Kassenärztliche Bundesvereinigung
Körperschaft des öffentlichen Rechts

Sicheres Netz der KVen

Richtlinie Business Continuity Management

[KBV_SNK_RLEX_BCM]

Dezernat 6
Informationstechnik, Telematik und Telemedizin

10623 Berlin, Herbert-Lewin-Platz 2

Kassenärztliche Bundesvereinigung

Version	1.0
Datum:	12.12.2011
Klassifizierung:	Öffentlich
Status:	In Kraft

DOKUMENTENHISTORIE

Version	Datum	Autor	Änderung	Begründung	Seite
1.0	12.12.2011	KBV	Erstellung, QS und Freigabe des Dokuments		

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.

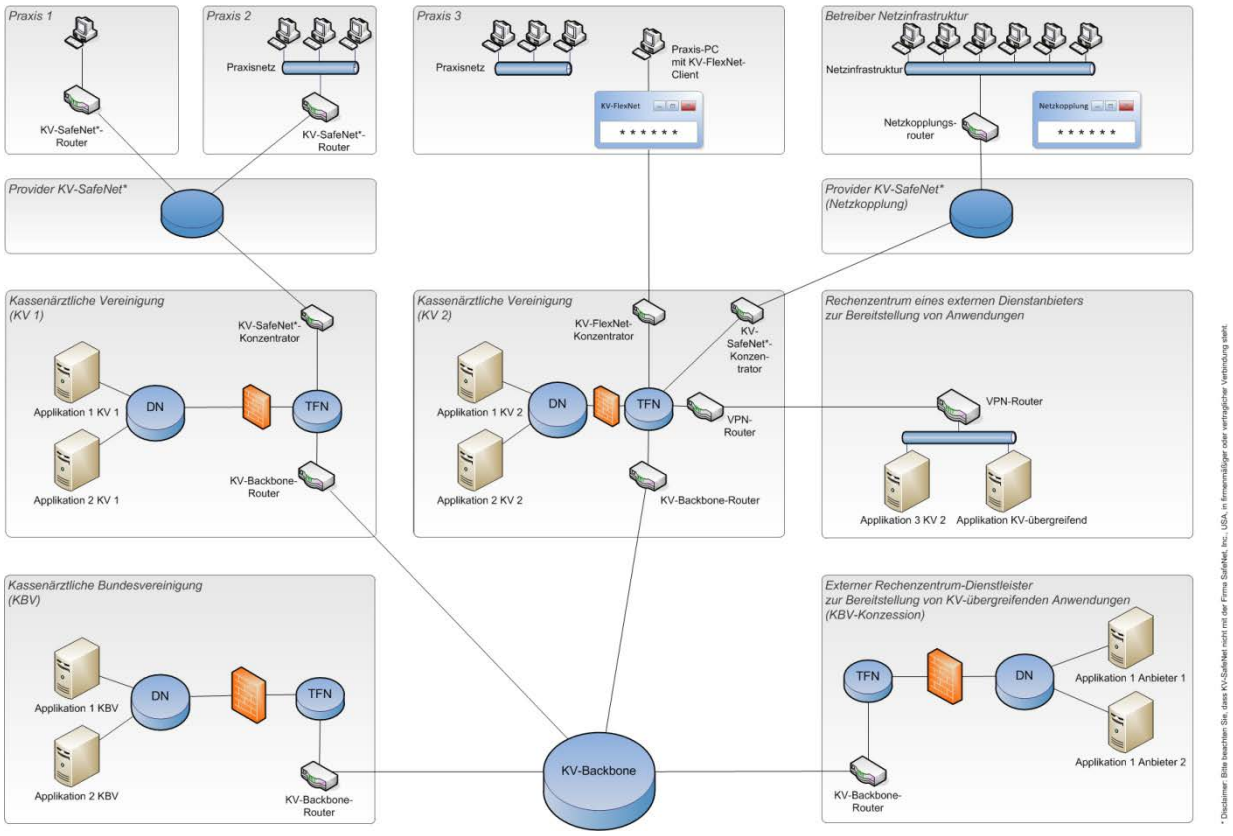

Abbildung 1: Beispielhafte Netztopologie

Teilnehmer am *Sicheren Netz der KVen* sind die Mitglieder der Kassenärztlichen Vereinigungen, also Vertragsärzte und –psychotherapeuten oder ein anderes nach den Richtlinien der KBV zugelassenes Mitglied des *Sicheren Netzes der KVen*. Ihnen werden sichere Zugangswege 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 Mög-

lichkeiten 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

Gemäß Richtlinie [KBV_SNK_RLEX_Informationssicherheit] ist Business Continuity Management ein wesentlicher Baustein für die Informationssicherheit. Dieses Dokument beschreibt die grundsätzliche Vorgehensweise zum BCM im *Sicheren Netz der KVen* und gibt konkrete Empfehlungen und Beispiele für die organisationsspezifische Umsetzung für alle beteiligten Akteure.

Business Continuity Management, auch betriebliches Kontinuitätsmanagement genannt, beschäftigt sich mit der Vorsorge für Notfallsituationen und der Sicherstellung des Geschäftsbetriebs in Notfallsituationen. Ziel ist der Schutz von kritischen Geschäftsprozessen vor den Auswirkungen größerer Störungen und die Sicherstellung der rechtzeitigen Wiederaufnahme. Business Continuity Management ist daher eine Strategie zur vorausschauenden Sicherstellung des Geschäftsbetriebs.

Die Richtlinie zum BCM im *Sicheren Netz der KVen* definiert entsprechende Vorgaben für ein Business Continuity Management System (BCMS), um diese Ziele zu erreichen.

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 KVen, Provider, Anbieter von Applikationen und durch die KBV oder KVen beauftragte externe Dienstleister.

* 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 Regelungen

2.1 Rahmen und Ziele

Business Continuity Management ist ein zentraler Baustein im Rahmen des Regelkreises zur Aufrechterhaltung und kontinuierlichen Verbesserung des Informationssicherheitsmanagements gemäß der Richtlinie [KBV_SNK_RLEX_Informationssicherheit]. Methodische Voraussetzung für das Business Continuity Management System (BCMS) ist ein Risikomanagement gemäß der Richtlinie [KBV_SNK_RLEX_Risikomanagement].

Das BCM des *Sicheren Netzes der KVen* ist auf alle Verantwortungsbereiche und alle für diese Verantwortungsbereiche zuständigen Organisationen gemäß Richtlinie Informationssicherheit [KBV_SNK_RLEX_Informationssicherheit] im *Sicheren Netz der KVen* anzuwenden.

Jede Organisation im *Sicheren Netz der KVen* soll für ihre Verantwortungsbereiche ein BCMS etablieren und aufrechterhalten, welches den Maßgaben dieser Richtlinie entspricht. Die konkrete Form der Umsetzung obliegt der zuständigen Organisation.

2.2 Zusammenarbeit zwischen den Organisationen

Grundlegend ist jede Organisation verantwortlich für das Betreiben des eigenen BCMS. Störungen des Geschäftsbetriebes ohne Einfluss auf andere Verantwortungsbereiche und Organisationen müssen durch die verantwortliche Organisation selbst gelöst werden.

Störungen von kritischen Geschäftsprozessen mit Einfluss auf andere Verantwortungsbereiche und Organisationen müssen an die KBV und die betreffenden Organisationen gemeldet werden. Hier greifen die Prozesse des Security Incident Management im *Sicheren Netz der KVen*.

2.3 Aufbau und Betrieb des BCMS

Die folgenden Abschnitte definieren die Maßgaben, die für den Betrieb eines BCMS innerhalb einer Organisation notwendig und mindestens umzusetzen sind.

2.3.1 BCM-Verantwortlicher

In jeder Organisation muss ein Verantwortlicher für das BCM benannt werden. Dieser hat in seiner Organisation folgende Aufgaben

- Betrieb und Weiterentwicklung des BCMS
- Identifikation der kritischen Geschäftsprozesse
- Erstellung und Pflege der BCMS-Rahmen-Dokumente, u. a. interne Richtlinien und Vorlagen für Notfallpläne
- Erstellung und Pflege der Notfallpläne
- Durchführung und Dokumentation regelmäßiger Tests und Übungen der Notfallpläne

2.3.2 Prozess zur Sicherstellung des BCMS

Die Organisation muss einen gelenkten BCM-Prozess entwickeln, umsetzen und aufrechterhalten. Die wesentlichen Prozessschritte dabei sind:

- Identifikation und Priorisierung kritischer Geschäftsprozesse
- Identifikation der organisationseigenen Werte, die zu kritischen Geschäftsprozessen gehören
- Identifikation der Risiken, denen die Organisation ausgesetzt ist, sowie deren Wahrscheinlichkeit und Auswirkung eines Schadensereignisses
- Identifikation von vorbeugenden und schadensmindernden Maßnahmen und Umsetzung dieser Maßnahmen
- Erstellung und Pflege von Notfallplänen, die der Sicherstellung des Geschäftsbetriebs dienen
- Regelmäßige Tests und Aktualisierungen der Notfallpläne und Prozesse
- Sicherstellung der Integration des BCM in die Prozesse und Strukturen der Organisation

2.3.3 Identifikation der kritischen Geschäftsprozesse und Risikobewertung

Die Organisation muss ihre kritischen Geschäftsprozesse identifizieren. Für diese Geschäftsprozesse sind die Anforderungen an die betriebliche Kontinuität zu definieren.

Es soll eine Risikobewertung durchgeführt werden. Folgende Schritte sind dabei grundsätzliche zu befolgen:

- Einschätzung der Kritikalität (Vertraulichkeit, Integrität, Verfügbarkeit)
- Ermittlung der Bedrohungen und Ereignisse, die Störungen von kritischen Geschäftsprozessen verursachen können
- Analyse der möglichen Auswirkungen einer Störung auf die kritischen Geschäftsprozesse (Abschätzung der Wahrscheinlichkeit des Eintritts des Ereignisses und der Auswirkung der Störung)

Im Rahmen der Risikobehandlung müssen vorbeugende Maßnahmen definiert werden, um die Wahrscheinlichkeit einer Störung zu verringern, den Störungszeitraum zu verkürzen oder die Auswirkung der Störung zu reduzieren.

Es wird empfohlen, die Risikobewertung entsprechend der Richtlinie Risikomanagement [KBV_SNK_RLEX_Risikomanagement] durchzuführen.

2.3.4 Rahmenwerk für Notfallpläne

Ein Rahmenwerk für die Erstellung von Notfallplänen zur Aufrechterhaltung des Geschäftsbetriebes ist zu entwickeln und umzusetzen. Das einheitliche Rahmenwerk stellt sicher, dass alle Notfallpläne widerspruchsfrei und einheitlich sind.

Das Rahmenwerk muss Folgendes mindestens enthalten:

- Definition der Prozesse des BCM in der Organisation
- Definition von Schadensereignisklassen
- Vorlagen für Notfallpläne
- Vorlagen für Test und Übung der Notfallpläne

2.3.4.1 Schadensereignisklassen

Ein Schadensereignis ist eine Situation, die eine Störung, einen Notfall, eine Krise oder eine Katastrophe verursachen kann.

Die Definition von Schadensereignisklassen muss in Abhängigkeit von den möglichen Auswirkungen einer Störung verschiedene Gewichtungen vorsehen, mindestens aber die Schadensereignisklassen Störung und Notfall.

Schadensereignisklasse	Definition
Störung	Eine Störung ist eine Situation, in der Prozesse oder Ressourcen einer Organisation nicht wie vorgesehen funktionieren. Die dadurch entstehenden Schäden sind als gering einzustufen. Störungen werden durch die in das allgemeine Tagesgeschäft integrierte Störungsbehebung beseitigt.
Notfall	Ein Notfall ist ein Schadensereignis, bei dem Prozesse oder Ressourcen einer Institution nicht wie vorgesehen funktionieren. Die Verfügbarkeit der entsprechenden Prozesse oder Ressourcen kann innerhalb einer geforderten Zeit nicht wieder hergestellt werden. Der Geschäftsbetrieb ist stark beeinträchtigt. Es entstehen hohe bis sehr hohe Schäden, die sich signifikant und in nicht akzeptablem Rahmen auf die Aufgabenerfüllung auswirken. Notfälle können nicht mehr im allgemeinen Tagesgeschäft abgewickelt werden, sondern erfordern gesonderte Maßnahmen zur Notfallbewältigung.
Krise	Unter einer Krise wird eine vom Normalzustand abweichende Situation verstanden, die trotz vorbeugender Maßnahmen jederzeit eintreten und mit der normalen Aufbau- und Ablauforganisation nicht bewältigt werden kann. Das Krisenmanagement wird aktiv. Für die Bewältigung existieren keine Ablaufpläne, sondern lediglich Rahmenanweisungen und -bedingungen. Ein typisches Merkmal einer Krise ist die Einmaligkeit des Ereignisses.

2.3.4.2 Notfallpläne

Für die Behandlung von Notfällen sind konkrete Notfallpläne zu erstellen. Notfallpläne beschreiben das konkrete Vorgehen im Falle eines als Notfall eingestuften Schadensereignisses vom unverzüglichen Notbetrieb bis zur Wiederherstellung des Normalbetriebs.

Empfehlungen für den Inhalt eines Notfallplans sind in Anhang A aufgeführt.

Es sind Mustervorlagen für Notfallpläne zu erstellen.

Es müssen in diesem Zusammenhang auch Regelungen existieren, die das Vorgehen definieren, falls in einem konkreten Notfall kein Notfallplan verfügbar ist. Für diesen Fall sollten das grundlegende Vorgehen und Rahmenbedingungen definiert werden.

2.3.5 Entwickeln und Umsetzen von Notfallplänen

Konkrete Notfallpläne sind auf Basis des in Abschnitt 2.3.4 definierten Rahmenwerkes für Notfallpläne zu entwickeln, um sicherzustellen, dass wesentliche Geschäftsprozesse aufrechterhalten werden können oder in der erforderlichen Zeit und dem erforderlichen Maße wiederhergestellt werden können.

Die Notfallpläne sollten sich wie in Abschnitt 2.3.3 auf die kritischen Geschäftsprozesse fokussieren und die Schwachstellen der Organisation behandeln.

2.3.6 Testen, Instandhaltung und Neubewertung von Notfallplänen

Die erstellten Notfallpläne müssen regelmäßig getestet und aktualisiert werden, um sicherzustellen, dass sie auf dem neuesten Stand sind.

Änderungen in Geschäftsabläufen sollen zu Aktualisierungen der entsprechenden Notfallpläne führen.

Notwendige Schritte für das BCMS in der jeweiligen Organisation sind daher:

- Auswahl und Festlegung der zu verifizierenden Notfallpläne
- Festlegung einer adäquaten Testmethodik bzw. Teststrategie für jeden zu verifizierenden Notfallplan
- Festlegung einer Testplanung für die zu prüfenden Pläne
- Durchführung von regelmäßigen Tests und Übungen der ausgewählten Notfallplänen
- Dokumentation und Bewertung der durchgeführten Tests und Übungen
- Evtl. sofortige Festlegung von Korrekturmaßnahmen nach Durchführung von Tests und Übungen

Die Tests und Übungen sind so zu gestalten, dass das Risiko einer Störung der Geschäftsprozesse minimiert wird. Übungen, die Mängel oder Ungenauigkeiten in Notfallplänen aufgedeckt haben, sollten ggf. wiederholt werden.

Wichtige Dritte, wie z. B. externe Dienstleister für Stromversorgung oder Gebäudemanagement, sollten in die Übungen involviert werden, wenn zu erwarten ist, dass diese bei der Durchführung von Notfallplänen auch im Schadensfall involviert werden müssen.

Es sind Mustervorlagen für die Testdokumentation zu erstellen.

3 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
Business Continuity Management (BCM)	Business Continuity Management, auch betriebliches Kontinuitätsmanagement genannt, beschäftigt sich mit der Vorsorge für Notfallsituationen und der Sicherstellung des Geschäftsbetriebs in Notfallsituationen. Ziel ist der Schutz von kritischen Geschäftsprozessen vor den Auswirkungen größerer Störungen und die Sicherstellung der rechtzeitigen Wiederaufnahme. Business Continuity Management ist daher eine Strategie zur vorausschauenden Sicherstellung des Geschäftsbetriebs.
Business Continuity Management System (BCMS)	Managementsystem für ein BCM. Siehe Business Continuity Management (BCM).
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.
Informationssicherheit	Aufrechterhaltung der Vertraulichkeit, Integrität und Verfügbarkeit von Informationen; andere Eigenschaften wie Authentizität, Zurechenbarkeit und Verlässlichkeit können ebenfalls berücksichtigt werden.
Informationssicherheitsmanagementsystem (ISMS)	Teil des gesamten Managementsystems, der auf der Basis eines Geschäftsrisikoansatzes die Entwicklung, Implementierung, Durchführung, Überwachung, Überprüfung, Instandhaltung und Verbesserung der Informationssicherheit abdeckt.
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.

Begriff	Erklärung
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.
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.

4 Referenzierte Dokumente

Referenz	Dokument
KBV_SNK_RLEX_Informationssicherheit	Richtlinie Informationssicherheit
KBV_SNK_RLEX_Risikomanagement	Richtlinie Risikomanagement

ANHANG

A Inhalt eines Notfallplans

Ein Notfallplan beschreibt das konkrete Vorgehen im Falle eines als Notfall eingestuften Schadensereignisses vom unverzüglichen Notbetrieb bis zur Wiederherstellung des Normalbetriebs. Die jeweilige Organisation sollte für ihren Verantwortungsbereich Mustervorlagen definieren.

Ein Notfallplan sollte mindestens die in diesem Abschnitt definierten Informationen beinhalten.

- Metadaten des Notfallplanes
  - Dokumentenname
  - Autor
  - Version und Dokumentenhistorie
  - Status (z. B. in Arbeit, in Kraft)
- Beschreibung des Notfallszenarios
- Bedingungen für das Inkrafttreten des Notfalls und damit des Notfallplans
- Benennung der betroffenen Geschäftsprozesse und/oder Ressourcen
  - Für das Notfallszenario wird eine Benennung der betroffenen Wertegruppen und Werte und der ggf. wirkenden Bedrohungen entsprechend der Richtlinie Risikomanagement [KBV_SNK_RLEX_Risikomanagement] empfohlen
- Benennung der Verantwortlichkeiten für
  - die Gesamtverantwortung für den Notfallplan
  - die Durchführung der einzelnen Schritte des Notfallplans bei einem Schadensereignis
  - den Test des Notfallplans
- Verfahren zum Notbetrieb
  - Die einzelnen Schritte zur Herstellung eines Notbetriebs sind in einem ausreichend detailliertem Umfang zu definieren, sodass ein Sachkundiger in der Lage ist, einen Notbetrieb herzustellen.
  - Sowohl die technischen Schritte als auch die organisatorisch notwendigen Schritte zur Einleitung der Maßnahmen, Kommunikation mit den Beteiligten usw. sind zu beschreiben.
- Verfahren zur Wiederherstellung des Normalbetriebs
  - Die einzelnen Schritte zur Wiederherstellung des normalen Betriebs sind zu dokumentieren.
  - Sowohl die technischen Schritte als auch die organisatorisch notwendigen Schritte zur Beendigung des Notfalls sind zu definieren.
- Notwendige Ressourcen und Bedingungen
  - Personal, ggf. externe Dienstleister mit ihren Kontaktdaten und Verantwortlichkeiten
  - Technik
- Verweise auf evtl. notwendige technische Informationen, die bei Eintritt des Notfalls zur Problemlösung herangezogen werden können
- Test und Übung des Notfallplans