Kassenärztliche Bundesvereinigung

Körperschaft des öffentlichen Rechts

Sicheres Netz der KVen

Merkblatt Sicherheitsanforderungen KV-SafeNet-Arbeitsplätze

[KBV_SNK_MBEX_Sicherheit_Arbeitsplätze]

Dezernat 6
Informationstechnik, Telematik und Telemedizin

10623 Berlin, Herbert-Lewin-Platz 2

Kassenärztliche Bundesvereinigung

Version	1.1
Datum:	31.10.2011
Klassifizierung:	Öffentlich
Status:	In Kraft

DOKUMENTENHISTORIE

Version	Datum	Autor	Änderung	Begründung	Seite
1.1	31.10.2011	KBV	Dokumentenlenkung, und redaktionelle Anpassungen		
1.0	06.03.2009	KBV	Initiales Dokument		

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.

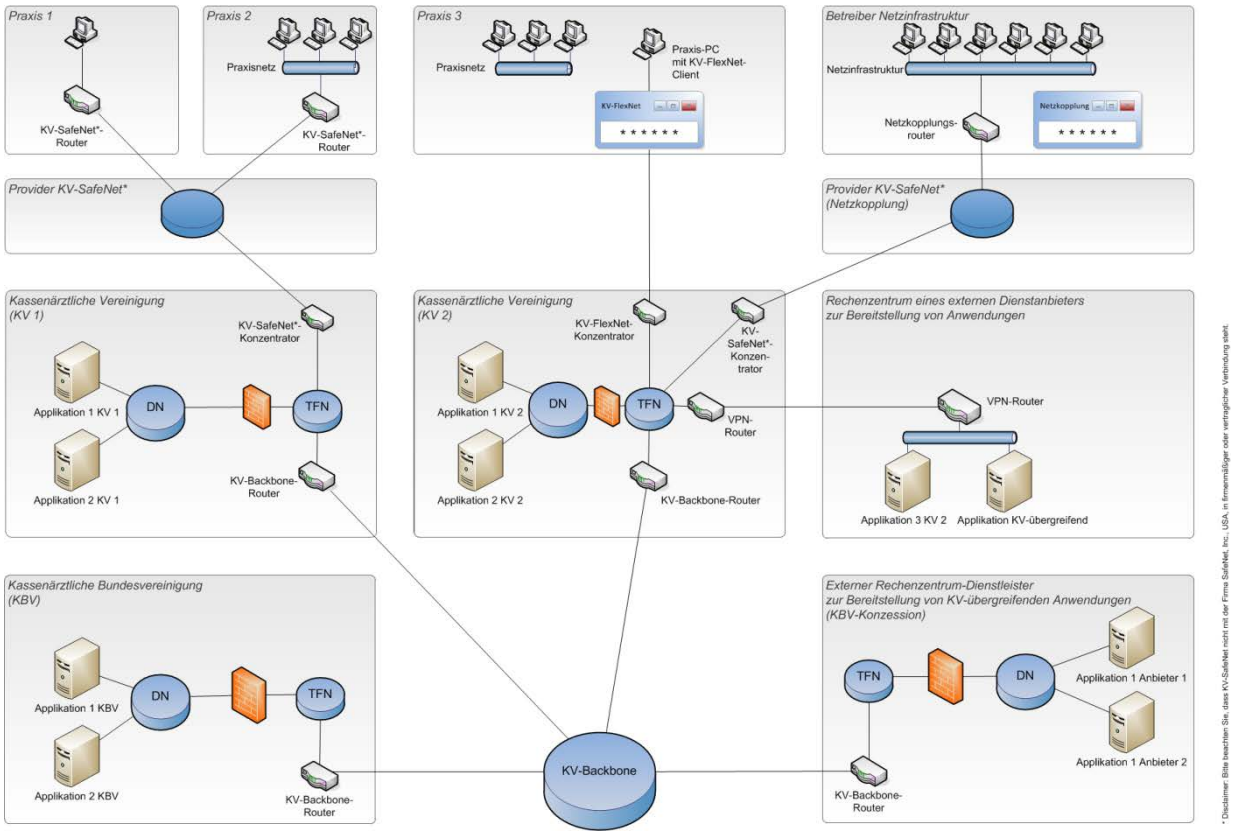

Abbildung 1: Beispielhafte Netztopologie

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

Durch Nutzung von Onlinediensten außerhalb des KV-SafeNet-Angebots, wie z.B. das Internet, werden die PC-Arbeitsplätze im internen Praxisnetz einer nicht zu unterschätzenden Gefahr durch Angriffe ausgesetzt. Diese Gefahr muss durch konsequenten und verantwortungsvollen Einsatz organisatorischer und technischer Sicherungsmaßnahmen minimiert werden.

Die vorhandenen Patientendaten haben einen besonderen Schutzbedarf, wie er auch durch die allgemein bekannte ärztliche Schweigepflicht ausgedrückt wird. Die eingesetzten Sicherungsmechanismen sind an den besonderen Schutzbedarf anzupassen.

Der Arzt trägt die Verantwortung für Sicherheit seiner Praxis-IT und für den Schutz der Patientendaten. Ziel dieses Dokumentes ist es in diesem Zusammenhang, Empfehlungen und Vorgaben für die sichere Nutzung des Internets als Mehrwertdienst der KV-SafeNet-Anbindung im Praxisumfeld zu geben.

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 Provider und die Teilnehmer am *Sicheren Netz der KVen*.

* 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

Im Allgemeinen ist ausdrücklich auf die Bekanntmachung im Deutschen Ärzteblatt (DÄB), Jg. 105, Heft 19 vom 9. Mai 2008 zum Thema „Empfehlungen zur ärztlichen Schweigepflicht, Datenschutz und Datenverarbeitung in der Arztpraxis“[2] hinzuweisen.

2.1 Sicherheitsmaßnahmen

Die Hinweise in diesem Abschnitt zeigen Maßnahmen, die ein Administrator zum Schutz von PCs vor unerlaubten Zugriff durchführen kann.

2.1.1 Beschränkung der Arbeit mit Administratorrechten

Benutzerrechte während des Parallelbetriebs müssen auf die nötigsten Dienste und Berechtigungen reduziert werden. Der Betrieb mit Administratorenrechten ist nur bei administrativen Tätigkeiten (siehe 2.1.2 Softwareaktualisierung) zulässig.

2.1.2 Softwareaktualisierung

Durch zeitnahe Installation von empfohlenen Programm-Updates, wodurch bekannt gewordene Sicherheitslücken der beteiligten Softwarekomponenten[3] geschlossen werden, ist dessen größtmöglicher Sicherheitszustand zu gewährleisten.

2.1.3 Einstellung von Webbrowsern

Bei der Einstellung der browserinternen Sicherheitsstufen ist die höchstmögliche Sicherheit zu wählen. Es dürfen nur die aktiven Inhalte (Web-Scripting, PlugIns) zugelassen werden, die für den Betrieb zwingend notwendig sind. Die Einschränkung des Zugriffs auf die absolut notwendigen Seiten bietet einen hohen Schutz und kann organisatorisch oder technisch umgesetzt werden.

2.2 Sicherheitssoftware

In diesem Abschnitt werden Softwarekomponenten beschrieben, wodurch PCs eines Netzwerkes vor unerlaubten Zugriffen und Angriffen geschützt werden können.

2.2.1 Einsatz von lokalen Firewalls

Generell ist jeder an einem Netzwerk angeschlossener Computer mittels einer Desktop-Firewall vor unerlaubten Zugriffen zu schützen. Die Firewall-Regeln sind so restriktiv zu konfigurieren, dass nur die für den Betrieb zwingend notwendigen Verbindungen möglich sind.

Die Firewall im KV-SafeNet-Router ersetzt nicht die lokalen Desktop-Firewalls.

[2] Dieser Beitrag ist auch im Internet unter der Adresse http://www.bundesaerztekammer.de/page.asp?his=0.7.47.6188 verfügbar.
[3] Hierzu zählen grundlegende Programme wie Betriebssystem, Internetbrowser und Client-Programme (z.B. E-Mail-Client) sowie die zur Systemsicherung eingesetzten Programme wie Firewall, Malware-Schutzprogramm usw.

2.2.2 Einsatz von Malware[4]-Schutzprogrammen

Der Einsatz von aktuellen und anerkannten Malware-Schutzprogrammen ist für alle Rechner im Praxisnetz anzuwenden.

2.2.3 Content-Security für Web-Scriptings[5]

Als konsequente Erweiterung des Schutzes vor Malware-Programmen ist auch die sichere Abwehr vor bösartigem Inhalt auf Internetseiten zu gewährleisten. Hier ist der Gefahrenquelle des Web-Scriptings durch geeignete Verfahren entgegen zu wirken.

2.3 Netzwerk

Dieser Abschnitt enthält Sicherheitsmaßnahmen für das PC-Netzwerk in der Praxis.

2.3.1 Zugriffe über einen dedizierten Internet-Rechner

Um das Gefährdungspotential so niedrig wie möglich zu halten, dürfen Rechner mit Patientendaten generell nur dann mit dem Haus Netz verbunden sein, wenn dieses zwingend nötig ist (Minimierungsprinzip).

Die Verwendung eines dedizierten Internet-Rechners für die Nutzung der Mehrwertdienste reduziert die Systemverletzlichkeit des Hausnetzes und der angeschlossenen Arbeitsplätze erheblich. Soweit der produktive Betrieb der Praxissoftware keinen direkten Internetzugang benötigt, ist der Einsatz eines gesonderten Internet-Rechners unbedingt angeraten.

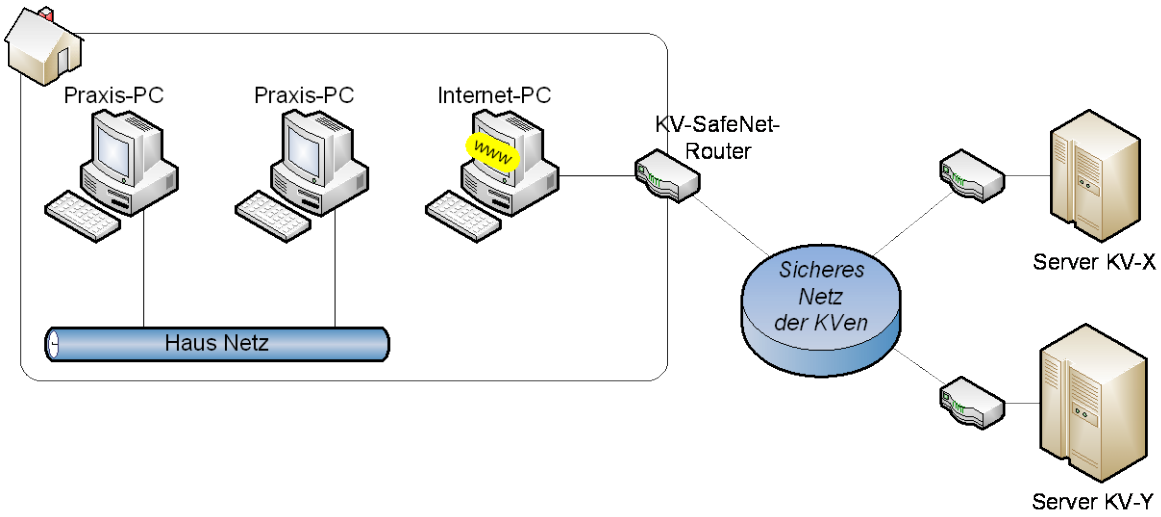

Abbildung 2: Einsatz eines gesonderten Internet-PCs

2.3.2 Zugriffe über eigenen Proxy

Wenn die Verwendung eines gesonderten Internet-Rechners nicht möglich ist, empfiehlt sich der Einsatz eines Proxys für den Datenaustausch mit dem Internet. Ein Proxy arbeitet als Vermittler, der Anfragen auf dem Haus Netz entgegennimmt, um diese dann stellvertretend ans Internet weiterzuleiten und die Rückmeldungen wieder auf dem Hausnetz zurückzugeben.

[4] **Maleware** ist der Oberbegriff für schädliche und unerwünschte Computerprogramme, welche die Funktion und Sicherheit des Rechnersystems negativ beeinflussen. Hierzu zählen Computerviren, Trojaner, Würmer, Spyware, Scareware, usw.
[5] Mit **Web-Scripting** wird die Programmiertechnik dynamischer Web-Seiten mit JavaScript, Dynamic HTML, ColdFusion, Flash usw. bezeichnet.

Somit wird die Bedrohung vermindert, dass die PCs des Praxisnetzes angegriffen werden können.

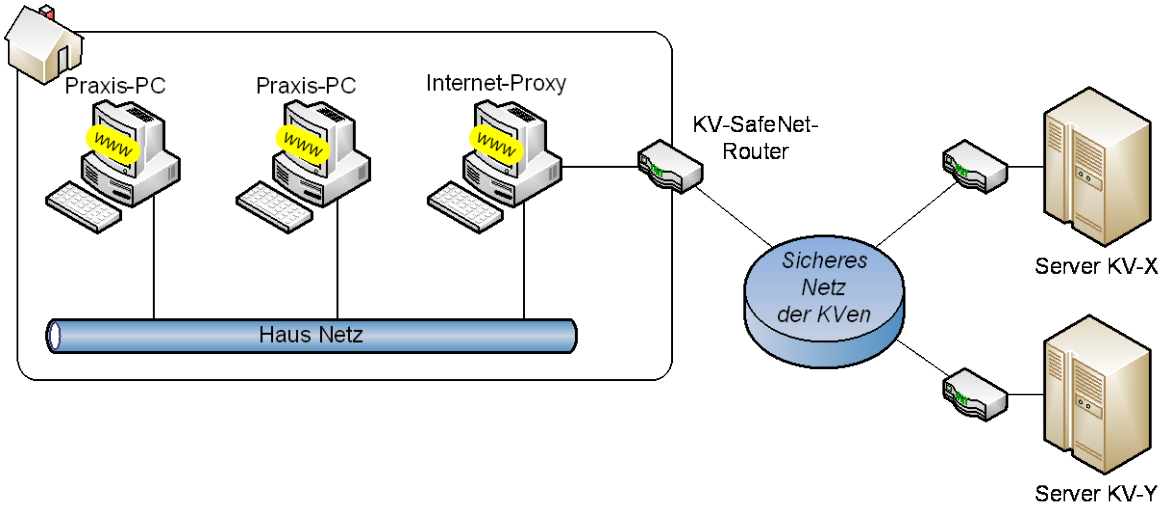

Abbildung 3: Einsatz eines Internet-Proxy

2.3.3 Keine Nebenzugänge zum Internet

Außer dem KV-SafeNet-Zugang dürfen keine weiteren Verbindungen zum Internet bestehen, da sonst die Sicherheit des gesamten Praxis-EDV-Systems nicht mehr gewährleistet ist. Besonders von Rechnern mit Funknetzanschlüssen (sog. Wireless LAN oder WLAN) geht hier eine besondere Gefahr aus. Blockieren Sie sämtliche Funknetzverbindungen mit Gegenstellen außerhalb des PC-Netzes Ihrer Praxis.

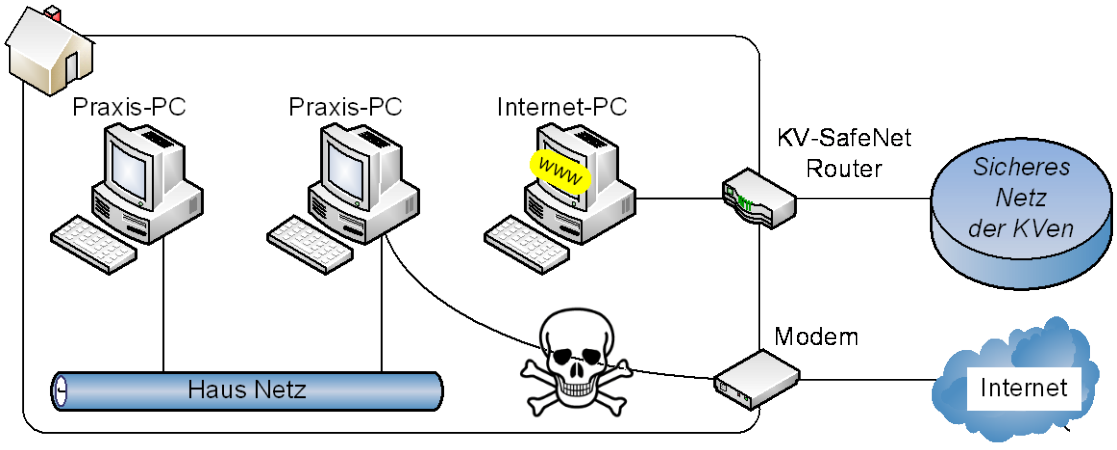

Abbildung 4: Unsichere Nutzung des Internets

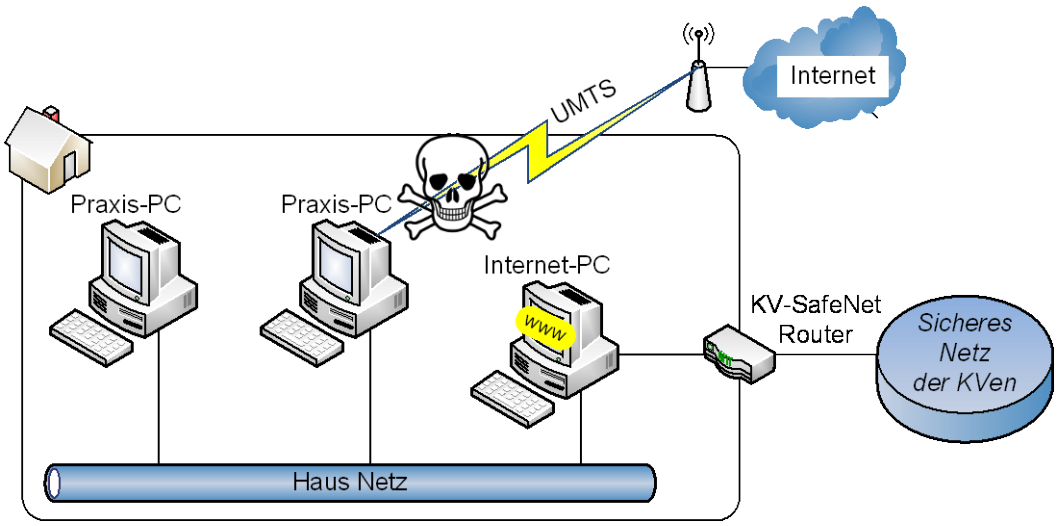

Abbildung 5: Unsichere Verwendung des Internets via UMTS

2.4 Anforderungen an KV-SafeNet-Provider

Die Anbieter (Provider) von KV-SafeNet-Zugängen sind prinzipiell auch in der Lage, Sie als angeschlossenen Teilnehmer beim Schutz vor Angriffen aus dem Internet zu unterstützen. Hier unterscheiden sich jedoch die Leistungen je nach Vertragsart und Geschäftsbeziehung.

2.4.1 Proxy-, Gateway- und Sicherheitssysteme des Providers

Um das Gefährdungspotential bereits im Vorfeld von den angeschlossenen Praxen fernzuhalten, empfehlen wir, die Teilnehmer ausschließlich über ein gesichertes und vom Anbieter administriertes Transfernetzwerk[6] ans Internet anzuschließen.

Der Übergang zwischen Transfernetzwerk und Internet ist durch geeignete Proxy-, Gateway- und Sicherheitssysteme vor Zugriffen aus dem Internet zu schützen. Der Proxy befindet sich in einer sog. Demilitarisierten Zone (DMZ) wodurch ein direkter Durchgriff des Internets auf das Providernetz verhindert wird.

Dieser Service erhöht die Sicherheit des Praxisnetzes vor unerlaubten Zugriffen erheblich, da sich das Sicherheitssystem der Praxis sowie das Sicherheitssystem des Providers ergänzen.

[6] Das **Transfernetzwerk** besteht lediglich aus Teilnehmern des Anbieters und ist über ein Proxy-Gateway mit dem Internet verbunden.

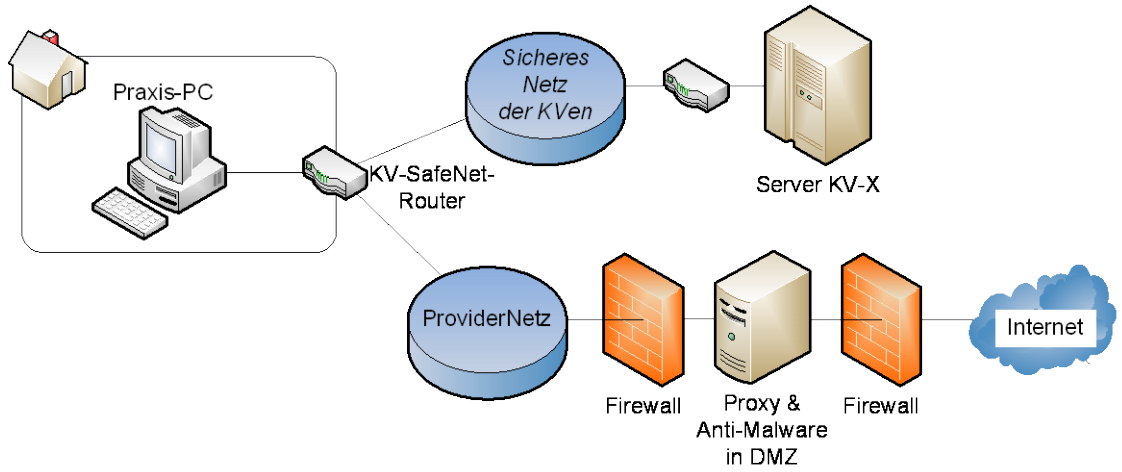

Abbildung 6: Einsatz einer DMZ im Providernetz

2.4.2 Sicherheitsstandards für Provider

Achten Sie darauf, dass Ihr Provider die allgemeinen Hinweise aus dem IT-Grundschutz-Katalog des Bundesamts für Sicherheit in der Informationstechnik (BSI) umsetzt.

Bei fahrlässiger Unterlassung der Sicherheitsmaßnahmen behalten sich die KVen und KBV vor, den Zugang des einzelnen Teilnehmers oder sogar des Anbieters zu sperren.

2.5 Sicherheitsszenarien

Je nach Kommunikationspartner werden unterschiedliche Sicherheitsszenarien definiert.

2.5.1 Szenario 1

Der Datenaustausch erfolgt ausschließlich innerhalb des *Sicheren Netzes der KVen*. In diesem Szenario kann von einem sehr geringen Angriffspotential ausgegangen werden, zumal auch alle Teilnehmer bekannt sind.

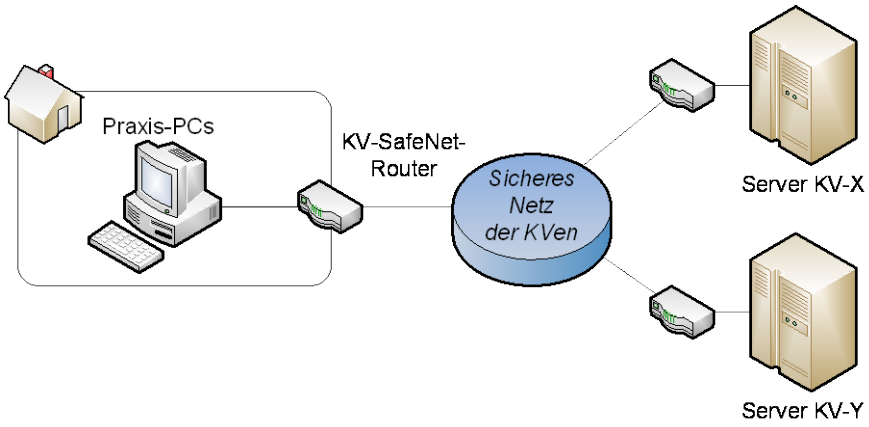

Abbildung 7: Sicherheitsszenario 1

2.5.2 Szenario 2

Der Datenaustausch erfolgt ausschließlich innerhalb des *Sicheren Netzes der KVen*. Hier werden Datendienste benutzt, die nicht durch die KVen kontrolliert werden, wie z.B. ein gemeinsamer Server eines Versorgungszentrums. In diesem Szenario kann von einem mäßigen Angriffspotential ausgegangen werden.

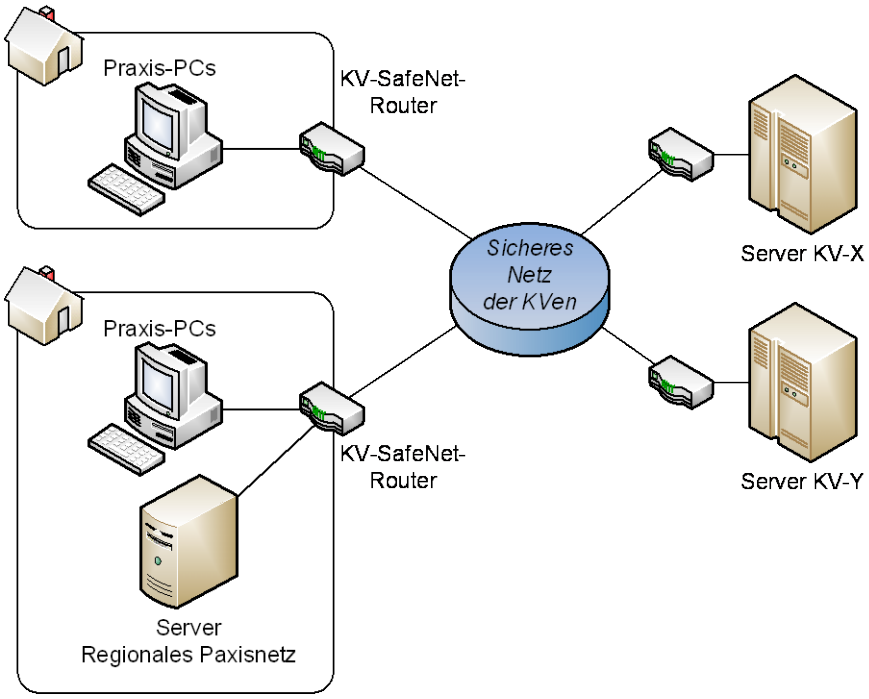

Abbildung 8: Sicherheitsszenario 2

2.5.3 Szenario 3

Der Datenaustausch erfolgt auch außerhalb des *Sicheren Netzes der KVen*. Hier werden auch Datendienste aus dem Internet benutzt, wie z.B. das Internet.

Da auf Seiten des Internets ein sehr großes Angriffspotential liegt, muss in diesem Szenario von einem großen Angriffspotential ausgegangen werden. Die Sicherheitsmaßnahmen des Providers können die Gefahr vor Angriffen aus dem Internet jedoch reduzieren.

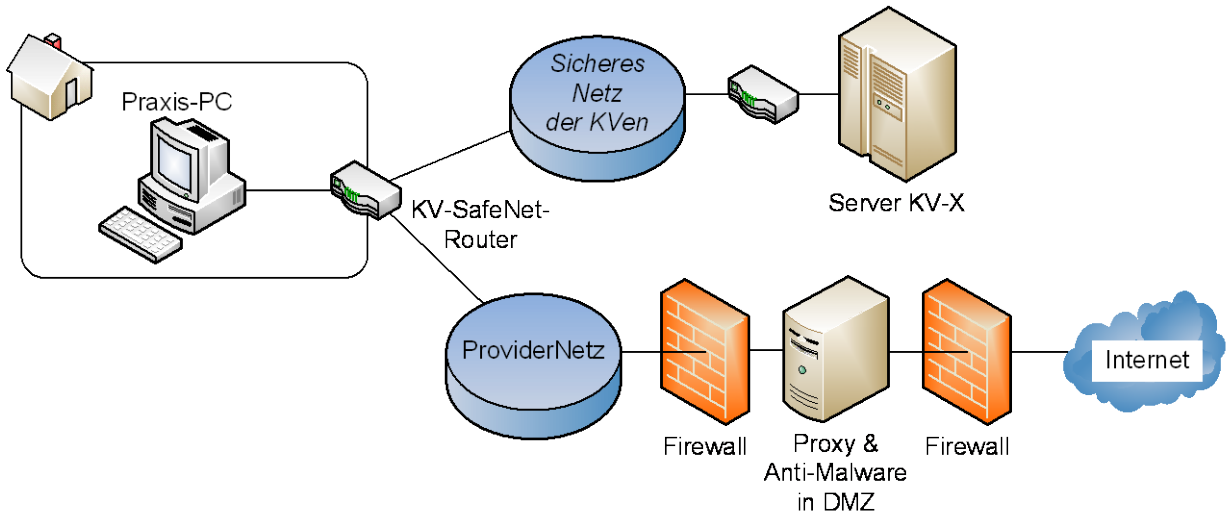

Abbildung 9: Sicherheitsszenario 3

2.5.4 Szenario 4

Der Datenaustausch erfolgt wie in Szenario 3 außerhalb des *Sicheren Netzes der KVen*. Es existiert jedoch kein abgeschirmtes Providernetz, sondern ein direkter Anschluss des KV-SafeNet-Routers an das Internet.

Da auf Seiten des Internets ein sehr großes Angriffspotential liegt, muss in diesem Szenario ebenfalls von einem großen Angriffspotential ausgegangen werden. Sämtliche Sicherheitsmaßnahmen vor unerlaubten Zugriffen auf das Praxisnetz sind auf dem KV-SafeNet-Router zu konfigurieren.

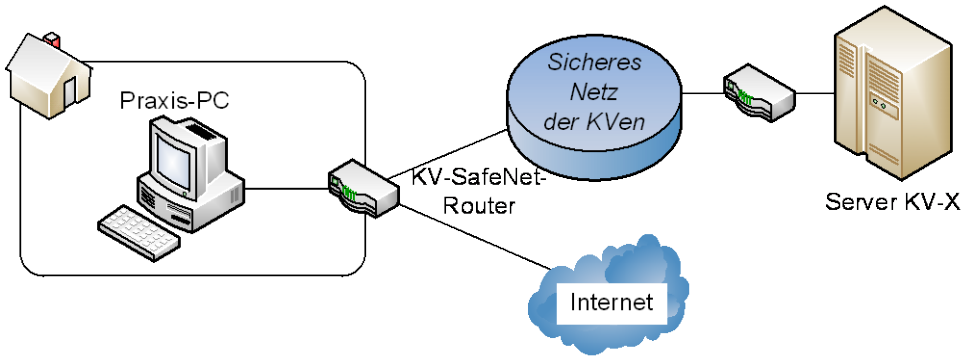

Abbildung 10: Sicherheitsszenario 4

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.
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*.
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.