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)"

- Entwurf -

Version: 0.1
Stand: 11.05.2016

Bearbeiter und Herausgeber:

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

Änderungshistorie

Version	Datum	Anlass	Autor
0.1	Mai 2016	Entwurf eines Anforderungskatalogs gemäß § 113f TKG	Bundesnetzagentur, Referat IS16

Inhaltsverzeichnis

1. Begriffsbestimmungen

Abfrageclient	Arbeitsplatzrechner, von dem aus die Abfragen im VDS-System initiiert werden und der die ausgeleiteten Abfrageergebnisse zur Beauskunftung entgegen genommen werden
Ablagesystem	Komponenten (Hardware/Software) zur Verschlüsselung der speicherpflichtigen Verkehrsdaten und Ablage im Datenspeicher.
Datenspeicher	Speichereinrichtung, in der die speicherpflichtigen Verkehrsdaten vorgehalten werden
Schlüsselmanagement	Komponenten (Hardware/Software) zur Erzeugung, Verteilung, Speicherung und Löschung der Verschlüsselungsschlüssel
VDS-System	Gesamtheit aller Einzelsysteme (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.
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).
Zugriffssystem	Komponenten (Hardware/Software), die die Abfrage von Daten im Datenspeicher realisieren und die Abfrageergebnisse ausleiten und hierzu die Entschlüsselung durchführen.

Hinweis zum Entwurf: Die technischen Begriffsbestimmungen werden nach Fertigstellung des Gesamtdokumentes überarbeitet.

2. Abkürzungen

bS	berechtigte Stelle nach §113 Abs. 3 TKG
CD	Compact Disc
HSM	Hardware Security Module
RAM	Random Access Memory
SINA	Sichere Inter-Netzwerk Architektur
SSD	Solid-State-Drive
TKG	Telekommunikationsgesetz vom 22.06.2004 (BGBl. I, Seite 1190)
TKÜV	Verordnung über die technische und organisatorische Umsetzung von Maßnahmen zur Überwachung der Telekommunikation vom 03.11.2005 (BGBl. I S. 3136)
TR TKÜV	Technische Richtlinie nach § 110 Abs. 3 TKG zur Umsetzung gesetzlicher Maßnahmen zur Überwachung der Telekommunikation, Erteilung von Auskünften
VDS	Verkehrsdatenspeicherung
VPN	Virtual Private Network

Hinweis zum Entwurf: Die Liste der Abkürzungen wird nach Fertigstellung des Gesamtdokumentes überarbeitet.

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 Verkehrsdatenspeicherung insgesamt in einer physisch sicheren Umgebung durch Realisierung eines Basisschutzes erfolgt. Das darüber hinausgehende in diesem Katalog beschriebene Schutz- und Sicherheitsniveau zur Gewährleistung eines besonders hohen Standards 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 allgemeinen 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 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.

Der vorliegende Katalog ist gemäß § 113f Abs. 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 Abs. 3 Satz 1 i.V. mit § 109 Abs. 6 Satz 2 TKG Gelegenheit zur Stellungnahme gegeben worden.

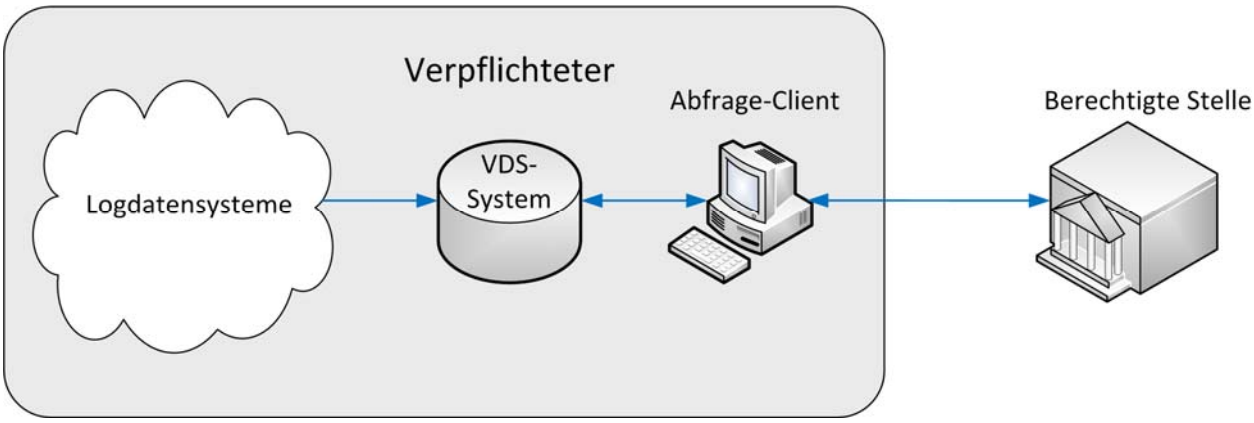
Die technischen Vorkehrungen und sonstigen Maßnahmen hinsichtlich der Übermittlung der Daten an die in § 113c Abs. 1 TKG genannten Stellen richten sich gemäß § 113c Abs. 3 TKG nach der TKÜV und der TR TKÜV.

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 Verfügbarkeit, Unversehrtheit und Vertraulichkeit der speicherpflichtigen Verkehrsdaten mittels Sicherheitsvorkehrungen in den jeweiligen informationstechnischen Systemen, Komponenten oder Prozessen oder bei deren Anwendung sicherstellt. Diese Verkehrsdaten müssen soweit wie möglich vor Beeinträchtigungen oder Missbrauch bewahrt werden. Hierzu zählt auch der Schutz vor Verlust der Daten, etwa mittels Backup-Systemen.

Das folgende Schaubild erläutert die Einzelkomponenten des Gesamtsystems zur Beauskunftung von speicherpflichtigen Verkehrsdaten:



Die in den Netzelementen des Providernetzes anfallenden Abrechnungs-, Log- und/oder Signalisierungsdaten werden zunächst einer Kontroll- und Filtereinrichtung zugeführt. Diesbezügliche Anforderungen in diesem Anforderungskatalog beziehen sich insbesondere auf die Datenqualität und die Transportsicherung. Nach dieser Einrichtung stehen dem Unternehmen Verkehrsdaten zur Verfügung, die nach §§ 96 ff. TKG gespeichert werden dürfen (nicht Gegenstand dieses Anforderungskatalogs) und Verkehrsdaten, die nach § 113b TKG gespeichert werden müssen. Die letztgenannten, speicherpflichtigen Verkehrsdaten werden dem VDS-System zugeführt und stehen dort für Beauskunftungen den Behörden zur Verfügung. Die zur Beauskunftung nötigen Abfragesysteme werden von diesem Anforderungskatalog sowie der TKÜV bzw. der TR TKÜV gleichermaßen erfasst.

Beim Transport von speicherpflichtigen Verkehrsdaten zwischen den einzelnen Komponenten des VDS-Systems sowie bei Zuleitung zum VDS-System (Einlieferung der speicherpflichtigen Verkehrsdaten) und Ausleitung aus dem VDS-System (Export der Abfrageergebnisse) muss eine Transportsicherung die Vertraulichkeit, Integrität und Authentizität der Daten schützen.

Erfolgt der Datentransport über ungesicherte Netze (wie z.B. das Internet), muss eine geeignete Transportverschlüsselung mit Authentizitäts-/Integritätsschutz, z.B. TLS, IPSec oder SSH (siehe BSI-TR-02101-2/3/4), eingesetzt werden. Zur Initialisierung der sicheren Kommunikationsverbindung muss dabei eine gegenseitige Authentisierung der Kommunikationsendpunkte erfolgen. Falls die Daten ausschließlich über dedizierte, gesicherte Verbindungen, z.B. eigene physische Leitungen im besonders physisch gesicherten Bereich, 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 VDS-System, wie z.B. automatisierte Fehlererkennungsverfahren, Plausibilitätsprüfungen

3. Maßnahmen bei festgestellten Fehlern

Die Datenqualität soll zudem durch regelmäßige Tests mit der 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 für die zu speichernde Zeitangabe von Beginn und Ende der Verbindung nach § 113b Abs. 2 Satz 1 Nr. 2

TKG, der ersten Aktivierung nach § 113b Abs. 2 Satz 1 Nr. 4 c) TKG, der Versendung und des Empfangs der Nachricht nach § 113b Abs. 2 Satz 2 Nr. 1 TKG, von Beginn und Ende der Internetnutzung nach § 113b Abs. 3 Nr. 3 sowie des Zeitpunkts des Zugriffs nach § 113e Abs. 1 Satz 2 Nr. 1 TKG relevant.

4.2.2 Maßnahmen zur Sicherstellung der Richtigkeit und Vollständigkeit bei der Zuführung der speicherpflichtigen Verkehrsdaten in das VDS-System

Vor der Einspeicherung in die Speichereinrichtung sollen die speicherpflichtigen Verkehrsdaten automatisiert gegen die erwarteten Formate geprüft werden, um eine grundsätzliche Plausibilitätskontrolle durchzuführen und ggf. Maßnahmen zur Fehlerbeseitigung (siehe Abschnitt 4.2.3) einzuleiten.

Zur Fehlererkennung können die 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 Abs. 1 Nr. 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 Abs. 2 Satz 2 TKG zertifizieren zu lassen, um sicherzustellen, dass die Zuordnung der erfassten Zeit mit den vereinbarten Tarifen übereinstimmt.

Ebenso können bei dem TK-Unternehmen bestehende Rechnungsprüfungsverfahren oder Mißbrauchserkennungssysteme eingesetzt werden. Angelehnt an solche, üblicherweise im Billing-Prozess eingesetzten Verfahren, können dadurch Unregelmäßigkeiten, wie 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, wie z.B. Betriebsausfälle oder fehlerhaft gespeicherte Verkehrsdaten (etwa aufgrund einer falschen Zeitbasis in einem Netzelement), muss der Verpflichtete die berechtigten Stellen, die im betroffenem Zeitraum entsprechende speicherpflichtige Verkehrsdaten abgefragt haben oder abfragen, 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. zu konkreten

Telefonverbindungen oder zugewiesenen IP-Adressen) 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. Die Verkehrsdaten müssen ihren Ursprung direkt aus den Abrechnungs-, Log- oder Signalisierungsdaten haben. Dadurch wird sichergestellt, dass nur dann Daten erzeugt werden, wenn auch tatsächliche Verbindungen aufgebaut wurden, bzw. es zu Verbindungsversuchen kam.

Es ist sicherzustellen, dass Verkehrsdaten, die in eigenen Netzen 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 ist die Integrität der Verkehrsdaten und der Systeme sowie die Vollständigkeit und Korrektheit der Verkehrsdaten zu gewährleisten. Für Backup-Daten gelten dieselben Anforderungen an die Datensicherheit wie für die Originaldaten.

Die Speichereinrichtungen müssen über eine ausreichende Leistungsfähigkeit verfügen, um alle anfallenden Verkehrsdaten und eingehenden Abfragen verarbeiten zu können.

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

Personen, Behörden und Organisationen in sozialen oder kirchlichen Bereichen i.S.v. § 113b Abs. 6 i.V.m. § 99 Abs. 2 Satz 1 und 3 TKG teilen der Bundesnetzagentur die nach § 99 Abs. 2 TKG von der Speicherung auszunehmenden Rufnummern mit und übermitteln ihr die Bescheinigung nach § 99 Abs. 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 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 Abs. 7 TKG

Nach § 113b Abs. 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 bzw. zentral abrufbar sein. Zudem müssen die Systeme für die Zuführung der Verkehrsdaten aus den Netzelementen des eigenen Netzes so ausgestaltet sein, dass die Verkehrsdaten binnen 24 Stunden nach dem jeweiligen Ereignis dem VDS-Speicher zugeführt werden.

5.1.4 Löschung der Verkehrsdaten gemäß § 113b Abs. 8 TKG

Die Speicherung der Verkehrsdaten hat so zu erfolgen, dass die Möglichkeit einer vollständigen und rechtzeitigen Löschung gewährleistet ist. Die diesbezüglichen technischen Anforderungen sind in Abschnitt 5.2.5 geregelt.

5.1.5 Verwendung der Daten gemäß § 113c Abs. 3 TKG

Bis zur Aufnahme von Regelungen für die Übermittlung von speicherpflichtigen Verkehrsdaten in die TKÜV 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 sich in diesen Fällen mit der Bundesbeauftragten für den Datenschutz und die Informationsfreiheit abstimmt.

Darüber hinaus muss sichergestellt werden, dass im Zuge von Auskunftsersuchen verarbeitete Verkehrsdaten nach der Übermittlung bzw. der Verwendung nach § 113c Abs 1 TKG unverzüglich nach dem Stand der Technik irreversibel gelöscht werden. Bei Verwendung von RAM als Speichermedium gelten die gleichen Anforderungen zur Löschung der Verkehrsdaten wie im Zugriffssystem (siehe Abschnitt 5.2.5). Sollen andere Verfahren eingesetzt werden, sind diese nach Anschnitt 5.1.5 vorher abzustimmen.

5.2 Gewährleistung der Sicherheit der Daten gemäß § 113d TKG

Um einen besonders hohen Standard der Datensicherheit im VDS-System gewährleisten zu können (siehe § 113f TKG), müssen generell alle Komponenten des Systems die Anforderungen nach IT-Grundschutz des BSI mit dem Schutzbedarf „hoch“ (siehe BSI-Standard 100-2 IT-Grundschutz-Vorgehensweise) erfüllen. Bezüglich der kryptographischen Absicherung des Systems müssen die Empfehlungen aus der Technischen Richtlinie „Kryptographische Verfahren: Empfehlungen und Schlüssellängen“ des BSI (siehe BSI-TR-02102) beachtet werden.

Ein sicheres VDS-System 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.

Bevor die einzelnen technischen Anforderungen erläutert werden, soll zunächst die grundsätzliche Architektur dargestellt werden.

5.2.1 Grundsätzliche Architektur der Anlagen

An dem nachfolgenden Umsetzungsbeispiel sollen zunächst die grundlegenden Funktionen und Prozesse erläutert werden. Anschließend werden die verschiedenen technischen Anforderungen beschrieben.

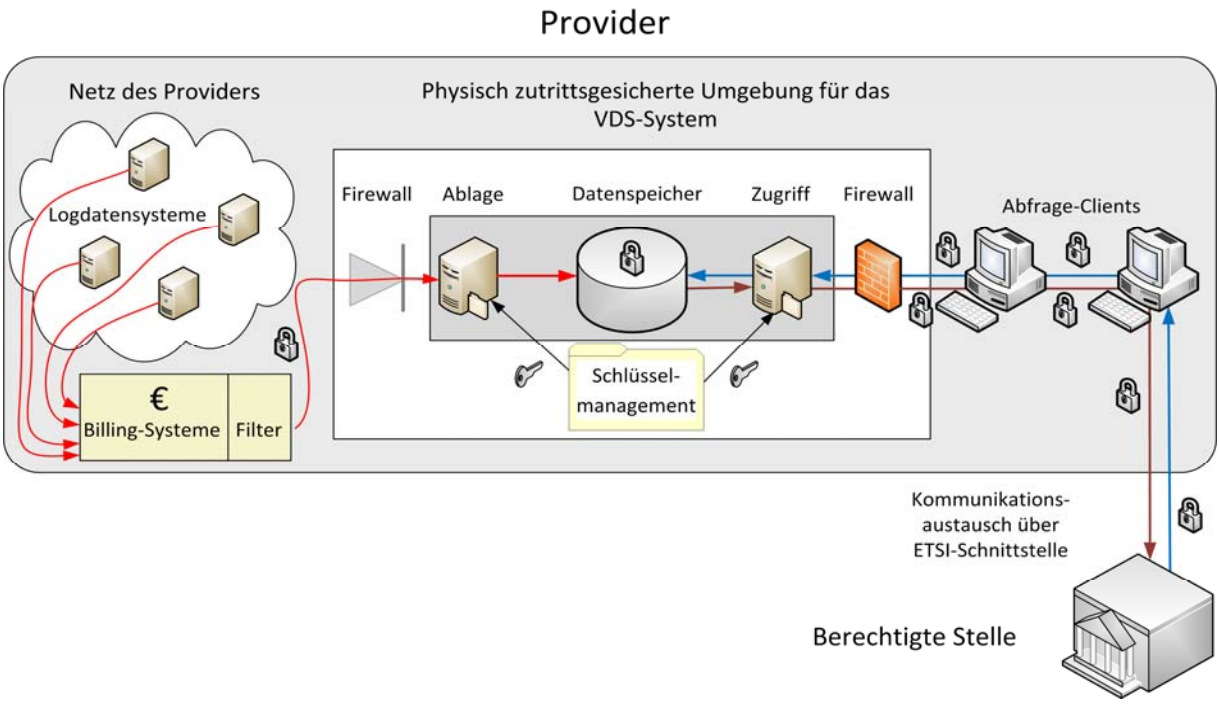


Abbildung: Umsetzungsbeispiel der VDS-Grundarchitektur.

Der Verpflichtete extrahiert die nach Gesetz zu speichernden Verkehrsdaten aus der Summe der durch die Netzelemente bereitgestellten Daten und speichert diese automatisch in der zentralen Speicherinfrastruktur, z.B. einer redundant ausgelegten Datenbank.

Zur Entkopplung vom Internet ist ein manuelles Verfahren aufgrund der zu erwartenden großen Datenmengen in der Regel nicht praktikabel und würde zusätzliche Sicherheitsprobleme hervorrufen.

Die zentrale Speicherinfrastruktur (Ablage, Datenspeicher und Zugriff) muss gegen unberechtigten Zugriff nach Stand der Technik abgesichert sein. Dazu benötigt man u.a. eine Firewallinfrastruktur, die den unberechtigten Zugriff von außen wirkungsvoll unterbindet, für die zu speichernden Daten sowie die Abfragen der berechtigten Stellen aber durchlässig ist.

Das Filtersystem ist der Firewallinfrastruktur vor- oder nachgelagert.

Die den Anfragen entsprechenden Daten werden in der Speicherinfrastruktur gesucht und ausgelesen. Dies geschieht über ein dafür vorgesehenes Zugriffssystem. Die Ergebnisse müssen den berechtigten Stellen wiederum auf sicheren Verbindungen übermittelt werden.

Das Beispiel geht davon aus, dass sich alle Komponenten des VDS-Systems im Besitz ein und desselben Verpflichteten befinden. Im Falle von Auslagerungen an Dritte oder der Notwendigkeit des Transports von Daten außerhalb des physisch gesicherten Bereiches ergeben sich weitere umzusetzende Maßnahmen, wie z.B. eine Verschlüsselung auf dem Transportweg. Auch sammeln viele Unternehmen Daten

zunächst in ihren Billing-Systemen, bevor sie in die VDS-Speicherinfrastruktur gelangen. Die hier gezeigte Ablage als Teil der Speicherinfrastruktur übernimmt auch die Rolle der Verschlüsselung und verfügt daher über einen Anschluss an das Schlüsselmanagement.

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

Die Speicherung der Verkehrsdaten muss nach § 113d TKG so realisiert werden, dass die Vertraulichkeit der Verkehrsdaten in der Speichereinrichtung sichergestellt ist. Dazu dürfen die Daten 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) 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 Beauskunftung zulässig und sollte deshalb im Zugriffssystem lokalisiert sein, vorzugsweise in einer eigenen Komponente. Danach können die Abfrageergebnisse im Zugriffssystem entweder unverschlüsselt im RAM oder verschlüsselt im persistenten Speicher zwischengespeichert 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 (siehe Abschnitt 5.2.6.1) möglich sein.

Ein wesentlicher Bestandteil der technischen Realisierung der gemäß § 113b TKG geforderten irreversiblen Löschung von Verkehrsdaten ist die Löschung der zur Verschlüsselung der Verkehrsdaten verwendeten Schlüssel (siehe Abschnitt 5.2.5). Um die gesetzlich geforderten Löschfristen für Verkehrsdaten einhalten zu können, müssen deshalb auch die Schlüssel fristgerecht gelöscht werden. 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 wieder die Empfehlungen aus BSI-TR-02102-1 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 flüchtigen Speicher (RAM) zu halten, wobei für den Fall eines Stromausfalls eine unabhängige Sicherung der Schlüssel unbedingt nötig ist.

Für die verwendeten Schlüssel 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 Protokollierung aller Backup-Maßnahmen vorzusehen.

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

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

Die Verkehrsdaten nach § 113b TKG müssen auf physisch gesonderten Speichereinrichtungen gespeichert werden, die von den üblichen für betriebliche Aufgaben genutzten Speichereinrichtungen getrennt sind.

Im Datenspeicher des VDS-Systems, auch in einer virtuellen Umsetzung, 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 Daten mit sonstigen Daten ist aus Gründen 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 mit der Verarbeitung und Speicherung der Daten 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 Sicherheits-Updates müssen zeitnah eingespielt werden.

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

Um die Verkehrsdaten vor dem Zugriff aus dem Internet, vor dem Verlust der Vertraulichkeit, Integrität und Authentizität zu schützen, ist eine Entkopplung der Speicherung vom Internet herzustellen.

Diese Entkopplung ließe sich realisieren, indem der Datenspeicher physisch von den Internet-Systemen getrennt wird. Jedoch fallen die zu speichernden Verkehrsdaten gerade an den Systemen an, die die öffentlichen TK-Netze (und damit auch das Internet) aufspannen, oder sind mit diesen direkt oder indirekt verbunden. Die zu speichernden Daten müssten folglich bei einer physischen Trennung manuell in den Datenspeicher übertragen werden, was in der Regel aufgrund der zu erwartenden Menge nicht praktikabel ist. Die empfohlene Lösung, um den Datenspeicher vom Internet (bzw. von den öffentlichen TK-Netzen) zu entkoppeln, ist der Einsatz einer geeigneten Firewallinfrastruktur. Diese Firewallinfrastruktur muss so beschaffen sein, dass ausschließlich dafür vorgesehene berechtigte Systeme Daten 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 Firewallszenarien ist darauf zu achten, dass ein Verbindungsaufbau nur aus dem zu schützenden Bereich initiiert werden darf. Niemals darf eine Verbindung von außen über die ausgewählte mit Proxy-Eigenschaften ausgestattete Firewall hinweg in den zu schützenden Bereich initiiert werden. Es dürfen somit keine Dienste nach außen angeboten werden. Es müssen ausreichend detaillierte Firewalllogs für drei Monate vorgehalten werden. Der Detaillierungsgrad muss so gewählt werden, dass mögliche Vorfälle im genauen zeitlichen Verlauf nachvollziehbar sind. Die Logs sind regelmäßig auf Auffälligkeiten hin zu untersuchen.

Um die Anfragen der berechtigten Stellen durch ermächtigte Mitarbeiter des Verpflichteten bearbeiten zu können, muss im Vier-Augen-Prinzip ein kontrollierter Zugriff auf den Datenspeicher erfolgen können. Ein Zugriffssystem muss somit die Daten entschlüsseln und entsprechend den Anfragen den Datenspeicher durchsuchen können. Die ermächtigten Mitarbeiter müssen aus ihrem Netz verschlüsselt auf das Zugriffssystem zugreifen können. Um Missbrauch auszuschließen, muss auch das Zugriffssystem durch eine Firewall, die mindestens IP-Adress- und

Portnummernbereiche filtert, geschützt werden, wenn mehr als nur die hierfür vorgesehenen Abfrage-Clients am internen Netz angeschaltet sind. Diese Firewall muss so konfiguriert sein, dass ein Zugriff durch die Firewall hindurch nur von autorisierten Abfrage-Clients erlaubt ist. Die Abfrageergebnisse dürfen durch die Firewall hindurch wiederum nur an autorisierte Clients verschlüsselt gesendet werden können. Weitere Dienste dürfen nach außen nicht angeboten werden. Auch auf dieser Firewall müssen ausreichend detaillierte Firewalllogs für drei Monate vorgehalten werden. Der Detaillierungsgrad muss so gewählt werden, dass Vorfälle im genauen zeitlichen Verlauf nachvollziehbar sind. Die Logs sind regelmäßig auf Auffälligkeiten hin zu untersuchen.

Die ermächtigten Personen müssen sich mit individuellen Benutzerkennungen am Abfrage-Client authentisieren. Die auf der Firewall autorisierten Clients sind nach Stand der Technik abzusichern. Die Absicherung muss im Sicherheitskonzept dargestellt werden.

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

5.2.5 Umsetzung der Löschung von Verkehrsdaten gemäß § 113b Abs. 8 TKG

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

Die gesetzliche Forderung nach einer irreversiblen Löschung der Verkehrsdaten muss also technisch realisiert werden durch die Löschung der zur verschlüsselten Ablage der Verkehrsdaten (siehe Abschnitt 5.2.2) verwendeten Schlüssel. 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), Vernichtung von Schlüsselobjekten (RAM) oder mechanische Vernichtung 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 mechanische Vernichtung im Vier-Augen-Prinzip notwendig. Die mechanische Zerstörung ist mit Datum, Uhrzeit, Namen und Unterschrift der Mitarbeiter zu protokollieren.

Das verwendete Vernichtungsverfahren muss entsprechend dem hohen Schutzbedarf der Verkehrsdaten geeignet gewählt werden. Vorgaben dazu finden sich z.B. in den BSI-Grundschutz-Katalogen.

Die bei der Verarbeitung von Suchanfragen im Zugriffssystem anfallenden Klardaten (Schlüssel, entschlüsselte Verkehrsdaten und andere temporäre Daten) sind direkt nach Verwendung aus dem RAM des Zugriffssystems zu löschen. 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 Nr. 4 TKG

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

5.2.6.1 Rollenkonzept

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

- Zum einen gibt es ermächtigte Mitarbeiter, die Anfragen berechtigter Stellen entgegen nehmen, 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 zu geschehen. Alle Tätigkeiten werden lückenlos und revisionssicher protokolliert.

- Zum anderen gibt es ermächtigte Mitarbeiter, die für die hardware- und softwaretechnische Wartung des VDS-Systems zuständig sind. Ein Zugang darf auch hierbei nur im Vier-Augen-Prinzip erfolgen. Für verschiedene administrative Tätigkeiten (z.B. Kryptomanagement, Firewallkonfiguration, 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 unberechtigterweise Zutritt zu den Systemen im physisch gesicherten Bereich, muss automatisch ein Alarm ausgelöst werden, der durch hierfür bestimmte Personen sofort verfolgt wird. Abfrageclients, die zur Bearbeitung der Anfragen berechtigter Stellen eingesetzt werden, müssen in verschließbaren Räumen aufgestellt und besonders zugriffsgeschützt sein.

Für den Fall, dass ein Verpflichteter einen Dritten mit Aufbau und Betrieb des VDS-Systems beauftragt, muss der Verpflichtete mittels vertraglicher Regelungen dafür Sorge tragen, dass nur durch ihn besonders ermächtigte Mitarbeiter des Auftragnehmers zum Einsatz kommen. Der Verpflichtete hat dies regelmäßig zu überprüfen. Kontrollen durch die BNetzA und die BfDI müssen im gesetzlichen Umfang möglich sein.

5.2.6.2 Physische Absicherung der Speichereinrichtung

Bei der Planung und beim Betrieb der Speichereinrichtungen ist auf eine hinreichende physische Sicherheit zu achten. Insbesondere der Teil des Rechenzentrums, in dem die Hardware-Komponenten des VDS-Systems 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 VDS-Systems müssen vor unbefugtem Zutritt durch hochwertige Zutrittskontrollmechanismen geschützt werden. Bei unberechtigtem Zutritt muss ein Alarm ausgelöst werden, der durch entsprechendes Sicherheitspersonal sofort verfolgt wird.
Alle Clients, die zur Beauskunftung oder Wartungszwecken eingesetzt werden (z.B. Management-Konsole), müssen physisch gegen den Zugriff durch nicht ermächtigte Personen geschützt sein.
Die Vergabe und Rücknahme von Zutrittsberechtigungen ist zu dokumentieren. Zur Überwachung der Zutrittsberechtigung können Personen (Pförtner, Schließdienst, Sicherheitspersonal) oder technische Einrichtungen (Ausweisleser, biometrische Verfahren wie Irisscanner oder Fingerabdruck, Sicherheitstürschloss bzw. Schließanlage) eingesetzt werden.

Der Zugang zum VDS-System zu Wartungszwecken darf erst nach einer Identifikation und einer Zwei-Faktor-Authentisierung unter Anwendung des Vier-Augen-Prinzips möglich sein. Die Ausgabe bzw. der Entzug von Zugangsmitteln wie Benutzer-Kennungen oder Chipkarten ist zu dokumentieren. Die Authentisierungsvorgänge sowie sämtliche Systemeingaben müssen revisionssicher protokolliert werden. Jeder Protokollierungseintrag sollte Datum, Uhrzeit, Art des Ereignisses, Bezeichnung des Subjektes sowie Erfolg bzw. Misserfolg der Aktion enthalten.

5.2.7 Notwendige Mitwirkung von mindestens zwei Personen beim Zugriff auf die Daten gemäß § 113d Satz 2 Nr. 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 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 bzw. 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 bzw. behördlichen Ersuchen feststellen und die Anfrage bei Abweichungen zur Korrektur an die Behörde 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 bzw. behördlichen Ersuchen umfassten übereinstimmen. Sollte das nicht der Fall sein, muss die erste Person hierüber informiert und die Abfrage von dieser erneut initiiert werden.

Werden die notwendigen technischen Abfrageparameter neben der richterlichen Anordnung von der Sicherheitsbehörde 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 Behörde ggf. veränderte Abfrageparameter erfragen.

Werden die technischen Abfrageparameter nicht elektronisch von der Behörde 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 Daten kommt, die nicht vom Eingabebefehl umfasst sind, sind regelmäßig technische Tests unter Einsatz von hierfür im Netz generierten Testdaten (Dummy Data) zur Überprüfung des Systems durchzuführen.

5.2.7.2 Vier-Augen-Prinzip beim betrieblichen Zugriff

Für einen betrieblichen Zugriff (z.B. Wartungsarbeiten am VDS-System), dürfen der physikalische Zugriff auf die Komponenten des VDS-Systems (z.B. zum Austausch von Hardwarekomponenten oder Update der Software) sowie die damit verbundenen Arbeiten nur im Vier-Augen-Prinzip erfolgen (siehe Abschnitt 5.2.6.1), d.h. ein physischer Zugriff auf die Komponenten des VDS-Systems erfolgt nur gemeinsam durch zwei ermächtigte Personen. Die Anforderungen zur physischen Absicherung der zu Wartungszwecken eingesetzten Clients sind in Abschnitt 5.2.6.2 beschrieben.

Im Rahmen dieser Tätigkeiten kann ein ausschließlich lesender Fernzugriff für Dritte (z.B. ein Spezialist der Herstellerfirma) zur Unterstützung der beiden 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 VDS-Systems betrieben werden.
2. Ein schreibender Zugriff für einen Dritten wird wirkungsvoll unterbunden; zur Unterstützung der beiden ermächtigten Personen ist lediglich ein lesender Zugriff erlaubt. Auch das aus der Ferne unterstützende Personal ist zuverlässig und authentisiert. Die 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 Netze sind immer durch eine Transportsicherung (d.h. Transportverschlüsselung mit Integritäts- und Authentizitätsschutz) abgesichert.
4. Das Netz sowie der Client, von dem aus der Fernwartungszugang erfolgt, sind nach IT-Grundschutz abgesichert.
5. Es wird sichergestellt, dass unverschlüsselte Verkehrsdaten und 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 Abs. 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 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 protokolliert werden, die die einzelnen Bearbeitungsschritte enthält.

Die Protokolldaten dürfen keinen Aufschluss über die gelöschten oder verarbeiteten Verkehrsdaten geben und sind in speziell hierfür vorgesehenen, gesicherten Speichereinrichtungen zu speichern. So dürfen Antworten an Sicherheitsbehörden 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 Unternehmen.

6. Quellenverzeichnis

[BSI1] Bundesamt für Sicherheit in der Informationstechnik: Managementsysteme für Informationssicherheit (ISMS), BSI-Standard 100-1, Version 1.5, Mai 2008, www.bsi.bund.de

[BSI2] Bundesamt für Sicherheit in der Informationstechnik: IT-Grundschutz-Vorgehensweise, BSI-Standard 100-2, Version 2.0, Mai 2008, www.bsi.bund.de

[BSI3] Bundesamt für Sicherheit in der Informationstechnik: Risikoanalyse auf der Basis von IT-Grundschutz, BSI-Standard 100-3, Version 2.5, Mai 2008, www.bsi.bund.de

[BSI4] Bundesamt für Sicherheit in der Informationstechnik: Notfallmanagement, BSI-Standard 100-4, Version 1.0, November 2008, www.bsi.bund.de

[BSI5] Bundesamt für Sicherheit in der Informationstechnik: BSI-IT-Grundschutz-Katalog

[BSI6] Technische Richtlinie BSI TR-02102 Kryptographische Verfahren: Empfehlungen und Schlüssellängen

Anlage

Sicherheitskonzept (§ 113g)

Der nach § 113a TKG Verpflichtete hat der Bundesnetzagentur das Sicherheitskonzept nach § 113g TKG unverzüglich nach Beginn der Speicherung und erneut bei jeder Änderung vorzulegen.

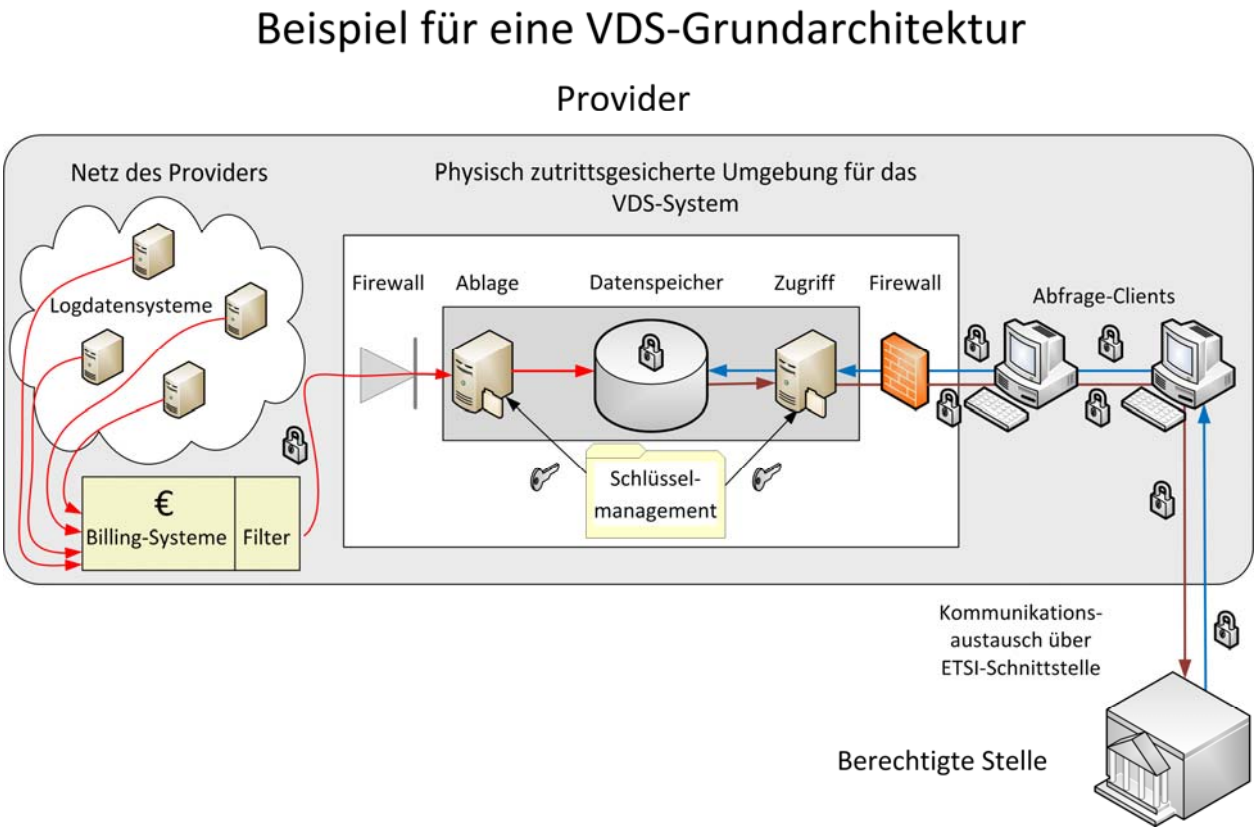
Hierzu wird empfohlen, das Sicherheitskonzept nach § 109 Abs. 4 TKG um einen inhaltlich geschlossenen, spezifischen Teil nach § 113g TKG (z.B. „Sicherheitskonzept technischer Vorkehrungen und sonstiger Maßnahmen für Speicherpflichten und Höchstspeicherfristen für Verkehrsdaten nach § 113g TKG“) zu erweitern, um darin die Schutzmaßnahmen zur Sicherstellung der besonders hohen Anforderungen nach Kapitel 4 und 5 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 Abs. 4 TKG zu dokumentieren. Zur Vorgehensweise wird auf den Katalog von Sicherheitsanforderungen nach § 109 Abs. 6 TKG und auf einschlägige Beschreibungen zum BSI- Grundschutz verwiesen.

Die Maßnahmen zur Realisierung der besonders hohen Anforderungen nach Kapitel 4 und 5 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, Zugriff (Schnittstelle zu Abfrage- und Freigabeclient,) zu bilden und entsprechend im Sicherheitskonzept sowohl grafisch als auch schriftlich zu beschreiben.



2. Zuordnung der besonders hohen Anforderungen (Abschnitt 4 und 5)

2.1 Zuordnung von Gefährdungen

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.

2.2 Zuordnung der Schutzmaßnahmen nach Abschnitt 4 und 5 zu Sicherheitsteilsystemen

Die zu treffenden Schutzmaßnahmen zur Erfüllung der gesetzlichen Anforderungen entsprechend Abschnitt 4 und 5 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 Abs. 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.