Kassenärztliche Bundesvereinigung
Körperschaft des öffentlichen Rechts

Sicheres Netz der KVen

Richtlinie KV-Apps

[KBV_SNK_RLEX_KV-Apps]

Dezernat 6 – Informationstechnik, Telematik und Telemedizin

10623 Berlin, Herbert-Lewin-Platz 2

Kassenärztliche Bundesvereinigung

Version 3.0
Datum: 13.12.2012
Klassifizierung: Öffentlich
Status: In Kraft

DOKUMENTENHISTORIE

Version	Datum	Autor	Änderung	Begründung	Seite
3.0	13.12.2012	KBV	Einarbeitung von Kommentaren aus dem KV-Kommentierungsverfahren.		
3.0 Beta	20.11.2012	KBV	Neustrukturierung und Ergänzungen	ISMS, Regelungen für verschiedene Anforderungen	
2.1	31.03.2011	KBV	Vereinheitlichung der Begriffe und des Dokumentenlayouts	Maßgaben der Dokumentenlenkung	
2.0	27.01.2010	KBV			

INHALTSVERZEICHNIS

ABBILDUNGSVERZEICHNIS

1 Präambel

1.1 Das *Sichere Netz der KVen*

Die Kassenärztliche Bundesvereinigung und die Kassenärztlichen Vereinigungen haben eine Online-Infrastruktur aufgebaut, die den hohen Anforderungen an Datenschutz und Datensicherheit Rechnung trägt und die u.a. für die Übermittlung von Patienten- und Honorardaten geeignet ist – das *Sichere Netz der KVen*.

Informationssicherheit im *Sicheren Netz der KVen* ist eines der wichtigsten Ziele aller Beteiligten. Von besonderer Bedeutung ist dabei der Schutz der Sozialdaten und weiterer personenbezogener Daten. Für diese und andere Informationen und Werte werden im Rahmen des Sicherheitsmanagements Schutzziele definiert. Im Mittelpunkt dabei stehen die Sicherung der Vertraulichkeit, die Gewährleistung der Integrität und die Aufrechterhaltung der Verfügbarkeit. Zur Einhaltung dieser Ziele trifft die KBV regulatorische Maßgaben in Form von Richtliniendokumenten und Zertifizierungen. Die Umsetzung obliegt allen Beteiligten.

Die Rechenzentren der Kassenärztlichen Vereinigungen (KVen) und der Kassenärztlichen Bundesvereinigung (KBV) sind hierzu über den KV-Backbone, einem logisch vom Internet getrennten Netzwerk, miteinander verbunden. Die KBV ist der Betreiber des KV-Backbones.

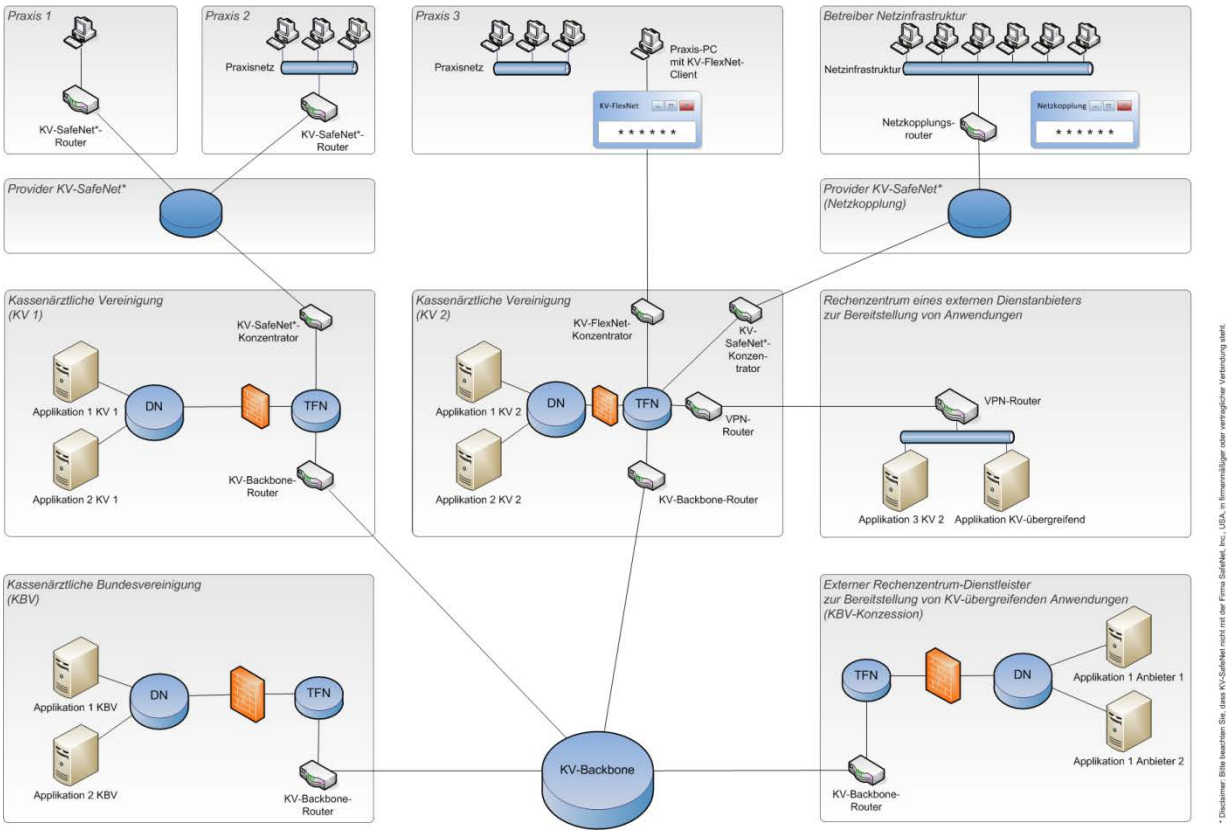

Abbildung 1: Beispielhafte Netztopologie

Teilnehmer am *Sicheren Netz der KVen* sind die Mitglieder der Kassenärztlichen Vereinigungen, also Vertragsärzte und –psychotherapeuten oder ein anderer nach den Richtlinien der KBV zugelassener Teilnehmer des *Sicheren Netzes der KVen*. Ihnen werden sichere Zu-

gangswege zu den Diensten und Anwendungen bereitgestellt. Die Anbindung der Teilnehmer an das *Sichere Netz der KVen* erfolgt mittels einer VPN-Verbindung. Es gibt hierbei zwei Möglichkeiten der sicheren Anbindung, einerseits über das KV-SafeNet*, einem Hardware-VPN und andererseits über das KV-FlexNet[1] einem Software-VPN. Die Bereitstellung eines Zugangs über die Variante KV-FlexNet liegt in der Hoheit der jeweiligen KV. Beide Zugangsvarianten ermöglichen eine sichere Anbindung an das *Sichere Netz der KVen*.

Der Anschluss von Teilnehmern aus bereits in sich abgesicherten gesundheitsmedizinischen Netzinfrastrukturen an das *Sichere Netz der KVen* erfolgt mittels KV-SafeNet (Netzkopplung). Diese gesicherte Anbindung basiert auf der Zugangsvariante KV-SafeNet und erweitert diese um einen Authentisierungsdienst.

Im *Sicheren Netz der KVen* werden den Teilnehmern von den KVen und der KBV Dienste und Anwendungen zur Verfügung gestellt, die mit dem Begriff Applikationen (oder auch KV-Apps) zusammengefasst werden. Es besteht auch für KV-fremde Dienstanbieter die Möglichkeit, Dienste anzubieten, Voraussetzung hierfür ist eine Zertifizierung der betreffenden Applikation durch die KBV.

Der Anschluss mittels KV-SafeNet erfolgt durch einen von der KBV zertifizierten Provider. Dieser stellt einem Teilnehmer alle technischen Voraussetzungen zur Anbindung an das *Sichere Netz der KVen* mittels einer Hardware-VPN-Lösung zur Verfügung und garantiert für die Sicherheit dieser Verbindung. Der Provider stellt dem Teilnehmer hierzu einen KV-SafeNet-Router zur Verfügung.

Beim Anschluss eines Teilnehmers über KV-FlexNet stellt die jeweilige KV des Teilnehmers eine von der KBV zugelassene Software-VPN-Lösung zur Verfügung und garantiert für die Sicherheit der Verbindung.

1.2 Ziel des Dokuments

Applikationen im *Sicheren Netz der KVen* müssen hohen Anforderungen an Datenschutz und Datensicherheit Rechnung tragen.

Diese Richtlinie definiert die Anforderungen an

- den Anbieter der Applikation,
- die Applikation und
- den Betrieb und die Betriebsumgebung der Applikation,

sowie den Prozess der Zertifizierung bzw. Registrierung von Applikationen im *Sicheren Netz der KVen*.

1.3 Klassifizierung und Adressaten des Dokuments

Dieses Dokument ist öffentlich zu verwenden. Es richtet sich an alle am *Sicheren Netz der KVen* beteiligten Akteure, insbesondere an Applikationsanbieter.

* Disclaimer: Bitte beachten Sie, dass KV-SafeNet nicht mit der Firma SafeNet, Inc., USA, in firmenmäßiger oder vertraglicher Verbindung steht.
[1] In der jeweiligen KV kann diese Lösung auch einen anderen Namen haben.

2 Gültigkeit, Anwendungsbereich und Abgrenzung

Ein Applikationsanbieter ist die Organisation, welche eine Applikation anbietet und für den Betrieb der Applikation im *Sicheren Netz der KVen* verantwortlich ist. Die vorliegende Richtlinie unterscheidet bei Applikationen zwischen

- Applikationen, welche von KVen und/oder KBV (KV-System) bereitgestellt werden und
- Applikationen, welche von KV-fremden Anbietern von Applikationen, sogenannten *externen Applikationsanbietern*, bereitgestellt werden.

Die Richtlinie KV-Apps ist gültig für Bereitstellung von Applikationen im *Sicheren Netz der KVen* durch KVen, die KBV oder externe Applikationsanbieter.

Applikationen, die im *Sicheren Netz der KVen* bereitgestellt und betrieben werden sollen, müssen entsprechend den Maßgaben dieser Richtlinie zertifiziert bzw. registriert werden.

Es ist nicht erlaubt, eine Applikation im *Sicheren Netz der KVen* ohne erfolgte Zertifizierung oder Registrierung zu betreiben. Die KBV behält sich vor, den Betrieb einer nicht zertifizierten bzw. nicht registrierten Applikation zu verbieten.

Mit Inkrafttreten dieses Dokumentes ist die Zertifizierung oder Registrierung von Applikationen für den Betrieb im *Sicheren Netz der KVen* ausschließlich nach den Maßgaben dieser Richtlinie zulässig.

Bereits in Betrieb befindliche Applikationen ohne Zertifizierung bzw. Registrierung müssen unverzüglich konform zu dieser Richtlinie zertifiziert bzw. registriert werden.

Die Richtlinie KV-Apps regelt nicht die Bereitstellung von Applikationen außerhalb des *Sicheren Netzes der KVen*, z. B. dem Internet, kann aber als dringende Empfehlung für diesen Bereich durch Applikationsanbieter angewendet werden.

3 Grundlegendes Vorgehen und Verantwortlichkeiten

Diese Richtlinie unterscheidet grundsätzlich zwischen dem Prozess der Zertifizierung und dem Prozess der Registrierung einer Applikation.

Im Zertifizierungsverfahren (siehe Abschnitt 4) wird durch die KBV geprüft, ob die Applikation, der Applikationsanbieter und die Betriebsumgebung den Maßgaben dieser Richtlinie entsprechen. Die KBV erteilt bei Erfolg das entsprechende Zertifikat.

Im Registrierungsverfahren (siehe Abschnitt 5) wird durch eine KV geprüft, ob die Applikation, der Applikationsanbieter und die Betriebsumgebung den Maßgaben dieser Richtlinie entsprechen. Die KV registriert die Applikation anschließend bei der KBV.

Die Festlegung, ob für eine Applikation eine Zertifizierung oder eine Registrierung erfolgen muss, ist vorrangig abhängig von der geplanten Nutzergruppe der Applikation und dem Applikationsanbieter.

Bei der Nutzergruppe der Applikation ist zu unterscheiden zwischen *regionalen* und *übergreifenden* Applikationen. Eine Applikation, die ausschließlich für die Nutzer einer einzigen KV angeboten wird, wird *regionale Applikation* genannt. Eine Applikation, die für Nutzer aus mehr als einem KV-Gebiet angeboten wird, wird *übergreifende Applikation* genannt.

Sowohl KVen/KBV als auch externe Applikationsanbieter können regionale oder übergreifende Applikationen im *Sicheren Netz der KVen* bereitstellen.

Will ein Anbieter mehrere Applikationen im *Sicheren Netz der KVen* bereitstellen, so hat er dafür auch mehrere Zertifizierungs- bzw. Registrierungsverfahren zu durchlaufen.

Die verschiedenen Möglichkeiten der Bereitstellung von Applikationen und die Festlegung, ob im jeweiligen Fall eine Zertifizierung oder eine Registrierung durchzuführen ist, wird in den folgenden Abschnitten beschrieben.

3.1.1 Bereitstellung einer regionalen Applikation durch eine KV/KBV

Regionale Applikationen, die durch eine KV oder die KBV bereitgestellt werden, bedürfen einer Registrierung gemäß Abschnitt 5.

Die betreffende KV als Applikationsanbieter registriert die Applikation bei der KBV.

3.1.2 Bereitstellung einer übergreifenden Applikation durch KVen/KBV

Übergreifende Applikationen, die durch eine KV oder die KBV bereitgestellt werden, bedürfen einer Zertifizierung gemäß Abschnitt 4.

Die betreffende KV als Applikationsanbieter zertifiziert die Applikation bei der KBV.

3.1.3 Bereitstellung einer regionalen Applikation durch einen externen Anbieter

Regionale Applikationen, die durch einen externen Anbieter bereitgestellt werden, bedürfen einer Registrierung gemäß Abschnitt 5. Die betreffende KV überprüft die Einhaltung der Maßgaben dieser Richtlinie und registriert die Applikation bei der KBV.

3.1.4 Bereitstellung einer übergreifenden Applikation durch einen externen Anbieter

Übergreifende Applikationen, die durch einen externen Applikationsanbieter bereitgestellt werden, bedürfen einer Zertifizierung gemäß Abschnitt 4.

Der externe Applikationsanbieter zertifiziert die Applikation bei der KBV.

Weiterhin ist grundsätzlich zu beachten, dass Applikationsanbieter im *Sicheren Netz der KVen* nur durch die KBV zugelassene Arten von übergreifend angebotenen Applikationen bereitstellen dürfen, siehe hierzu auch Abschnitt 4.1 „Voraussetzungen für die Zertifizierung“.

3.1.5 Bereitstellung von Applikationen des *Sicheren Netzes der KVen* für Nutzer aus anderen Netzen

Applikationen können aus verschiedenen Gründen die Notwendigkeit haben, sowohl für Teilnehmer aus dem *Sicheren Netz der KVen*, als auch gleichzeitig für Nutzer aus anderen Netzen, z.B. dem Internet, bereitgestellt zu werden.

Hierbei sind erhöhte Anforderungen an Datenschutz und Datensicherheit einzuhalten. Insbesondere sind die Applikation, die Betriebsumgebung der Applikation und das *Sichere Netz der KVen* gegen unbefugte Zugriffe abzusichern. Die Anforderungen des Abschnitts 7.4.7 sind zwingend zu beachten und deren Einhaltung nachzuweisen.

3.1.6 Gesamtverantwortung für das *Sichere Netz der KVen*

Die KBV hat die Gesamtverantwortung für das *Sichere Netz der KVen*. Die KBV behält sich daher vor, den Betrieb von Applikationen, die die Maßgaben dieser Richtlinie verletzen oder die Sicherheit und Nutzbarkeit des *Sicheren Netzes der KVen* einschränken oder gefährden, zu untersagen und das Zertifikat bzw. die Registrierung zu entziehen (Abschnitt 4.12 und 5.7).

4 Zertifikat

Eine übergreifende Applikation im *Sicheren Netz der KVen*, d.h. eine Applikation, die von einer KV, der KBV oder einem externen Applikationsanbieter für Nutzer aus mehr als einem KV-Gebiet angeboten werden soll, muss durch die KBV zertifiziert werden.

Im Rahmen der Zertifizierung wird die Konformität der Applikation, des Applikationsanbieters und der Betriebsumgebung der Applikation gemäß den Maßgaben dieser Richtlinie überprüft.

Das Zertifikat bescheinigt dem Anbieter, dass seine Applikation den Bestimmungen dieser Richtlinie genügt.

Das grundlegende Vorgehen und die Festlegung, in welchen Fällen eine Zertifizierung durchgeführt werden muss, ist im Abschnitt 3 erläutert.

Die nachfolgenden Abschnitte regeln den Prozess, um eine Zertifizierung zu erlangen und aufrechtzuerhalten.

4.1 Voraussetzungen für die Zertifizierung

Die zu zertifizierende Applikation muss einen erhöhten Schutzbedarf haben, z.B. aufgrund der Verarbeitung von sensiblen und schützenswerten Daten wie medizinischen Falldaten, und einem gesundheitsmedizinischen Zweck dienen.

Voraussetzung für die Einleitung des Zertifizierungsverfahrens für eine Applikation ist die grundlegende Zulassung der betreffenden Applikationsart durch den Vorstand der KBV.

Der Applikationsanbieter erklärt vor Einleitung des Zertifizierungsverfahrens der KBV die Absicht, eine Applikation im *Sicheren Netz der KVen* bereitstellen zu wollen. Der Applikationsanbieter beschreibt in Kurzform den Zweck und den technischen Aufbau der Applikation, insbesondere eine Auflistung der zur Verfügung gestellten Funktionalitäten.

Die KBV prüft die Absichtserklärung des Applikationsanbieters bzgl. Konformität der geplanten Applikationsart mit den vom Vorstand der KBV zugelassenen Applikationsarten und erteilt die Zustimmung zur Einleitung des Zertifizierungsverfahrens (Abschnitt 4.2) oder die Ablehnung.

4.2 Zertifizierung

Wenn die Voraussetzungen für die Zertifizierung aus dem Abschnitt 4.1 erfüllt sind, kann der Anbieter das Zertifizierungsverfahren durch das Einreichen der Ergänzenden Erklärung [KBV_SNK_FOEX_EE_KV-Apps] einleiten. Mit dem Antrag auf eine Zertifizierung verpflichtet sich der Anbieter zur Einhaltung dieser Richtlinie.

Der Applikationsanbieter muss im Rahmen der Zertifizierung nachweisen, dass die Anforderungen an die Applikation, den Applikationsanbieter und die Betriebsumgebung gemäß dieser Richtlinie erfüllt sind. Der Applikationsanbieter muss hierzu alle zur Zertifizierung notwendigen Unterlagen vollständig zusammen mit der Ergänzenden Erklärung einreichen.

Die Zertifizierung erfolgt durch die KBV anhand des Dokuments [KBV_SNK_LFEX_Zert_KV-Apps]. Die Kosten der Zertifizierung trägt der Anbieter. Die Zertifizierung der Applikation wird von allen, am *Sicheren Netz der KVen* beteiligten KVen, anerkannt.

4.3 Durchführung der Zertifizierung

Grundsätzlich überprüft und zertifiziert die KBV die Applikation, den Applikationsanbieter und die Betriebsumgebung auf Einhaltung der Maßgaben dieser Richtlinie und dem Leitfaden zur Zertifizierung von Applikationen [KBV_SNK_LFEX_Zert_KV-Apps].

Die Anforderungen und Maßgaben sind in dieser Richtlinie aufgeführt, unterteilt in

- Anforderungen an die Applikation (Abschnitt 7),
- Anforderungen an den Applikationsanbieter (Abschnitt 8) und
- Anforderungen an die Betriebsumgebung (Abschnitt 9).

Im Rahmen der Zertifizierung überprüft die KBV u.a.

- die durch den Applikationsanbieter eingereichten Dokumente,
- die Betriebsumgebung, in der die Applikation betrieben werden soll, bzw. deren Anbindung,
- den Applikationsanbieter, insbesondere die Prozesse des Informationssicherheitsmanagements des Applikationsanbieters und
- die Sicherheit der Applikation in der jeweiligen Betriebsumgebung.

Die (Re-)Zertifizierung muss grundsätzlich innerhalb des Zeitraumes von sechs Monaten erfolgreich abgeschlossen sein. Bei Überschreitung des Zeitraumes wird die (Re-)Zertifizierung abgebrochen.

Innerhalb des (Re-)Zertifizierungsprozesses hat der Antragsteller maximal vier Wochen nach Benachrichtigung durch die Prüfstelle Zeit, fehlende bzw. nachzubessernde Unterlagen einzureichen. Fristverlängerungen werden in Einzelfällen gewährt. Werden die erforderlichen Unterlagen nicht eingereicht, so wird das (Re-)Zertifizierungsverfahren abgebrochen.

Der Abbruch des (Re-)Zertifizierungsverfahrens durch eigenes Verschulden entbindet den Antragsteller nicht von der Pflicht, die (Re-)Zertifizierungspauschale zu bezahlen. Dem Antragsteller steht frei, nach Abbruch des (Re-)Zertifizierungsverfahrens, eine erneute Beantragung zur Zertifizierung durchzuführen.

4.4 Bereitstellung von Testzugängen

Der Anbieter hat der KBV mindestens einen Testzugang für die Applikation bereitzustellen. Dieser Zugang muss wenigstens für die Laufzeit des Zertifizierungsverfahrens bereitgestellt werden. Die Testzugänge müssen den gleichen Funktionsumfang bereitstellen, der auch dem Anwender zur Verfügung steht.

4.5 Erteilung des Zertifikats

Die KBV erteilt das Zertifikat für den Betrieb der Applikation im *Sicheren Netz der KVen* nach erfolgreichem Abschluss der Prüfung der Umsetzung der Maßgaben dieser Richtlinie.

Nach Erteilung des Zertifikates werden die technisch notwendigen Schritte umgesetzt, u. a. die Einrichtung des DNS Eintrags, ggf. Aufnahme in das Monitoring und Verlinkung auf http://portal.kv-safenet.de, usw.

4.6 Laufzeit

Ein ausgestelltes Zertifikat erlischt nach drei Jahren und muss vom Anbieter neu beantragt werden. Der Prozess der Rezertifizierung ist in Abschnitt 4.11 beschrieben.

4.7 Überprüfung während der Zertifikatslaufzeit

Die KBV behält sich das Recht vor, die Einhaltung aller Maßgaben dieser Richtlinie durch den Anbieter in regelmäßigen Abständen durch eine zur Verschwiegenheit verpflichtete und von der KBV zu bestimmende Person überprüfen zu lassen. Diese Person ist von der KBV und dem Anbieter dazu berechtigt und verpflichtet, der KBV Mitteilung über Verstöße gegen die Anforderungen dieser Richtlinie zu machen. Der Anbieter hat die Verstöße innerhalb eines von der KBV zu bestimmenden, angemessenen Zeitraums zu beseitigen.

Die Kosten der Überprüfungen trägt der Anbieter.

Die folgenden Überprüfungsmaßnahmen können einmal im Rahmen der Zertifikatslaufzeit, frühestens mit Beginn des zweiten Jahres, nach den Maßgaben der KBV durchgeführt werden:

- Auditierung
  Es werden Überprüfungen der Einhaltung organisatorischer Maßgaben dieser Richtlinie durchgeführt. Diese Audits beinhalten eine Vor-Ort-Prüfung beim Anbieter sowie eine Prüfung ausgewählter Dokumente.
- Penetrationstest
  Die Applikation wird einer sicherheitstechnischen Überprüfung unterzogen.

4.8 Änderung der Applikation oder der Betriebsumgebung

Die Zertifizierung gilt ausschließlich für die Gesamtheit bestehend aus eingereichter Applikation, dem Applikationsanbieter und der Betriebsumgebung.

Plant ein Anbieter Änderungen in einem dieser Bereiche, die Auswirkungen auf die Sicherheit, Verfügbarkeit oder die in dieser Richtlinie definierten Anforderungen haben, so hat der Anbieter vor der praktischen Umsetzung die Prüfstelle entsprechend zu informieren.

Je nach Art um Umfang der Änderung entscheidet die Prüfstelle über eine nähere Prüfung der Änderungen und ggf. auch über die Notwendigkeit einer Rezertifizierung.

Nicht angemeldete Änderungen können dazu führen, dass die Verfügbarkeit der betroffenen Applikation im *Sicheren Netz der KVen* unterbrochen wird.

4.9 Formelle Änderungen nach abgeschlossener Zertifizierung

Nach abgeschlossener Zertifizierung ist der Anbieter verpflichtet, formelle Änderungen unverzüglich (innerhalb von 3 Werktagen) der KBV-Prüfstelle bekannt zu geben.

Zu den formellen Änderungen gehören u.a.

- Änderungen des Softwareverantwortlichen,
- Änderungen der Ansprechpartner für Ärzte und die KBV,
- Umfirmierungen des Applikationsanbieters und
- Applikationsnamens- und Systemnamensänderungen.

Formelle Änderungen müssen der Prüfstelle der KBV in schriftlicher Form angezeigt werden.

4.10 Änderungen der Richtlinie

Bei Änderungen dieser Richtlinie stellt die KBV die jeweils aktuelle Version zur Verfügung und informiert die Anbieter. Einem Anbieter einer bereits zertifizierten Applikation steht es frei, die Applikation schon vor Ablauf des gültigen Zertifikats nach der neuen Richtlinie rezertifizieren zu lassen.

Bestehende Zertifizierungen von Applikationen behalten bis zum Ende der Laufzeit des Zertifikates ihre Gültigkeit.

4.11 Rezertifizierung

Eine Rezertifizierung erfolgt entsprechend den Bestimmungen der zum Zeitpunkt der Rezertifizierung aktuellen Version dieser Richtlinie.

Im Rahmen der Rezertifizierung müssen bis spätestens vier Monate vor Ablauf des derzeit gültigen Zertifikats die Applikation, die Betriebsumgebung und der Applikationsanbieter durch die KBV-Prüfstelle erfolgreich rezertifiziert sein, ansonsten kann die Rezertifizierung aufgrund grob fahrlässiger oder vorsätzlicher Verletzung dieser Vorgaben verweigert werden.

Strebt der Anbieter keine Rezertifizierung an bzw. hat er die Rezertifizierung durch die Einreichung des vollständig ausgefüllten Formulars Ergänzende Erklärung [KBV_SNK_FOEX_KV-Apps] bei der Prüfstelle der KBV nicht mindestens sechs Monate vor Ablauf des Zertifikates beantragt, so muss er dies den Nutzern der Applikation, den KVen und der KBV mit einer Vorlaufzeit von einem halben Jahr mitteilen. Sollte der Anbieter diese Frist nicht einhalten, so hat er für etwaige Kosten, die zum Informieren der Anwender durch die KBV und die KVen entstehen, aufzukommen.

Die Kosten für die Rezertifizierung trägt der Anbieter.

4.12 Entzug des Zertifikats

Im Falle einer grob fahrlässigen oder vorsätzlichen Verletzung von Maßgaben dieser Richtlinie ist die KBV berechtigt, dieses Zertifikat wieder zu entziehen und die Nutzer und KVen über den Entzug der Zertifizierung zu informieren.

Der Betrieb der Applikation ist daraufhin sofort einzustellen.

Die KBV behält sich vor, technische Maßnahmen einzuleiten, um in diesem Fall den Betrieb der Applikation zu unterbinden.

Des Weiteren muss der Anbieter alle Anwender über den Entzug des Zertifikates und die damit verbundene Einstellung des Betriebs der Applikation informieren.

Alle anfallenden Kosten, die im Zusammenhang mit dem Entzug des Zertifikates stehen, hat der Anbieter zu übernehmen.

4.13 Einstellung des Betriebs

Die Einstellung des Betriebs einer Applikation ist dem betroffenen Anwenderkreis und der KBV mindestens ein halbes Jahr im Voraus anzukündigen. Die KBV ist über die Beendigung zu informieren. Anschließend wird die Zertifizierung der Applikation aufgehoben und gebundene Ressourcen freigegeben.

5 Registrierung

Eine regionale Applikation im *Sicheren Netz der KVen*, d.h. eine Applikation, die von einer KV, der KBV oder einem externen Applikationsanbieter für Nutzer aus einem einzigen KV-Gebiet angeboten werden soll, muss bei der KBV registriert werden.

Die Registrierung kann gemäß Abschnitt 3 ausschließlich von einer KV oder der KBV beantragt werden. Applikationen externer Anbieter müssen durch eine KV oder die KBV registriert werden.

Das grundlegende Vorgehen und die Festlegung, in welchen Fällen eine Registrierung durchgeführt werden muss, ist im Abschnitt 3 erläutert.

Die nachfolgenden Abschnitte regeln den Prozess, um eine Registrierung zu erlangen und aufrechtzuerhalten.

Die Registrierung der Applikation wird von allen, am *Sicheren Netz der KVen* beteiligten KVen, anerkannt.

Bei Änderungen dieser Richtlinie stellt die KBV die jeweils aktuelle Version zur Verfügung und informiert die Anbieter.

5.1 Durchführung der Registrierung

Im Rahmen der Registrierung prüft die zuständige KV die Konformität der Applikation, des Applikationsanbieters und der Betriebsumgebung der Applikation gemäß den Maßgaben dieser Richtlinie. Die zuständige KV verpflichtet sich zur Einhaltung dieser Richtlinie und bestätigt die Konformität durch Einreichung des Registrierungsformulars und der geforderten Eigenerklärungen bei der KBV.

5.2 Änderung der Applikation oder der Betriebsumgebung

Die Registrierung gilt ausschließlich für die Gesamtheit bestehend aus eingereichter Applikation, dem Applikationsanbieter und der Betriebsumgebung.

Plant ein Anbieter Änderungen in einem dieser Bereiche, die Auswirkungen auf die Sicherheit, Verfügbarkeit oder die im Anhang definierten Anforderungen haben, so hat der Anbieter vor der praktischen Umsetzung die Prüfstelle entsprechend zu informieren.

Je nach Art und Umfang der Änderung entscheidet die Prüfstelle über eine nähere Prüfung der Änderungen und ggf. auch über die Notwendigkeit einer Re-Registrierung.

Nicht angemeldete Änderungen können dazu führen, dass die Verfügbarkeit der betroffenen Applikation im *Sicheren Netz der KVen* unterbrochen wird.

5.3 Formelle Änderungen nach abgeschlossener Registrierung

Nach abgeschlossener Registrierung ist der Anbieter verpflichtet, formelle Änderungen unverzüglich (innerhalb von 3 Werktagen) der KBV-Prüfstelle bekannt zu geben.

Zu den formellen Änderungen gehören u.a.

- Änderungen des Softwareverantwortlichen,
- Änderungen der Ansprechpartner für Ärzte und die KBV,
- Umfirmierungen des Applikationsanbieters und
- Applikationsnamens- und Systemnamensänderungen.

Formelle Änderungen müssen der Prüfstelle der KBV in schriftlicher Form angezeigt werden.

5.4 Entzug der Registrierung

Im Falle einer grob fahrlässigen oder vorsätzlichen Verletzung von Maßgaben dieser Richtlinie ist die KBV berechtigt, diese Registrierung wieder zu entziehen und die Nutzer und KVen über den Entzug der Registrierung zu informieren.

Der Betrieb der Applikation ist daraufhin sofort einzustellen.

Die KBV behält sich vor, technische Maßnahmen einzuleiten, um in diesem Fall den Betrieb der Applikation zu unterbinden.

Des Weiteren muss der Anbieter alle Anwender über den Entzug der Registrierung und die damit verbundene Einstellung des Betriebs der Applikation informieren.

Alle anfallenden Kosten, die im Zusammenhang mit dem Entzug der Registrierung stehen, hat der Anbieter zu übernehmen.

5.5 Einstellung des Betriebs

Die Einstellung des Betriebs einer Applikation ist dem betroffenen Anwenderkreis und der KBV mindestens ein halbes Jahr im Voraus anzukündigen. Die KBV ist über die Beendigung zu informieren. Anschließend wird die Registrierung der Applikation aufgehoben und gebundene Ressourcen freigegeben.

6 Zulässige Betriebsumgebungen

Eine Applikation muss in einer definierten Betriebsumgebung betrieben werden. Die Anforderungen an die Betriebsumgebung sind in Abschnitt 9 dieses Dokumentes definiert und umfassen u.a. Maßgaben zur Organisation, Gebäude und IT-Systemen.

Dieser Abschnitt definiert die grundlegend zugelassenen Betriebsumgebungen für Applikationen im *Sicheren Netz der KVen*.

Die grundlegend zugelassenen Betriebsumgebungen sind wie folgt:

- Betriebsumgebung der KVen/KBV
- Betriebsumgebung des Rechenzentrum-Dienstleisters (RZ-DL)
- Betriebsumgebung eines externen Applikationsanbieters

Die Betriebsumgebung einer Applikation muss sich auf dem Gebiet der Bundesrepublik Deutschland befinden.

Die Bereitstellung von Applikationen über einen Teilnehmeranschluss ist nicht zulässig.

6.1 Betriebsumgebung der KVen/KBV

KVen und die KBV betreiben eigene Rechenzentren im *Sicheren Netz der KVen*.

KVen dürfen in den KV-eigenen Betriebsumgebungen die KV-eigenen regionalen oder übergreifenden Applikationen betreiben.

Weiterhin dürfen KVen in den KV-eigenen Betriebsumgebungen die regionalen oder übergreifenden Applikationen von externen Applikationsanbietern betreiben.

Für die Betriebsumgebung einer KV stellt die jeweilige KV sicher, dass die Maßgaben dieser Richtlinie eingehalten werden und bestätigt das im Rahmen der Registrierung bzw. Zertifizierung der Applikation.

6.2 Betriebsumgebung des Rechenzentrum-Dienstleisters (RZ-DL)

In *Sicheren Netz der KVen* gibt es die Möglichkeit, Applikationen in der Betriebsumgebung eines Rechenzentrums-Dienstleisters (RZ-DL) zu betreiben. Der Rechenzentrums-Dienstleister ist ein im Rahmen einer Konzession von der KBV beauftragtes Unternehmen. Die Anbindung des Rechenzentrums-Dienstleisters an das *Sichere Netz der KVen* erfolgt über einen dedizierten Backbone-Router.

Die Betriebsumgebung des RZ-DL ist bereits von der KBV im Rahmen der Konzessionsvergabe überprüft worden. Damit ist sichergestellt, dass die Anforderungen an die Betriebsumgebung entsprechend Abschnitt 9 dieser Richtlinie durch den Rechenzentrums-Dienstleister erfüllt sind. Eine weitere Überprüfung der Betriebsumgebung im Rahmen der Bereitstellung einer Applikation ist nicht notwendig.

Im Rahmen der Konzessionsvergabe dürfen in der Betriebsumgebung des RZ-DL ausschließlich übergreifend bereitgestellte Applikationen externer Applikationsanbieter betrieben werden.

Falls KVen für die Bereitstellung von Applikationen den RZ-DL in Anspruch nehmen möchten, muss zwischen der entsprechenden KV und dem RZ-DL ein eigener Vertrag abgeschlossen werden.

6.3 Betriebsumgebung eines externen Applikationsanbieters

Ein externer Applikationsanbieter kann eine Applikation auch in seiner eigenen Betriebsumgebung betreiben. Die Betriebsumgebung muss dann an das *Sichere Netz der KVen* angebunden werden.

Die Anbindung erfolgt hierbei mittels VPN-Routern an eine KV, die KBV oder über das Rechenzentrum des sogenannten Rechenzentrum-Dienstleisters (RZ-DL).

Externe Betriebsumgebungen werden direkt im Transfernetz gemäß Abbildung 2 angebunden. Der Datenaustausch muss vor einem Zugriff Dritter durch einen verschlüsselten VPN Tunnel geschützt sein.

Der Tunnelaufbau über das Internet darf erst nach einer gegenseitigen Authentifikation der Tunnelendpunkte (durch PKI Zertifikat) erfolgen.

Die eingesetzten Verfahren zur Authentifizierung, Verschlüsselung und Signierung müssen dem Stand der Technik entsprechen und können dem Dokument „Kryptographische Verfahren: Empfehlungen und Schlüssellängen“ entnommen werden[2].

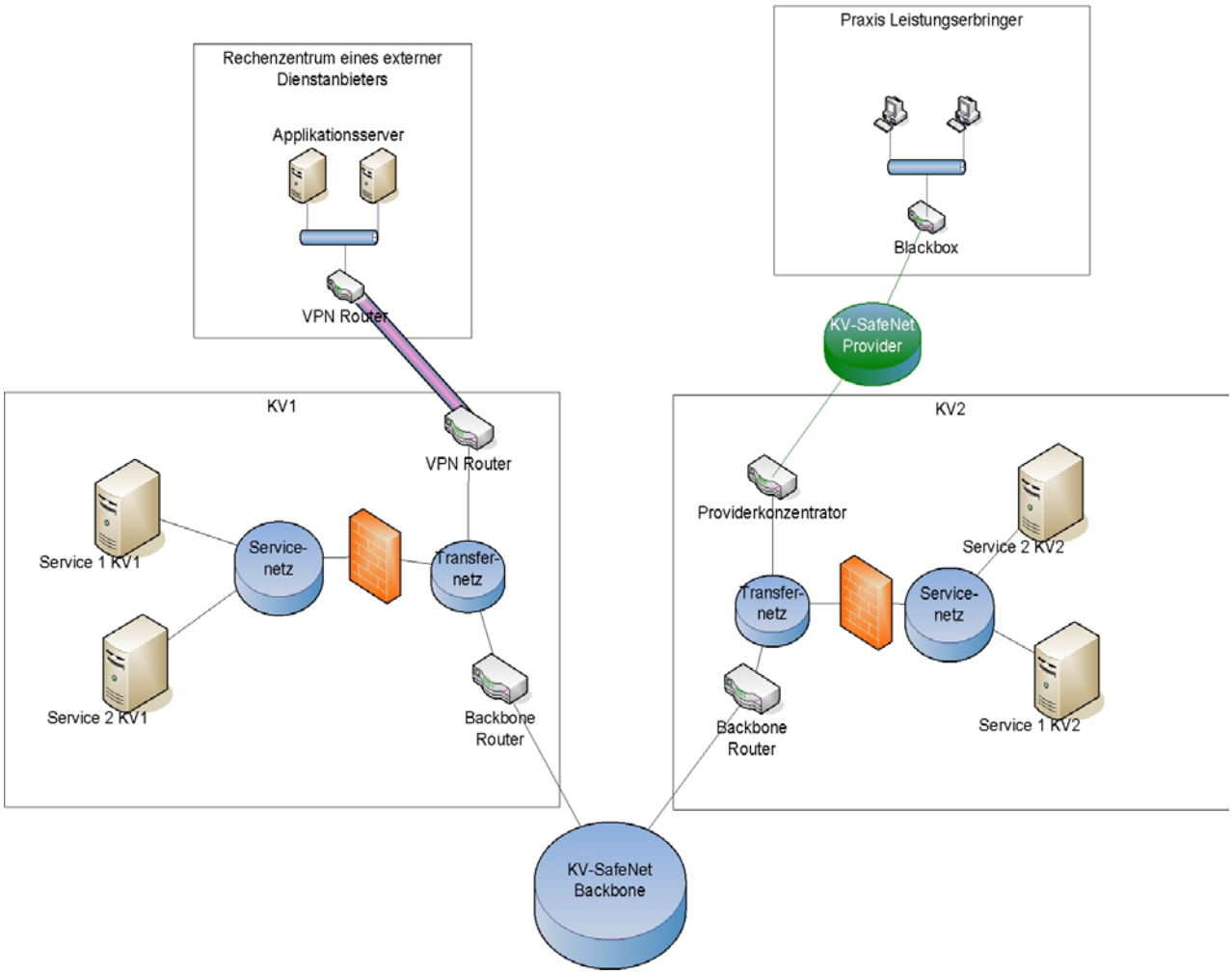

Abbildung 2: Anbindungen externer Betriebsumgebungen an eine KV

[2] https://www.bsi.bund.de/ContentBSI/Publikationen/TechnischeRichtlinien/tr02102/index_htm.html

Der externe Applikationsanbieter ist verantwortlich für die Gewährleistung der Anbindung an das Rechenzentrum der KBV/KV oder deren Rechenzentrums-Dienstleister.

Die KBV/KV behält sich das Recht vor, eine kompromittierte Anbindung des Anbieters jederzeit zu unterbrechen, um Schaden an Daten oder angeschlossenen Systemen zu vermeiden.

Bevor die Anbindung unterbrochen wird, wird der Anbieter informiert. Kann seitens des Anbieters die Ursache der Kompromittierung sofort beseitigt werden, wird von einer Unterbrechung abgesehen.

Nach einer Unterbrechung wird dem Anbieter die Gelegenheit gegeben, die Anbindung wieder in einen kompromittierungsfreien Zustand zu überführen und Sicherheitslücken zu beseitigen. Erst danach wird das System wieder angebunden.

Die Betriebsumgebung eines externen Applikationsanbieters und deren Anbindung an das *Sichere Netz der KVen* werden im Falle einer Zertifizierung durch die KBV überprüft. Im Falle einer Registrierung überprüft die jeweilige KV die Betriebsumgebung des externen Applikationsanbieters und deren Anbindung und bestätigt der KBV die Einhaltung der Maßgaben gemäß Abschnitt 9.

7 Anforderungen an Applikationen

Dieser Abschnitt beschreibt die Anforderungen an Applikationen im *Sicheren Netz der KVen*.

Eine im S*icheren Netz der KVen* betriebene Applikation muss grundlegend die in diesem Kapitel gestellten Sicherheitsanforderungen erfüllen. Diese sind im Folgenden beschrieben und werden in die drei Aspekte Betrieb, Sicherheit und Auswertung aufgeteilt.

Hierbei werden insbesondere Anforderungen an

- Dateninhalt und Datenumfang,
- Nutzbarkeit,
- Protokollierung und Auswertung,
- Betriebszeit und Verfügbarkeit,
- Servicezeiten,
- Authentifizierung und Autorisierung und
- Datenintegrität und Datenübertragung

definiert.

Weiterhin werden Voraussetzungen und Randbedingungen sowie Empfehlungen für Applikationen im *Sicheren Netz der KVen* definiert.

Die im Folgenden empfohlenen Maßnahmen stützen sich vor allem auf die Formulierungen und Anforderungen aus dem IT-Grundschutzkatalog des BSI[3].

7.1 Voraussetzungen

7.1.1 Schutzbedarf der Applikation

Eine zu zertifizierende Applikation muss aufgrund der Verarbeitung von sensiblen und schützenswerten Daten einen erhöhten Schutzbedarf haben und einem gesundheitsmedizinischen Zweck dienen.

Applikationen im *Sicheren Netz der KVen* dürfen keine Werbung beinhalten.

Voraussetzung für die Zertifizierung einer Applikation ist die grundlegende Zulassung der betreffenden Applikationsart durch den Vorstand der KBV.

7.1.2 Unterstützung von Anbindungsvarianten

Applikationen im *Sicheren Netz der KVen* müssen mindestens die Anbindungsvarianten KV-SafeNet und KV-SafeNet (Netzkopplung) unterstützen. Die Unterstützung der Anbindungsvariante KV-FlexNet liegt im Ermessen des Applikationsanbieters.

Hierbei ist jedoch allein die objektive Einschätzung der Sicherheit dieser Zugangsvariante in Zusammenhang mit der angebotenen Applikation maßgeblich. Die Einhaltung der Maßgaben des regional zuständigen Datenschutzbeauftragten ist bindend.

Die Anbindungsvariante KV-WebNet ist für Applikationen im *Sicheren Netz der KVen* nicht zugelassen und nicht Inhalt dieser Richtlinie.

[3] https://www.bsi.bund.de/cln_174/DE/Themen/weitereThemen/ITGrundschutzKataloge/itgrundschutzkataloge_node.html

7.1.3 Multimediainhalte/ -datenströme

Der Einsatz von Multimediainhalten für Applikationen mit medizinischen Bezug bzw. Fokus im SNK ist ausdrücklich erlaubt. Dies betrifft u.a.:

- Einsatz von Video- und Audiostreaming
- Realisierung von Telekonsilen und Tumorkonferenzen
- Videokonferenzen und Voice over IP (VoIP)
- Download von Multimediainhalten

Beim Einsatz von Multimedia-Inhalten in browserbasierten Applikationen sind solche Formate zu bevorzugen, die von aktuellen Browsern nativ, d.h. ohne Installation von externen Plugins, dargestellt werden.

Falls die Verwendung eines Plugins unumgänglich ist, sollte wenn möglich das Installationspaket des Plugins innerhalb der Applikation herunterladbar sein, da die Nachinstallation eines Plugins aus dem Internet für Anbindungen ohne Internet-Zugang nur erschwert möglich ist.

7.2 Schnittstellen und Protokolle

7.2.1 Interoperabilität von Applikationen

Applikationen im *Sicheren Netz der KVen* dürfen keine Verknüpfung bzw. Verbindung an eine bestimmte Software, z.B. eines bestimmen Praxisverwaltungssystems, voraussetzen oder erzwingen.

Der Austausch von Daten und Informationen innerhalb der Applikation, zwischen unterschiedlichen Applikationen und zwischen der Applikation und den Nutzern sollte auf Basis von anerkannten und offenen Standards erfolgen, die Verwendung proprietärer Methoden ist zu vermeiden.

7.2.2 Föderiertes Identitätsmanagement (FIM)

Übergreifende Applikationen im *Sicheren Netz der KVen* sollten über die Möglichkeit verfügen, an das föderierte Identitätsmanagement der KVen (FIM) entsprechend der Richtlinie FIM [KBV_SNK_RLKV_FIM] angebunden zu werden.

Die Verwendung von nicht in der Richtlinie FIM definierten Vorgaben zum (föderierten) Identitätsmanagement von übergreifenden Applikationen ist nicht zulässig.

7.2.3 Nachrichtenversand an Teilnehmer aus Fremdnetzen

Der Nachrichtenversand wird im Konzept als eine gerichtete Kommunikation vom Applikationsanbieter zum Teilnehmer verstanden. KV-Apps können eine Kommunikationsschnittstelle (z.B. E-Mail, SMS, etc.) einer KV oder der KBV nutzen um den Teilnehmer Statusinformationen oder Informationen ohne Schutzbedarf zu zusenden. Diese Kommunikation erfolgt dabei immer vom *Sicheren Netz der KVen* in Richtung eines Fremdnetzes (z.B. das Internet), die Kommunikation in umgekehrter Richtung, also in das *Sichere Netz der KVen* hinein, ist ausgeschlossen. Ebenso ausgeschlossen ist der Eingang/Annahme von Antworten auf diese Nachrichten.

Der Anbieter einer KV-App hat die KV bzw. KBV, deren Kommunikationsschnittstelle genutzt werden soll, über die Art und Weise sowie Inhalt des Nachrichtenversandes zu informieren und Volumina zu benennen. Die KV/KBV behält sich das Recht vor dies nach Prüfung abzulehnen.

Inhalt und Umfang der versendeten Nachrichten

KV-Apps können die Kommunikationsschnittstelle einer KV bzw. der KBV nutzen um den Teilnehmern Statusinformationen oder Informationen ohne Schutzbedarf zu zusenden. Für den gleichen Inhalt kann eine KV ebenfalls eine SMS-Schnittstelle anbieten. Der Versand datenschutzrelevanter Inhalte ist ausgeschlossen.

Beim Nachrichtenversand sollte auf eine umgängliche Größe geachtet werden, so dass Nachrichten vom Teilnehmer in einer akzeptablen Zeit empfangen werden können. Aus diesem Grund sollte von Dateianhängen Abstand genommen werden. Prinzipiell ist ein Versand mit Dateianhang möglich, wenn dies im Interesse des Teilnehmers ist und der Inhalt Informationen ohne Schutzbedarf entspricht.

Virenschutz

Der Anbieter gewährleistet mit einem Virenschutz, dass Nachrichten geprüft und ohne Viren versendet werden. Hierfür betreibt der Anbieter eine entsprechende Software. Der Anbieter gewährleistet weiterhin, dass Virenschutzdefinitionen mind. regelmäßig geprüft und aktualisiert werden. Die Anforderungen des Abschnitts 7.4.7 sind zwingend zu beachten und einzuhalten.

7.3 Betrieb und Wartung

Der Betrieb einer Applikation fordert eine ordnungsgemäße Installation, eine hohe Verfügbarkeit sowie einen schnell zu erreichenden Support, der etwaige Servicearbeiten unter Gewährleistung der vorgegebenen Sicherheitsmaßnahmen zeitnah durchführen kann.

7.3.1 **Betriebszeit**

Der Anbieter hat die Betriebszeiten seiner Applikation bekannt zu geben. Dem Anwender muss mitgeteilt werden, in welchem Umfang und zu welchen Zeiten die Applikation verfügbar ist.

7.3.2 **Verfügbarkeit**

Der Applikationsanbieter ist verantwortlich für die Verfügbarkeit der Applikation. Entsprechende Vereinbarungen zwischen

- dem Applikationsanbieter und den Nutzern und
- ggf. zwischen Applikationsanbieter und dem Betreiber der Betriebsumgebung

mit eindeutigen und verbindlichen Regelungen zur Verfügbarkeit der Applikation, der Betriebsumgebung und der Wiederherstellung nach einem Ausfall sind zu definieren.

Der Anbieter kann Vorbereitungen für einen Notfallplan treffen, um die Wiederherstellung der Verfügbarkeit sicherzustellen.

Die Erreichbarkeit der Applikation sollte an die typischen Arbeitszeiten der Anwender angepasst sein und 40 Stunden pro Woche nicht unterschreiten.

7.3.3 Zeitraum der Wartungsarbeiten

Der Applikationsanbieter muss den Nutzern frühzeitig den Zeitraum von Wartungsarbeiten mitteilen, falls im Rahmen von Wartungsarbeiten die Verfügbarkeit der Applikation eingeschränkt sein wird.

Wartungsarbeiten außerhalb dieser angekündigten Zeiträume dürfen nur aus wichtigem Grund stattfinden.

7.3.4 Prüfung und Bewertung notwendiger Updates

Bei der Durchführung von Updates/Upgrades von Soft- und Hardware im Netzbereich kann der entsprechende Abschnitt im Maßnahmenkatalog (M 4.83) des IT-Grundschutzkatalogs des BSI als Umsetzungsrichtlinie verwendet werden. Dort werden vor allem Regelungen zum Etablieren einer internen Qualitätssicherung getroffen. Gleichzeitig wird dort erläutert, wie ein automatischer Updateschutz die Gewährleistung der fortlaufenden Aktualität der Anwendung sicherstellen kann.

7.3.5 Zeitlich begrenzte Verbindung zu anderen Netzen für Wartungsarbeiten

Eine zeitlich begrenzte Verbindung zu anderen Netzen zum Zweck von Wartungsarbeiten, z.B. für Software- oder Firmware-Updates der Applikation und der Betriebsumgebung ist zulässig. Eine solche Verbindung darf ausschließlich über ein Sicherheitsgateway realisiert werden. Es ist sicherzustellen, dass die in diesem Abschnitt definierten grundsätzlichen Anforderungen weiterhin erfüllt sind. In der folgenden Abbildung ist die Verbindung schematisch dargestellt.

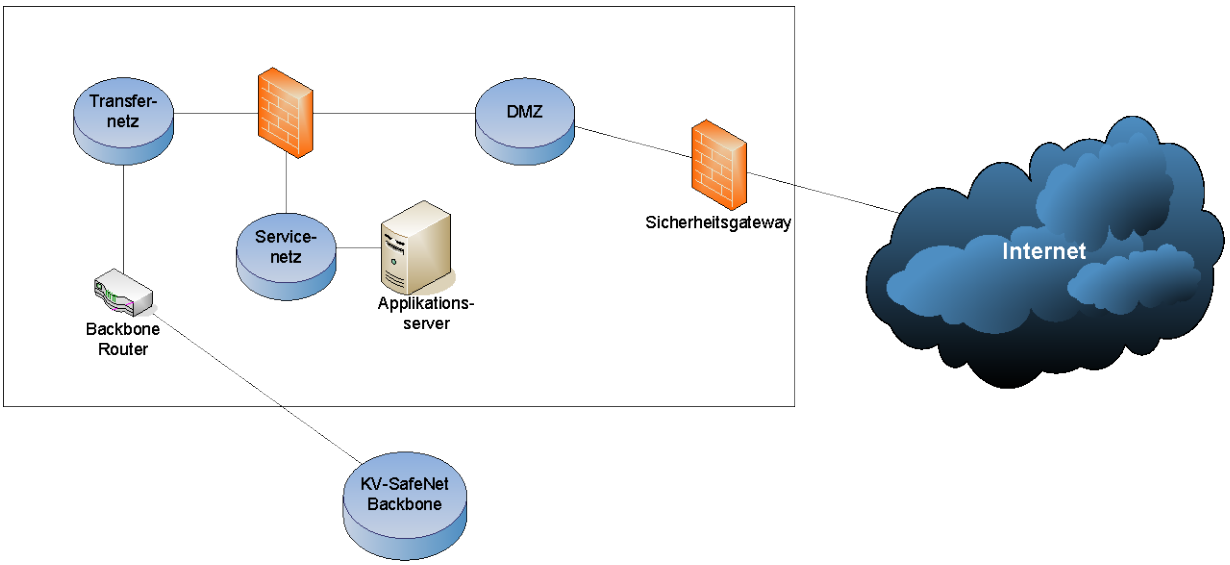

Abbildung 3: Updatezugang für Betriebsumgebungen

7.3.6 Support

Der Applikationsanbieter ist verantwortlich für die Bereitstellung des Supports für die Applikation.

Der Support umfasst sowohl die Behandlung von inhaltlichen Anfragen zur Applikation, als auch zur Meldung von technischen Störungen.

Der Applikationsanbieter stellt den Anwendern hierzu die Kontaktdaten (Ansprechpartner, Telefonnummer, Zeiten der Erreichbarkeit) zur Verfügung.

Für die Organisation und Leitung des Supports kann das Kapitel „Geeignetes Konzept für Personaleinsatz und -qualifizierung“ aus dem BSI Grundschutzkatalog (M 3.51) verwendet werden. Hier werden weiterführende Regelungen und Anforderungen an das Wartungs- und Administrationspersonal gestellt (M 3.11).

7.3.7 Monitoring

Die KBV betreibt ein Monitoring System im *Sicheren Netz der KVen*. Dieses Monitoring System hat die Aufgabe, die grundlegende Verfügbarkeit der Applikation in regelmäßigen Abständen zu überprüfen.

Die KBV behält sich vor, die Applikation in regelmäßigen Abständen auf Verfügbarkeit zu überprüfen und hierfür in Abstimmung mit dem Applikationsanbieter entsprechende Monitoring Möglichkeiten, Schnittstellen und/oder Erweiterungen auf dem System der Applikation installieren zu lassen.

7.3.8 Ausschluss des Support durch die KBV/KV

Wenn die KBV/KV nicht selbst Anbieter der Applikation ist, übernimmt sie keinerlei Supportanfragen der Anwender.

Davon ausgenommen sind vertragliche Vereinbarungen, die die Bearbeitungen von Supportanfragen regeln.

7.4 Sicherheit

Applikationen im *Sicheren Netz der KVen* unterliegen einem erhöhten Schutzbedarf.

Durch die Bereitstellung der Applikation im *Sicheren Netz der KVen* wird bereits grundlegend der Zugriff auf die Applikation mittels der Zugangsvarianten KV-SafeNet bzw. KV-FlexNet auf die Teilnehmer im *Sicheren Netz der KVen* eingeschränkt.

Applikationen müssen sicherstellen, dass der Datenschutz und die Datensicherheit bei Verwendung der Applikation gewährleistet sind.

Für jede im SNK betriebene Applikation sind daher Datenschutz- und Sicherheitskonzepte zu den folgenden Punkten zu erstellen und umzusetzen:

- Konzept zur Absicherung gegen unbefugte Zugriffe aus anderen Netzen
- Rechte- und Rollenkonzept zur Authentisierung und Autorisierung der Nutzer und ggf. Administratoren vor dem Zugriff auf schützenswerte Bereiche
- Gesicherte verschlüsselte Übertragung von schützenswerten Daten zwischen dem Nutzer und der Applikation
- Gesicherte und verschlüsselte Speicherung von schützenswerten Daten in der Applikation
- Konzept zum Betrieb einer Firewall, welches u.a. Vorgaben zu Konfiguration, Changeprozessen, Aufstellort und Sicherungsmechanismen macht

Dazu müssen insbesondere die „Empfehlungen zur ärztlichen Schweigepflicht, Datenschutz und Datenverarbeitung in der Arztpraxis“[4] sowie die dazugehörige Technische Anlage (ebd.[5]) berücksichtigt werden.

7.4.1 Dateninhalt und Datenumfang

Der Anbieter hat den Inhalt und den Umfang der Daten, die durch seine Applikation verarbeitet werden, anzugeben.

Insbesondere der Zweck der Applikation, der Inhalt der Daten und die erwartete Datenmenge sind anzugeben.

7.4.2 Nutzbarkeit

Der Anbieter hat den Anwender über die Nutzung der Applikation ausreichend zu informieren.

Dazu gehören unter anderem die Systemanforderungen an Hard- und Software, die für die optimale Nutzung der Applikation erforderlich sind. Ebenfalls gehört dazu eine genaue Beschreibung der Applikation inkl. Nutzerdokumentation und der Dateiformate und -inhalte, die bei der Übertragung versendet werden.

7.4.3 Authentifizierung und Autorisierung

Der Anbieter verpflichtet sich, ausschließlich berechtigten Anwendern den Zugang zur Applikation zu gewähren. Dabei darf ein Anwender lediglich auf die für ihn relevanten Bereiche zugreifen. Insbesondere müssen sensible Daten (z. B. Patientendaten, Abrechnungsdaten, usw.) durch verstärkte Sicherheitsmaßnahmen gesichert werden.

Der Anbieter hat sicherzustellen, dass die Applikation sowohl von Anwenderseite als auch von Administrationsseite vor Datenmissbrauch und -verlust geschützt wird.

Der Applikationsanbieter erstellt hierzu ein Rechte- und Rollenkonzept mit detaillierter Beschreibung der Authentisierungs- und Autorisierungsverfahren der Anwender und Administratoren.

7.4.4 Datenintegrität und Datenübertragung

Die Übertragung von Daten mit datenschutzrelevanten Inhalten wie z.B. medizinische Falldaten oder Daten mit Personenbezug sind zu verschlüsseln. Die eingesetzten Verfahren zur Authentifizierung, Verschlüsselung und Signierung müssen entsprechend der Forderungen aus der Technischen Richtlinie des BSI zu „Kryptographische Algorithmen und Parameter“ (BSI-TR-03116)[6] umgesetzt werden.

7.4.5 Datenschutz und Datensicherheit

Der Applikationsanbieter ist verpflichtet die einschlägigen rechtlichen Maßgaben zum Datenschutz einzuhalten. Sofern eine Meldepflicht für die Verarbeitung von Daten mit datenschutzrelevantem Inhalt besteht, ist dieser vor der Veröffentlichung bzw. Inbetriebnahme einer Applikation nachzukommen und zusätzlich der KBV anzuzeigen.

[4] http://www.aerzteblatt.de/plus1908
[5] http://www.aerzteblatt.de/v4/plus/down.asp?typ=PDF&id=2316
[6] https://www.bsi.bund.de/cln_174/ContentBSI/Publikationen/TechnischeRichtlinien/tr03116/index_htm.html

Soll eine Applikation als übergreifende Applikation (Abschnitte 3.1.2 und 3.1.4) für Nutzer aus mehr als einem KV-Gebiet angeboten werden, so müssen die Datenschutzgesetzgebungen eines jeden betroffenen Bundeslandes eingehalten werden.

Bei Verstößen gegen die Datenschutzgesetzgebung haftet ausschließlich der Applikationsanbieter, nicht die KBV als Netzbetreiber.

Bei der Umsetzung eines anwendungsspezifischen Schutzes der Benutzerdaten - der Grundbedarf muss je nach Applikation evaluiert werden - können die folgenden BSI-Richtlinien eine unterstützende Rolle spielen:

- Identifikation und Authentisierung, insbesondere das Kapitel „Geeignete Auswahl von Authentikationsmechanismen“ (M 4.133)
- Regeln und Richtlinien zur Datenauthentisierung, bspw. bei „Nutzung eines Authentisierungsservers bei Remote-Access-VPNs“ (M 4.113)
- Zugriffskontrollfunktionen: „Zugangsbeschränkungen für Accounts und / oder Terminals“ (M 4.16)

7.4.6 **Datensicherung**

Der Anbieter muss sicherstellen, dass die Daten der Applikationen in regelmäßigen Abständen gesichert werden und jederzeit vollständig wiederhergestellt werden können.

Bei der Umsetzung können die Empfehlungen des BSI-Grundschutzkataloge des Bausteins B 1.4 „Datensicherungskonzept“ eine unterstützende Rolle spielen, insbesondere die Maßnahmen

- Entwicklung eines Datensicherungskonzeptes (M 6.33)
- Festlegung der Verfahrensweise für die Datensicherung (M 6.35)
- Dokumentation der Datensicherung (M 6.37)
- Geeignete Aufbewahrung der Backup-Datenträger (M 6.20)
- Sporadische Überprüfung auf Wiederherstellbarkeit von Datensicherungen (M 6.22)
- Regelmäßige Datensicherung (M 6.32)

sind zu beachten.

7.4.7 Absicherung gegen unbefugte Zugriffe aus anderen Netzen

Grundsätzlich muss sichergestellt werden und vom Applikationsanbieter zugesichert werden, dass unter keinen Umständen

- ein unbefugter Zugriff auf die Applikation oder die Betriebsumgebung der Applikation aus einem anderen Netz erfolgen kann,
- ein über die Nutzung der Applikation hinausgehender Zugriff auf das *Sichere Netz der KVen* aus einem anderen Netz erfolgen kann und
- ein Teilnehmer über die Applikation oder die Betriebsumgebung der Applikation aus dem *Sicheren Netz der KVen* in andere Netze gelangen kann bzw. Dienste, welche in anderen Netzen betrieben werden, nutzen kann.

Applikationen und Betriebsumgebungen, die ausschließlich für Teilnehmer im *Sicheren Netz der KVen* bereitgestellt werden, dürfen keine direkte oder indirekte Verbindung zu anderen Netzen, z.B. dem Internet, haben.

Applikationen, die gleichzeitig sowohl Nutzern aus dem *Sicheren Netzes der KVen* als auch aus anderen Netzen bereitgestellt werden sollen, müssen eine strikte Trennung der beteiligten Netze nachweisen, um die weiter oben definierten Anforderungen dieses Kapitels umsetzen zu können.

Eine zeitlich begrenzte Verbindung zu anderen Netzen zum Zweck von Wartungsarbeiten ist erlaubt und in Abschnitt 7.3.5 beschrieben.

7.4.8 Schutz von Produktivdaten

Auf den Einsatz von Produktivdaten sollte im Rahmen von Anwendungstests verzichtet werden. Für den Fall, dass im Zuge der Entwicklung nicht auf den Einsatz von Produktivdaten zu Testzwecken verzichtet werden kann, muss der Schutz der verwendeten Produktivdaten gewährleistet (Wahrung der Schutzziele Integrität, Vertraulichkeit und Verfügbarkeit) und die jeweils gültigen Regelungen zum Datenschutz eingehalten werden.

Besonderem Schutz unterliegen insbesondere Sozialdaten nach §67 SGB X. Wenn Sozialdaten im Auftrag durch andere Stellen erhoben, verarbeitet oder genutzt werden ist § 80 SGB X zu beachten.

7.5 Auswertung

7.5.1 Protokollierung und -auswertung

Der Anbieter hat sowohl über gewöhnliche Vorgänge als auch über außergewöhnliche Vorgänge ausreichend Informationen aufzuzeichnen, damit etwaige Sicherheitsverletzungen erkannt werden können.

Sollte dennoch eine Sicherheitsverletzung vorliegen, muss die jeweilige KV - bei KV-übergreifenden Applikationen betrifft dies die KBV - unverzüglich informiert werden. Die Fehlerbehebung muss in Abstimmung mit der KV getroffen und in einem Ablaufdiagramm nachgewiesen werden.

Die Generierung und Analyse der Protokolldaten kann der Richtlinie zur Protokollierung der Sicherheitsgateway-Aktivitäten (M 4.47) des BSI entnommen werden.

Des Weiteren sollte bei der Durchsicht und Auswahl der protokollierten Daten ein Audit der Netzaktivitäten (M 4.81) stattfinden.

Schließlich müssen jederzeit die Hinweise zu den Datenschutzaspekten bei der Protokollierung (M 2.110) beachtet werden.

7.5.2 **Technische Berichte**

Der Anbieter muss alle Störungen oder außerordentlichen Vorkommnisse seitens der Applikation (bzw. der gesamten Betriebsumgebung) protokollieren und diese Protokolle über einen definierten Zeitraum vorhalten. Die Mindestangaben pro Datensatz sind:

1. Ausfälle, Störungen, außergewöhnliche Vorgänge,
2. Beschreibung des Vorfalls,
3. Datum,
4. Uhrzeit Beginn,
5. Uhrzeit Ende,
6. Ursache (falls bekannt, sonst „unbekannt“)
7. Wenn zutreffend: Anzahl und Volumen der in Fremdnetze versendete Nachrichten (vergl. Abschnitt 7.2.3)

Eine Übergabe des Protokolls an die KBV / KV ist nur im Bedarfsfall erforderlich.

8 Anforderungen an Applikationsanbieter

8.1 Informationssicherheitsmanagement

Der Applikationsanbieter verpflichtet sich, Leistungen im Zusammenhang mit dem *Sicheren Netz der KVen*, nach Maßgaben und Best Practices eines standardisierten Informationssicherheitsmanagements zu erbringen.

Die folgenden Eckpunkte umreißen die Anforderungen an ein standardisiertes Informationssicherheitsmanagement:

- Sicherheitsleitlinie und Organisation der Sicherheit
- Datenschutz, Vertraulichkeit und Zugangskontrolle
- Personalsicherheit
- Gebäude- und Arbeitsplatzsicherheit
- Management der Betriebs- und Kommunikationsprozesse
- Beschaffung, Entwicklung und Wartung
- Management von Informationssicherheitsereignissen (Incident Management)
- Business Continuity Management (BCM)
- Compliance

Es wird dringend empfohlen, diese Maßgaben aus der ISO 27001 bzw. aus dem IT-Grundschutz des Bundesamtes für die Sicherheit in der Informationstechnik (BSI) abzuleiten und durch unabhängige Dritte überprüfen zu lassen. Die Zertifizierung des Informationssicherheitsmanagementsystems (ISMS) eines Anbieters gemäß ISO 27001 mit einem Anwendungsbereich, der die Leistungen zum *Sicheren Netz der KVen* abdeckt, wird empfohlen. Die Vorlage eines entsprechenden Zertifikats kann zudem den KBV-Zertifizierungsprozess eines Applikationsanbieters beschleunigen.

8.2 Bestimmungsgemäße Nutzung

Der Applikationsanbieter darf das *Sichere Netz der KVen* nur in dem für die Bereitstellung der Applikation notwendigen Umfang nutzen.

Die Nutzung über den im Rahmen der Zertifizierung bzw. Registrierung eingereichten Unterlagen hinaus ist untersagt.

Das *Sichere Netz der KVen* darf nicht missbräuchlich genutzt werden, insbesondere:

- dürfen keine gesetzlich verbotenen, unaufgeforderten Informationen, Objekte und sonstige Leistungen übersandt werden, wie z.B. unerwünschte und unverlangte Werbung ebenso wenig wie nicht gesetzeskonforme Applikationen
- darf keine rechtswidrige Kontaktaufnahme durch Telekommunikationsmittel erfolgen (§ 238 StGB).
- dürfen keine Informationen mit rechts- oder sittenwidrigen Inhalten übermittelt oder in das *Sichere Netz der KVen* eingestellt werden und es darf nicht auf solche Informationen hingewiesen werden. Dazu zählen vor allem Informationen, die im Sinne der §§ 130, 130a und 131 StGB der Volksverhetzung dienen, zu Straftaten anleiten oder Gewalt verherrlichen oder verharmlosen, sexuell anstößig sind, im Sinne des § 184 StGB pornografisch sind, geeignet sind, Kinder oder Jugendliche sittlich schwer zu gefähr-

den oder in ihrem Wohl zu beeinträchtigen oder das Ansehen der KBV/KVen schädigen können. Die Bestimmungen des Jugendmedienstaatsvertrages und des Jugendschutzgesetzes sind zu beachten.

- ist dafür Sorge zu tragen, dass durch die Inanspruchnahme einzelner Funktionalitäten und insbesondere durch die Einstellung oder das Versenden von Nachrichten keinerlei Beeinträchtigungen für die KBV/KVen, andere Anbieter oder sonstige Dritte entstehen.
- sind die nationalen und internationalen Urheber- und Marken-, Patent-, Namens- und Kennzeichenrechte sowie sonstige gewerbliche Schutzrechte und Persönlichkeitsrechte Dritter zu beachten.

8.3 Beendigung der Nutzung der Applikation durch einen Nutzer

Der Applikationsanbieter ist verpflichtet, einen Prozess zur Beendigung der Nutzung der Applikation durch Nutzer, die die Applikation nicht mehr nutzen möchten oder nicht mehr nutzen dürfen, zu definieren (Rückabwicklung).

Es muss u.a. geregelt sein, dass ein Nutzer, der keine Berechtigung für den Zugriff auf die Applikation mehr hat, keine Möglichkeiten des Zugangs zur Applikation erhalten kann, z.B. durch Entzug der Berechtigungen oder Löschung der Nutzerkennung innerhalb der Applikation.

9 Anforderungen an Betriebsumgebungen

Im Folgenden sind die Anforderungen an die Betriebsumgebungen im *Sicheren Netz der KVen* formuliert. Weiterhin sind Maßnahmen aus dem BSI-Grundschutzkatalog aufgeführt, die Hilfestellung zur Umsetzung der Forderungen geben. Im Dokument wird Bezug auf Maßnahmen aus dem BSI-Grundschutzkatalog genommen. Es können jedoch auch in ihrer Sicherheitsstärke gleichwertige Maßnahmen anderer Zusammenstellungen wie z.B. ISO, DIN etc. herangezogen werden.

Die nachfolgend formulierten Anforderungen resultieren aus dem hohen Schutzbedarf der durch die Applikationen im *Sicheren Netz der KVen* verarbeiteten, transportierten und gespeicherten Daten.

Eine Applikation im *Sicheren Netz der KVen* darf ausschließlich in einem Rechenzentrum oder einem Serverraum betrieben werden, in welchem die nachfolgenden Anforderungen umgesetzt sind. Ein Betrieb in anderweitigen Räumlichkeiten ist grundsätzlich ausgeschlossen.

9.1 Organisation

9.1.1 Rollenkonzept

Es ist ein Rollenkonzept zu erstellen. Dabei sind die im Folgenden aufgeführten Rollenausschlüsse zu beachten:

- Keine Leitungsfunktion soll operative oder administrative Aufgaben übernehmen.
- Keine Kontrollfunktion soll operative oder administrative Aufgaben übernehmen.
- Reduzierung der vollen Zutritts- bzw. Zugriffsrechte auf wenige Personen.

Maßnahmen: Mögliche Rollen sind den Rollendefinitionen des BSI Grundschutzkatalogs zu entnehmen.

9.1.2 Zutrittskonzept

Es ist ein Zutrittskonzept zu erstellen. Es ist dabei zu beachten, dass die Anzahl der Zutrittsberechtigten auf das notwendige Maß beschränkt wird. Es ist sicherzustellen, dass sich in Räumen, in denen IT-Systeme mit vertraulichen Daten betrieben werden, niemals nur ein Mitarbeiter allein aufhält (strikte Einhaltung des Vier-Augen-Prinzips). Eine Zutrittsregelung für eigene und für zeitweilig beschäftigte Mitarbeiter muss vorhanden sein. Diese muss verhindern, dass Personen außerhalb ihres Tätigkeitsbereiches Zugriff auf Systeme erhalten. Anhand eines Rollenkonzepts sind Zutrittsberechtigungen und Ausschlüsse entsprechend zu definieren.

Maßnahmen: M 2.5, M 2.6, M 2.7, M 2.8, M 2.17

9.1.3 Verfügbarkeitskonzept

Die Architektur und die Infrastruktur der Betriebsumgebung sind so auszulegen, dass die Vorgaben an die Verfügbarkeit erfüllt werden. Dazu muss ein entsprechendes Verfügbarkeitskonzept erstellt werden. Das Verfügbarkeitskonzept sollte die Themenschwerpunkte Fehlerintoleranz und Fehlertoleranz beinhalten und darstellen, wie diese Anforderungen erfüllt werden.

Der Betreiber der Betriebsumgebung überwacht die Verfügbarkeit und kann anhand von Daten darlegen, dass die geforderte Verfügbarkeit nicht unterschritten wurde.

Maßnahmen: Geeignete Maßnahmen zur Erreichung der im Verfügbarkeitskonzept festgelegten Verfügbarkeitsziele können sein:

- *Auswahl geeigneter und zuverlässiger Hardware*
- *ausreichender Gebäudeschutz*
- *Brandschutz*
- *Wasser- und Feuchtigkeitsschutz*
- *ausreichend dimensionierte Energieversorgung*
- *Klimatisierung*
- *Gefahrenmeldeanlage*
- *Redundanz*
- *Überwachung und Alarmierung*

9.1.4 **Notfallkonzept**

Ein auf die örtlichen Gegebenheiten angepasstes Notfallkonzept muss erstellt werden. Als Notfälle werden alle Ereignisse betrachtet, welche die Verfügbarkeit der bestehenden materiellen und technischen Infrastruktur derart bedrohen, dass besondere Maßnahmen zur Sicherung oder Wiederaufnahme des Betriebs notwendig sind. Ein Ausfall des Betriebs kann sowohl durch technisch bedingte Störungen wie Stromausfall, Wasserschaden, Brand, als auch durch vorsätzliche oder fahrlässige Handlungen wie Fehlbedienung oder Sabotage hervorgerufen werden. Nicht jeder Teil- oder Gesamtausfall des Systems stellt dabei einen Notfall dar. Das Notfallkonzept führt die Maßnahmen auf, die bei bestimmten Notsituationen durchzuführen sind, nennt weiterhin die entsprechenden Verantwortlichen und definiert die einzuleitenden Schritte nach dem Notfall zur Wiedererlangung des Wirkbetriebs.

Maßnahmen: Es sollte mindestens eine Übersicht über die Verfügbarkeitsanforderungen, einen Alarmierungsplan und die Regelungen der Verantwortungen im Notfall enthalten. Für die autorisierte und rechtzeitige Einleitung von Notfallmaßnahmen bedarf es der Benennung eines Notfall-Verantwortlichen. Dieser muss sowohl für die Entscheidung autorisiert sein, ob ein Notfall eingetreten ist, als auch für die Einleitung erforderlicher Notfallmaßnahmen. Einen umfassenden Maßnahmenüberblick gibt der Maßnahmenkatalog Notfallvorsorge des BSI Grundschutzkatalogs.

9.1.5 **Wartungskonzept**

Es ist ein Wartungskonzept zu erstellen, dass die von den Herstellern empfohlenen Wartungsintervalle und -vorschriften berücksichtigt. Diese sollten unbedingt eingehalten werden. Neben der normalen Wartung sollten ältere Anlagen einer intensiveren Inspektion unterzogen werden, bei denen insbesondere verschlissene Teile erkannt und rechtzeitig ausgetauscht werden. Dies betrifft insbesondere größere Aggregate der Gebäudetechnik, beispielsweise zentrale Heizungs- und Klimatisierungsanlagen, sowie mechanisch stark beanspruchte Anlagen. Gegebenenfalls sollte die Unterstützung durch technische Sachverständige in Anspruch genommen werden. Besondere Beanspruchung oder außergewöhnliche Betriebsbedingungen können zu zusätzlichem Wartungsaufwand führen.

Maßnahmen: Die Maßnahmen M 2.4 des BSI Grundschutzkatalogs sind anzuwenden und die Einhaltung zu überprüfen.

9.1.6 Schutzbedarfskonzept

Der Schutzbedarf von IT-Systemen hängt im Wesentlichen von dem Schutzbedarf der zu betreibenden Anwendung ab. Der Schutzbedarf der Anwendung vererbt sich grundsätzlich auf den Schutzbedarf des IT-Systems. Dabei können verschiedene Prinzipien wie Maximum-, Kumulations- und Verteilungsprinzip zum Tragen kommen. Der Schutzbedarf aller Einrichtungen und Komponenten muss daher aufeinander abgestimmt sein und sollte in einem Konzept beschrieben werden.

9.2 Infrastruktur

Zur Erlangung einer Infrastruktur mit der geforderten Sicherheit müssen mindestens folgende Anforderungen realisiert werden:

9.2.1 Organisatorische Anforderungen

Über die organisatorischen Konzepte hinaus ist die Infrastruktur durch hinreichende organisatorische Maßnahmen zu schützen. Dadurch wird verhindert, dass unbefugte Personen Zugriff auf darin befindliche Unterlagen und IT-Einrichtungen erlangen.

Maßnahmen: Die Maßnahmen M 1.15 und M 1.23 des BSI Grundschutzkatalogs sind anzuwenden und die Einhaltung zu überprüfen.

9.2.2 Gebäude

- Die erforderlichen technischen Einrichtungen müssen in einem Rechenzentrum/ Serverraum untergebracht sein.
- Potentielle Gefährdungen z. B. durch Umgebungseinflüsse sind zu minimieren.
- Ein angemessener baulicher und technischer Einbruchschutz ist vorhanden.
- Die Vermischung der Basistechnik (Energieversorgung, Klima etc.) und der Informationstechnik (Server, aktive Netzkomponenten etc.) ist zu vermeiden und nach Möglichkeit in separaten Räumen unterzubringen.

Maßnahmen: Die Maßnahmen M 1.12, M 1.18, M 1.24, M 1.27, M 1.52, M 1.53 des BSI Grundschutzkatalogs geben wertvolle Hinweise zur Absicherung bzw. Auslegung des Gebäudes.

9.2.3 Brandschutz

Brandschutzmaßnahmen sind in ausreichendem Umfang umzusetzen. Handfeuerlöscher, Brandmeldeanlage und Rauchschutzeinrichtungen sind obligatorisch. Brandfrühesterkennung, Raumlöschanlage etc. sind optional. Im Rechenzentrum/Serverraum besteht Rauchverbot.

Maßnahmen: Die Artikel M 1.6, M 1.9, M 1.47 und M 2.21 des Maßnahmenkatalogs aus dem BSI Grundschutzkatalog beschreiben die Umsetzung von Brandschutzmaßnahmen.

9.2.4 Stromversorgung

Die Stromversorgung ist auf den tatsächlichen Bedarf abzustimmen. Die Verteilung der Lasten auf die Stromkreise ist gleichmäßig. Es stehen ausreichende Reserven zur Verfügung. Ein ausreichend dimensionierter Potentialausgleich ist vorhanden und umgesetzt. Ein ausrei-

chendes Überspannungsschutzkonzept ist vorhanden und wurde umgesetzt. Es wurden im Rechenzentrum/Serverraum ausreichende Maßnahmen gegen elektrostatische Aufladungen getroffen. Je nach Anforderung an die Verfügbarkeit ist ein Notstromkonzept vorhanden und umgesetzt. Evtl. ist eine sekundäre Stromversorgung vorhanden.

Maßnahmen: Zusätzliche Hinweise zur Umsetzung können den Maßnahmen M 1.1, M 1.3, M 1.4, M 1.5, M 1.25, M 1.26 und M 1.28 des Maßnahmenkatalogs der BSI Grundschutzkataloge entnommen werden.

9.2.5 Spezifische Sicherheitsbereiche im Rechenzentrum

Das Rechenzentrum/Serverraum ist als geschlossener Sicherheitsbereich konzipiert. Alle IT-Systeme müssen im Serverraum aufgestellt und betrieben werden. Der Serverraum muss zutrittsgeschützt und mit einer Zutrittskontrolltechnik versehen sein.

Alle IT-Systeme auf denen Klartextverarbeitung mit Daten gemäß SGB stattfinden, müssen in einem separaten Sicherheitsbereich im Rechenzentrum aufgestellt und betrieben werden. Der Sicherheitsbereich muss zutrittsgeschützt und mit einer Zutrittskontrolltechnik versehen sein.

Für die Administration der IT-Systeme und Anwendungen muss ein separater Sicherheitsbereich im Rechenzentrum eingerichtet werden. Der Sicherheitsbereich muss zutrittsgeschützt und mit einer Zutrittskontrolltechnik versehen sein.

Das Datensicherungsarchiv muss im Rechenzentrum in einem weiteren Brandabschnitt untergebracht sein. Der Sicherheitsbereich muss zutrittsgeschützt und mit einer Zutrittskontrolltechnik versehen sein.

9.2.6 Zutrittsschutz

Alle Zutrittsmöglichkeiten zu IT- und Infrastrukturräumen werden kontrolliert und sind gegen unberechtigten Zutritt durch hochwertige Zutrittskontrollmechanismen und -anlagen zu schützen. Dabei ist durch geeignete bauliche Maßnahmen oder auch die Verwendung anderer materieller Sicherungstechnik sicherzustellen, dass ein Zutritt Unbefugter hinreichend sicher ausgeschlossen werden kann. Die Zutritte werden überwacht und dokumentiert.

Im Bezug auf externe Täter bedeutet dies, dass die eingesetzte Infrastruktur einen so hohen Widerstandswert haben muss, dass der Versuch des unbefugten Zutritts so lange abgewehrt wird, wie es dauert, bis alarmierte Einsatzkräfte eintreffen. Hieraus folgt, dass mindestens eine Gefahrenmeldeanlage zu betreiben ist, die dem Stand der Technik entspricht. Weiterhin muss sichergestellt werden, dass auf entsprechende Alarmmeldungen unverzüglich und angemessen reagiert wird.

Im Bezug auf Innentäter bedeutet dies, dass insbesondere eine hinreichende Zutrittskontrolltechnik zum Einsatz kommt.

Dort wo aufgrund baulicher Gegebenheiten die hier beschriebenen Anforderungen nicht möglich sind, ist der Einsatz entsprechender Schutzschränke in Betracht zu ziehen.

Maßnahmen: M 1.18, M 1.19 und M 2.17 des BSI Grundschutzkatalogs

9.3 IT-Systeme

9.3.1 Netzwerke

Der Zugriff von Servern auf das Internet darf zum Zweck von Sicherheits- und Softwareupdates über ein Sicherheitsgateway realisiert werden. Die IT-Systeme der Betriebsumgebung werden ausschließlich über ein separates Managementnetz administriert.

9.3.2 Anforderungen an die Remote-Administration der IT-Systeme

Die Remote-Administration der IT-Systeme in den verschiedenen Sicherheitszonen und der Firewall-Systeme darf nur über einen gesicherten Weg erfolgen. Der Kanal, durch den die Administration der IT-Systeme und Applikationen erfolgt, muss durch starke Verschlüsselung und starke Authentisierung geschützt werden.

Sofern die Remote-Administration aus Räumen erfolgt, die zu der gleichen Liegenschaft wie das Rechenzentrum gehören, muss der administrative Remote-Zugriff auf die IT-Systeme durch geeignete Authentifizierungsverfahren – mindestens durch ein sicheres Passwort – geschützt sein. Erfolgt die Remote-Administration aus einem – im Bezug auf das Rechenzentrum – externen Gebäude, ist eine Zwei-Faktor-Authentisierung (Besitz und Wissen) anzuwenden.

9.3.3 Aktualität der IT-Systeme

Soweit eingesetzte IT-Systeme nicht sicherheitszertifiziert sind, ist sicherzustellen, dass alle relevanten Sicherheitspatches installiert werden. Vor der Installation sind die im Rahmen des Changemanagements entwickelten Regeln zu beachten.

Sofern zertifizierte IT-Systeme zum Einsatz kommen gilt Folgendes:

- Sofern ein relevanter Patch bereits Gegenstand einer Re-Evaluierung war, so hat auch hier nach erfolgtem Freigabeverfahren die unverzügliche Installation zu erfolgen.
- Sofern ein Sicherheitspatch noch nicht Gegenstand der Re-Evaluierung war, ist durch das IT-Management zu entscheiden, wie zu verfahren ist. Dabei sind die möglichen Risiken gegeneinander abzuwägen. Das Ergebnis dieser Abwägung ist zu dokumentieren und umzusetzen.

Maßnahmen: Bei der Durchführung von Updates/Upgrades von Soft- und Hardware im Netzbereich kann der entsprechende Abschnitt im Maßnahmenkatalog M 4.83 des IT-Grundschutzkatalogs des BSI als Umsetzungsrichtlinie verwendet werden. Ein Umgang mit AutoUpdate Funktionen wird im Abschnitt M 4.324 des Maßnahmenkatalogs behandelt.

9.3.4 Sichere Installation und Betrieb der eingesetzten IT-Systeme

Folgende Anforderungen sind für alle IT-Systeme, die im *Sicheren Netz der KVen* eingesetzt werden, mit geeigneten Maßnahmen umzusetzen:

- Die eingesetzten IT-Systeme sind sicher zu installieren. Dabei sind insbesondere die Hinweise des jeweiligen Herstellers zu berücksichtigen.
- Die eingesetzten IT-Systeme sind sicher zu betreiben. Auch hier haben die entsprechenden Hinweise des Herstellers Berücksichtigung zu finden.
- Soweit zertifizierte IT-Systeme zum Einsatz kommen, sind die Auflagen hinsichtlich der Anforderungen an die Einsatzumgebung einzuhalten.
- Alle IT-Systeme sind auf der Grundlage gehärteter Betriebssysteme zu installieren und zu betreiben. Hinsichtlich der verwendeten Betriebssysteme bedeutet dies, dass diese minimal zu installieren sind. Insbesondere sind alle nicht benötigten Dienste zu deaktivieren. Sie sind zudem zu deinstallieren, sofern dies das jeweilige Betriebssystem zulässt. Alle nicht benötigte Software darf nicht installiert werden, bzw. ist zuverlässig zu deinstallieren.
- Vor Inbetriebnahme sind die Systeme ausgiebig auf Funktionalität zu testen. Ein besonderer Fokus muss dabei auf den Sicherheitsfunktionen liegen. Hierzu ist ein gesondertes Testkonzept zu erstellen. Die Ergebnisse der Tests sind nachvollziehbar zu dokumentieren. Dies gilt analog nach der Installation von Patches und Updates.

- Es gilt der Grundsatz der minimalen Rechtevergabe für Benutzer; d. h. es dürfen nur die für die Aufgabenerfüllung absolut notwendigen Rechte vergeben werden. Die Rechtevergabe ist zu dokumentieren und zu begründen.
- Durch geeignete Maßnahmen ist zu erzwingen, dass ein Systemstart nur vom Standard-Laufwerk aus erfolgt.
- Das Betriebssystem und die jeweilige Applikation müssen so konfiguriert werden, dass die im Rahmen des IT-Sicherheitskonzepts festgelegten Authentisierungsmechanismen genutzt werden.
- Durch geeignete technische Maßnahmen ist sicherzustellen, dass die Anmeldung eines Berechtigten an einem im *Sicheren Netz der KVen* betriebenen IT-Systems nicht durch einen Unbefugten missbraucht werden kann. Daher ist sicherzustellen, dass, sofern der angemeldete Berechtigte seinen Arbeitsplatz auch nur kurzfristig verlässt, das betroffene IT-System für weitere Zugriffe gesperrt wird. Die Sperre darf nur aufgehoben werden, wenn eine erneute Authentisierung gegenüber dem IT-System erfolgt.

9.3.5 Integritätsschutz für IT-Systeme

Zur Vorbeugung gegen Systeminstabilitäten durch Inkonsistenzen oder Angriffe, sind alle im *Sicheren Netz der KVen* betriebenen IT-Systeme regelmäßig mit geeigneten technischen Maßnahmen, auf Integrität zu prüfen. Die Prüfung und das Ergebnis sind zu dokumentieren.

Sofern bei einer solchen Prüfung festgestellt wird, dass die Integrität des Systems verletzt wurde, sind unverzüglich geeignete Gegenmaßnahmen zu ergreifen. Hierzu ist präventiv ein entsprechender Ablaufplan, beispielsweise in Form einer Checkliste, zu erstellen.

Die detaillierte Vorgehensweise beschreibt die Maßnahme M 4.93 aus dem BSI Grundschutzkatalog.

9.3.6 Betriebshandbücher

Für jedes IT-System ist ein Betriebshandbuch zu führen. Dieses muss die aktuelle Konfiguration und Parametrisierung des Betriebssystems, der Dienste und der darauf installierten Applikationen enthalten. Änderungen an der Konfiguration sind zu vermerken und zu begründen.

9.3.7 Protokollierung

Alle sicherheitskritischen IT-Systeme müssen eine Protokollierungskomponente enthalten die in der Lage ist, jedes der folgenden Ereignisse revisionsfähig zu protokollieren:

- Anmeldevorgänge am System (erfolgreiche als auch nicht erfolgreiche),
- versuchter Zugriff auf eine der Rechteverwaltung unterliegende Komponente,
- alle Administrations-Verbindungsversuche.

Bei nicht erlaubten Verbindungsversuchen muss eine fest definierte Alarmmeldung ausgegeben werden.

Um unautorisiertes teilweises oder komplettes Löschen von Daten zu verhindern und um entsprechende Nachweise zu führen ist sicherzustellen, dass entsprechende Zugriffe durch das mit der Administration betraute Personal zuverlässig protokolliert werden.

Maßnahmen: Im Maßnahmenkatalog Hardware und Software des BSI Grundschutzkatalogs werden die Protokollmöglichkeiten für verschiedenste Systeme beschrieben. Je nach Art und Umfang der Betriebsumgebung sind die entsprechenden Punkte zu beachten. Darüber

hinaus können die Maßnahmen M 2.110 und M 5.9 wertvolle Hinweise zur Umsetzung liefern.

9.3.8 Kommunikationsverbindungen

Nicht authentifizierte sowie direkte Verbindungsversuche auf interne Systeme sind zu blockieren. Die Anforderungen der spezifischen Kommunikationsverbindungen finden sich in der Richtlinie KV-SafeNet [KBV_SNK_RLEX_KV-SafeNet], KV-SafeNet(Netzkopplung) [KBV_SNK_RLEX_Netzkopplung], der Richtlinie KV-FlexNet [KBV_SNK_RLKV_KV-FlexNet] sowie in der Dokumentation zum KV-Backbone wieder. Alle Kommunikationsverbindungen vom externen Netz in das interne Netz und umgekehrt müssen über einen Sicherheitsgateway laufen. Der Einsatz eines Intrusion Detection Systems (IDS) wird empfohlen.

Maßnahme: M 5.1

9.3.8.1 Router und Switche

Die sichere Aufstellung und der Betrieb der Router und Switche in der Betriebsumgebung muss durch den Applikationsanbieter nachgewiesen werden. Die Umsetzung der folgenden Maßnahmen des BSI Grundschutzkataloges ist empfohlen

- Erstellung einer Sicherheitsrichtlinie für Router und Switches (M 2.279)
- Kriterien für die Beschaffung und geeignete Auswahl von Routern und Switches (M 2.280)
- Dokumentation der Systemkonfiguration von Routern und Switches (M 2.281)
- Regelmäßige Kontrolle von Routern und Switches (M 2.282)
- Software-Pflege auf Routern und Switches (M 2.283)

9.3.8.2 Firewalls (Paketfilter) und Sicherheitsgateways

Die Trennung der Sicherheitszonen muss durch ein Sicherheitsgateway erfolgen. Das Sicherheitsgateway muss dem Stand von Wissenschaft und Technik entsprechen. Es muss aus einer Kombination von Paketfiltern und Application-Layer-Gateway (ALG) bestehen.

Das Sicherheitsgateway ist so sicher zu betreiben, dass unbefugte Zugriffe auf die dahinter liegenden IT-Systeme von außerhalb wirksam unterbunden werden.

Für das System ist ein Betriebshandbuch zu führen. Die Konfiguration sowie Patchlevel sind zu dokumentieren. Änderungen an der Hard - und Software dürfen erst in Betrieb genommen werden, wenn zuvor die Funktionalität entsprechend getestet wurde.

Die anfallenden Protokolle sind regelmäßig, mindestens aber einmal täglich zu überprüfen. Auf erkannte Angriffsversuche ist angemessen zu reagieren.

Die Wirksamkeit des Sicherheitsgateway ist regelmäßig durch Penetrationstests zu überprüfen.

Es ist ein Sicherheitskonzept für die Firewalls und Sicherheitsgateways zu erstellen, welche die Konfiguration beschreibt, die Aufstellung beschreibt und den Prozess der Freigabe und Durchführung von Änderungen.

Maßnahmen: Es wird empfohlen, die Maßnahmen M 2.70 – M 2.78 des BSI Grundschutzkatalogs zu berücksichtigen und vollständig anzuwenden.

9.3.8.3 Intrusion Detection System

Der Betreiber kann durch den Betrieb eines Intrusion Detection Systems, das dem Stand der Technik entspricht, sicherzustellen, dass Angriffe auf die Betriebsumgebung zuverlässig detektiert werden. Es kann zudem durch geeignete organisatorische und technische Maßnahmen sichergestellt werden, dass bei sicherheitskritischen Angriffen eine zuverlässige unverzügliche Alarmierung erfolgt und unverzüglich auf einen solchen Angriff reagiert wird.

Maßnahmen: *Es wird empfohlen, bei der Installation und dem Betrieb des Intrusion Detection Systems den BSI-Leitfaden zur Einführung von Intrusion-Detection-Systemen*[7] *insbesondere Kapitel 2.5 der Intrusion Detection Grundlagen angemessen zu berücksichtigen.*

[7] https://www.bsi.bund.de/cln_134/ContentBSI/Publikationen/studien/ids02/index_htm.htm

10 Berichtswesen

10.1 Technische Berichte

Der Anbieter muss alle sicherheitsrelevanten Vorfälle und Störungen oder außerordentlichen Vorkommnisse seitens der Applikation und ihrer gesamten Betriebsumgebung protokollieren und bereithalten. Die Mindestangaben pro Datensatz sind:

1. Beschreibung des Vorfalls,
2. Datum,
3. Uhrzeit Beginn,
4. Uhrzeit Ende,
5. Ursache (falls bekannt, sonst „unbekannt“) sowie
6. durchgeführten und geplanten Maßnahmen.

Eine Übergabe des Protokolls an die KBV ist nur im Bedarfsfall erforderlich. Die Aufbewahrungsfrist für die technischen Berichte beträgt zwei Kalenderjahre.

Im Rahmen der unter Abschnitt 7.3 geregelten Update- und Wartungszugänge zum Internet ist ein detaillierter Bericht über die offenen Ports und die Sicherheitsgateway-Einstellungen vorzuhalten. Dieser beinhaltet pro eingestellte Regel mindestens die folgenden Angaben:

1. Source-Address
2. Source-Port(s)
3. Target-Address
4. Target-Port(s)
5. Service
6. Timevalue

Eine Übergabe des Berichts an die KBV ist nur im Bedarfsfall erforderlich. Er muss jedoch jederzeit für eine Sicherheitsanalyse verfügbar sein.

10.2 Anwenderstatistiken

Der Anbieter stellt der KBV jedes Quartal eine Übersicht über die Anzahl der in der Applikation registrierten Anwender und der im letzten Quartal aktiven Anwender zur Verfügung. Bei bundesweiter Nutzung der Applikation sind diese Angaben zusätzlich nach KVen zu gruppieren.

10.3 Bandbreitenstatistiken

Der Anbieter stellt der KBV jedes Quartal zwei Auswertungen zur Verfügung.

In der ersten Auswertung sind der tatsächlich verursachte maximale Datendurchsatz und der durchschnittliche Datendurchsatz des letzten Quartals. Diese ist je Applikation für jeden Monat zu untergliedern.

Die zweite Übersicht ist perspektivisch anzugeben. Hier ist sowohl der zu erwartende alltägliche Datendurchsatz als auch der verursachte Datendurchsatz für die maximale Anzahl der gleichzeitigen Anwender anzugeben.

11 Haftungsausschluss

Die KBV und die Kassenärztlichen Vereinigungen übernehmen gegenüber dem Applikationsanbieter keinerlei Haftung aus Anlass der Vorgaben technischer und/oder wirtschaftlicher sowie damit im Zusammenhang stehender Art und/oder aus der Umsetzung dieser Vorgaben

Die KBV übernimmt keine Gewähr für die Verfügbarkeit und Störungsfreiheit der Applikationen, welche die KVen anbieten. Weder die KBV noch die KVen übernehmen die Gewähr für die Verfügbarkeit und Störungsfreiheit der Applikationen externer Anbieter.

Ferner übernimmt die KBV keine Haftung für den Betrieb, die Nutzung oder Schadensereignisse im Zusammenhang mit der von den KVen bereitgestellten Applikationen. Weder die KBV noch die KVen übernehmen die Haftung für den Betrieb, die Nutzung oder Schadensereignisse im Zusammenhang mit von externen Anbietern bereitgestellten Applikationen.

Der Applikationsanbieter ist verantwortlich für den Betrieb, die Verfügbarkeit und Störungsfreiheit der Applikation sowie für die Schadensereignisse. Die KBV/KVen übernehmen keine Gewähr für die Verfügbarkeit und Störungsfreiheit einer Applikation, es sei denn, sie sind als Applikationsanbieter dafür verantwortlich.

12 Salvatorische Klausel

Sollten Teile oder einzelne Formulierungen dieser Richtlinien aus irgendeinem Grund ungültig sein, bleiben die übrigen Teile des Dokuments in ihrem Inhalt und ihrer Gültigkeit unberührt.

13 Glossar

Begriff	Erklärung
Anbieternetz	Zum Netz des Anbieters zählen alle notwendigen Dienste und Infrastrukturelemente, die zur Einrichtung, Aufrechterhaltung und Wartung der KV-SafeNet Anbindung zwischen Teilnehmer und KV notwendig sind.
Applikation	Services und Anwendungen im *Sicheren Netz der KVen*
Applikationsanbieter	Anbieter eines Dienstes
BCM	Business Continuity Management (BCM) beschäftigt sich mit der Sicherstellung des Geschäftsbetriebs in Notfallsituationen und der Vorsorge für Notfallsituationen. Ziel ist der Schutz der kritischen Geschäftsprozesse vor den Auswirkungen größerer Störungen.
Compliance	Einhaltung von Vorgaben des ISMS
Dienstenetz (DN)	Das Dienstenetz ist das Netz der Services und Anwendungen. Hier werden alle Anwendungsserver des *Sicheren Netzes der KVen* installiert und verfügbar gemacht. Die Organisation des Dienstenetzes liegt in der Verantwortung der Applikationsanbieter bzw. des Rechenzentrumsdienstleisters.
Einwahlknoten / Konzentrator	Der Einwahlknoten ist der Endpunkt des Anbieternetzes, der in der KV installiert ist und den Übergang vom Anbieternetz zum *Sicheren Netz der KVen* darstellt.
Firewall	Eine Firewall dient dazu, den Netzwerkzugriff zu beschränken, basierend auf Absender- oder Zieladresse und genutzten Diensten. Die Firewall überwacht den durch sie hindurch laufenden Datenverkehr und entscheidet anhand festgelegter Regeln, ob bestimmte Netzwerkpakete durchgelassen werden, oder nicht. Auf diese Weise versucht die Firewall unerlaubte Netzwerkzugriffe zu unterbinden.
Firmware	Firmware bezeichnet Software, die in elektronische Geräte fest eingebettet und somit mit dem Gerät untrennbar verbunden ist. Eine Firmware benötigt u.U. in regelmäßigen Abständen ein Update.
Fremdprovider / VPN-Provider	Ein VPN-Provider stellt im Gegensatz zum ISDN, DSL oder UMTS Provider nicht die technischen Voraussetzungen bzgl. der Übertragungstechnik zur Verfügung, sondern nutzt eine bereits bestehende Internetverbindung.
KV-App	Siehe Applikation.
KV-Backbone	Der KV-Backbone ist ein geschütztes, logisch vom Internet getrenntes, vollvermaschtes VPN-Netzwerk auf Basis eines von der KBV definierten Konzeptes. Die Rechenzentren der Kassenärztlichen Vereinigungen (KVen) und der Kassenärztlichen Bundesvereinigung (KBV) sind über den KV-Backbone miteinander vernetzt. Die KBV ist der Betreiber des KV-Backbones.
KV-FlexNet	Anbindungsmöglichkeit eines Teilnehmers an das *Sichere Netz der KVen* mittels einer Software-VPN-Lösung. Der Anschluss erfolgt über die KV des Teilnehmers.
KV-SafeNet	Anbindungsmöglichkeit eines Teilnehmers an das *Sichere Netz der KVen* mittels einer Hardware-VPN-Lösung, dem KV-SafeNet-Router. Der Anschluss erfolgt über einen KV-SafeNet-Provider.
KV-SafeNet-Provider	Von der KBV nach der KV-SafeNet-Richtlinie zertifizierter Provider, der Teilnehmern einen Zugang über die Anschlussvariante „KV-SafeNet“ zum *Sicheren Netz der KVen* ermöglicht.

Begriff	Erklärung
KV-SafeNet-Router	Ein KV-SafeNet-Router ist ein nicht manipulierbarer Router. Dieser wird zwischen Internetanschluss und Praxisnetzwerk geschaltet. Dieser Router baut ein virtuelles privates Netzwerk (VPN) zu einem Einwahlknoten in der KV auf, welches die Verbindung vom normalen Internet abschottet und so einen abgesicherten Datenaustausch mit dem *Sicheren Netz der KVen* ermöglicht. Gleichzeitig blockiert der Router den Zugriff von außen auf das Praxis-Netzwerk und die dortigen Daten, da er den Zugriff aus dem Anbieternetz in das Teilnehmernetz verhindert. Die Verantwortung für den KV-SafeNet-Router trägt der KV-SafeNet-Provider.
Servicenetz	Siehe Dienstenetz
Sicheres Netz der KVen	Das *Sichere Netz der KVen* ist eine von der KBV und den KVen bereitgestellte Infrastruktur, bestehend aus einem vollvermaschten VPN-Netzwerk (KV-Backbone), im Netzwerk befindlichen Diensten und Anwendungen (KV-Apps) und den definierten Anbindungsmöglichkeiten an das Netzwerk (KV-SafeNet und KV-FlexNet). Diese Infrastruktur trägt den Anforderungen an Datenschutz und Datensicherheit Rechnung und ist für die Übermittlung von Sozialdaten geeignet.
Teilnehmer	Ein Teilnehmer ist ein Vertragsarzt, -psychotherapeut oder ein anderes nach den Richtlinien der KBV zugelassenes Mitglied des *Sicheren Netzes der KVen*. Grundsätzlich bestimmen die KVen den Teilnehmerkreis.
Teilnehmernetz	Die untereinander lokal vernetzten Teilnehmercomputer bilden das Netzwerk des Teilnehmers. Hier können sich weitere vernetzte Endsysteme (z.B. Server, Drucker, Kartenleser) befinden.
Transfernetz (TFN)	Das Transfernetz dient der Weiterleitung der Datenpakete vom Teilnehmer zu den Applikationsservern und zurück. Es wird durch den KV-Backbone-Router realisiert. Die Organisation des Transfernetzes liegt in Verantwortung des KV-Backbone-Betreibers.
Tunnel / VPN-Tunnel	Für die Kommunikation des zugeordneten Netzes mit einem seiner VPN-Partner werden am VPN-Gateway die ursprünglichen Netzwerkpakete in ein VPN-Protokoll gepackt. Daher spricht man bei VPN vom Tunnel.
Zertifizierung	Prozess in dem explizit nachgewiesen wird, wie der Antragsteller die in der Richtlinie geregelten Anforderungen umsetzt. Wird dieses Verfahren erfolgreich abgeschlossen, erhält der Antragsteller eine Konformitätserklärung.
Zugangsnetz	Dazu gehören Netzelemente und Vermittlungsstellen, die Grundlagen der techn. Infrastruktur zwischen Anbieter- und Teilnehmeranschluss schaffen.

14 Referenzierte Dokumente

Referenz	Dokument
[KBV_SNK_RLEX_KV-SafeNet]	Richtlinie KV-SafeNet
[KBV_SNK_RLEX_Netzkopplung]	Richtlinie KV-SafeNet(Netzkopplung)
[KBV_SNK_RLKV_KV-FlexNet]	Richtlinie KV-FlexNet
[KBV_SNK_LFEX_Überpüfung_KV-Apps]	Leitfaden Überprüfung KV-Apps
[KBV_SNK_LFEX_KV-Apps]	Leitfaden Zertifizierung/Registrierung KV-Apps
[KBV_SNK_RLEX_Informationssicherheit]	Richtlinie Informationssicherheit
[KBV_SNK_RLEX_Risikomanagement]	Richtlinie Risikomanagement
[KBV_SNK_RLEX_BCM]	Richtlinie Business Continuity Management
	Ergänzende Erklärung??
	Registrierungsformular ???
	Selbstauskünfte ???