Kassenärztliche Bundesvereinigung
Körperschaft des öffentlichen Rechts

Sicheres Netz der KVen

Leitfaden
Überprüfung Provider

[KBV_SNK_LFEX_Überprüfung_Provider]

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 Leitfaden		alles

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.

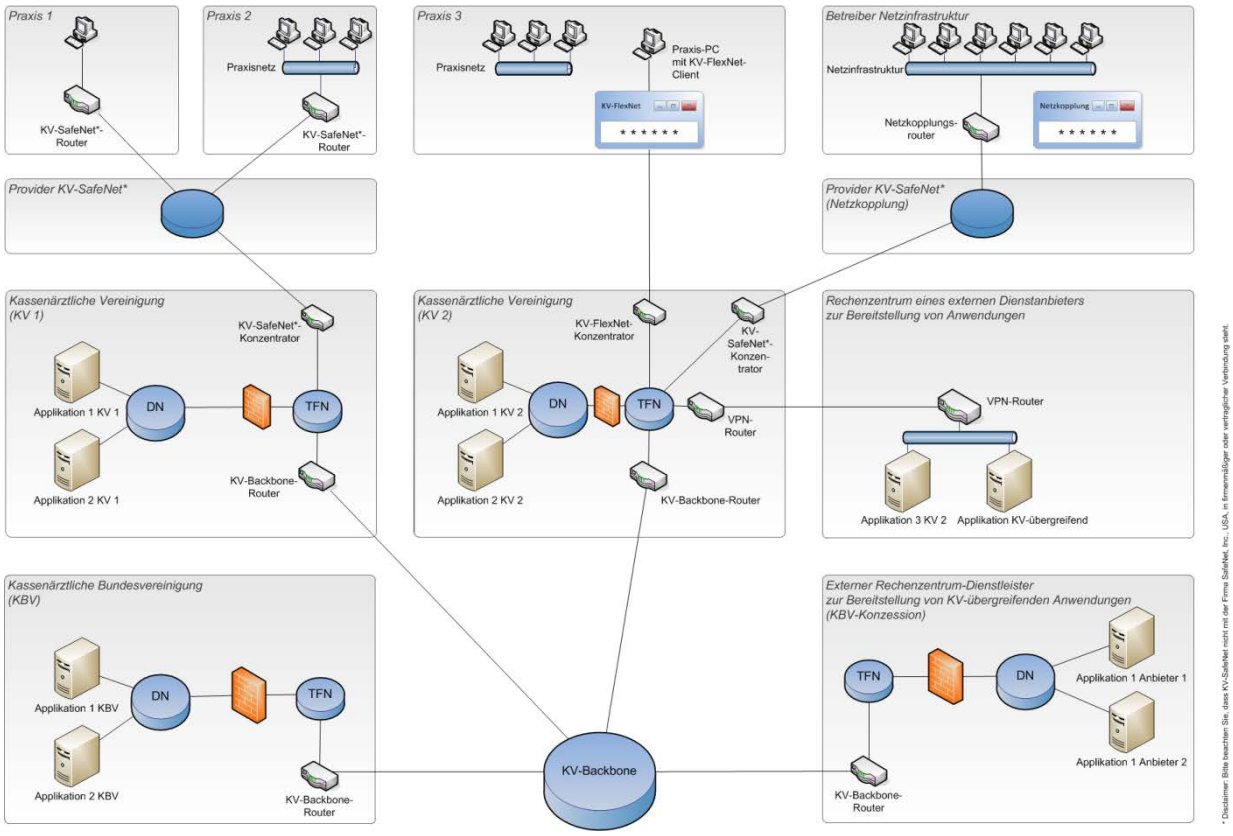

Abbildung 1: Beispielhafte Netztopologie

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

Dieses Dokument stellt den Leitfaden zur Überprüfung von KV-SafeNet-Providern und Netzkopplungsprovidern dar.

Kriterium der Überprüfung für KV-SafeNet-Provider ist die Einhaltung der Anforderungen der Richtlinie [KBV_SNK_RLEX_KV-SafeNet] und für Netzkopplungsprovider die Einhaltung der Anforderungen der Richtlinie [KBV_SNK_RLEX_Netzkopplung].

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 Anbieter von KV-SafeNet- und Netzkopplungslösungen.

* 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

Gemäß der Richtlinie [KBV_SNK_RLEX_KV-SafeNet] und darauf aufbauend der Richtlinien [KBV_SNK_RLEX_Netzkopplung] ist die KBV berechtigt, die Einhaltung aller Maßgaben dieser Richtlinien durch den Anbieter in regelmäßigen Abständen durch eine zur Verschwiegenheit verpflichtete und von der KBV zu bestimmende Person überprüfen zu lassen.

Das vorsätzliche oder grob fahrlässige Verschweigen oder Verfälschen von Informationen durch den Provider im Rahmen von Überprüfungsmaßnahmen ist als Verstoß gegen Maßgaben der Richtlinien [KBV_SNK_RLEX_KV-SafeNet] bzw. [KBV_SNK_RLEX_Netzkopplung] zu werten und kann zudem weitere juristische Maßnahmen zur Folge haben.

2.1 Gegenstand der Überprüfung

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

2.1.1 Auditierung

Es werden Überprüfungen der Einhaltung organisatorischer Maßgaben und Prozesse der Richtlinien [KBV_SNK_RLEX_KV-SafeNet] bzw. [KBV_SNK_RLEX_Netzkopplung] durchgeführt. Diese Audits beinhalten eine Vor-Ort-Prüfung beim Anbieter sowie eine Prüfung ausgewählter Prozesse und Dokumente.

2.1.2 Penetrationstest

Es werden durch die KBV zwei ausgewählte KV-SafeNet-Router unterschiedlichen Typs oder ein Netzkopplungsrouter sowie ein Konzentrator einer sicherheitstechnischen Überprüfung unterzogen. Die Auswahl der Geräte obliegt der KBV.

2.2 Prüfer

Die Überprüfung wird durch eine zur Verschwiegenheit verpflichtete und von der KBV bestimmte Person (im folgenden Prüfer genannt) durchgeführt.

Der Prüfer ist von der KBV und dem Anbieter dazu berechtigt und verpflichtet, der KBV Mitteilung über Verstöße gegen die Anforderungen der Richtlinien [KBV_SNK_RLEX_KV-SafeNet] bzw. [KBV_SNK_RLEX_Netzkopplung] zu machen.

2.3 Pflichten des Providers

Der Provider sichert die notwendige personelle Unterstützung des Prüfers durch Mitarbeiter des Providers zu.

Der Provider sichert die Möglichkeit zur Einsichtnahme des Prüfers in alle zur Überprüfung notwendigen Dokumente, Prozesse und Werkzeuge zu und gewährt dem Prüfer Zutritt zu seinen Räumlichkeiten.

Für die Dauer der Penetrationstests stellt der Provider dem Prüfer die von der KBV benannten KV-SafeNet-Router bzw. Netzkopplungsrouter unentgeltlich zur Verfügung. Nach erfolgter Prüfung erhält der Provider die Geräte zurück.

Der Provider hat entsprechend Abschnitt 2.8 identifizierte Schwachstellen bzw. Abweichungen innerhalb eines von der KBV zu bestimmenden, angemessenen Zeitraums zu beseitigen und der KBV Mitteilung über den erfolgreichen Abschluss der Maßnahmen machen.

2.4 Pflichten des Prüfers

Der Prüfer muss den konkreten Termin zur Durchführungen von Audits und zur Durchführung von Penetrationstests rechtzeitig, mindestens mit einem Vorlauf von einem Monat, mit dem Provider abstimmen.

Der Prüfer hat die Pflicht, die Ergebnisse durchgeführter Überprüfung entsprechend Abschnitt 2.7 zu dokumentieren.

2.5 Vorgehensweise bei Überprüfungen

Die Grundlage der Überprüfungen bilden der Prüfkatalog Auditierung (siehe Kapitel 3) und die Maßgaben zur Durchführung von Penetrationstests (siehe Kapitel 4). Der Prüfkatalog Auditierung enthält die zu überprüfenden Themen. Anhand dieser sind die konkreten Fragestellungen und zu prüfenden Dokumente abzuleiten. Die Maßgaben zur Durchführung von Penetrationstests legen den Rahmen für die Durchführung der sicherheitstechnischen Überprüfungen der Geräte fest.

Die Überprüfung eines Providers läuft wie folgt ab:

- Die KBV legt den zu prüfenden Provider sowie Art (KV-SafeNet oder Netzkopplung) und Routertyp der Überprüfungen fest und bittet den Prüfer um Durchführung.
- Der Prüfer stimmt die Überprüfung mit dem Provider ab und schließt einen entsprechenden Vertrag mit dem zu prüfenden Provider.
- Der Prüfer teilt der KBV den Prüftermin sowie den Zeitraum der Überprüfung mit.
- Der Prüfer führt die Überprüfung durch und übermittelt der KBV und dem Provider die Prüfergebnisse entsprechend Abschnitt 2.7.
- Die KBV stimmt ggf. erforderliche Maßnahmen mit dem Provider ab und setzt eine angemessene Frist zur Umsetzung.
- Der Provider meldet der KBV fristgerecht die Umsetzung der festgelegten Maßnahmen.

2.6 Kosten der Überprüfung

Die Kosten der Überprüfung trägt der Provider. Der Kostenrahmen ist wie folgt festgelegt.

Art der Prüfung	Kosten in €
Auditierung (Dokumentenprüfung und Vor-Ort-Audit inklusive Dokumentation)	**3.500,-**
Penetrationstest (zwei KV-SafeNet-Router unterschiedlichen Typs oder ein Netzkopplungsrouter sowie ein Konzentrator inklusive Dokumentation)	**6.500,-**

Der genannte Kostenrahmen versteht sich als Obergrenze und zuzüglich der gesetzlich vorgeschriebenen Mehrwertsteuer.

2.7 Dokumentation der Überprüfungsergebnisse

Die im Test ermittelten Schwachstellen sind in einem ausführlichen Testbericht für den Provider und die KBV zu dokumentieren. Der Bericht muss mindestens folgende Teile enthalten:

- Management Summary
  In diesem Abschnitt sind die Ergebnisse der Tests in nichttechnischer Sprache zusammen zu fassen. Zudem muss das Management Summary einen Überblick über die ermittelten Schwachstellen und den Handlungsbedarf enthalten.
- Übersicht über alle gefundenen Schwachstellen
  In diesem Abschnitt sind alle ermittelten Schwachstellen tabellarisch aufzuführen. Die ermittelten Schwachstellen sind nach ihrer Kritikalität zu sortieren.
- Detaillierte Ergebnisse der Audits und Penetrationstests
  In diesem Abschnitt sind detailliert alle ermittelten Schwachstellen zu beschreiben. Hierzu gehören Angaben zu:
  - Schwachstellentyp
  - Detailbeschreibung zur Nachvollziehbarkeit der Schwachstelle
  - Beschreibung zur Ausnutzbarkeit der Schwachstelle durch einen Angreifer
  - Einschätzung des Risikos (Wahrscheinlichkeit und Schadensausmaß)
  - Vorschläge zur Behandlung des Risikos (Maßnahmenvorschläge)
- Zusammenfassung und Priorisierung der Maßnahmenvorschläge
  In diesem Abschnitt sind die Maßnahmenvorschläge zusammenzufassen und mit konkreten Vorschlägen zur Umsetzung zu versehen.

2.8 Bewertung der Ergebnisse und Umsetzung der Maßnahmen

Die Bewertung der Ergebnisse und Ableitung von notwendigen Maßnahmen erfolgt immer durch die KBV. Entsprechende Maßnahmen sind durch den Provider umzusetzen.

Werden die Maßnahmen nicht innerhalb einer von der KBV zu bestimmenden, angemessenen Frist umgesetzt, ist die KBV bei einer grob fahrlässigen oder vorsätzlichen Verletzung dieser Vorgaben berechtigt, dem Provider das Zertifikat wieder zu entziehen und den Teilnehmer umgehend über den Entzug der Zertifizierung zu informieren.

2.9 Verschwiegenheit

Alle Ergebnisse einer Überprüfung unterliegen der strengsten Vertraulichkeit. Eine Weitergabe von Informationen über durchgeführte Überprüfungsmaßnahmen ist nur in Ausnahmefällen und in Absprache mit der KBV möglich.

2.10 Ausschluss der Haftung

Die Haftung der KBV oder durch die KBV beauftragte Prüfer für Schäden, die aufgrund der Maßnahmen der Überprüfung entstanden sind, ist auf Vorsatz und grobe Fahrlässigkeit beschränkt, soweit es sich nicht um die Verletzung einer vertragswesentlichen Pflicht oder die Verletzung des Lebens, des Körpers oder der Gesundheit handelt. Gleiches gilt für etwaige Erfüllungsgehilfen.

3 Prüfkatalog Auditierung

3.1 Sicherheitsleitlinie, Organisation der Sicherheit

- Nachweis zu Richtungsvorgaben des Managements zur Informationssicherheit
- Definition und organisationsweite Veröffentlichung einer Sicherheitsleitlinie
- Nachweis des Engagements des Managements für Informationssicherheit
- Dokumentation der Verantwortlichkeiten zur Informationssicherheit, u.a.
    - Management
    - Informationssicherheitsbeauftragter
    - Datenschutzbeauftragter
    - Administratoren
    - Weitere Verantwortlichkeiten
- Nachweis des Prozesses der Lenkung von Dokumenten und Aufzeichnungen und der sicheren Dokumentenablage

3.2 Datenschutz, Vertraulichkeit und Zugangskontrolle

- Dokumentation und Umsetzung von grundsätzlichen Regelungen zum Datenschutz und zur Vertraulichkeit
- Dokumentation und Umsetzung von formalen Verfahren zur Vergabe und Kontrolle von Zugangsrechten[2] (Benutzerverwaltung)
- Nachweis, dass nur berechtigte Personen Zugang zu KV-SafeNet-Routern, Netzkopplungsroutern und Konzentratoren sowie zu verwendeten Administrationswerkzeugen und entsprechenden Dokumenten (z.B. Verträge) erlangen können
- Nachweis, dass die berechtigte Personen zur Verschwiegenheit verpflichtet sind

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

3.3 Personalsicherheit

3.3.1 Ein-/Austritt von Mitarbeitern

- Nachweis geregelter Prozesse bei Ein- und Austritt von Mitarbeitern, insbesondere
  - Überprüfung der Eignung von Mitarbeitern vor der Einstellung
  - Nachweis der korrekten Zuordnung von Rechten und Rollen zu Mitarbeitern
  - Gewährleistung, dass Mitarbeiter nach Austritt keinen Zugang mehr zu Informationssystemen des Unternehmens haben
  - Nachweis der Deaktivierung und Löschung von Rechten und Rollen nach Austritt des Mitarbeiters

3.3.2 Sensibilisierung und Schulung

- Nachweis über die Durchführung regelmäßiger Maßnahmen zur Schulung und Sensibilisierung der Mitarbeiter

3.3.3 Vertretungsregelungen

- Nachweis von Vertretungsregelungen für definierte Rollen und Prozesse
- Nachweise dokumentierter Übergaben von Verantwortlichkeiten

3.3.4 Regelungen mit Erfüllungsgehilfen, Auftragnehmern und Dritten

- Nachweis der vertraglichen Regelungen zwischen Provider und Auftragnehmern, insbesondere
  - Vertraulichkeitserklärungen
  - Erklärung über die Einbeziehung von Erfüllungsgehilfen

3.4 Gebäude- und Arbeitsplatzsicherheit

3.4.1 Zutrittsregelungen

- Definition geeigneter Sicherheitsbereiche
- Nachweis der Zutrittsregelungen zu Gebäuden, Räumlichkeiten, Systemen (technisch und organisatorisch)

3.4.2 Einbruchsicherungen, Überwachungen, Alarmierungen

- Nachweis von Überwachungs- und Alarmierungssystemen zur Feststellung von unbefugtem Eindringen
- Angemessener baulicher und technischer Einbruchsschutz

3.4.3 Versorgung

- Nachweis der gemäß definierten Verfügbarkeitsanforderungen angemessenen Versorgung mit Strom, Klimatisierung, Internet etc.
- Nachweis einer redundanten Auslegung kritischer Systeme

3.5 Management der Betriebs- und Kommunikationsprozesse

3.5.1 Betriebs- und Supportprozesse Konzentrator

- Technische Dokumentation des Konzentrators und der Schutzmaßnahmen
- Dokumentation der Betriebs- und Supportprozesse zum Konzentrator
- Nachweis der vertraglichen Vereinbarungen mit der KV (Aufstellungsort, Raum, Service usw.)

3.5.2 Betriebs- und Supportprozesse KV-SafeNet-Router, Netzkopplungsrouter

- Technische Dokumentation der KV-SafeNet-Router und Netzkopplungsrouter und der Schutzmaßnahmen
- Dokumentation der Betriebs- und Supportprozesse zum KV-SafeNet-Router und Netzkopplungsrouter (Teilnehmersupport)
- Nachweis der vertraglichen Vereinbarungen mit dem Teilnehmer (Teilnehmervertrag)

3.5.3 Änderungsmanagement

- Nachweis eines geregelten Verfahrens zur Durchführung von Änderungen an Informationssystemen (Change Management)
- Nachweis der Einhaltung der Richtlinien-Vorgaben zur Fernwartung der KV-SafeNet-Router und Netzkopplungsrouter

3.5.4 Prozesse zur Verwaltung von Teilnehmeranschlüssen

- Nachweis zur Umsetzung folgender Prozesse:
    - Einrichtung eines neuen Zugangs
    - Temporäre Sperrung eines Zugangs
    - Erneute Freischaltung eines Zugangs
    - Endgültige Sperrung bei Kündigung

3.5.5 Netzwerkmanagement

- Nachweis zu eingesetzten Verfahren und Werkzeugen zur Netzwerküberwachung sowie zu Intrusion Detection / Intrusion Prevention
- Nachweis über dokumentierte Prozesse des Erkennens, Abwehrens und Verhinderns von Störungen und Angriffen

3.6 Beschaffung, Entwicklung und Wartung

- Nachweis über die Analyse und Spezifikation von Sicherheitsanforderungen bei der Beschaffung, Entwicklung und Wartung von Informationssystemen, insbesondere bezogen auf:
    - KV-SafeNet-Router
    - Netzkopplungsrouter
    - Konzentrator
- Dokumentierte Regelungen zur Anwendung kryptografischer Maßnahmen sowie Nachweis über deren Umsetzung
- Nachweis über geeignete Maßnahmen zum Schutz von Systemdaten, Konfigurationsdaten und Testdaten
- Nachweis über geeignete Testverfahren für entwickelte, beschaffte bzw. gewartete Informationssysteme vor Inbetriebnahme
- Nachweis über die regelmäßige Kontrolle von technischen Schwachstellen

3.7 Management von Informationssicherheitsereignissen

- Nachweis eines geregelten Verfahrens zum Umgang mit Informationssicherheitsereignissen und Verbesserungen
    - Dokumentation des Prozesses
    - Dokumentation der Verantwortlichkeiten
    - Lernen aus Sicherheitsereignissen
- Nachweise über die Behandlung von Informationssicherheitsereignissen (Störfälle, Angriffe, Schwachstellen etc.):
    - Melden von Ereignissen, Funktionsfähigkeit der Hotline
    - Aufnahme, Dokumentation und Klassifizierung
    - Bearbeitung, Abschluss und Dokumentation der Lösung
    - Kommunikation

3.8 Business Continuity Management (BCM)

- Dokumentation des BCM- / Notfallkonzeptes für kritische Prozesse und Systeme auf der Grundlage einer Business Impact Analyse / Risikoanalyse
- Nachweise über
    - Alarmierungsplan bei Notfällen
    - Grundlegende Festlegungen für Notfallpläne
    - Test von Notfallplänen
    - Festlegung von Verantwortlichkeiten
- Nachweise über aktuelle Notfallpläne für die Szenarien
    - Ausfall Konzentrator
    - Ausfall KV-SafeNet-Router bzw. Netzkopplungsrouter
    - Ausfall von Versorgungseinrichtung am Standort des Providers

3.9 Compliance

3.9.1 Einhaltung der gesetzlichen und organisationsinternen Vorgaben

- Nachweis über die Identifikation, Dokumentation und die Überprüfung der Einhaltung der anwendbaren Gesetze und vertraglichen Vorgaben
- Nachweis über die Überprüfung der Einhaltung der organisationsinternen Sicherheitsrichtlinien und Standards

3.9.2 Einhaltung der Richtlinien-Maßgaben

- Nachweis zur Einhaltung der Maßgaben der zum Zeitpunkt der Zertifizierung gültigen Richtlinie [KBV_SNK_RLEX_KV-SafeNet] bzw. [KBV_SNK_RLEX_Netzkopplung], insbesondere zu
    - Anbindung der Teilnehmer
    - Schutz der Anbindung
    - Berichtswesen
    - Teilnehmervertrag
    - Technischen Anforderungen

3.9.3 Aktualität der bei der Zertifizierung gemachten Angaben

- Prüfung der Vollständigkeit und Aktualität der zur Zertifizierung, Rezertifizierung oder Konformitätserklärung eingereichten Unterlagen, u.a.
    - Ergänzende Erklärung
    - Ansprechpartner
    - Bezeichnung der zertifizierten KV-SafeNet-Router, Netzkopplungsrouter und Konzentratoren
    - Muster-Teilnehmervertrag
    - Ansprechpartner, Hotline

4 Maßgaben zur Durchführung von Penetrationstests

4.1 Testgegenstand

Der Penetrationstest ist die technische Überprüfung der Sicherheit der zertifizierten Geräte (KV-SafeNet-Router, Netzkopplungsrouter, Konzentrator). Durch kontrollierte Angriffe auf die Geräte können sicherheitsrelevante Schwachstellen aufgezeigt werden.

Für die Durchführung von Penetrationstests der KV-SafeNet-Router und Netzkopplungsrouter sind Testgeräte zu verwenden. Die Penetrationstests des Konzentrators werden nur in enger Absprache mit Provider, KBV und betroffenen KVen durchgeführt.

Im Test ist zu untersuchen, ob die Router der Provider geeignet gegen Angriffe und Manipulation geschützt sind. Hierzu gehört insbesondere der Schutz des Praxisnetzes vor unberechtigten Zugriffen. Ebenso wird die Sicherheit der eingesetzten VPN-Konzentratoren getestet.

4.2 Testschwerpunkte

Ziel des Penetrationstests ist es, mögliche sicherheitsrelevante Schwachstellen aufzudecken. Folgende Testschwerpunkte sind beachten:

- Vertraulichkeit
  Die zu testenden Systeme verwalten verschiedene vertrauliche Daten. Im Test ist zu prüfen, inwieweit ein Angreifer Zugriff auf diese Informationen erlangen kann.
- Integrität
  Es ist zu testen, ob ein Angreifer gespeicherte Daten unberechtigt manipulieren kann.
- Verfügbarkeit
  Ein gezielter Angriff auf die Verfügbarkeit der Systeme ist nicht Teil des Tests, da dieser den produktiven Betrieb erheblich stören kann. Sollten im Testverlauf Möglichkeiten für einfache Angriffe auf die Verfügbarkeit auffallen, so sind diese erst nach Rücksprache weiter zu untersuchen.

5 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 Dienstnetzes 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.
Netzkopplungsprovider	Von der KBV nach der Richtlinie KV-SafeNet (Netzkopplung) zertifizierter Anbieter, der die Netzkopplung durchführt und damit Teilnehmern aus angeschlossenen Netzinfrastrukturen einen Zugang zum *Sicheren Netz der KVen* ermöglicht. Siehe auch KV-SafeNet-Provider.
Netzkopplungsrouter	Ein Netzkopplungsrouter dient dem Anschluss größerer Netzinfrastrukturen an das *Sichere Netz der KVen*. Er wird von einem Netzkopplungsprovider bereitgestellt. Ein Netzkopplungsrouter ist ein nicht manipulierbarer Router. 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 den Rechenzentren der jeweiligen KV und der KBV ermöglicht. Teilnehmer aus der angeschlossenen Netzinfrastruktur müssen sich vor einem Zugriff auf *Das Sichere Netz der KVen* am Netzkopplungsrouter mit sicheren Verfahren authentifizieren. Die Zugriffe auf das *Sichere Netz der KVen* werden protokolliert. Die Verantwortung für den Netzkopplungsrouter trägt der 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.

6 Referenzierte Dokumente

Referenz	Dokument
[KBV_SNK_RLEX_KV-SafeNet]	Richtlinie KV-SafeNet
[KBV_SNK_LFEX_Zert_KV-SafeNet]	Leitfaden Zertifizierung KV-SafeNet-Provider
[KBV_SNK_RLEX_Netzkopplung]	Richtlinie KV-SafeNet (Netzkopplung)
[KBV_SNK_LFEX_Zert_Netzkopplung]	Leitfaden Zertifizierung Netzkopplungsprovider