Kassenärztliche Bundesvereinigung
Körperschaft des öffentlichen Rechts

Sicheres Netz der KVen

Richtlinie Informationssicherheit

[KBV_SNK_RLEX_Informationssicherheit]

Dezernat 6
Informationstechnik, Telematik und Telemedizin

10623 Berlin, Herbert-Lewin-Platz 2

Kassenärztliche Bundesvereinigung

Version	1.0
Datum:	31.10.2011
Klassifizierung:	Öffentlich
Status:	In Kraft

DOKUMENTENHISTORIE

Version	Datum	Autor	Änderung	Begründung	Seite
1.0	31.10.2011	KBV	Erstellung und Freigabe der Richtlinie		alle

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.

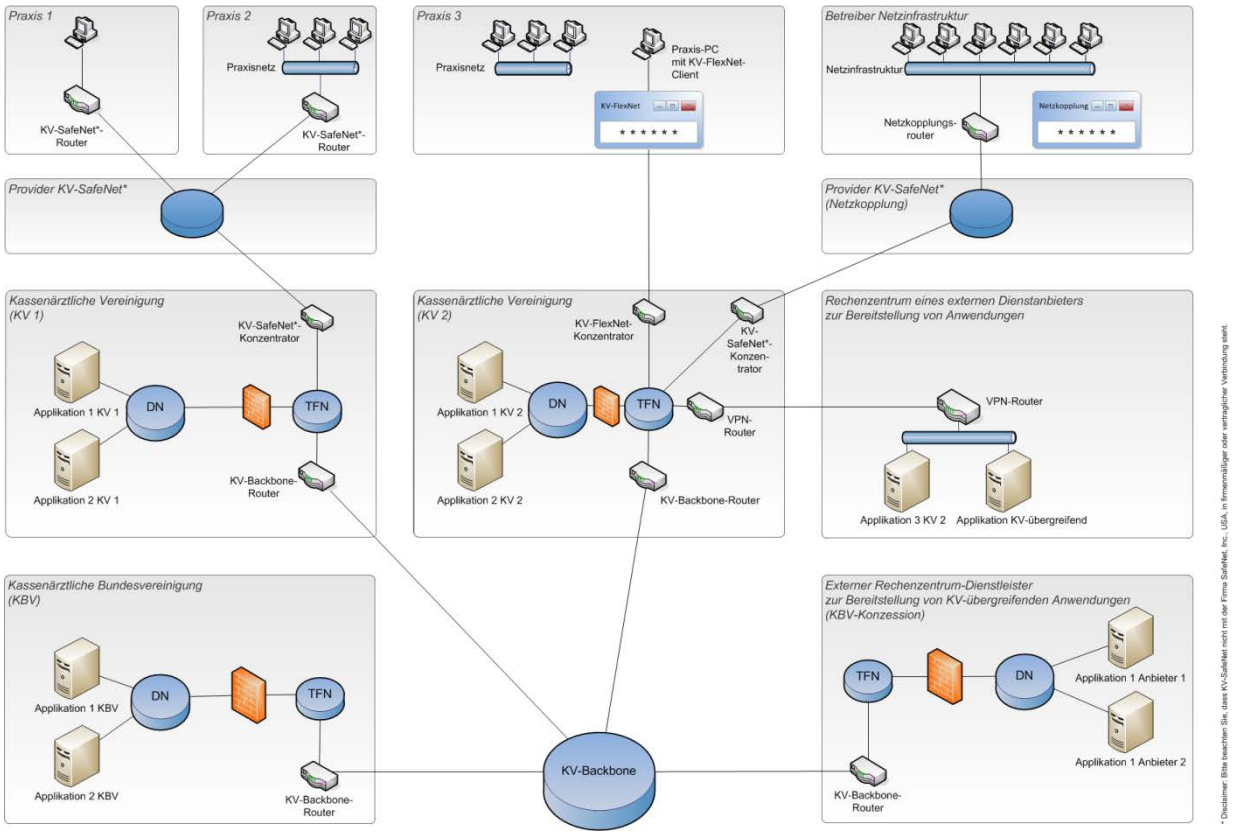

Abbildung 1: Beispielhafte Netztopologie

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

Ziel dieser Richtlinie ist es, die Sicherheitsziele im *Sicheren Netz der KVen* zu definieren. Darüber hinaus werden die zuständigen Organisationen und jeweiligen Verantwortungsbereiche benannt und beschrieben sowie Maßgaben für die jeweiligen organisationsinternen Regelungsbereiche definiert, um die Einhaltung der Sicherheitsziele zu gewährleisten.

1.3 Klassifizierung und Adressaten des Dokuments

Dieses Dokument ist öffentlich zu verwenden. Es richtet sich an die am *Sicheren Netz der KVen* beteiligten Akteure.

* 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 Sicherheitsziele

Informationssicherheit im *Sicheren Netz der KVen* ist eines der wichtigsten Ziele aller Beteiligten. Im Mittelpunkt steht damit die Gewährleistung folgender Grundeigenschaften:

- Verfügbarkeit,
  d. h. Eigenschaft von Werten, auf Verlangen zugänglich und nutzbar zu sein
- Integrität,
  d. h. Eigenschaft der Absicherung von Richtigkeit und Vollständigkeit von Werten
- Vertraulichkeit,
  d. h. Eigenschaft, dass Informationen unberechtigten Personen, Einheiten oder Prozessen nicht verfügbar gemacht oder enthüllt werden

Sicherheitsziele für das Sichere Netz der KVen

Von besonderer Bedeutung ist der Datenschutz, insbesondere von Sozialdaten und weiteren personenbezogenen Daten. Die Anforderungen an Vertraulichkeit und Integrität orientieren sich an der Gesetzeskonformität. Die Anforderungen des Datenschutzes sind bei der Bearbeitung personenbezogener Daten uneingeschränkt zu erfüllen.

Informationen und Systeme werden bezüglich ihrer Verfügbarkeit so gesichert, dass die zu erwartenden Ausfallzeiten toleriert werden können. Ausfallzeiten, die zu größeren Arbeitsverzögerungen oder Fristversäumnissen führen können, sollen durch entsprechende Maßnahmen vermieden werden.

Maßnahmen zur Informationssicherheit müssen in einem wirtschaftlich vertretbaren Verhältnis zum Wert der zu schützenden Informationen stehen. Schadensfälle mit hohen finanziellen oder immateriellen Auswirkungen müssen verhindert werden.

Zur Erreichung der Sicherheitsziele und kontinuierlichen Verbesserung des Sicherheitsniveaus im *Sicheren Netz der KVen* werden nachfolgend die Verantwortungs- und Regelungsbereiche der beteiligten Akteure beschrieben.

Grundsätzlich lassen sich die Maßgaben für die Informationssicherheit dabei aus ISO 27001 und ISO 27002 und darüber hinaus aus den Anforderungen des Bundesamtes für Sicherheit in der Informationstechnik (BSI) sowie weiterer anerkannter Organisationen ableiten.

Die beteiligten Akteure sind aufgefordert, ein dokumentiertes Informationssicherheitsmanagementsystem (ISMS) festzulegen, umzusetzen, durchzuführen, zu überwachen, zu überprüfen, instand zu halten und zu verbessern. Idealerweise streben die beteiligten Akteure eine Zertifizierung ihres Informationssicherheitsmanagementsystems nach ISO 27001 an.

2.2 Akteure und Verantwortungsbereiche

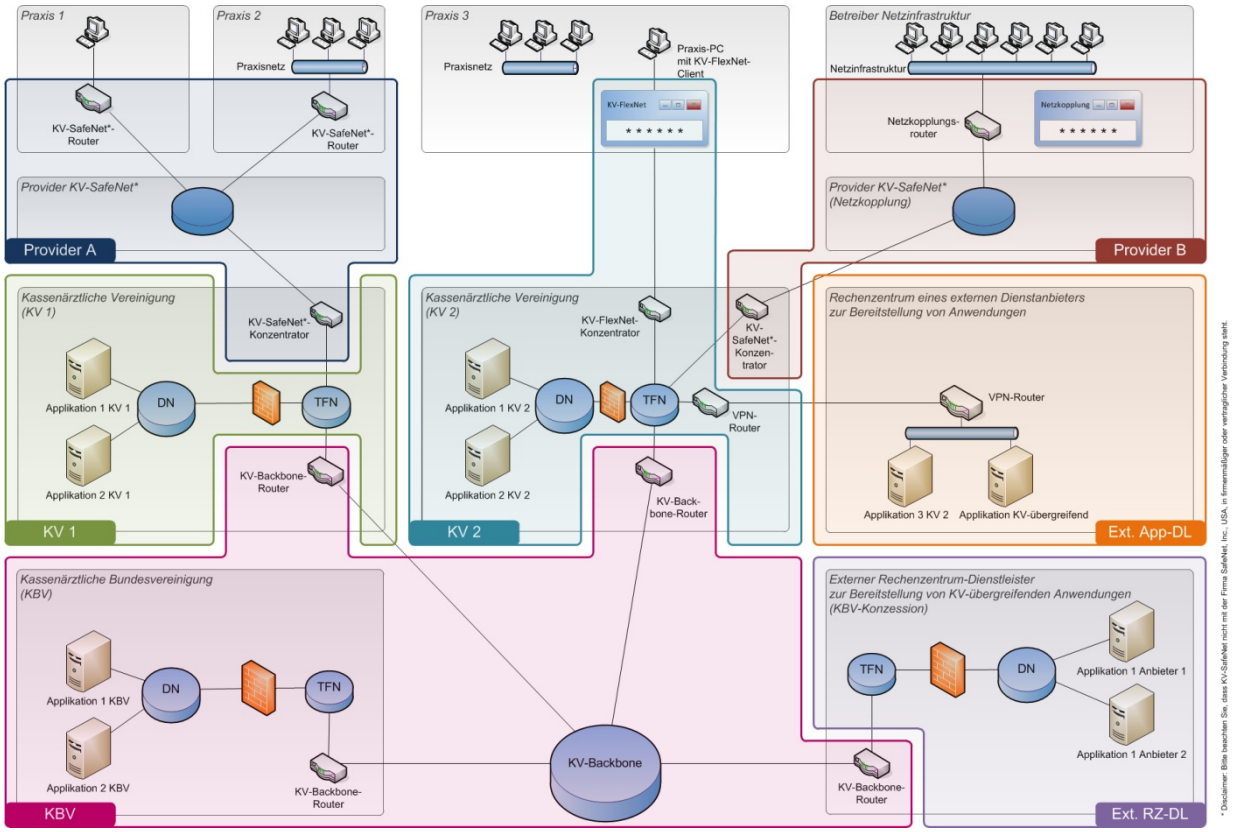

Abbildung 2: Grafische Darstellung der Verantwortungsbereiche

Abbildung 2 verdeutlicht schematisch die Verantwortungsbereiche und zuständigen Akteure im *Sicheren Netz der KVen*. Dies sind die Kassenärztliche Bundesvereinigung, die Kassenärztlichen Vereinigungen, externe Applikationsdienstleister und Rechenzentrumsdienstleister sowie KV-SafeNet-Zugangsprovider. Im Folgenden werden für die genannten Organisationen die Verantwortungsbereiche definiert.

2.2.1 Kassenärztliche Bundesvereinigung

Die KBV übernimmt im Rahmen des *Sicheren Netzes der KVen* folgende Verantwortung:

- Koordinierung übergreifender Regelungen und Maßnahmen
- Übergreifendes Sicherheitsmanagement und Koordination von Datenschutzfragen
- Regulierung der Zugangsvarianten:
  KV-SafeNet, KV-SafeNet (Netzkopplung), KV-FlexNet
- Zertifizierung und Überprüfung der Zugangsprovider:
  KV-SafeNet, KV-SafeNet (Netzkopplung), KV-FlexNet
- Regulierung der Applikationen (KV-Apps)
- Zertifizierung / Registrierung der KV-Apps
- Konzessionsvergabe für Rechenzentrumsdienstleister
- Betrieb des KV-Backbone (inkl. KV-Backbone-Router in den KVen und beim Rechenzentrumsdienstleister)
- Infrastrukturdienste wie Domain Name Service und Network Time Protocol
- IP-Adressvergabe an Provider, Applikationsdienstleister und KVen
- Routingvorgaben
- Netzüberwachung (Monitoring) des KV-Backbone
- Betrieb von KBV-Applikationen
- Betrieb des Transfer- und Servicenetzes der KBV

2.2.2 Kassenärztliche Vereinigung

Die KVen übernehmen im Rahmen des *Sicheren Netzes der KVen* folgende Verantwortung:

- Zulassung der Teilnehmer
- Evtl. Anbindung der Teilnehmer (KV-FlexNet)
- Evtl. Betrieb der Infrastruktur zu KV-FlexNet
- Zertifizierung von regionalen Applikationen externer Anbieter
- Betrieb von registrierten KV-Applikationen
- Evtl. Betrieb von zertifizierten überregionalen Applikationen
- Betrieb des Transfer- und Servicenetzes der KV
- Evtl. Domain Name Service
- Evtl. Anbindung von externen Applikationsdienstleistern

2.2.3 Externer Applikationsdienstleister

Der externe Dienstanbieter ist verantwortlich für den Betrieb von zertifizierten Applikationen.

2.2.4 Rechenzentrumsdienstleister

Der Rechenzentrumsdienstleister übernimmt im Rahmen des *Sicheren Netzes der KVen* folgende Verantwortung:

- Betrieb von zertifizierten Applikationen entsprechender Applikationsdienstleister
- Betrieb des Transfer- und ggf. auch eines Servicenetzes

2.2.5 KV-SafeNet-Zugangsprovider

Die KV-SafeNet-Provider übernehmen im Rahmen des *Sicheren Netzes der KVen* folgende Verantwortung:

- Anbindung der Teilnehmer: KV-SafeNet, KV-SafeNet (Netzkopplung)
- Betrieb der jeweiligen KV-SafeNet-Infrastruktur (inklusive Konzentrator in der KV)

2.3 Bereiche des Informationssicherheitsmanagements

Die in Abschnitt 2.2 definierten Organisationen im *Sicheren Netz der KVen* tragen eine hohe Verantwortung für die Sicherheit und Funktionsfähigkeit des Netzes, der Kommunikation und des Datenaustauschs. Von besonderer Bedeutung ist dabei der Schutz der personenbezogenen Sozialdaten. Diese Verantwortung muss dadurch gewährleistet werden, dass jeder Partner in seinem Verantwortungsbereich klare Maßgaben zur Erreichung in Abschnitt 2.1 definierten Sicherheitsziele trifft und deren Einhaltung überwacht.

Insbesondere in den folgenden Bereichen sollen die beteiligten Organisationen daher gemäß dem PDCA-Modell[2] interne Regelungen treffen, umsetzen, überprüfen und kontinuierlich verbessern:

- 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

Die für diese Bereiche notwendigen Regelungen und Maßnahmen sind in den nachfolgenden Abschnitten umrissen.

2.3.1 Sicherheitsleitlinie und Organisation der Sicherheit

Es sollen grundsätzliche Regelungen zum Sicherheitsmanagement der Organisation getroffen werden. Hierzu gehören unter anderem:

- Definition der organisationsweiten Sicherheitsziele und deren strategische Einordnung sowie deren Veröffentlichung in der Sicherheitslinie der Organisation
- Verantwortung des Managements für die Informationssicherheit
- Regelungen zu Dokumenten und Aufzeichnungen
- Maßnahmen zur kontinuierlichen Überprüfung der Informationssicherheit

[2] PDCA: Plan – Do – Check – Act (Regelkreis).

Darüber hinaus soll die Sicherheitsorganisation beschrieben sein. Hierbei sind die verantwortlichen Stellen und Aufgaben zu benennen, u.a.

- Management
- Informationssicherheitsbeauftragter
- Datenschutzbeauftragter
- Administratoren
- Weitere Verantwortlichkeiten

Zur regelmäßigen Einschätzung des Sicherheitsniveaus und der Priorisierung von Maßnahmen wird die *Umsetzung eines Risikomanagements* empfohlen.

2.3.2 Datenschutz, Vertraulichkeit und Zugangskontrolle

Unter der Berücksichtigung der rechtlichen Maßgaben sollen Regelungen zum Datenschutz und zur Vertraulichkeit getroffen werden. Darüber hinaus sollen Maßgaben beschrieben sein, die die Vertraulichkeit von Informationen und die Wahrung des Datengeheimnisses gewährleisten. Es empfiehlt sich zudem klare Regelungen zur Klassifizierung (sicherheitsrelevante Einstufung) von Daten und Informationen zu definieren.

Darüber hinaus sollen formale Verfahren zur Vergabe und Kontrolle von Zugangsrechten[3] (Benutzerverwaltung) dokumentiert und umgesetzt sein. Entsprechende vergebene Berechtigungen sind zu dokumentieren. Es soll gewährleistet werden, dass nur berechtigte Personen Zugang zu Informationssystemen und entsprechenden Dokumenten (z.B. Verträge) erlangen können. Berechtigte Personen sind dabei zur Verschwiegenheit verpflichtet.

2.3.3 Personalsicherheit

Die Personalsicherheit der Organisation soll geregelt sein. Hierzu gehören insbesondere alle Maßnahmen bezogen auf:

- Personalbeschaffung und -auswahl
- Arbeitsvertragliche Regelungen
- Sensibilisierung, Ausbildung und Schulung des Personals
- Disziplinarische Maßnahmen bei Regelverstößen
- Verantwortlichkeiten bei Beendigung von Arbeitsverhältnissen

2.3.4 Gebäude- und Arbeitsplatzsicherheit

Im Rahmen der Gebäude- und Arbeitsplatzsicherheit sollen unter anderem zu folgenden Bereichen Regelungen getroffen werden:

- Zutritt zu Gebäude und Gebäudeteilen (Zutrittskontrolle)
- Einbruchssicherung, Überwachung und Alarmierung
- Versorgung (Strom. Klima, Internet etc.)

[3] Mit Zugang ist nicht der Zutritt zu Gebäuden und Räumlichkeiten gemeint, vielmehr geht es hier um Zugang zu Informationssystemen und Zugriff auf Daten.

2.3.5 Management der Betriebs- und Kommunikationsprozesse

Im Rahmen des Betriebs- und Kommunikationsmanagements soll die Organisation unter anderem Folgendes regeln:

- Dokumentation der Betriebs- und Supportprozesse
- Systemplanung und –abnahme
- Änderungsmanagement (Change Management)
- Datensicherung und –wiederherstellung
- Systemadministration
- Netzwerkmanagement und -überwachung (Monitoring)
- Regelung zur Dienstleistungserbringung Dritter

2.3.6 Beschaffung, Entwicklung und Wartung

Neben den Betriebsprozessen sollen auch die Prozesse für Beschaffung, Entwicklung und Wartung von Informationssystemen definiert sein. Dabei sind unter anderem die folgenden Bereiche zu beachten:

- Genehmigungsverfahren sowie Entwicklungs- und Testmethoden
- Maßnahmen zum Schutz von Systemdaten, Konfigurationsdaten und Testdaten
- Kryptographische Maßnahmen
- Changemanagement

2.3.7 Management von Informationssicherheitsereignissen

Informationssicherheitsereignisse sind alle Ereignisse, die beeinträchtigend auf die Vertraulichkeit, Integrität oder Verfügbarkeit von Informationen wirken. Dazu zählen u. a.

- Verlust von Einrichtungen, Geräten oder Diensten
- Störungen oder Überlastung von Systemen
- Menschliche Fehler
- Nichteinhaltung von Richtlinien und Verfahren
- Verstöße gegen physische Sicherheitsmaßnahmen
- Unkontrollierte Änderungen an Systemen
- Fehler in Hard- oder Software
- Verletzung von Zutritts-, Zugangs- oder Zugriffsregeln

Je Organisation sollen Regelungen zur Klassifizierung und zum Umgang mit Informationssicherheitsereignissen gelten und im Rahmen eines Incident Management umgesetzt sein.

2.3.8 Business Continuity Management

Business Continuity Management (BCM), auch betriebliches Kontinuitätsmanagement genannt, beschäftigt sich mit der Notfallvorsorge 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.

Ausgehend von der grundsätzlichen organisatorischen Regelung zum BCM sollen, insbesondere für kritische Geschäftsprozesse Notfallpläne vorliegen, die im konkreten Schadensfall die Aufrechterhaltung des Betriebs ermöglichen.

2.3.9 Compliance

Unter Compliance wird die Einhaltung der gesetzlichen, unternehmensinternen und vertraglichen Regelungen verstanden. Darüber hinaus gilt insbesondere im *Sicheren Netz der KVen* die Einhaltung der anwendbaren Richtlinien und daraus abgeleiteter dokumentierter Maßgaben (zum Beispiel Leitfäden).

2.4 Umsetzung

Zur Erreichung der in Abschnitt 2.1 definierten Sicherheitsziele, die die in Abschnitt 2.2 beschriebenen Bereiche umspannen, ist es erforderlich ein Informationssicherheitsmanagementsystem (ISMS) zu etablieren. Dies für das gesamte *Sichere Netz der KVen* zentral zu betreiben ist nicht möglich. Daher begründet sich die Forderung, dass die beteiligten Akteure für sich ein dokumentiertes ISMS festlegen, umsetzen, durchführen, überwachen, überprüfen, instand halten und verbessern sowie idealerweise nach ISO 27001 zertifizieren.

Die KBV betreibt ein Informationssicherheitsmanagementsystem (ISMS), welches nach der internationalen Norm ISO 27001 zertifiziert ist. Die KBV referenziert im Zusammenhang mit dem Sicheren Netz der KVen auf die Regelungen und Maßnahmen ihres ISMS bzw. adaptiert diese entsprechend. Dienstleister, die Aufgaben im Rahmen des Verantwortungsbereiches der KBV übernehmen, werden unter anderem auch nach Gesichtspunkten des ISMS ausgewählt, vertraglich gebunden und gesteuert.

Die konkreten Anforderungen in den jeweiligen Regelungsbereichen sind in Form von Richtlinien und zu gehörigen Dokumenten definiert. Hierzu zählen insbesondere:

- Richtlinie KV-SafeNet [KBV_SNK_RLEX_KV-SafeNet]:
  Regulierung der Zugangsvariante KV-SafeNet
- Richtlinie KV-SafeNet (Netzkopplung) [KBV_SNK_RLEX_Netzkopplung]:
  Regulierung der Zugangsvariante KV-SafeNet (Netzkopplung)
- Richtlinie KV-FlexNet [KBV_SNK_RLKV_KV-FlexNet]:
  Regulierung der Zugangsvariante KV-FlexNet
- Richtlinie KV-Apps [KBV_SNK_RLKV_KV-Apps]:
  Regulierung von Applikationen im *Sicheren Netz der KVen*
- Richtlinie Föderiertes Identitätsmanagement [KBV_SNK_RLKV_FIM]:
  Maßgaben zum Benutzer-Management
- Richtlinie Dokumentenlenkung [KBV_SNK_RLKV_Dokumentenlenkung]:
  Maßgaben zur Lenkung von Dokumenten
- Richtlinie Übergreifendes Risikomanagement [KBV_SNK_RLEX_Risikomanagement]:
  Maßgaben und Beispiele zur Risikomanagementmethode
- Richtlinie Übergreifendes Business Continuity Management [KBV_SNK_RLEX_BCM]:
  Maßgaben und Beispiele zum Business Continuity Management

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
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.
Informationssicherheits-managementsystem (ISMS)	Teil des gesamten Managementsystems, der auf der Basis eines Geschäftsrisikoansatzes die Entwicklung, Implementierung, Durchführung, Überwachung, Überprüfung, Instandhaltung und Verbesserung der Informationssicherheit abdeckt.
Integrität	Eigenschaft der Absicherung von Richtigkeit und Vollständigkeit von Werten.
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.

Begriff	Erklärung
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.
Risiko	Möglichkeit, dass eine gegebene Bedrohung eine Schwachstelle eines Wertes oder eine Gruppe von Werten ausnutzt und dabei Schaden für die Organisation verursacht. Es wird als Kombination von Eintrittswahrscheinlichkeit und Auswirkung errechnet (Risikograd).
Risikomanagement	Gesamte Vorgehensweise des Identifizierens, Steuerns, Eliminierens oder Minderns unbestimmter Risiken, die Werte beeinträchtigen können.
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.
Verfügbarkeit	Eigenschaft von Werten, auf Verlangen zugänglich und nutzbar zu sein.
Vertraulichkeit	Eigenschaft, dass Informationen unberechtigten Personen, Einheiten oder Prozessen nicht verfügbar gemacht oder enthüllt werden.
Wert	Werte sind alle Informationen und Geschäftsprozesse (primäre Werte) sowie Hardware, Soft-ware, Netzwerk, Personal, Standorte und die Organisation (unterstützende Werte), die einen Schutzbedarf bezogen auf ihre Verfügbarkeit, Vertraulichkeit bzw. Integrität haben.
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_KV-SafeNet]	Richtlinie KV-SafeNet
[KBV_SNK_RLEX_Netzkopplung]	Richtlinie KV-SafeNet (Netzkopplung)
[KBV_SNK_RLKV_KV-FlexNet]	Richtlinie KV-FlexNet
[KBV_SNK_RLKV_KV-Apps]	Richtlinie KV-Apps
[KBV_SNK_RLKV_FIM]	Richtlinie Föderiertes Identitätsmanagement
[KBV_SNK_RLKV_Dokumentenlenkung]	Richtlinie Dokumentenlenkung
[KBV_SNK_RLEX_Risikomanagement]	Richtlinie Risikomanagement
[KBV_SNK_RLEX_BCM]	Richtlinie Business Continuity Management