Bundesnetzagentur

Bundesnetzagentur
für Elektrizität, Gas, Telekommunikation,
Post und Eisenbahnen

Anforderungskatalog
nach § 113f TKG

Katalog von technischen Vorkehrungen und sonstigen Maßnahmen zur Umsetzung des Gesetzes zur Einführung einer Speicherpflicht und einer Höchstspeicherfrist für Verkehrsdaten vom 10.12.2015 (BGBl. I S. 2218)

Version: 1.0
Stand: 23.11.2016

Bearbeiter und Herausgeber:

Bundesnetzagentur für Elektrizität, Gas, Telekommunikation, Post und Eisenbahnen
Postfach 80 01
55003 Mainz

Änderungshistorie

Version	Datum	Anlass	Autor
1.0	23.11.2016	Erste Veröffentlichung des Anforderungskatalogs gemäß § 113f TKG	Bundesnetzagentur, Referat IS16

Inhaltsverzeichnis

1. Begriffsbestimmungen

Abfragesystem	IT-System, welches typischerweise aus Abfrageclient und Abfrageserver besteht, von dem aus die Abfragen im Vier-Augen-Prinzip initiiert werden und welches die Abfrageergebnisse entgegennimmt und nach § 113c TKG verwendet
Ablagesystem	Komponenten (Hardware/Software) zur Verschlüsselung der speicherpflichtigen Verkehrsdaten und zur Ablage im Datenspeicher
Datenspeicher	Speichereinrichtung, in der die speicherpflichtigen Verkehrsdaten vorgehalten werden
Schlüsselmanagement	Komponenten (Hardware/Software) zur Erzeugung, Verteilung, Speicherung und Löschung der kryptographischen Schlüssel der Verschlüsselungsverfahren
Verkehrsdaten	Daten, die bei der Erbringung eines Telekommunikations-dienstes erhoben, verarbeitet oder genutzt werden (§ 3 Nr. 30 TKG). Im Rahmen des Anforderungskatalogs wird – abhängig von der Verwendung – zwischen zwei Kategorien von Verkehrsdaten unterschieden: 1. Verkehrsdaten, die nach §§ 96 ff. TKG gespeichert werden (betrieblich gespeicherte Verkehrsdaten), 2. Verkehrsdaten, die gem. § 113b TKG zu speichern sind (speicherpflichtige Verkehrsdaten).
Verkehrsdatenspeichersystem	Gesamtheit aller Einzelkomponenten (Datenspeicher, Ablagesystem, Zugriffssystem, Schlüsselmanagement), die für die sichere Ablage und den sicheren Zugriff auf die speicherpflichtigen Verkehrsdaten notwendig sind, zuzüglich der technischen Komponenten, die für die Absicherung und Abschottung der Systeme nach außen verantwortlich sind.
Zugriffssystem	Komponenten (Hardware/Software), die die Abfrage von speicherpflichtigen Verkehrsdaten im Datenspeicher realisieren und die Abfrageergebnisse ausleiten und hierbei die Entschlüsselung durchführen.

2. Abkürzungen

CD	Compact Disc
ETSI-ESB	Schnittstelle zur technischen Umsetzung gesetzlicher Maßnahmen zur Erteilung von Auskünften nach Teil B der TR TKÜV
HSM	Hardware Security Module
RAM	Random Access Memory
SINA	Sichere Inter-Netzwerk Architektur
SSD	Solid-State-Drive
TKG	Telekommunikationsgesetz
TKÜV	Verordnung über die technische und organisatorische Umsetzung von Maßnahmen zur Überwachung der Telekommunikation (Telekommunikations-Überwachungsverordnung)
TR TKÜV	Technische Richtlinie zur Umsetzung gesetzlicher Maßnahmen zur Überwachung der Telekommunikation, Erteilung von Auskünften
VPN	Virtual Private Network

.

3. Präambel

Dieser Katalog bestimmt Anforderungen an die technischen Vorkehrungen und sonstigen Maßnahmen zur Gewährleistung eines besonders hohen Standards der Datensicherheit und Datenqualität bei der Umsetzung der Verpflichtungen gemäß den §§ 113b bis 113e TKG.

Die Anforderungen lassen die Verpflichtungen für angemessene technische Schutzmaßnahmen nach § 109 TKG oder für den IT-Grundschutz unberührt. Es ist sicherzustellen, dass die Speicherung von speicherpflichtigen Verkehrsdaten insgesamt in einer technisch und physisch sicheren Umgebung durch Realisierung eines Basisschutzes erfolgt. Das darüber hinausgehende, in diesem Anforderungskatalog beschriebene Schutz- und Sicherheitsniveau zur Gewährleistung eines besonders hohen Standards der Datensicherheit und Datenqualität gemäß § 113f TKG ist zusätzlich einzuhalten und zu dokumentieren. Insofern wird auf die in der Anlage beschriebene Vorgehensweise zur Erstellung des Sicherheitskonzeptes nach § 113g TKG verwiesen.

Werden die Anforderungen an die Datensicherheit und Datenqualität sowie die technischen Vorkehrungen und sonstigen Maßnahmen dieses Katalogs erfüllt, wird die Einhaltung des nach § 113f Absatz 1 Satz 1 TKG geforderten besonders hohen Standards der Datensicherheit und Datenqualität vermutet.

Soweit die Verpflichteten gemäß § 113a TKG alternative technische Vorkehrungen und sonstige Maßnahmen zur Gewährleistung eines besonders hohen Standards der Datensicherheit und Datenqualität treffen, müssen diese dem gleichen Schutz- und Sicherheitsniveau wie die Vorgaben des Anforderungskatalogs entsprechen. Die Abweichungen müssen im Sicherheitskonzept beschrieben und die Einhaltung des gleichen Schutz- und Sicherheitsniveaus begründet werden.

Der vorliegende Katalog ist gemäß § 113f Absatz 1 Satz 2 TKG von der Bundesnetzagentur im Benehmen mit dem Bundesamt für Sicherheit in der Informationstechnik und der Bundesbeauftragten für den Datenschutz und die Informationsfreiheit erstellt worden. Den Herstellern, den Verbänden der Betreiber öffentlicher Telekommunikationsnetze und den Verbänden der Anbieter öffentlich zugänglicher Telekommunikationsdienste ist gemäß § 113f Absatz 3 Satz 1 i.V. mit § 109 Absatz 6 Satz 2 TKG Gelegenheit zur Stellungnahme gegeben worden.

Die technischen Vorkehrungen und sonstigen Maßnahmen hinsichtlich der Übermittlung der Daten an die in § 113c Absatz 1 TKG genannten berechtigten Stellen richten sich gemäß § 113c Absatz 3 TKG nach der TKÜV und der TR TKÜV.

4. Allgemeine Anforderungen an die Datensicherheit und Datenqualität

4.1 Gewährleistung eines besonders hohen Standards der Datensicherheit

Es ist ein besonders hoher Sicherheitsstandard zu gewährleisten, der die Unversehrtheit, Vertraulichkeit und Verfügbarkeit der speicherpflichtigen Verkehrsdaten mittels Sicherheitsvorkehrungen in den jeweiligen technischen Systemen, Komponenten oder Prozessen oder bei deren Anwendung sicherstellt. Diese Verkehrsdaten müssen nach dem Stand der Technik vor Beeinträchtigungen oder Missbrauch, das heißt insbesondere vor unbefugter Kenntnisnahme und Verwendung, bewahrt werden. Hierzu zählt auch der Schutz vor Verlust der Verkehrsdaten, etwa mittels Backup-Systemen.

Im Folgenden ist die Grundarchitektur des Gesamtsystems dargestellt:

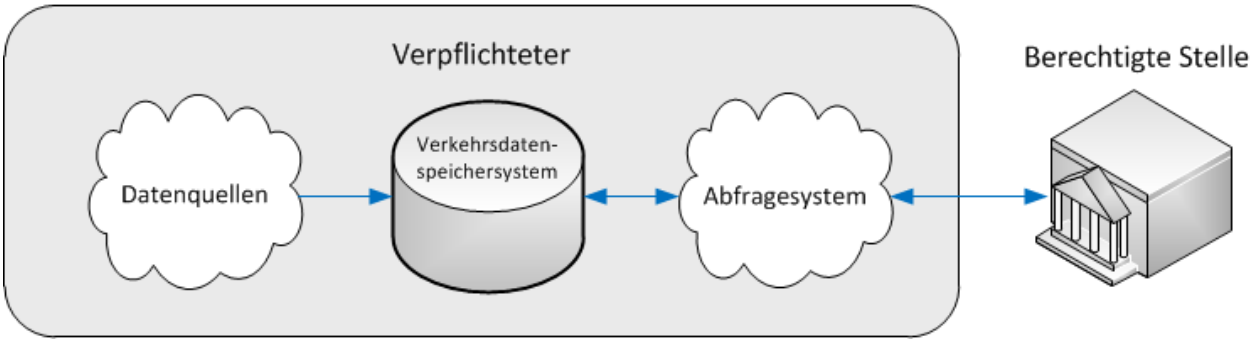

Abbildung 1: Vereinfachte Darstellung der Grundarchitektur

Die in den Einzelkomponenten des Telekommunikationsnetzes anfallenden Daten aus unterschiedlichen Datenquellen (beispielsweise Abrechnungs-, Log- oder Signalisierungsdaten) werden regelmäßig zunächst einer Kontroll- und Filtereinrichtung zugeführt. Diesbezügliche Anforderungen in diesem Anforderungskatalog beziehen sich ausschließlich auf die Datenqualität und die Transportsicherung.

Nach dieser Kontroll- und Filtereinrichtung stehen dem Unternehmen die nach § 113b TKG [TKG] speicherpflichtigen Verkehrsdaten unter Berücksichtigung der Anforderung nach § 113b Abs. 6 TKG zur Verfügung. Diese werden im Verkehrsdatenspeichersystem gespeichert und stehen dort für Beauskunftungen gegenüber den berechtigten Stellen (§ 113c Absatz 1 Nummer 1 und 2 TKG) zur Verfügung. Die zur Beauskunftung nötigen Abfragesysteme werden von diesem Anforderungskatalog sowie der TKÜV [TKÜV] und der TR TKÜV [TR TKÜV] gleichermaßen erfasst.

Grundsätzlich ist die Auslagerung des gesamten Verkehrsdatenspeichersystems inkl. Abfragesystem oder von Einzelkomponenten an einen sog. Erfüllungsgehilfen im Inland einschließlich der damit zusammenhängenden Aufgaben möglich. Die Verantwortung für die

Umsetzung des Anforderungskatalogs und für die Einreichung des Sicherheitskonzeptes verbleibt jedoch bei dem Verpflichteten.

Beim Transport von speicherpflichtigen Verkehrsdaten zwischen den einzelnen Komponenten des Verkehrsdatenspeichersystems sowie bei Zuleitung zum Verkehrsdatenspeichersystem (Einlieferung der speicherpflichtigen Verkehrsdaten) und Ausleitung aus dem Verkehrsdaten-speichersystem (Export der Abfrageergebnisse) muss eine Transportsicherung die Vertraulichkeit, Integrität und Authentizität der Verkehrsdaten gewährleisten.

Erfolgt der Datentransport über ungesicherte Netze (z.B. das Internet), muss eine geeignete Transportverschlüsselung mit Authentizitäts-/Integritätsschutz (z.B. TLS, IPSec oder SSH, siehe BSI-TR-02102-2/3/4 [BSI4]) eingesetzt werden. Zur Initialisierung der sicheren Kommunikationsverbindung muss dabei eine gegenseitige Authentisierung der Kommunikationsendpunkte erfolgen. Falls die Verkehrsdaten ausschließlich über dedizierte, gesicherte Verbindungen, z.B. eigene physische Leitungen zwischen den Komponenten des Verkehrsdatenspeichersystems im physisch besonders gesicherten Bereich (siehe Abschnitt 5.2.6.2) übertragen werden, ist dadurch bereits eine ausreichende Transportsicherung gegeben.

Die technischen Vorkehrungen und sonstigen Maßnahmen für die Umsetzung nach §§ 113b bis e TKG sind ab Kapitel 5 beschrieben.

4.2 Gewährleistung eines besonders hohen Standards der Datenqualität

Zur Gewährleistung eines besonders hohen Standards der Qualität der speicherpflichtigen Verkehrsdaten werden verlangt:

1. Maßnahmen zur Sicherstellung der Genauigkeit zu speichernder Zeitangaben,

2. Maßnahmen zur Sicherstellung der Richtigkeit und Vollständigkeit bei der Zuführung der speicherpflichtigen Verkehrsdaten in das Verkehrsdatenspeichersystem, z.B. automatisierte Fehlererkennungsverfahren und Plausibilitätsprüfungen,

3. Maßnahmen bei festgestellten Fehlern.

Die Datenqualität kann zudem durch regelmäßige Tests durch die Bundesnetzagentur überprüft werden, indem über hierfür vorgehaltene Testanschlüsse Verkehrsdaten erzeugt werden. Die näheren Vorgaben enthält die TKÜV.

4.2.1 Maßnahmen zur Sicherstellung der Genauigkeit zu speichernder Zeitangaben

Um die Genauigkeit der zu speichernden Zeitangaben zu gewährleisten, ist die jeweilige Uhrzeit von Zeitservern zu beziehen, die auf der amtlichen Zeit basieren. Damit gilt der Zeitstempel als ausreichend, um die gesetzlichen Anforderungen zu erfüllen.

Die Genauigkeit der erfassten Zeitangabe ist insbesondere relevant:

- für die zu speichernde Zeitangabe von Beginn und Ende der Verbindung (§ 113b Absatz 2 Satz 1 Nummer 2 TKG),
- für die erste Aktivierung des mobilen Telefondienstes (§ 113b Absatz 2 Satz 1 Nummer 4 lit. c) TKG),
- für die Versendung und den Empfang der Nachricht (§ 113b Absatz 2 Satz 2 Nummer 1 TKG),
- für den Beginn und das Ende der Internetnutzung (§ 113b Absatz 3 Nummer 3 TKG) sowie
- bei der Protokollierung für den Zeitpunkt des Zugriffs (§ 113e Absatz 1 Satz 2 Nummer 1 TKG).

4.2.2 Maßnahmen zur Sicherstellung der Richtigkeit und Vollständigkeit bei der Zuführung der speicherpflichtigen Verkehrsdaten in das Verkehrsdatenspeichersystem

Vor der Einspeicherung in den Datenspeicher müssen die speicherpflichtigen Verkehrsdaten gegen die erwarteten Formate geprüft werden, um bei Abweichungen Korrekturen vorzunehmen und um ggf. die berechtigten Stellen nach Maßgabe des Abschnittes 4.2.3 zu informieren.

Zur Fehlererkennung sollen prinzipielle Erkenntnisse aus bereits bestehenden Fehlererkennungsverfahren für betrieblich gespeicherte Verkehrsdaten genutzt werden. Dies gilt beispielsweise für eine regelmäßige Kontrolle und Verifikation der betrieblich gespeicherten Verkehrsdaten nach § 45g Absatz 1 Nummer 4 TKG. Danach haben die Verpflichteten ihre Abrechnungssysteme in gewissen Zeitabständen auf Genauigkeit und Übereinstimmung mit den vertraglich vereinbarten Entgelten zu überprüfen und nach § 45g Absatz 2 Satz 1 TKG durch Sachverständige oder vergleichbare Stellen prüfen zu lassen, um sicherzustellen, dass die Zuordnung der erfassten Zeit mit den vereinbarten Tarifen übereinstimmt.

Ebenso sollen bei dem Verpflichteten bestehende Rechnungsprüfungsverfahren oder Missbrauchserkennungssysteme eingesetzt werden. Angelehnt an solche, üblicherweise im Billing-Prozess eingesetzten Verfahren, können dadurch Unregelmäßigkeiten, z.B. nicht ausgelöste Gespräche oder gleichzeitige Telefonate von unterschiedlichen Orten, erkannt werden. Daneben können Fehler auch im betrieblichen Ablauf auffallen, etwa im Rahmen der Fehlererkennung bei Einsatz der betrieblichen Fraud- oder ähnlicher Systeme oder bei entsprechenden Hinweisen durch die Interconnection-Partner.

4.2.3 Maßnahmen bei festgestellten Fehlern

Werden Fehler erkannt, die die ordnungsgemäße Bereitstellung der speicherpflichtigen Verkehrsdaten beeinträchtigen, z.B. Betriebsausfälle oder fehlerhaft gespeicherte Verkehrsdaten (etwa aufgrund einer falschen Zeitbasis in einem Netzelement), muss der Verpflichtete die berechtigten Stellen, die für den betroffenen Zeitraum entsprechende speicherpflichtige Verkehrsdaten abfragen oder abgefragt haben, unverzüglich informieren.

Sofern die Information personenbezogene Daten enthält, muss sichergestellt werden, dass diese keine Rückschlüsse auf konkrete Kommunikationsvorgänge ermöglichen können. Insbesondere dürfen keine kompletten Verkehrsdatensätze (z.B. Verkehrsdaten zu einer konkreten Telefonverbindung oder einer zugewiesenen IP-Adresse) übermittelt werden. Die Information muss sich vielmehr in der Auskunft erschöpfen, dass zu einem personenbezogenen Datum (z.B. einer Telefonnummer) ein Fehler festgestellt wurde, ohne diesen konkret zu benennen. Die berechtigten Stellen können dann kontrollieren, ob es sich um ein Datum handelt, das Gegenstand eines von ihnen gestellten Auskunftsersuchens war. Sollte dies der Fall sein, können die Verpflichteten kontaktiert werden, um weitere Details zu dem festgestellten Fehler zu erfragen. Auf diesem Weg wird sichergestellt, dass berechtigte Stellen nur im Einzelfall und im Rahmen des erwirkten Gerichtsbeschlusses eine entsprechende Auskunft erhalten.

5. Technische Vorkehrungen und sonstige Maßnahmen für die Umsetzung der Verpflichtungen nach §§ 113b bis e TKG

5.1 Speicherung von Verkehrsdaten nach § 113b TKG

5.1.1 Allgemeine Anforderungen

Die Speicherung der speicherpflichtigen Verkehrsdaten nach § 113b TKG (im Folgenden nur noch als Verkehrsdaten bezeichnet) hat im Inland zu erfolgen. Dies erfordert eine Speicherung der Verkehrsdaten auf Speichereinrichtungen, die physisch innerhalb der Staatsgrenzen der Bundesrepublik Deutschland gelegen sind.

Die Verkehrsdaten nach § 113b TKG dürfen nur verschlüsselt auf persistenten Speichermedien gespeichert werden. Es müssen Verkehrsdaten ankommender und abgehender Verbindungen gespeichert werden. Diese Verkehrsdaten sollen direkt aus den Abrechnungs-, Log-, Signalisierungsdaten oder sonstigen Daten der Telekommunikationsanlagen abgeleitet werden. Dadurch wird sichergestellt, dass nur dann Daten erzeugt werden, wenn auch tatsächliche Verbindungen aufgebaut wurden oder es zu Verbindungsversuchen kam.

Es ist sicherzustellen, dass Verkehrsdaten, die in eigenen Telekommunikationsnetzen bzw. -anlagen erhoben werden, den tatsächlichen Telekommunikationsvorgängen entsprechen und vollständig gespeichert werden. Dies wird regelmäßig so realisiert, dass die Verkehrsdaten der Signalisierung entnommen werden. Bei Verkehrsdaten, die aus der Signalisierung oder Abrechnung von Interconnection-Partnern stammen, ist deren Richtigkeit und Vollständigkeit durch regelmäßige Prüfungen sicherzustellen.

Es sind die Integrität der Verkehrsdaten und der zur Speicherung von Verkehrsdaten betriebenen Systeme sowie die Vollständigkeit und Korrektheit der Verkehrsdaten zu gewährleisten.

Die zur Speicherung von Verkehrsdaten betriebenen Systeme müssen über eine nach dem Stand der Technik ausreichende Leistungsfähigkeit und Verfügbarkeit verfügen, um alle anfallenden Verkehrsdaten und eingehenden Abfragen verarbeiten zu können.

Für die hierzu erforderlichen Backup-Daten oder die ggf. eingesetzten Redundanzsysteme gelten dieselben Anforderungen.

5.1.2 Ausschluss der Verkehrsdatenspeicherung nach § 113b Absatz 6 i.V.m. § 99 Absatz 2 TKG

Personen, Behörden und Organisationen in sozialen oder kirchlichen Bereichen i.S.v. § 113b Absatz 6 i.V.m. § 99 Absatz 2 Satz 1 und 3 TKG teilen der Bundesnetzagentur die nach § 99

Absatz 2 TKG von der Speicherung auszunehmenden Rufnummern mit und übermitteln ihr die Bescheinigung nach § 99 Absatz 2 Satz 4 TKG. Die Bundesnetzagentur nimmt die ihr mitgeteilten Rufnummern in eine Liste auf und hält diese zum Download für die Verpflichteten bereit. Zur sicheren Gestaltung des Abrufverfahrens sind der Zugriff mittels Nutzername und Passwort sowie eine Transportverschlüsselung gemäß BSI TR 02102-2 vorgesehen. Zur Umsetzung der Verpflichtung nach § 113b Absatz 6 i.V.m. § 99 Absatz 2 TKG ist der Abruf dieser Liste zwingend vorgegeben. Zur Teilnahme am Verfahren haben sich die Verpflichteten an folgende Kontaktadresse zu wenden:

Bundesnetzagentur

Referat IS 17

Postfach 10 04 43

66004 Saarbrücken

Telefax 0681/9330 734

E-Mail: IS17.Postfach@Bundesnetzagentur.de

5.1.3 Gewährleistung der unverzüglichen Beantwortung von Auskunftsersuchen der berechtigten Stellen nach § 113b Absatz 7 TKG

Nach § 113b Absatz 7 TKG hat die Speicherung der Verkehrsdaten so zu erfolgen, dass Auskunftsersuchen der berechtigten Stellen unverzüglich beantwortet werden können. Zur Umsetzung dieser Vorgabe müssen die Verkehrsdaten in den Speichereinrichtungen zentral vorgehalten werden oder zentral abrufbar sein. Zudem müssen die Systeme für die Zuführung der Verkehrsdaten aus den Netzelementen des eigenen Telekommunikationsnetzes so ausgestaltet sein, dass die erhobenen Verkehrsdaten binnen 24 Stunden nach dem jeweiligen Ereignis dem Verkehrsdatenspeichersystem zugeführt werden. In begründeten Einzelfällen kann nach Absprache mit der Bundesnetzagentur von dieser Frist abgewichen werden.

5.1.4 Löschung der Verkehrsdaten gemäß § 113b Absatz 8 TKG

Die Speicherung der Verkehrsdaten hat so zu erfolgen, dass eine vollständige und fristgerechte Löschung der gespeicherten Verkehrsdaten gewährleistet ist. Die diesbezüglichen technischen Anforderungen sind in Abschnitt 5.2.5 geregelt.

5.1.5 Verwendung der Verkehrsdaten gemäß § 113c Absatz 3 TKG

Solange in der TKÜV keine Regelungen für die Übermittlung von speicherpflichtigen Verkehrsdaten enthalten sind, ist zur Gewährleistung der Datensicherheit und des Datenschutzes bei der Übermittlung die in der TR TKÜV vorgesehene Schnittstelle oder ein ansonsten mit der Bundesnetzagentur abzustimmendes Verfahren einzusetzen. Die

Bundesnetzagentur stimmt sich in diesen Fällen mit der Bundesbeauftragten für den Datenschutz und die Informationsfreiheit ab.

Darüber hinaus muss sichergestellt werden, dass Verkehrsdaten, die im Zusammenhang mit einem Auskunftsersuchen verarbeitet werden, nach der Übermittlung oder der Verwendung nach § 113c Absatz 1 TKG unverzüglich nach dem Stand der Technik irreversibel gelöscht werden (siehe Abschnitt 5.2.5).

5.2 Gewährleistung der Sicherheit der Verkehrsdaten gemäß § 113d TKG

Um einen besonders hohen Standard der Datensicherheit im Verkehrsdatenspeichersystem gewährleisten zu können (siehe § 113f Absatz 1 TKG), muss nicht nur das gesamte Verkehrsdatenspeichersystem, sondern müssen alle Komponenten des Systems die Anforderungen nach IT-Grundschutz des BSI mit dem Schutzbedarf „hoch“ (siehe IT-Grundschutz-Vorgehensweise, BSI-Standard 100-2 [BSI1]) erfüllen. Bezüglich der kryptographischen Absicherung des Systems müssen die Empfehlungen aus den Technischen Richtlinien „Kryptographische Verfahren: Empfehlungen und Schlüssellängen“ des BSI (siehe BSI-TR-02102 [BSI4]) berücksichtigt werden.

Ein sicheres Verkehrsdatenspeichersystem lässt sich nur durch die Kombination aus einer sicheren Ablage der Verkehrsdaten, einer physischen und organisatorischen Absicherung der Systemkomponenten, einer wirksamen Kontrolle der Kommunikation nach außen und einer Absicherung des Datenflusses zwischen den Systemkomponenten realisieren. Die Gesamtsicherheit des Systems kann dabei nur so hoch sein wie das Schutzniveau der schwächsten aller eingesetzten Sicherheitsmaßnahmen.

5.2.1 Grundsätzliche Architektur der Anlagen

Bevor die einzelnen technischen Anforderungen erläutert werden, soll zunächst anhand des nachfolgenden Umsetzungsbeispiels die grundsätzliche Architektur mit ihren grundlegenden Funktionen und Prozessen dargestellt werden.

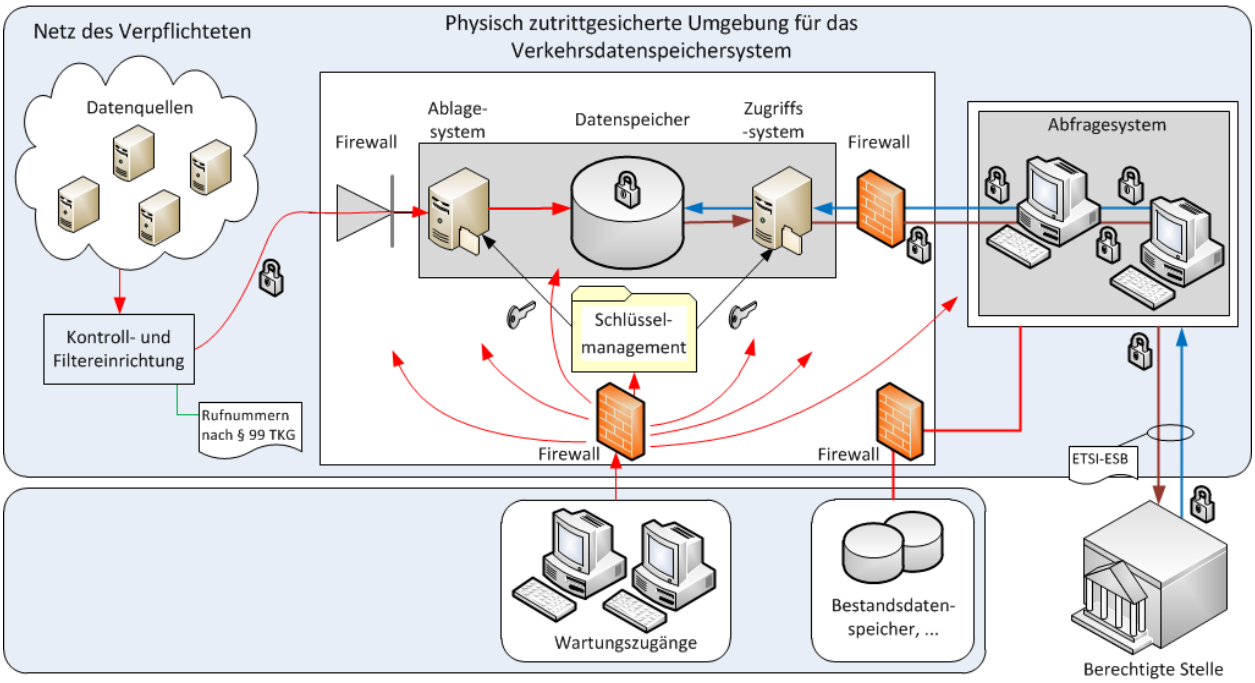

Abbildung 2: Umsetzungsbeispiel der Grundarchitektur

Im illustrierten Beispiel extrahiert der Verpflichtete die nach Gesetz zu speichernden Verkehrsdaten aus der Gesamtheit der durch die Netzelemente bereitgestellten Daten und speichert diese automatisch in der zentralen Speicherinfrastruktur.

Die zentrale Speicherinfrastruktur (Ablagesystem, Datenspeicher und Zugriffssystem) muss gegen unberechtigten Zugriff nach Stand der Technik abgesichert sein. Dazu wird u.a. eine Firewall-Infrastruktur eingesetzt, die den unberechtigten Zugriff wirkungsvoll unterbindet, jedoch für die zu speichernden Verkehrsdaten sowie für die Abfragen, die auf den Auskunftsersuchen der berechtigten Stellen beruhen, durchlässig ist. Das hier genutzte Ablagesystem als Teil der Verkehrsdatenspeichersystems übernimmt die Funktion der Verschlüsselung und das hier dargestellte Zugriffssystem ebenfalls als Teil des Verkehrsdatenspeichersystems erbringt die Funktion der Entschlüsselung; beide Systeme verfügen daher über einen Anschluss an das Schlüsselmanagement.

Die Kontroll- und Filtereinrichtung ist der Firewall-Infrastruktur vor- oder nachgelagert; im illustrierten Beispiel ist sie der Firewall vorgelagert.

Mittels Abfragen, die auf den Auskunftsersuchen der berechtigten Stellen beruhen, werden die entsprechenden Verkehrsdaten unter Verwendung des Abfrage- und Zugriffssystems im Datenspeicher gesucht und ausgelesen. Die Abfrageergebnisse müssen den berechtigten Stellen wiederum verschlüsselt über sichere Verbindungen übermittelt werden.

Das Umsetzungsbeispiel geht davon aus, dass sich alle Komponenten des Verkehrsdatenspeichersystems im Besitz ein und desselben Verpflichteten befinden. Im Falle

von Auslagerungen an sog. Erfüllungsgehilfen oder der Notwendigkeit des Transports von Daten außerhalb des physisch gesicherten Bereiches ergeben sich weitere umzusetzende Maßnahmen, z.B. eine Verschlüsselung auf dem Transportweg. Auch sammeln viele Unternehmen Daten zunächst in ihren Billing-Systemen, bevor sie in das Verkehrsdatenspeichersystem gelangen.

Im Umsetzungsbeispiel sind zudem die Möglichkeiten einer gemeinsamen Nutzung des Abfragesystems für andere Auskunftserteilungen nach Abschnitt 5.2.4 und eines Wartungszugangs nach Abschnitt 5.2.7.2 illustriert.

5.2.2 Besonders sicheres Verschlüsselungsverfahren gemäß § 113d Satz 2 Nummer 1 TKG

Die Speicherung der Verkehrsdaten muss nach § 113d TKG so realisiert werden, dass der Schutz gegen unbefugte Kenntnisnahme und Verwendung der Verkehrsdaten sichergestellt ist. Dazu dürfen die Verkehrsdaten in persistenten Speichermedien nur in verschlüsselter Form vorliegen.

Als besonders sicher werden nur solche Verschlüsselungsverfahren anerkannt, deren Überwindung für Unberechtigte einen unverhältnismäßig großen Aufwand erfordern würde.

Die Verkehrsdaten müssen vor Eingang in den Datenspeicher mit einem geeigneten Verschlüsselungsverfahren (siehe BSI-TR-02102-1 [BSI4]) verschlüsselt werden. Dabei ist darauf zu achten, dass eine effiziente Speicherung, Suche und Abfrage der Verkehrsdaten möglich bleiben, um Auskunftsersuchen der berechtigten Stellen unverzüglich beantworten zu können. Dies kann z.B. durch eine transparente Datenbankverschlüsselung oder eine Container-Verschlüsselung auf Basis von AES umgesetzt werden.

Auch Sicherungskopien der Verkehrsdaten im Rahmen von Backup-Maßnahmen müssen sicher gespeichert, d.h. insbesondere verschlüsselt abgelegt, werden.

Eine Entschlüsselung von Verkehrsdaten ist ausschließlich zum Zwecke der Bearbeitung von Auskunftsersuchen der berechtigten Stellen zulässig (vgl. § 113c TKG) und sollte deshalb im Zugriffssystem lokalisiert sein, vorzugsweise in einer eigenen Komponente. Danach können die Abfrageergebnisse im Zugriffssystem entweder unverschlüsselt im flüchtigen Speicher (RAM) oder verschlüsselt im persistenten Speicher zwischengespeichert werden. Zur Übermittlung der Abfrageergebnisse können diese im RAM oder verschlüsselt in einem persistenten Speicher des Abfragesystems zwischengepuffert werden.

Das Schlüsselmanagement sollte getrennt vom eigentlichen Datenspeicher gehalten und administriert werden. Die benötigten Schlüssel müssen durch das Schlüsselmanagement erzeugt, gespeichert, gelöscht und an die Ver- bzw. Entschlüsselungseinheit verteilt werden. Ein Zugang zum Schlüsselmanagement darf nur nach persönlicher Freischaltung durch gemäß ihrer Rolle dazu berechtigte Mitarbeiter möglich sein, die dazu unter Berücksichtigung von § 113d Satz 2 Nummer 4 TKG durch den Verpflichteten besonders ermächtigt sind (siehe Abschnitt 5.2.6.1).

Ein wesentlicher Bestandteil der technischen Realisierung der gemäß § 113b TKG geforderten irreversiblen Löschung von Verkehrsdaten ist die Löschung der Schlüssel, die im gewählten

Verschlüsselungsverfahren für die sichere Ablage der Verkehrsdaten verwendet werden (siehe Abschnitt 5.2.5). Um die gesetzlich geforderten Löschfristen für Verkehrsdaten einhalten zu können, müssen deshalb auch die Schlüssel fristgerecht gelöscht werden können. Dazu müssen Schlüssel mit ausreichender Granularität erzeugt und verwendet werden. Es bietet sich hierbei z.B. der Einsatz von Tagesschlüsseln an, wobei auch eine nicht-deterministische Ableitung von Tagesschlüsseln aus einem Masterschlüssel möglich ist, ebenso wie die Ableitung von weiteren Unterschlüsseln aus den Tagesschlüsseln. Für die Wahl ausreichender Schlüssellängen und einer geeigneten Schlüsselableitung müssen die Empfehlungen aus BSI-TR-02102-1 [BSI4] beachtet werden.

Zur Speicherung der Schlüssel ist ein Speichermedium zu wählen, das eine zuverlässige Löschung der Schlüssel (siehe Abschnitt 5.2.5) ermöglicht. Dafür geeignet ist z.B. ein hardwarebasierter Schlüsselspeicher wie ein HSM, der gleichzeitig auch als Ver-/Entschlüsselungseinheit eingesetzt werden kann. Eine andere Möglichkeit besteht darin, alle aktuellen Schlüssel im RAM zu halten, wobei für den Fall eines Stromausfalls eine unabhängige Sicherung der Schlüssel unbedingt nötig ist. Außerdem muss die ungesicherte Auslagerung (Swap) von Schlüsseln aus dem RAM verhindert werden.

Von den verwendeten Schlüsseln sind in jedem Fall Sicherungskopien zu erstellen, so dass ein Zugriff auf diese Schlüssel jederzeit möglich ist. Im Falle eines HSMs als Schlüsselspeicher ist z.B. ein zweites HSM mit paralleler Datenhaltung denkbar, für RAM-Schlüssel kann eine Kopie auf einem Wechseldatenträger (z.B. CD) erstellt werden. Falls Schlüssel auf Wechseldatenträgern gespeichert werden sollen, muss eine sichere Ablage, z.B. in einem Tresor, gewährleistet werden.

Es muss in jedem Fall sichergestellt werden, dass keine unkontrollierten Datensicherungen vorgenommen werden können. Dazu ist eine lückenlose automatisierte Protokollierung aller Backup-Maßnahmen vorzusehen.

Für die Erzeugung der für die Verschlüsselungsverfahren und/oder Schlüsselerzeugung bzw. -ableitung benötigten Zufallszahlen muss eine geeignete Zufallsquelle zur Verfügung stehen (siehe BSI-TR-02102-1 [BSI4]).

5.2.3 Speicherung in gesonderten Speichereinrichtungen gemäß § 113d Satz 2 Nummer 2 TKG

Die nach § 113b TKG zu speichernden Verkehrsdaten müssen in physisch gesonderten, von den für die üblichen betrieblichen Aufgaben getrennten Speichereinrichtungen gespeichert werden. Diese Forderung gilt auch beim Einsatz von virtuellen Systemen.

Im Datenspeicher des Verkehrsdatenspeichersystems dürfen darüber hinaus neben den Verkehrsdaten nach § 113b TKG und den notwendigen Systemdateien keine sonstigen Daten gespeichert werden, insbesondere keine Daten für die in § 96 TKG genannten Zwecke. Eine Vermischung der nach § 113b gespeicherten Verkehrsdaten mit sonstigen Daten ist aus Gründen der Zweckbindung, der Datensicherheit und zur Vermeidung der Entstehung komplexer Systeme unzulässig.

Auf dem zur Speicherung der Verkehrsdaten eingesetzten System müssen Härtungsmaßnahmen nach Stand der Technik umgesetzt sein. Dies bedeutet, dass

ausschließlich die unmittelbar für die Verarbeitung und Speicherung der Verkehrsdaten notwendigen Programme (Prozesse und Dienste) auf dem System installiert sein dürfen (Minimalsystem); alle weiteren Softwarebestandteile und Funktionen, die zur Speicherung und Verarbeitung der Verkehrsdaten nicht zwingend erforderlich sind, sind zu entfernen. Es ist eine geeignete sichere Konfiguration der Systembestandteile zu gewährleisten. Vom Hersteller bereitgestellte und getestete Sicherheits-Updates müssen zeitnah eingespielt werden.

5.2.4 Hoher Schutz vor dem Zugriff aus dem Internet nach § 113d Satz 2 Nummer 3 TKG

Um die Speicherung der Verkehrsdaten mit einem hohen Schutz vor dem Zugriff aus dem Internet und damit vor dem Verlust der Vertraulichkeit, Integrität und Authentizität zu schützen, ist nach § 113d Satz 2 Nummer 3 TKG eine Entkopplung der Datenspeicher vom Internet herzustellen.

Diese Entkopplung ließe sich grundsätzlich realisieren, indem der Datenspeicher physisch von den mit dem Internet verbundenen Systemen getrennt wird. Jedoch fallen die zu speichernden Verkehrsdaten gerade in den Systemen an, die Teil des öffentlichen Telekommunikationsnetzes (und damit auch des Internets) sind, oder mit diesen direkt oder indirekt verbunden sind. Die zu speichernden Verkehrsdaten müssten folglich bei einer physischen Trennung manuell in den Datenspeicher übertragen werden, was in der Regel aufgrund der zu erwartenden Menge nicht praktikabel ist und zusätzliche Sicherheitsprobleme hervorrufen würde.

Die empfohlene Lösung, um den Datenspeicher vom Internet (bzw. von den öffentlichen Telekommunikationsnetzen) zu entkoppeln, ist der Einsatz einer geeigneten Firewall-Infrastruktur. Diese Firewall-Infrastruktur muss so beschaffen sein, dass ausschließlich dafür vorgesehene berechtigte Systeme Verkehrsdaten in den zu schützenden Bereich einliefern können, es dürfen jedoch keine Daten abfließen. Die sicherste Lösung ist daher der Einsatz einer Daten-Diode. Diese sorgt dafür, dass keine Daten den zu schützenden Bereich verlassen können, und übernimmt im Rahmen des verwendeten Verbindungsprotokolls gegebenenfalls notwendige Quittierungen. Bei der Verwendung alternativer zustandsbehafteter Firewall-Szenarien ist darauf zu achten, dass ein Verbindungsaufbau nur aus dem zu schützenden Bereich initiiert werden darf. Niemals darf eine Verbindung von außerhalb des Verkehrsdatenspeichersystems über die ausgewählte mit Proxy-Eigenschaften ausgestattete Firewall hinweg in den zu schützenden Bereich initiiert werden. Es dürfen somit keine Dienste nach außerhalb des Verkehrsdatenspeichersystems angeboten werden. Es müssen ausreichend detaillierte Firewall-Logs für drei Monate vorgehalten werden. Der Detaillierungsgrad muss so gewählt werden, dass mögliche Vorfälle im genauen zeitlichen Verlauf nachvollziehbar sind. Die Log-Dateien sind so regelmäßig auf Auffälligkeiten hin zu untersuchen, dass Sicherheitsverletzungen rechtzeitig erkannt bzw. vermieden werden können.

Um die Auskunftsersuchen der berechtigten Stellen durch besonders ermächtigte Mitarbeiter des Verpflichteten bearbeiten zu können, muss im Vier-Augen-Prinzip ein kontrollierter Zugriff auf den Datenspeicher erfolgen. Ein Zugriffssystem muss somit bei entsprechenden Anfragen die Daten entschlüsseln und entsprechend der Anfragen den Datenspeicher durchsuchen können. Der Zugriff auf das Zugriffssystem muss verschlüsselt erfolgen. Um Missbrauch auszuschließen, muss auch das Zugriffssystem durch eine Firewall, die mindestens IP-Adress-

und Portnummernbereiche filtert, geschützt werden. Diese Firewall muss so konfiguriert sein, dass ein Zugriff durch die Firewall hindurch nur vom autorisierten Abfragesystem erlaubt ist. Die Abfrageergebnisse dürfen durch die Firewall hindurch wiederum nur an autorisierte Abfragesysteme verschlüsselt gesendet werden können. Weitere Dienste dürfen nach außen nicht angeboten werden. Auch auf dieser Firewall müssen ausreichend detaillierte Firewall-Logs für drei Monate vorgehalten werden. Der Detaillierungsgrad muss so gewählt werden, dass Vorfälle im genauen zeitlichen Verlauf nachvollziehbar sind. Die Log-Dateien sind so regelmäßig auf Auffälligkeiten hin zu untersuchen, dass Sicherheitsverletzungen rechtzeitig erkannt bzw. vermieden werden können.

Die besonders ermächtigten Personen müssen sich mit individuellen Benutzerkennungen am Abfragesystem authentisieren. Das auf der Firewall autorisierte Abfragesystem ist nach dem Stand der Technik abzusichern. Die Absicherung muss im Sicherheitskonzept gemäß § 113g TKG dargestellt werden.

Wenn das Abfragesystem auch für weitere Auskunftserteilungen verwendet wird, für die die TKÜV die Nutzung eines gemeinsamen Übermittlungsverfahren zulässt, muss sichergestellt sein, dass die Anbindung von hierfür erforderlichen weiteren Systemen über eine Firewall gesichert wird. Hierbei dürfen nur die Verbindungen zu den erforderlichen Systemen und die erforderlichen Protokolle freigeschaltet werden. Die vorstehenden Ausführungen zu Log-Dateien gelten entsprechend.

Generelle Anforderungen an sichere Firewalls (bzw. Sicherheitsgateways) sind in den BSI-IT-Grundschutz-Katalogen [BSI3] und in der Studie „Sichere Anbindung von lokalen Netzen an das Internet (ISi-LANA)“ [BSI5] beschrieben.

5.2.5 *Umsetzung der Löschung von Verkehrsdaten gemäß § 113b Absatz 8 TKG*

Eine explizite Löschung von Verkehrsdaten aus persistenten Speichern (z.B. durch Überschreiben) ist nicht immer zuverlässig möglich, insbesondere bei Verwendung von Flash-Speichern (SSDs). Eine sichere Datenlöschung wird aber durch eine geeignete Verschlüsselung der Daten (siehe Abschnitt 5.2.2) und anschließende Löschung der kryptographischen Schlüssel erreicht.

Die gesetzliche Forderung nach einer irreversiblen Löschung der Verkehrsdaten muss also technisch realisiert werden durch die Löschung der Schlüssel, die im gewählten Verschlüsselungsverfahren für die sichere Ablage der Verkehrsdaten verwendet wurden (siehe Abschnitt 5.2.2). Aufgrund des geringeren Datenvolumens ist eine irreversible Löschung der Schlüssel möglich.

Dazu muss als Schlüsselspeicher ein Speichermedium gewählt werden, das eine zuverlässige Löschung von Daten erlaubt, z.B. HSM, RAM oder CD. Eine Schlüssellöschung ist dann möglich z.B. durch Löschen von Schlüsselreferenzen und Überschreiben von Schlüsseldateien (HSM), durch Vernichtung von Schlüsselobjekten (RAM) oder durch Zerstörung des Speichermediums (CD).

Um Zukunftssicherheit für das beschriebene Löschverfahren zu erreichen, müssen die verschlüsselten Verkehrsdaten zusätzlich aus dem persistenten Speicher gelöscht werden.

Dabei ist eine einfache Löschung durch Freigabe der entsprechenden Speicherbereiche ausreichend.

Die nach § 113b Abs. 8 TKG geforderten Löschfristen für Verkehrsdaten werden dann durch eine fristgerechte Löschung der Schlüssel und eine fristgerechte Löschung der Verkehrsdaten aus dem Datenspeicher realisiert. Bei Austausch oder Entsorgung eines persistenten Speichermediums, das zur Ablage von Verkehrsdaten verwendet worden ist, ist eine irreversible Zerstörung im Vier-Augen-Prinzip notwendig. Die irreversible Zerstörung ist mit Datum, Uhrzeit, Namen und Unterschriften der Mitarbeiter zu protokollieren.

Das zur Zerstörung verwendete Verfahren muss entsprechend dem hohen Schutzbedarf der Verkehrsdaten geeignet gewählt werden. Vorgaben dazu finden sich z.B. in den BSI-Grundschutz-Katalogen [BSI3].

Die bei der Verarbeitung von Suchanfragen im Zugriffs- oder Abfragesystem anfallenden Klardaten (kryptographische Schlüssel, entschlüsselte Verkehrsdaten und andere temporäre Daten) sind direkt nach Verwendung aus dem RAM des Zugriffssystems zu löschen. Hierfür gelten die obigen Regelungen entsprechend. Außerdem muss eine ungesicherte Auslagerung (Swap) von sensitiven Daten aus dem RAM des Zugriffssystems verhindert werden, da diese Daten sonst im Klartext im persistenten Speicher liegen und auch nicht sicher wieder gelöscht werden können (siehe oben). Möglich ist das z.B. durch eine Deaktivierung oder Verschlüsselung der Auslagerungsdatei.

Die in diesem Abschnitt beschriebenen Anforderungen zur Löschung von Verkehrsdaten gelten inhaltsgleich auch für alle Sicherungskopien von Verkehrsdaten und Schlüsseln, die im Rahmen von Backup-Maßnahmen erstellt werden.

5.2.6 Beschränkung des Zutritts zu den Datenverarbeitungsanlagen gemäß § 113d Satz 2 Nummer 4 TKG

Die Beschränkung des Zutritts zu den Datenverarbeitungsanlagen nach § 113d Satz 2 Nummer 4 TKG muss personell, organisatorisch und technisch erfolgen.

5.2.6.1 Erstellung eines Rechte- und Rollenmanagements

Die Speicherung der Verkehrsdaten bei den Verpflichteten ist u.a. an eine hohe Vertraulichkeit geknüpft. Ein Missbrauch der gespeicherten Verkehrsdaten sowohl durch besonders ermächtigte als auch durch unberechtigte Personen oder Dritte ist zu verhindern. Das bedingt, dass Unberechtigte keinen und besonders Ermächtigte nur einen kontrollierten, ihrer jeweiligen Rolle entsprechenden Zugriff erhalten dürfen.

Verschiedene besonders ermächtigte Personen unterscheiden sich in ihrer Rolle wie folgt:

- Zum einen gibt es von den Verpflichteten besonders ermächtigte Personen, die Auskunftsersuchen berechtigter Stellen entgegennehmen, prüfen, die Suchanfrage im Datenspeicher initiieren und die Ergebnisse an die berechtigten Stellen versenden oder aus anderen Gründen auf Verkehrsdaten zugreifen dürfen. Dieser Vorgang hat im Vier-Augen-Prinzip nach Abschnitt 5.2.7.1 zu geschehen. Alle Tätigkeiten sind lückenlos und

revisionssicher automatisch zu protokollieren.

- Zum anderen gibt es besonders ermächtigte Personen, die für die hardware- und softwaretechnische Wartung des Verkehrsdatenspeichersystems zuständig sind. Für verschiedene administrative Tätigkeiten (z.B. Kryptomanagement, Firewall-Konfiguration, Datenbankkonfiguration oder allg. Administrationstätigkeiten) müssen, insbesondere wenn Tätigkeiten von verschiedenen Personen wahrgenommen werden, unterschiedliche individuell abgesicherte Benutzerkonten zum Einsatz kommen. Der Zugang und die Arbeiten an den Systemen sind lückenlos und revisionssicher zu dokumentieren. Möglichkeiten der Fernwartungszugänge sind in Abschnitt 5.2.7.2 beschrieben.

Verschafft sich jemand unberechtigter Weise Zutritt zu den Systemen im physisch gesicherten Bereich, muss automatisch ein Alarm ausgelöst werden, der sofortige Sicherheitsmaßnahmen auslöst. Das Abfragesystem, welches zur Bearbeitung der Auskunftsersuchen berechtigter Stellen eingesetzt wird, muss in verschließbaren Räumen in einer physisch gesicherten Umgebung aufgestellt und besonders zugriffsgeschützt sein.

Für den Fall, dass ein Verpflichteter einen Dritten mit Aufbau und Betrieb des Verkehrsdatenspeichersystems beauftragt, muss der Verpflichtete mittels vertraglicher Regelungen dafür Sorge tragen, dass nur durch ihn besonders ermächtigte Personen des Auftragnehmers zum Einsatz kommen. Der Verpflichtete hat dies regelmäßig zu überprüfen. Die Verpflichteten müssen dafür Sorge tragen, dass Kontrollen durch die Bundesnetzagentur und die Bundesbeauftragte für den Datenschutz und die Informationsfreiheit im gesetzlich vorgesehenen Umfang durchgeführt werden können.

5.2.6.2 Physische Absicherung der Speichereinrichtung

Bei der Planung und beim Betrieb der Speichereinrichtungen auf eine hinreichende physische Sicherheit zu achten. Insbesondere der Teil des Rechenzentrums, in dem die Hardware-Komponenten des Verkehrsdatenspeichersystems untergebracht sind, muss als geschlossener Sicherheitsbereich konzipiert sein. Alternativ sind separate Schutzschränke innerhalb des Rechenzentrums vorzusehen, um die Schutzwirkung für die Speichereinrichtungen zu erhöhen. Die Komponenten des Verkehrsdatenspeichersystems müssen vor unbefugtem Zutritt durch hochwertige Zutrittskontrollmechanismen geschützt werden. Bei unberechtigtem Zutritt muss ein Alarm ausgelöst werden, der sofortige Sicherheitsmaßnahmen auslöst.

Alle Clients, die zur Beauskunftung oder Wartungszwecken eingesetzt werden (z.B. Management-Konsole), müssen physisch gegen den Zugriff durch nicht besonders ermächtigte Personen geschützt sein.

Die Vergabe und Rücknahme von Zutrittsberechtigungen durch den Verpflichteten oder auf dessen Veranlassung ist lückenlos zu dokumentieren. Die Überwachung der Zutrittsberechtigung hat durch Personen (z.B. Pförtner, Schließdienst, Sicherheitspersonal) oder durch technische Einrichtungen (z.B. Ausweisleser, biometrische Verfahren wie Irisscanner oder Fingerabdruck, Sicherheitstürschloss, Schließanlage) zu erfolgen.

Der Zugang zum Verkehrsdatenspeichersystem zu Wartungszwecken darf erst nach einer Identifikation und einer Zwei-Faktor-Authentisierung unter Anwendung des Vier-Augen-Prinzips möglich sein. Die Ausgabe und der Entzug von Zugangsmitteln wie Benutzer-Kennungen oder Chipkarten durch den Verpflichteten oder von ihm eingesetzten Beauftragten sind zu dokumentieren. Die Authentisierungsvorgänge sowie sämtliche Systemeingaben müssen revisionssicher protokolliert werden. Jeder Protokollierungseintrag muss Datum, Uhrzeit, Zweck und durchgeführte Tätigkeit des Zutritts und den Namen der Person enthalten.

5.2.7 Notwendige Mitwirkung von mindestens zwei Personen beim Zugriff auf die Verkehrsdaten gemäß § 113d Satz 2 Nummer 5 TKG (Vier-Augen-Prinzip)

Es sind technische und organisatorische Vorkehrungen zur Gewährleistung des Vier-Augen-Prinzips durch zwei zum Zugriff auf die Verkehrsdaten durch den Verpflichteten besonders ermächtigte Personen zu treffen. Die Umsetzung der Anforderungen unterscheiden zwischen dem Abruf von Verkehrsdaten zur Beauskunftung eines Auskunftsersuchens und einem betrieblichen Zugriff.

5.2.7.1 Vier-Augen-Prinzip zur Beauskunftung eines Auskunftsersuchens

Bei der Beauskunftung eines Auskunftsersuchens muss die Übereinstimmung der in einer richterlichen Anordnung oder der in einem behördlichen Auskunftsersuchen enthaltenen Abfrageparameter mit den in das Zugriffssystem eingegebenen Daten durch zwei hierzu vom Verpflichteten besonders ermächtigte Personen geprüft werden.

Die erste Person soll dabei nach Eingang des Auskunftsersuchens die Übereinstimmung der angefragten Daten mit dem korrespondierenden Gerichtsbeschluss oder dem behördlichen Ersuchen feststellen und die Anfrage bei Abweichungen zur Korrektur an die berechtigte Stelle zurückweisen.

Die zweite Person hat dann eine entsprechende Prüfung in einem getrennten und unabhängigen weiteren Schritt durchzuführen. Hierbei ist erneut sicherzustellen, dass die im System abzufragenden Daten mit den vom korrespondierenden Gerichtsbeschluss oder dem behördlichen Ersuchen umfassten übereinstimmen. Sollte das nicht der Fall sein, muss die erste Person hierüber informiert und die Abfrage der Verkehrsdaten von dieser erneut initiiert werden.

Werden die notwendigen technischen Abfrageparameter neben der richterlichen Anordnung von der berechtigten Stelle mitgeliefert (ETSI-ESB), ist sicherzustellen, dass diese durch die Prüfung bei dem Verpflichteten nicht geändert werden können. Bei etwaigen Fehlern oder Unklarheiten muss der Verpflichtete bei der berechtigten Stelle ggf. veränderte Abfrageparameter erfragen.

Werden die technischen Abfrageparameter nicht elektronisch von der berechtigten Stelle bereitgestellt, sondern werden diese durch die erste prüfende Person erzeugt, ist sicherzustellen, dass diese durch die zweite prüfende Person nicht geändert werden können.

Erkannte fehlende Übereinstimmungen müssen durch die erste prüfende Person berichtigt und von der zweiten prüfenden Person vor der Freigabe nochmals geprüft werden.

Um sicherzustellen, dass es nicht aufgrund von technischen Fehlern zu einer Ausleitung von Verkehrsdaten kommt, die nicht vom Eingabebefehl umfasst sind, sind regelmäßig technische Tests unter Einsatz von hierfür im Telekommunikationsnetz generierten Testdaten (Dummy Data) zur Überprüfung des Systems durchzuführen.

5.2.7.2 Vier-Augen-Prinzip beim betrieblichen Zugriff

Wenn es bei einem betrieblichen Zugriff (z.B. Wartungsarbeiten am Verkehrsdatenspeicher-system) zu einem Zugriff auf die speicherpflichtigen Verkehrsdaten oder die kryptographischen Schlüssel kommen kann, dann dürfen der Zugriff auf die Komponenten des Verkehrsdatenspeichersystems (z.B. zum Austausch von Hardwarekomponenten oder Update der Software) und die damit verbundenen Arbeiten nur im Vier-Augen-Prinzip durch zwei besonders ermächtigte Personen erfolgen (siehe Abschnitt 5.2.6.1).

Die Wartungsarbeiten können durch eine einzelne Person erfolgen, wenn die folgenden Bedingungen erfüllt sind:

- Durch das für den Zugriff vorgesehene System (Managementkonsole) ist ausgeschlossen, dass es unmittelbar oder zu einem späteren Zeitpunkt zu einem direkten oder indirekten Zugriff auf die speicherpflichtigen Verkehrsdaten oder die Schlüssel kommen kann.
- Es ist ausgeschlossen, dass durch die Wartungsarbeiten ein nachträglicher Zugang zu den Verkehrsdaten oder den Schlüsseln ermöglicht wird.
- Die Person darf keinen Root-Zugang erhalten und die erteilten Zugangsrechte dürfen durch diese Person nicht verändert werden können.

Die Anforderungen zur physischen Absicherung der zu Wartungszwecken eingesetzten Systeme sind in Abschnitt 5.2.6.2 beschrieben.

Im Rahmen der Wartungsarbeiten, für die das Vier-Augen-Prinzip einzuhalten ist, sind die nachfolgenden Zugriffsmöglichkeiten erlaubt:

A: Wartungszugang von unterschiedlichen Standorten

Ist ein Wartungszugang für besonders ermächtigte Personen von unterschiedlichen Orten außerhalb des nach Abschnitt 5.2.6.2 physisch gesicherten Bereichs auf die Managementkonsole vorgesehen, müssen die nachfolgenden Anforderungen erfüllt sein:

1. Der Zugang auf die Managementkonsole darf nur erfolgen, wenn der Zugang über eine Zugangs- und Überwachungskontrolle erfolgt und diese sicherstellt, dass beide ermächtige Personen gleichzeitig zugreifen müssen und keine Umgehungsmöglichkeit der Zugangs- und Überwachungskontrolle besteht.
2. Die Zugangs- und Überwachungskontrolle muss sicherstellen, dass alle Eingaben und Bildschirmanzeigen beiden Personen inhaltlich identisch zur Ansicht gebracht werden und keine Möglichkeit besteht, diese Dopplung zu unterbinden.

3. Für derartige Wartungszugänge sind nur dedizierte Clientsysteme erlaubt, die sich gegenüber dem Zugriffssystem authentisieren müssen. Diese Verbindung ist immer durch eine Transportsicherung (d.h. Transportverschlüsselung mit Integritäts- und Authentizitätsschutz) abzusichern. Der Betrieb der Clientsysteme ist nur in den im Inland gelegenen Räumen der Unternehmen gestattet, die die besonders ermächtigten Personen beschäftigen.

4. Die Managementkonsole sowie die eingesetzten Clientsysteme sind nach Maßgabe des Abschnittes 5.2.4 vor unerlaubten Verbindungen und vor dem Internet durch eine Firewall zu schützen.

B: Fernzugriff für Dritte

Ein ausschließlich lesender Fernzugriff kann für Dritte (z.B. ein Spezialist der Herstellerfirma) zur Unterstützung der beiden besonders ermächtigten Personen, die die notwendigen Arbeiten selbst ausführen müssen, erlaubt werden, sofern nachfolgende Anforderungen erfüllt sind:

1. Der Fernzugriff erfolgt ausschließlich auf eine Management-Konsole, von der aus die anderen Komponenten des Verkehrsdatenspeichersystems betrieben werden.

2. Ein schreibender Zugriff für einen Dritten wird wirkungsvoll unterbunden; zur Unterstützung der beiden besonders ermächtigten Personen ist lediglich ein lesender Zugriff erlaubt. Auch das aus der Ferne unterstützende Personal ist authentisiert. Die besonders ermächtigten Personen haben eine Schulung im Umgang mit der zu administrierenden Systemkomponente, um die Auswirkungen von Empfehlungen eines Dritten vor der Umsetzung bewerten zu können.

3. Fernwartungszugänge über öffentliche Telekommunikationsnetze sind immer durch eine Transportsicherung (d.h. Transportverschlüsselung mit Integritäts- und Authentizitätsschutz) abgesichert.

4. Das lokale Netz sowie der Client, von dem aus der Fernwartungszugang erfolgt, sind nach IT-Grundschutz abgesichert.

5. Es wird sichergestellt, dass unverschlüsselte Verkehrsdaten und kryptographische Schlüssel nicht eingesehen werden können.

6. Der Fernwartungszugang ist entsprechend der im Abschnitt 5.2.4 dargestellten Maßnahmen vom Internet über eine Firewall entkoppelt. Die Verbindung wird direkt nach erfolgtem Fernzugriff physisch jedes Mal unterbunden (z.B. durch Ziehen des Verbindungskabels).

5.3 Anforderung an die Protokollierung gemäß § 113e TKG

Nach § 113e Absatz 1 TKG ist jeglicher Zugriff auf die Verkehrsdaten revisionssicher zu protokollieren. Die Protokollierung hat in dem System zu erfolgen, in dem sich die Verkehrsdaten befinden.

Nach § 113e TKG sind zu protokollieren:

1. Datum und Uhrzeit des Zugriffs,
2. Jeweilige Kennungen der auf die Verkehrsdaten zugreifenden Personen,
3. Zweck und Art des Zugriffs.

Es muss für die Dauer der Aufbewahrungspflicht nachvollzogen werden können, welche Personen über welche Clients auf die Verkehrsdaten zugegriffen haben. Soweit in den Protokolldaten nach § 113e TKG nur Kennungen hinterlegt sind, die keine unmittelbare Zuordnung zu einer natürlichen Person zulassen, muss die Zuordnung der zum Datenzugriff berechtigten Person zu der Kennung dokumentiert sein.

Die Protokollierung im Zusammenhang eines Auskunftsersuchens einer berechtigten Stelle erfolgt nach Maßgabe der TKÜV.

Für betriebliche Zugriffe kann der Zweck und die Art des Zugriffs z.B. durch eine History-Datei des Betriebssystems, die die einzelnen Bearbeitungsschritte enthält, protokolliert werden.

Die Protokolldaten dürfen keinen Aufschluss über den Inhalt der gelöschten oder verarbeiteten Verkehrsdaten geben. Sie sind in speziell hierfür vorgesehenen, gesicherten Speichereinrichtungen zu speichern. So dürfen Antworten an berechtigte Stellen oder die Ausgaben bei Anfragen an den Datenspeicher nicht in den Protokolldaten enthalten sein.

Die Löschung der Protokolldaten kann mit normalem Schutzbedarf nach IT-Grundschutz erfolgen. Dieser Löschvorgang ist ebenfalls wie folgt zu protokollieren:

1. Datum und Uhrzeit der Löschung von Protokolldaten,
2. Bearbeiter beim Verpflichteten bzw. beim durch den Verpflichteten beauftragten Unternehmen.

6. Quellenverzeichnis

[BSI1] Bundesamt für Sicherheit in der Informationstechnik: IT-Grundschutz-Vorgehensweise, BSI-Standard 100-2, Version 2.0, Mai 2008, https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzStandards/Standard02/ITGStandard02_node.html

[BSI2] Bundesamt für Sicherheit in der Informationstechnik: Risikoanalyse auf der Basis von IT-Grundschutz, BSI-Standard 100-3, Version 2.5, Mai 2008, https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzStandards/Standard03/ITGStandard03_node.html

[BSI3] Bundesamt für Sicherheit in der Informationstechnik: BSI-IT-Grundschutz-Katalog https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKataloge/itgrundschutzkataloge_node.html

[BSI4] Bundesamt für Sicherheit in der Informationstechnik: Technische Richtlinien BSI TR-02102 Kryptographische Verfahren: Empfehlungen und Schlüssellängen https://www.bsi.bund.de/DE/Publikationen/TechnischeRichtlinien/tr02102/index_htm.html

[BSI5] Bundesamt für Sicherheit in der Informationstechnik: Studie „Sichere Anbindung von lokalen Netzen an das Internet (ISi-LANA)“, 2007, https://www.bsi.bund.de/DE/Themen/StandardsKriterien/ISi-Reihe/ISi-LANA/lana_node.html

[TKG] Telekommunikationsgesetz vom 22.06.2004 (BGBl. I, Seite 1190), zuletzt geändert durch Gesetz vom 24.05.2016 (BGBl. I S. 1217)

[TKÜV] Verordnung über die technische und organisatorische Umsetzung von Maßnahmen zur Überwachung der Telekommunikation (Telekommunikations-Überwachungsverordnung) vom 03.11.2005 (BGBl I, Seite 3136, zuletzt geändert durch Art. 4 Terrorismusabwehr-G vom 25. 12. 2008 (BGBl. I S. 3083)

[TR TKÜV] Technische Richtlinie zur Umsetzung gesetzlicher Maßnahmen zur Überwachung der Telekommunikation, Erteilung von Auskünften, Version 6.3 vom 06.04.2016

Anlage

Sicherheitskonzept (§ 113g)

Der nach § 113a Absatz 1 TKG Verpflichtete hat der Bundesnetzagentur das Sicherheitskonzept nach § 113g TKG unverzüglich nach dem Beginn der Speicherung nach §113b und unverzüglich erneut bei jeder Änderung des Konzepts vorzulegen.

Hierzu wird empfohlen, das Sicherheitskonzept nach § 109 Absatz 4 TKG um einen inhaltlich geschlossenen, spezifischen Teil nach § 113g TKG (z.B. „Sicherheitskonzept technischer Vorkehrungen und sonstiger Maßnahmen für Speicherpflichten und Höchstspeicherfristen für Verkehrsdaten nach § 113g TKG“) zu erweitern, um darin die Schutzmaßnahmen zur Sicherstellung der besonders hohen Anforderungen nach den Kapiteln 4 und 5 des Anforderungskatalogs an Datenqualität und Datensicherheit zu beschreiben. Hierbei wird davon ausgegangen, dass die eigentliche Verkehrsdatenspeicherung nach §§ 113a ff. TKG in einem sicheren Umfeld mit existierendem Sicherheitskonzept zur Beschreibung eines Basisschutzes realisiert wird.

Sollte dies nicht der Fall sein, so sind auch die Maßnahmen zur Realisierung eines Basisschutzes nach § 109 Absatz 4 TKG zu dokumentieren. Zur Vorgehensweise wird auf den Katalog von Sicherheitsanforderungen nach § 109 Absatz 6 TKG und auf einschlägige Beschreibungen zum BSI-Grundschutz verwiesen.

Die Maßnahmen zur Realisierung der besonders hohen Anforderungen nach den Abschnitten 4 und 5 des Anforderungskatalogs sollen im Sicherheitskonzept wie folgt dargestellt werden:

1. Bestimmung der relevanten Sicherheitsteilsysteme

Damit Gefährdungen des Gesamtsystems zur Speicherung, Verarbeitung und Übertragung der speicherpflichtigen Verkehrsdaten nach §§ 113b bis 113e TKG identifiziert und differenziert betrachtet werden können, sind Sicherheitsteilsysteme (siehe nachfolgende Grafik) z.B. Netzelemente mit Logdatensystemen (Call Data Records, Schnittstelle Interconnection mit Call Data Records), Datenfilter, Datenspeicher, Abfrage- und Zugriffssystem zu bilden und entsprechend im Sicherheitskonzept sowohl grafisch als auch schriftlich zu beschreiben.

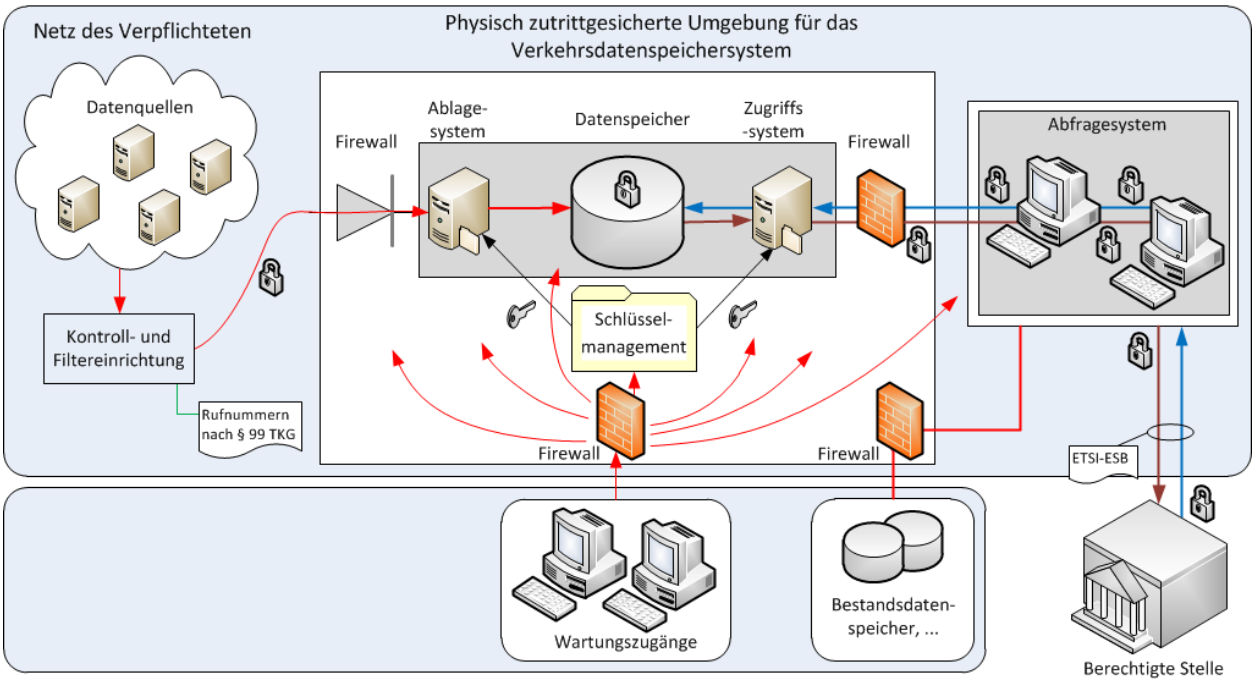

Abbildung 3: Umsetzungsbeispiel der Grundarchitektur

2. Zuordnung der besonders hohen Anforderungen (Abschnitte 4 und 5 des Anforderungskatalogs)

2.1 Gefährdungsanalyse

Die jeweiligen potentiell möglichen Gefährdungen des durch §§ 113b bis 113e TKG definierten Schutzniveaus sind zu identifizieren und zu beschreiben. Ergänzend sind individuelle Gegebenheiten zu berücksichtigen (ggf. in Form von zusätzlichen Teilsystemen), die zusätzlich relevante Gefährdungen verursachen können und somit ergänzende Maßnahmen zur Erzielung eines besonders hohen Standards der Datensicherheit und Datenqualität notwendig machen. Diese individuellen Gegebenheiten sollen Sachverhalte berücksichtigen, die ihre Ursache im konkreten Umfeld des einzelnen Verpflichteten haben. Die Risikoanalyse kann beispielsweise gemäß BSI-Standard 100-3 [BSI2] durchgeführt werden.

2.2 Zuordnung der Schutzmaßnahmen nach Abschnitten 4 und 5 des Anforderungskatalogs zu Sicherheitsteilsystemen

Die zu treffenden Schutzmaßnahmen zur Erfüllung der gesetzlichen Anforderungen entsprechend der Abschnitte 4 und 5 sowie die nach Kapitel 2.1 identifizierten ergänzenden Maßnahmen sind den jeweiligen Sicherheitsteilsystemen zuzuordnen und zu beschreiben.

Die Dokumentation kann in Form von Tabellen mit der jeweiligen Zuordnung „Anforderung, Gefährdung, Schutzmaßnahme“ erfolgen, vergleichbar der Vorgehensweise nach dem Katalog von Sicherheitsanforderungen nach § 109 Absatz 6 TKG.

3. Bewertung des Gesamtsystems

Auch wenn jedes einzelne Sicherheitsteilsystem die gesetzlichen Anforderungen nach §§ 113b bis 113e TKG (Abschnitt 4 und 5) erfüllt, so können mit Blick auf die Sicherheit des Gesamtsystems noch Restrisiken bestehen. Aus diesem Grund ist zusätzlich eine separate Bewertung nach hohem Schutzbedarf des Gesamtsystems erforderlich, bis auch dieses durch die geplanten Einzelmaßnahmen den vorgenannten gesetzlichen Anforderungen entspricht. Wie ein ggf. verbleibendes „Restrisiko“ behandelt wird, ist aufzuzeigen.