellcode- und Funktionsprüfung

Durch die Quellcodeprüfung soll gewährleistet werden, dass die Quellen-TKÜ-Software mit den Vorgaben dieser SLB übereinstimmt. Die Quellcodeprüfung soll von fachlich geeigneten Externen, bspw. BSI-akkreditierten Prüflaboren, vorgenommen werden, die der Geheimschutzbetreuung durch das BMWi unterliegen oder ein vergleichbares Schutzniveau aufweisen. In das Ergebnis der Quellcodeprüfung kann die für Zwecke der Datenschutzkontrolle zuständige Stelle Einsicht nehmen.

Entsprechend dem Stand der Technik ist die Software zur Quellen-TKÜ modular aufgebaut. Die für eine konkrete Quellen-TKÜ-Maßnahme genutzte Software besteht aus einer Reihe von Funktionsmodulen, die in nahezu allen Fällen Anwendung finden (Basismodule), und einigen maßnahmenspezifischen Anpassungen des Quellcodes, um den Vorgaben der anordnenden Stelle zu entsprechen und die im Einzelfall vorhandene Technik des Zielsystems zu berücksichtigen.

Angesichts des in jeder Maßnahme identischen Quellcodes der Basismodule ist es ausreichend, diese einmalig im Rahmen einer Typmusterprüfung zu analysieren und intensiv zu testen. Die Typmusterprüfung ist zu wiederholen, wenn wesentliche Veränderungen an Basismodulen vorgenommen werden (z. B. Aufnahme eines neuen Verschlüsselungs- oder Schlüsselaustauschverfahrens).

Demgegenüber führt die regelmäßig benötigte Anpassung des Quellcodes an die jeweiligen Umstände der Maßnahme (sog. Customizing) in der Regel nur zu geringen Änderungen, deren mögliche Auswirkungen auf ihre Sicherheitsrelevanz geprüft werden sollten. Dies kann im Rahmen der jeweils erfolgenden Funktionstests des Überwachungsprogramms durchgeführt werden. Im Falle geringer Sicherheitsrelevanz der Änderungen kann aufwendige Quellcodeprüfung durch externe Stellen durch die Protokollierung bzw. Archivierung des Quellcodes und des zugehörigen Überwachungsprogramms sowie der Funktionsprüfung ersetzt werden. Im Falle hoher Sicherheitsrelevanz der Änderungen ist eine erneute Tymusterprüfung erforderlich. Mit Hilfe dieser Protokollierung bzw. Archivierung ist es möglich, alle relevanten Parameter der Software im Nachhinein zu analysieren.

Das Verfahren hierzu ist durch die Länder bzw. durch den Bund in einer gesonderten Konzeption unter Benennung einer möglichst zentralen protokollierenden bzw. archivierenden Stelle zu beschreiben.

1.3 IT-Sicherheitskonzepte

Grundsätzlich ist ein den Gesamtprozess der Quellen-TKÜ (Software-Entwicklung und Test, Abnahme von Software, Durchführung von Maßnahmen) umfassendes IT-Sicherheitskonzept, das sich an den BSI-Standards 100-2, 100-3 und 100-4 orientiert, zu erstellen. Die Einhaltung dieses Konzeptes ist im Vorfeld sowie während und nach der Umsetzung der Maßnahmen zu gewährleisten. Entwicklung und Auslieferung der Quellen-TKÜ-Software sollte zur Gewährleistung der Vertrauenswürdigkeit in Anlehnung an die CC-Anforderungen zum Software-Life-Cycle ausgeführt werden.

Der Anbieter hat ein IT-Sicherheitskonzept für den von ihm zu vertretenden Teil im Rahmen der Angebotsabgabe der jeweiligen beauftragenden Stelle vorzulegen. Die Prüfung des Konzepts sowie die Einhaltung der festgelegten Maßnahmen sind zu gewährleisten.

1.4 Sicherung der Datenübertragung

Die eingesetzten Programme und die zwischen ihnen übertragenen Daten sind nach dem Stand der Technik gegen unbefugte Nutzung zu schützen. Dabei ist der Schutzbedarf der grundlegenden Sicherheitseigenschaften Vertraulichkeit, Integrität, Authentizität sowie Verfügbarkeit grundsätzlich hoch, bedarf jedoch der Festlegung im Einzelfall:

- Authentizität: Durch gegenseitige Authentisierung aller kommunizierenden Instanzen ist zu gewährleisten, dass die Datenübertragung ausschließlich zwischen dem Programm auf dem Zielsystem und dem zur Aufzeichnung und Steuerung genutzten Programm auf dem IT-System der einsetzenden Stelle erfolgt.

- Vertraulichkeit: Zur Wahrung der Vertraulichkeit auf dem Übertragungsweg ist sicherzustellen, dass alle Daten (d.h. z. B. auch Steuerungskommandos an das Zielsystem, Aktualisierung der Software auf dem Zielsystem, die Daten vom Zielsystem) zwischen Zielsystem und dem Aufzeichnungs- und Steuerungssystem der berechtigten Stelle mit einem dem Stand der Technik entsprechenden Verfahren durchgehend verschlüsselt werden.
- Integrität: Alle zu übertragenden Daten (d.h. z.B. auch Steuerungskommandos an das Zielsystem, Aktualisierung der Software auf dem Zielsystem, die Daten vom Zielsystem) sind durch digitale Signaturen und Signaturprüfungen gegen Veränderung zu sichern.
- Verfügbarkeit: Geeignete Maßnahmen sind zu treffen. Für den Fall, dass das Steuerungs- oder das Aufzeichnungssystem längere Zeit nicht mehr erreichbar ist, sind vorab geeignete Maßnahmen zu treffen (vgl. hierzu u.a. 2.7)

Durch o. g. Maßnahmen ist sicherzustellen, dass die Software nicht durch unbefugte Dritte angesprochen oder zweckentfremdet genutzt werden kann. Ebenso wird gewährleistet, dass sich die Software nicht an einem anderen als dem von der jeweiligen berechtigten Stelle eingesetzten Aufzeichnungs- und Steuerungssystem zurückmeldet. Die Gewährleistung der Integrität und Vertraulichkeit der Steuerbefehle und der ausgeleiteten Daten dient dabei zwei Zielen: Zum einen wird der Betroffene davor geschützt, dass die vom Zielsystem ausgeleiteten Daten nachträglich zufällig oder bewusst verändert werden oder Unbefugten zur Kenntnis gelangen. Zum anderen wird dem behördlichen und justiziellen Interesse an der Beweissicherheit der polizeilichen Erkenntnisse Rechnung getragen.

Die zur Verschlüsselung und Authentisierung einzusetzenden kryptografischen Verfahren sind entsprechend den Empfehlungen der BSI-Richtlinie „Kryptographische Verfahren: Empfehlungen und Schlüssellängen (BSI TR-02102)“ in der jeweils gültigen Fassung zu gestalten. Dabei wird im Rahmen der konkreten Ausgestaltung dafür gesorgt, dass ein ausgewogenes Verhältnis im Hinblick auf die Sicherheit der Übertragung und die Anforderungen, die sich aus der verdeckten Arbeitsweise des Programms ergeben, gewählt wird.

Die Schlüssel (ggf. Zertifikate) sind mit Ausnahme derjenigen, die für die Initialauthentisierung benötigt werden, für jede Sitzung neu zu generieren. Schlüssel (ggf. Zertifikate) für die Initialauthentisierung sind für jede Quellen-TKÜ-Maßnahme neu zu erstellen. Die Identitätsinformation der Steuerungskomponente soll dabei fest in der Software für das Zielsystem verankert werden.

Sofern Schlüssel oder Zertifikate auf dem Zielsystem abgelegt werden, sind diese durch geeignete Schutzmaßnahmen zu sichern. Dies gilt, mit Ausnahme des aus

technischen Gründen unvermeidlichen Zeitraums der Schlüsselnutzung, auch für Schlüssel oder Zertifikate, die zur Laufzeit benötigt werden.

1.5 Umfassende Protokollierung

Bei der Quellen-TKÜ handelt es sich um eine verdeckte Maßnahme. Der Nachweis der Herkunft, Integrität und Authentizität der Daten ist dabei von besonderer Bedeutung. Die Verwendung der Daten zur Strafverfolgung und Gefahrenabwehr setzt einen lückenlosen Nachweis von der Erhebung über die Bewertung und Weiterverarbeitung innerhalb der berechtigten Stelle voraus. Die Prozesse zur Erkenntniserlangung müssen auch in einem späteren Stadium des Verfahrens zweifelsfrei nachvollzogen werden können.

Die umfassende Protokollierung dient der Kontrolle der Rechtmäßigkeit der Maßnahme bzw. der Datenverarbeitung, der Gewährleistung eines effektiven Grundrechtschutzes der Betroffenen z.B. auch durch die Gewährleistung einer datenschutzrechtlichen Kontrolle, zugleich aber auch der Gewährleistung der Gerichtsfestigkeit der im Rahmen der Überwachung aufgezeichneten Daten. Insbesondere ermöglicht die Protokollierung den Nachweis, dass die Daten tatsächlich vom betroffenen informationstechnischen System stammen und nicht verändert worden sind.

Es erfolgt insbesondere eine umfassende Protokollierung:

- des eingesetzten Überwachungsprogramms, des dem Programm zugrundeliegenden Quellcodes sowie der exakten und vollständig verwendeten Entwicklungsumgebung inklusive nicht systemimmanenter Bibliotheken,
- der Funktionsprüfung nach der maßnahmenspezifischen Anpassung des Überwachungsprogramms,
- der Umsetzung der IT-sicherheitstechnischen Konzepte unter konkreter Bezeichnung der Verantwortlichkeiten,
- des gesamten umfassenden Zeitraums sowie der konkreten Zeitabschnitte des Einsatzes des Überwachungsprogramms,
- der zur Übertragung der auszuleitenden Daten genutzten technischen Einrichtungen und der jeweils getroffenen Sicherheitsvorkehrungen,
- der Angaben zur Identifizierung des informationstechnischen Zielsystems,
- der durchführenden Behörde bzw. Organisationseinheit,
- der Benutzer, der im Zusammenhang mit der Maßnahme administrative oder auswertende Tätigkeiten an dem zur Quellen-TKÜ genutzten Aufzeichnungs- und Steuersystem wahrgenommen hat,
- der Einstufung von Daten als kernbereichsrelevant sowie deren Löschung,

- der Löschung von aufgezeichneten Daten und der vorzeitigen Löschung von Protokolldaten,
- der Löschung des für die Maßnahme eingesetzten Überwachungsprogramms und der Maßnahmen, um die vorgenommenen nichtflüchtigen Änderungen am Zielsystem rückgängig zu machen.
- der erhobenen Daten inklusive der für die Maßnahme erforderlichen Metadaten,
- jedes Steuerbefehls an die Überwachungssoftware auf dem Zielsystem und der in diesem Zusammenhang erfolgten Statusmeldungen,
- der systemadministrativen Tätigkeiten einschließlich der Nutzung von Daten im Rahmen dieser Tätigkeiten,
- der am informationstechnischen Zielsystem vorgenommenen nicht nur flüchtigen Veränderungen.

Die Dauer der Aufbewahrung der Protokolldaten richtet sich nach den einschlägigen gesetzlichen Vorschriften des Bundes und der Länder.

2 Anforderungen an die Überwachungssoftware

2.1 Spezifische Programme für die Quellen-TKÜ

Für die Durchführung von Maßnahmen der Quellen-TKÜ wird jeweils ein dem richterlichen Beschluss oder der Anordnung angepasstes Programm erstellt, welches ausschließlich die Telekommunikationsüberwachung der im Beschluss bzw. in der Anordnung genannten Kommunikationskanäle und -dienste ermöglicht.

D. h. insbesondere, dass Programme für die Quellen-TKÜ keine Funktionen für andere Maßnahmen der informationstechnischen Überwachung enthalten.

2.2 Beschränkung auf den laufenden Kommunikationsvorgang

Die Erhebung der Kommunikationsdaten durch das Überwachungsprogramm wird durch technische Vorkehrungen auf Inhalte und Umstände aus einem laufenden, d.h. zum Zeitpunkt der Überwachung aktuell stattfindenden und dem Schutzbereich des Art. 10 GG unterliegenden Telekommunikationsvorgangs beschränkt.

Ein laufender Kommunikationsvorgang umfasst beispielhaft

- ein vom Zielrechner aus geführtes Gespräch unter Nutzung eines VoIP-Dienstes,
- eine im Sende- oder Empfangsstadium befindliche E-Mail

und ist beispielsweise gekennzeichnet durch

- Sende- und Empfangsaktivitäten des Kommunikationsprogramms oder
- Datenverkehr auf den vom Kommunikationsprogramm genutzten Ports.

Das Überwachungsprogramm überprüft z.B. die vorangehend genannten Bedingungen und erfasst die gerade zu versendenden bzw. empfangenen Daten an geeigneten Kommunikationsschnittstellen des Zielsystems. Dadurch wird gewährleistet, dass ausschließlich Inhalte und Umstände des laufenden Telekommunikationsvorgangs erfasst werden.

2.3 Nur unvermeidbare Änderungen am Zielsystem

Die Sicherheit und Stabilität des Zielsystems darf durch das Aufbringen, den Betrieb und die Löschung der Überwachungssoftware nicht mehr als unvermeidbar beeinträchtigt werden. Dazu ist sicherzustellen, dass an dem informationstechnischen System nur Veränderungen vorgenommen werden, die für die Erhebung und Ausleitung der Kommunikation unerlässlich sind.

Beispielsweise dürfen Maßnahmen, die das Zielsystem vor unberechtigten Zugriffen schützen (z.B. Firewalls, Antivirensoftware und Updateprozesse), nicht länger und nicht mehr als nötig eingeschränkt werden. Die von dem Überwachungsprogramm benötigte Schnittstelle zur Ausleitung der Daten und Steuerung wird durch die in Kapitel 1.4 geschilderten Maßnahmen gegen unbefugte Nutzung geschützt. Vor dem Aufbringen des Überwachungsprogramms ist im Rahmen von Tests an einem geeigneten Testsystem zu prüfen und zu dokumentieren (s. Kapitel 1.5), dass zu erwarten ist, dass das Zielsystem und insbesondere die dortigen Sicherungsmechanismen auch bei Ausführung des Überwachungsprogramms ordnungsgemäß funktionieren werden. Beeinträchtigungen der Systemleistung sind auf das Unvermeidbare zu begrenzen.

2.4 Software-Aktualisierungen

Für die Übertragung der ggf. notwendigen Software-Aktualisierungen gelten die gleichen Schutzmechanismen wie für die Übertragung von Telekommunikationsdaten (Kapitel 1.4). Durch die zu treffenden Maßnahmen zur Authentisierung aller kommunizierenden Instanzen in Verbindung mit der Verschlüsselung der Datenübertragung wird gewährleistet, dass Software-Aktualisierungen ausschließlich über die Aufzeichnungs- und Steuereinheit der einsetzenden Stelle erfolgen können. Ein Missbrauch der Updatefunktion durch Dritte wird somit ausgeschlossen. Durch die Protokollierung (s. Kapitel 1.5) kann jederzeit nachvollzogen werden, wann und welche Software-Aktualisierungen eingespielt worden sind.

2.5 Schutz vor Offenlegung

Eine Rückverfolgbarkeit der laufenden Maßnahme zur einsetzenden Behörde durch Außenstehende wird so weit technisch möglich ausgeschlossen. Zusätzlich ist die Überwachungssoftware gegen Erkennung und Reverse Engineering zu schützen. Die dazu notwendigen Vorkehrungen sind insbesondere in der Überwachungssoftware und auf dem Übertragungsweg zu treffen.

2.6 Schutz unbeteiligter Dritter

Das Zielsystem ist so genau wie möglich zu identifizieren. Die Überwachungssoftware muss über Mechanismen verfügen, um festzustellen, ob sie auf dem Zielsystem ausgeführt wird. Dabei werden nur solche Metadaten ausgeleitet, die zwingend zur sicheren Feststellung des Zielsystems benötigt werden; sie unterliegen einer hierauf bezogenen strikten Zweckbindung. Dies impliziert auch die Nichtexistenz einer Verbreitungsroutine. Diese Nichtexistenz wird von der Quellcodeprüfung umfasst und zusätzlich durch die Dokumentation und Archivierung des Programms und die Protokollierung des Einsatzes belegt.

Sollte die Software irrtümlich auf einem anderen als dem Zielsystem zum Einsatz kommen, muss sichergestellt werden, dass keine Ausleitung von Kommunikationsdaten erfolgt und die Software, soweit technisch möglich, automatisch gelöscht wird (s. Kapitel 2.7).

2.7 Löschung des Überwachungsprogramms vom Zielsystem

Spätestens mit Ablauf der Anordnungsfrist der Quellen-TKÜ-Maßnahme ist das Überwachungsprogramm unverzüglich zu löschen, und bewusst herbeigeführte Veränderungen an den System- und sonstigen Dateien sind, soweit technisch möglich, rückgängig zu machen. Dies erfolgt:

- aufgrund eines Befehls der Steuereinheit oder
- nach Eintritt definierter Ereignisse.

Der Vorgang ist so zu gestalten, dass eine Deinstallation spätestens nach Ablauf des Anordnungszeitraums, soweit technisch möglich, automatisch erfolgt; dies auch, wenn das Zielsystem zu diesem Zeitpunkt nicht durch die Aufzeichnungs- und Steuereinheit erreichbar ist. Hierzu hat das Überwachungsprogramm über entsprechende Funktionen zu verfügen. Sofern die technischen Voraussetzungen des Zielsystems dies zulassen, ist die Möglichkeit zur Wiederherstellung der Dateien des Überwachungsprogramms durch Überschreiben des Speicherbereichs auf dem Datenträger so weit als technisch möglich auszuschließen. Die BSI-Vorgaben der „Richtlinie für die Löschung und Vernichtung von Informationen (M 2.432)“ sind, soweit technisch umsetzbar, zu beachten.

3 Anforderungen an das Aufzeichnungs- und Steuersystem

3.1 Gewährleistung des Kernbereichsschutzes

Funktionen zum Schutz des Kernbereichs privater Lebensgestaltung beschränken sich im Rahmen einer TKÜ auf die Löschung der aufgezeichneten Daten nach Erkennung der Kernbereichsrelevanz[4]. Dies hat das BVerfG zuletzt in seiner Entscheidung „zur Verfassungsmäßigkeit von Vorschriften des Gesetzes zur Neuregelung der Telekommunikationsüberwachung vom 21. Dezember 2007“ vom 12. Oktober 2011 bestätigt.

Insofern kann die Löschung kernbereichsrelevanter Aufzeichnungen nur auf dem Aufzeichnungs- und Steuersystem erfolgen. Hier ist zu unterscheiden, ob für die Aufzeichnung die herkömmlichen TKÜ-Systeme bei den berechtigten Stellen eingesetzt werden, auf denen sich bereits anerkannte Methoden zur Kernbereichsbehandlung befinden, oder ob ein spezifisches Aufzeichnungs- und Steuersystem für die Quellen-TKÜ zum Einsatz kommt. Im letzteren Fall sind dort Methoden zur Kernbereichsbehandlung vorzusehen, die in Funktion und Qualität denen der herkömmlichen TKÜ-Systeme entsprechen.

Aus datenschutzrechtlicher und verfahrensrechtlicher Sicht sind die Vorgänge (Kennzeichnung als kernbereichsrelevant und Löschung) zu protokollieren (vgl. auch Punkt 1.5) und die Protokolldaten gesondert abzulegen.

3.2 Rechte- und Rollenkonzept

Das zur Aufzeichnung und Steuerung genutzte Programm sieht ein Rechte- und Rollenkonzept vor, mit welchem die Abgrenzung der Aufgabenbereiche sichergestellt werden kann.

Die Durchführung von Quellen-TKÜ-Maßnahmen umfasst verschiedene, fest umrissene Aufgabenbereiche (Rollen), die in der Regel von unterschiedlichen Personen bzw. Organisationseinheiten wahrgenommen werden. Das Rechte- und Rollenkonzept ist so zu gestalten, dass ein datenschutzrechtlich einwandfreier Zugriffsschutz und eine entsprechende Protokollierung ermöglicht werden.

Die konkrete Ausgestaltung des Rechte- und Rollenkonzepts obliegt der jeweils verantwortlichen Behörde auf Grundlage der jeweiligen organisatorischen Rahmenbedingungen.

[4] Automatisierte Verfahren zur Erkennung kernbereichsrelevanter Abschnitte bei der Datenerhebung entsprechen derzeit weder dem Stand der Technik noch dem der Wissenschaft.