Standardisierende Leistungsbeschreibung für Software zur Durchführung von Maßnahmen der Quellen-Telekommunikationsüberwachung und der Online-Durchsuchung (Stand 05. Oktober 2018)

1 Einführung

1.1 Zweck dieses Dokuments

Diese „Standardisierende Leistungsbeschreibung“ (SLB) konkretisiert die aus den rechtlichen Bestimmungen resultierenden Vorgaben und definiert Prozessabläufe für die Durchführung von Maßnahmen der Quellen-Telekommunikationsüberwachung (Q-TKÜ) bzw. der Onlinedurchsuchung (ODS). Sie dient den in Deutschland durchführenden Stellen von Q-TKÜ bzw. ODS sowie den Anbietern der entsprechenden Software als Richtlinie, um die Entwicklung, die Beschaffung und den Einsatz derartiger Software in Deutschland in einem einheitlichen Rahmen sicherzustellen.

1.2 Versionsstand/Historie, Aktualisierung

Um einen einheitlichen nationalen Qualitätsstandard bei der Entwicklung und dem Einsatz von Software zur Durchführung von Maßnahmen der Q-TKÜ für die Sicherheitsbehörden in Deutschland zu etablieren, wurde im Jahr 2012 gemeinsam durch Sicherheitsbehörden von Bund und Ländern die Standardisierende Leistungsbeschreibung erarbeitet. Die Arbeitskreise II und IV der Innenministerkonferenz haben in ihren jeweiligen Herbstsitzungen 2012 die SLB in der Version vom 02.10.2012 zur Kenntnis genommen und den Sicherheitsbehörden des Bundes und der Länder empfohlen, die SLB bei der Beschaffung oder Erstellung von Q-TKÜ-Software zugrunde zu legen.

Aufgrund der sich aus den kurzen Innovationszyklen moderner informationstechnischer Systeme und deren Software ergebenden fortlaufenden Änderungen von technischen Rahmenbedingungen sowie der mit Inkrafttreten des Gesetzes zur effektiveren und praxistauglicheren Ausgestaltung des Strafverfahrens am 24.08.2017 geänderten Gesetzeslage, war eine Modifizierung und technikoffenere Ausgestaltung der SLB erforderlich. Durch dieses Dokument wird die SLB vom 02.10.2012 fortgeschrieben und auf Maßnahmen der ODS erweitert. Auch zukünftig ist die SLB regelmäßig auf Aktualisierungsbedarf zu prüfen.

1.3 Rechtliche Rahmenbedingungen

Die Durchführung von Maßnahmen der Q-TKÜ und ODS richtet sich nach den entsprechenden Normen der Strafprozessordnung, den gefahrenabwehrrechtlichen Normen des Bundes und der Länder sowie den Befugnissen des Bundesamtes für Verfassungsschutz und der Landesämter für Verfassungsschutz. Darüber hinaus ist die Rechtsprechung des BVerfG zur Q-TKÜ und ODS (z. B. BVerfG, Urteil v. 27. Februar 2008, 1 BvR 370/07, 1 BvR 595/07 und BVerfG, Urteil v. 20. April 2016, 1 BvR 966/09, 1 BvR 1140/09) zu beachten.

2 Architektur

Systeme zur Durchführung von Q-TKÜ bzw. ODS-Maßnahmen bestehen in der Regel aus verschiedenen Komponenten, die als ein Gesamtsystem zusammenarbeiten:

- Ausleitungssoftware: Software, die auf dem Zielsystem aufgebracht wird, dort Daten erfasst und an die durchführende Stelle ausleitet.

- Steuer- und Aufzeichnungseinheit: Software-Einheit, die von der durchführenden Stelle genutzt wird, um die Ausleitungssoftware zu steuern, die vom Beschluss bzw. der Anordnung umfassten Daten der Aufzeichnung und Auswertung zugänglich zu machen und sämtliche Aktivitäten zu protokollieren. Die Steuer- und Aufzeichnungseinheit kann je nach Anbieter in weitere Sub-Systeme aufgeteilt werden.

- Netzwerkverbindung: Die Funktion dieser Systemkomponente ist das Weiterleiten der Kommunikation vom Zielsystem an die Steuer und Aufzeichnungseinheit und zurück. Die Daten zur Steuerung der Ausleitungssoftware, sowie die maßnahmenbezogene Datenausleitung werden unter Gewährleistung von Authentizität, Integrität und Vertraulichkeit dieser Daten übertragen. Die Rückverfolgbarkeit zur durchführenden Stelle muss soweit möglich verhindert werden.

- Sofern das Gesamtsystem auf externe Komponenten zugreift, müssen diese im Sicherheitskonzept berücksichtigt werden.

3 Schutzziele und Sicherheitsmaßnahmen zu deren Umsetzung

Während sich die Steuer- und Aufzeichnungseinheit und somit die Systeme zur Datenverwaltung und Auswertung der erhobenen Daten sowie der Protokolle in der Infrastruktur der durchführenden Stellen befinden, erfordert die Kontrolle der Ausleitungssoftware sowie der Netzwerkverbindung erhöhte Sicherheitsmaßnahmen, da diese sich auf dem zu überwachenden, von dem Betroffenen kontrollierten Zielsystem bzw. im Internet befinden. Im Weiteren wird daher ein Fokus auf die Beschreibung der Sicherheitsmaßnahmen für die Ausleitungssoftware, für die Netzwerkverbindung sowie für den Teil der Steuer- und Aufzeichnungseinheit gelegt, welcher mit dem Internet in Verbindung steht. Im Hinblick auf das Aufzeichnungs- und Auswertesystem im engeren Sinne sowie die Sicherung der internen IT-Infrastruktur der durchführenden Stellen gelten die dortigen, speziell dafür erarbeiteten Sicherheitskonzepte und Vorkehrungen.

Gemäß der Vorgaben des IT-Grundschutzes sind zur Feststellung der Schutzbedarfe für Maßnahmen der Q-TKÜ und ODS die drei wesentlichen Grundwerte der IT-Sicherheit (Verfügbarkeit, Vertraulichkeit, Integrität) im Rahmen von IT-Sicherheitskonzepten zu analysieren und die Risiken festzustellen und zu bewerten. Als Spezialfall der Integrität ist auch die Authentizität von Informationen in die Analysen und Bewertungen einzubeziehen. Im Einzelnen:

- Vertraulichkeit: Zur Wahrung der Vertraulichkeit auf dem Übertragungsweg ist sicherzustellen, dass alle Daten (d.h. z. B. auch Steuerungskommandos an das Zielsystem, Aktualisierung der Überwachungssoftware auf dem Zielsystem, die Daten vom Zielsystem), die innerhalb des Q-TKÜ- bzw. ODS-Systems zwischen Zielsystem und dem Aufzeichnungs- und Steuerungssystem der durchführenden Stelle übertragen werden, durch geeignete Verfahren gegen unbefugte Kenntnisnahme geschützt werden. Darüber hinaus ist die Ausleitungssoftware vor Erkennung und Offenlegung zu schützen.
- Integrität/Authentizität: Die erhobenen Daten sind durch geeignete Verfahren gegen Veränderungen zu sichern. Eine Manipulation von Daten muss erkennbar sein. Es ist sicherzustellen, dass die Datenübermittlung bzw. -kommunikation ausschließlich zwischen der Ausleitungssoftware auf dem Zielsystem und der Aufzeichnungs- und Steuerungseinheit der durchführenden Stelle erfolgt.
- Verfügbarkeit: Es sind geeignete Sicherheitsmaßnahmen zu treffen, um einen Verlust von ausgeleiteten Daten zu vermeiden und das Gesamtsystem gegen Ausfälle und Störungen zu schützen.

Zur Umsetzung o.g. Schutzziele sind die eingesetzten Programme und die zwischen ihnen übertragenen Daten nach dem Stand der Technik gegen unbefugte Kenntnisnahme, Zugriff oder Manipulation zu schützen. Es ist durch technische Sicherheitsmaßnahmen zu gewährleisten, dass die Ausleitungssoftware nicht durch unbefugte Dritte angesprochen oder zweckentfremdet genutzt werden kann und sich nicht auf andere als das definierte Zielsystem verbreitet.

Bei der Auswahl der einzusetzenden kryptografischen Verfahren ist der aktuelle Stand der Technik heranzuziehen.

Es sind geeignete Sicherheitsmaßnahmen zum Schutz vor dem Einspielen (Hinzufügen) zusätzlicher (gefälschter) Informationen, die die Funktion des Gesamtsystems beeinträchtigen oder die Integrität der erhobenen Informationen verletzen können, zu ergreifen.

4 Risikoanalyse/IT-Sicherheitskonzept

Für die IT-Verfahren der Q-TKÜ bzw. ODS sind behördenspezifische IT-Sicherheitskonzepte auf der Basis der IT-Grundschutzmethodik des BSI oder vergleichbarer in den Ländern angewandter Verfahren durch die durchführende Stelle zu erstellen und fortzuschreiben. Die Einhaltung der dort festgelegten Sicherheitsmaßnahmen ist durch den Anbieter und die durchführende Stelle jeweils für ihren Verantwortungsbereich zu gewährleisten. Für ein IT-Sicherheitskonzept, das sich aus mehreren Teilkonzepten zusammensetzt, ist sicherzustellen, dass die Teilkonzepte konsistent zusammenwirken und alle Schnittstellen abdecken.

Das IT-Sicherheitskonzept umfasst eine Risikoanalyse, in deren Rahmen die gefährdeten Objekte einzugrenzen und die relevanten Gefährdungen, die auf ein IT-Verfahren einwirken können, herauszuarbeiten und ggf. existierende Restrisiken zu identifizieren sind. Es sind hierbei die innerhalb der IT-Verfahren Q-TKÜ bzw. ODS gefährdeten Objekte (Systemkomponenten, z. B. Hardware, Applikation bzw. organisatorische / personelle Bereiche, z. B. Zugangsschutz, Administration) zu beschreiben und in einem Sicherheitskonzept zu bewerten. Das IT-Sicherheitskonzept hat angemessene, aktuelle und dem Stand der Technik entsprechende Sicherheitsmaßnahmen vorzusehen.

Die Ergebnisse der Risikoanalyse und der Schutzbedarfsfeststellungen sowie der sich daraus ergebenden Konsequenzen sowie deren Umsetzung sind im IT-Sicherheitskonzept zu dokumentieren.

5 Prozesse/Abläufe

Die Durchführung von Maßnahmen der Q-TKÜ bzw. ODS richtet sich grundsätzlich nach geltenden rechtlichen und organisatorischen Rahmenbedingungen sowie nach gemeinsam zwischen den Sicherheitsbehörden des Bundes und der Länder erarbeiteten Konzepten zu ablauforganisatorischen Prozessen und zur Qualitätssicherung. Hierdurch werden übergreifende Standards geschaffen, die die Durchführung von Maßnahmen der Q-TKÜ bzw. ODS optimieren sowie das Entdeckungsrisiko minimieren. Die standardisierte und rechtskonforme Nutzung der Software wird somit sichergestellt.

5.1 Beschluss-/Anordnungsumfang und Kernbereichsschutz

Durch geeignete technische und organisatorische Sicherheitsmaßnahmen ist zu gewährleisten, dass die mit der Überwachung betrauten Mitarbeiterinnen und Mitarbeiter der durchführenden Stellen ausschließlich von den vom jeweiligen Beschluss bzw. der Anordnung umfassten Inhalten Kenntnis erlangen. Dies ist entsprechend zu protokollieren bzw. zu dokumentieren.

Der Kernbereich privater Lebensgestaltung wird bei Maßnahmen der Q-TKÜ bzw. der ODS besonders geschützt. Die Prozesse orientieren sich an den jeweils einschlägigen gesetzlichen Vorgaben.

5.2 Rechte und Rollenkonzept

Das Rechte- und Rollenkonzept ist so zu gestalten, dass jeder Benutzer ausschließlich die für seine Rolle notwendigen Rechte erhält. Auf dieser Grundlage sind ein datenschutzrechtlich geeigneter Zugriffsschutz und eine entsprechende Protokollierung sowie insbesondere die Einhaltung der Vorgaben zum Kernbereichsschutz zu gewährleisten. Die konkrete Ausgestaltung des Rechte- und Rollenkonzepts obliegt der durchführenden Stelle auf Grundlage der jeweiligen organisatorischen und rechtlichen Rahmenbedingungen.

5.3 Veränderungen am Zielsystem

Die Sicherheit und Stabilität des Zielsystems darf durch das Einbringen, den Betrieb und die Löschung der eingesetzten Ausleitungssoftware nicht mehr als erforderlich beeinträchtigt werden. Die Beeinträchtigung darf außerdem hinsichtlich des Ziels der Q-TKÜ-/ODS-Maßnahme nicht unangemessen sein. Beispielsweise dürfen Sicherheitsmaßnahmen, die das Zielsystem vor Zugriffen von außen schützen, nicht länger und nicht mehr als nötig eingeschränkt werden. Die von der Ausleitungssoftware benötigte Schnittstelle zur Ausleitung der Daten und Steuerung wird durch geeignete Sicherheitsmaßnahmen gegen unbefugte Nutzung geschützt.

Vor der Einbringung der Ausleitungssoftware ist zu überprüfen und zu dokumentieren, dass lediglich eine auf das Unvermeidbare begrenzte Beeinträchtigung des Zielsystems zu erwarten ist.

Spätestens mit Ablauf der angeordneten Q-TKÜ- bzw. ODS-Maßnahme ist die Ausleitungssoftware unverzüglich zu löschen. Veränderungen an den System- und sonstigen Dateien auf dem Zielsystem sind, soweit technisch möglich, rückgängig zu machen. Dies hat auch zu erfolgen, wenn das Zielsystem zu diesem Zeitpunkt nicht durch die Steuer- und Aufzeichnungseinheit erreichbar ist. Hierzu hat die Ausleitungssoftware über entsprechende Funktionen zu verfügen.

5.4 Schutz unbeteiligter Dritter

Die Ausleitungssoftware darf ausschließlich auf dem von der Anordnung umfassten Zielsystem zum Einsatz kommen. Hierzu ist das Zielsystem so genau wie möglich zu identifizieren.

Sollte die Software auf einem anderen als dem Zielsystem gestartet werden, muss sichergestellt werden, dass – außer den im Rahmen einer eindeutigen Identifizierung des Zielsystems übertragenen Daten – keine Ausleitung von Daten erfolgt und die Ausleitungssoftware, soweit technisch möglich, umgehend gelöscht wird. Durch die Ausleitungssoftware verursachte Veränderungen an den System- und sonstigen Dateien auf dem System sind, soweit technisch möglich, rückgängig zu machen.

5.5 Programm-Aktualisierungen / Schutz vor Offenlegung

Für die Übertragung der Aktualisierungen der Ausleitungssoftware gelten die in Kapitel 3 genannten Vorgaben. Dadurch ist gewährleistet, dass Aktualisierungen der Ausleitungssoftware ausschließlich über die Aufzeichnungs- und Steuereinheit der durchführenden Stelle erfolgen und ein Missbrauch der Updatefunktion durch Dritte ausgeschlossen wird. Durch Protokollierung bzw. Dokumentation kann jederzeit nachvollzogen werden, wann und welche Aktualisierungen der Ausleitungssoftware durchgeführt worden sind.

Eine Entdeckung und Rückverfolgung der laufenden Q-TKÜ- bzw. ODS-Maßnahme zur durchführenden Stelle ist durch geeignete Sicherheitsmaßnahmen soweit technisch möglich auszuschließen. Insbesondere ist die Software gegen Erkennung und Reverse Engineering zu schützen.

Wenn Sicherheitsmängel im Gesamtsystem erkannt werden (beispielsweise in der Ausleitungssoftware oder in der Aufzeichnungs- und Steuereinheit), ist der Anbieter verpflichtet, diese Mängel unverzüglich zu beheben und entsprechende Updates be-

reitzustellen. Die durchführenden Stellen spielen diese Updates gemäß den Vorgaben des IT-Sicherheitskonzepts unverzüglich ein.

5.6 Nachvollziehbarkeit durch Protokollierung, Archivierung und Dokumentation

Bei der Q-TKÜ bzw. der ODS handelt es sich um verdeckte Maßnahmen. Der Nachweis der Integrität und Authentizität der Daten ist dabei von besonderer Bedeutung. Insbesondere die Verwendung der Daten zur Strafverfolgung und Gefahrenabwehr setzt einen lückenlosen Nachweis von der Erhebung über die Bewertung und Weiterverarbeitung der Daten innerhalb der durchführenden Stelle voraus. Die Prozesse zur Erkenntniserlangung müssen auch in einem späteren Stadium des Verfahrens zweifelsfrei nachvollzogen werden können. Die notwendige Protokollierung ergibt sich insbesondere aus den in Kapitel 1.3 genannten Normen.

Protokollierung und Dokumentation dienen der Kontrolle der Rechtmäßigkeit der Q-TKÜ-/ODS-Maßnahme und 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 Q-TKÜ bzw. ODS aufgezeichneten Daten. Insbesondere dient die Protokollierung dem Nachweis, dass die Daten tatsächlich vom Zielsystem stammen, vollständig sind und nicht verändert wurden. Um eine Nachvollziehbarkeit zu gewährleisten, soll außerdem eine Archivierung der eingesetzten Software umgesetzt werden.

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

6 Anbieter

Anbieter von Software für Q-TKÜ bzw. ODS sind sorgfältig im Hinblick auf ihre Fachkompetenz und Vertrauenswürdigkeit auszuwählen. Für die Anbieter ist im Inland die Geheimschutzbetreuung durch das BMWi bzw. bei ausländischen Firmen ein geeignetes Verfahren anzustreben.

Die Anbieter von Software für Q-TKÜ bzw. ODS sichern vertraglich die Einhaltung der Anforderungen und Rahmenbedingungen zu, die sich aus den gesetzlichen Normierungen sowie aus dieser SLB ergeben.

Die Anbieter sichern darüber hinaus zu,

- den Stand der Technik bei der sicheren Software-Entwicklung einzuhalten,

- den physischen Zutritt sowie den logischen Zugang und Zugriff auf die Entwicklungsumgebung auf die hierzu jeweils berechtigten Personen einzuschränken,
- externe Komponenten (z.B. Software-Bibliotheken) aus geprüften Quellen zu beschaffen und vor ihrer Verwendung hinsichtlich ihrer Sicherheitseigenschaften zu überprüfen,
- die durchführenden Stellen unverzüglich über Sicherheitsvorfälle, erkannte Sicherheitsmängel oder andere Ereignisse zu informieren, die die sichere, rechtmäßige und ordnungsgemäße Durchführung von Q-TKÜ-/ODS-Maßnahmen gefährden.

Durch die durchführende Stelle selbst bzw. von einer durch diese bestimmten Stelle findet – z.B. im Rahmen des Beschaffungsprozesses – eine Überprüfung dieser Anforderungen und Rahmenbedingungen statt.

7 Prüfung und Abnahme

Die Abnahme der Software erfolgt auf Grundlage eines definierten Testverfahrens, dessen Ergebnisse im Rahmen des Gesamtabnahmeprozesses dokumentiert werden.

Vor jedem zielsystemspezifischen Einsatz der Software werden zur Einhaltung der rechtlichen Anforderungen auf die konkreten Einsatzbedingungen angepasste Prüfungen durch die durchführende Stelle durchgeführt, z. B. Rechtmäßigkeit des Funktionsumfangs. Die Ergebnisse werden dokumentiert.