



Kassenärztliche
Bundesvereinigung

Körperschaft des öffentlichen Rechts

Sicherheitsanforderungen für KV-SafeNet-Arbeitsplätze

*Anlage zur Rahmenrichtlinie KV-
SafeNet*

Dezernat 6 – Informationstechnik, Telematik und
Telemedizin

10623 Berlin

Kassenärztliche Bundesvereinigung

Version 1.0

Datum: 06.03.2009

ÄNDERUNGSVERZEICHNIS

Version	Datum	Autor	Änderung	Begründung	Seite
V1.0	06.03.2009	KBV	Initiales Dokument		

INHALTSVERZEICHNIS

1	<u>PRÄAMBEL</u>	4
2	<u>EINLEITUNG</u>	5
3	<u>SICHERHEITSMABNAHMEN</u>	6
3.1	Administrative Hinweise.....	6
	3.1.1 Beschränkung der Arbeit mit Administratorrechten.....	6
	3.1.2 Softwareaktualisierung	6
	3.1.3 Einstellung von Webbrowsern	6
3.2	Sicherheitssoftware	6
	3.2.1 Einsatz von lokalen Firewalls	7
	3.2.2 Einsatz von Malware-Schutzprogrammen.....	7
	3.2.3 Content-Security für Web-Scriptings	7
3.3	Netzwerk.....	7
	3.3.1 Zugriffe über einen dedizierten Internet-Rechner.....	7
	3.3.2 Zugriffe über eigenen Proxy	8
	3.3.3 Keine Nebenzugänge zum Internet.....	8
3.4	Anforderungen an KV-SafeNet-Provider.....	9
	3.4.1 Proxy-, Gateway- und Sicherheitssysteme des Providers	9
	3.4.2 Sicherheitsstandards für Provider	10
4	<u>SICHERHEITSSZENARIEN</u>	11
4.1	Szenario 1.....	11
4.2	Szenario 2.....	11
4.3	Szenario 3.....	12
4.4	Szenario 4.....	12
5	<u>GLOSSAR</u>	13

1 Präambel

Die in diesem Dokument aufgeführten Vorgaben und Empfehlungen sind für Praxisinhaber bzw. deren technischen Betreuer oder Dienstleister bestimmt, die ein Praxis-EDV-System an das KV-SafeNet anschließen. Insbesondere wenn Sie Mehrwertdienste¹ nutzen möchten, ist ein besonderes Augenmerk auf den Schutz Ihrer Systeme und Daten zu legen.

¹ Als **Mehrwertdienst** wird der Datenaustausch mit Systemen bezeichnet, die nicht von KVen im KV-SafeNet betrieben werden, z.B. Web- oder Mailserver im Internet, Onlinebanking, Praxisnetze, usw.

2 Einleitung

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

Die vorhandenen Patientendaten unterliegen der besonderen Schutzwürdigkeit, wie sie auch durch die allgemein bekannte ärztliche Schweigepflicht ausgedrückt wird. Die eingesetzten Sicherungsmechanismen sind der besonderen Schutzwürdigkeit anzupassen.

3 Sicherheitsmaßnahmen

Als allgemeine Richtlinie möchten wir Sie 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“ hinweisen. Dieser Beitrag ist auch im Internet unter der Adresse <http://www.bundesaerztekammer.de/page.asp?his=0.7.47.6188>

verfügbar.

3.1 Administrative Hinweise

Die Hinweise in diesem Kapitel beschäftigen sich mit Maßnahmen, die der Administrator eines PCs zum Schutz des Rechners vor unerlaubtem Zugriff durchführen kann.

3.1.1 Beschränkung der Arbeit mit Administratorrechten

Um den Schaden im Fehlerfall zu begrenzen, müssen die Benutzerrechte während des Parallelbetriebs auf die nötigsten Dienste und Berechtigungen reduziert werden. Der Betrieb mit Administratorrechten ist nur bei administrativen Tätigkeiten (siehe 3.1.2 Softwareaktualisierung) zulässig.

3.1.2 Softwareaktualisierung

Durch zeitnahe Installation von empfohlenen Programm-Updates, wodurch bekannt gewordene Sicherheitslücken der beteiligten Softwarekomponenten² geschlossen werden, ist dessen größtmöglicher Sicherheitszustand zu gewährleisten.

3.1.3 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.

3.2 Sicherheitssoftware

In diesem Kapitel werden Softwarekomponenten beschrieben, wodurch die PCs eines Netzwerkes vor unerlaubtem Zugriff und Angriffen geschützt werden.

² 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.

3.2.1 Einsatz von lokalen Firewalls

Generell ist jeder an einem Netzwerk angeschlossene 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 in der Blackbox bzw. dem KV-SafeNet-Router ersetzt nicht die lokalen PC-Firewalls sondern erhöht lediglich das Sicherheitsniveau.

3.2.2 Einsatz von Malware³-Schutzprogrammen

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

3.2.3 Content-Security für Web-Scriptings⁴

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

3.3 Netzwerk

Dieses Kapitel beschäftigt sich mit den Sicherheitsmaßnahmen für das PC-Netzwerk in Ihrer Praxis.

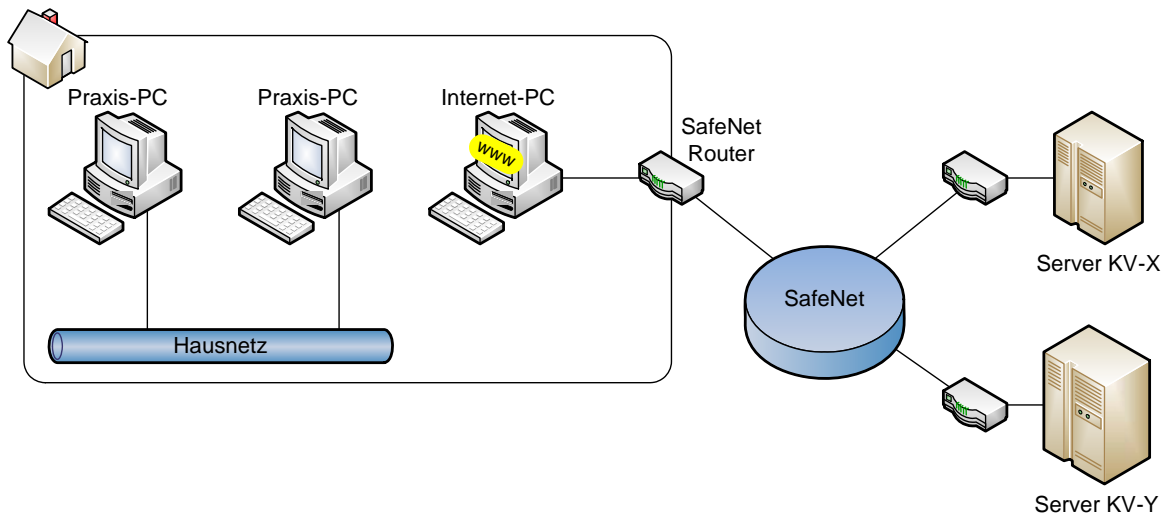
3.3.1 Zugriffe über einen dedizierten Internet-Rechner

Um das Gefährdungspotential so niedrig wie möglich zu halten, dürfen Rechner mit Patientendaten generell nur dann mit dem Hausnetz 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.

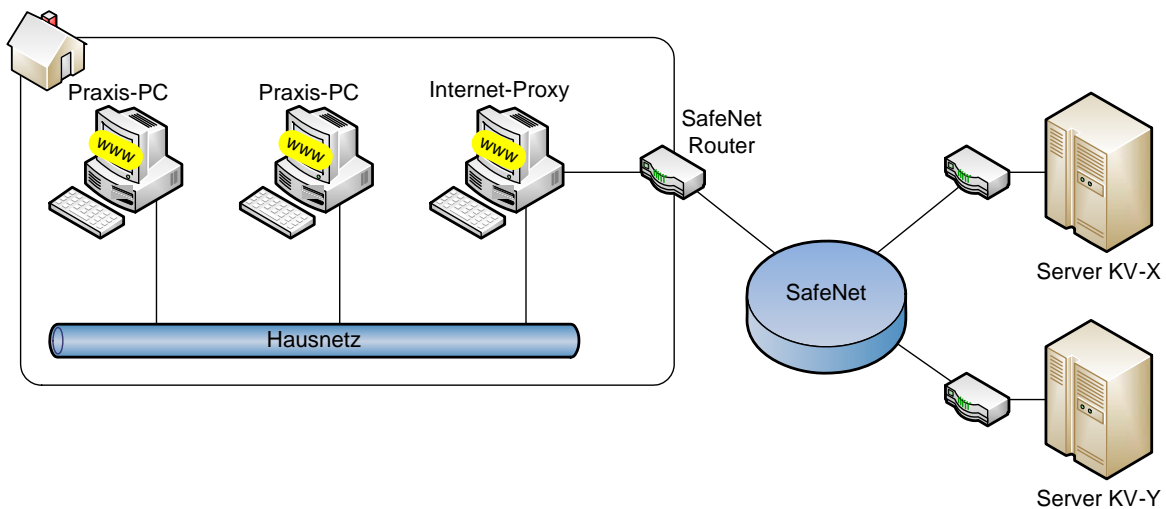
³ **Malware** ist der Oberbegriff für schädliche und unerwünschte Computerprogramme, welche die Funktion und Sicherheit des Rechnersystems negativ beeinflussen. Hierzu zählen Computerviren, Trojaner, Würmer, Spyware, Scareware, usw.

⁴ Mit **Web-Scripting** wird die Programmier technik dynamischer Web-Seiten mit JavaScript, dynamic HTML, ColdFusion, Flash usw. bezeichnet.



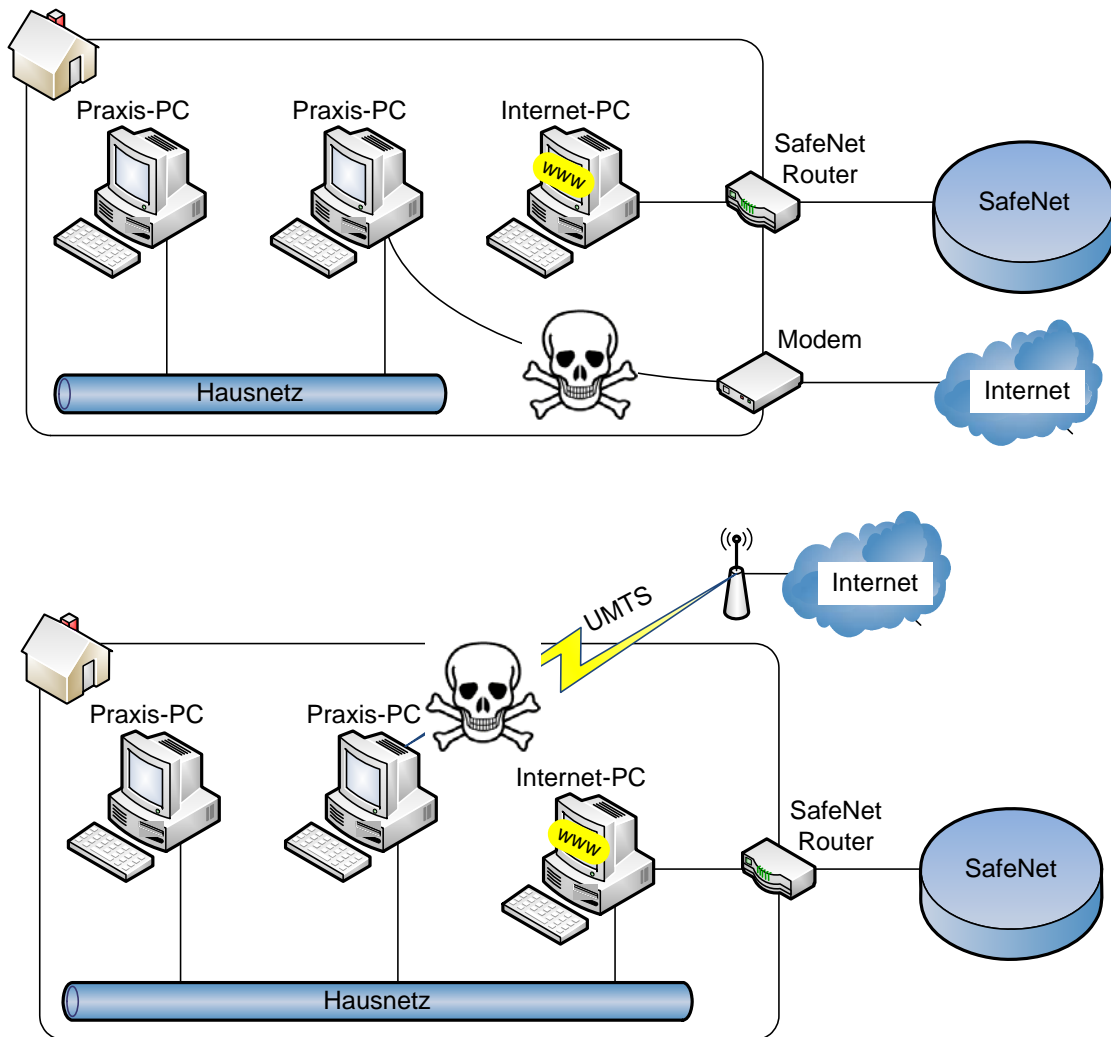
3.3.2 Zugriffe über eigenen Proxy

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 Hausnetz entgegennimmt, um diese dann stellvertretend ans Internet weiterzuleiten und die Rückmeldungen wieder auf dem Hausnetz zurückzugeben. Somit wird verhindert, dass die PCs des Praxisnetzes angegriffen werden können.



3.3.3 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.



3.4 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.

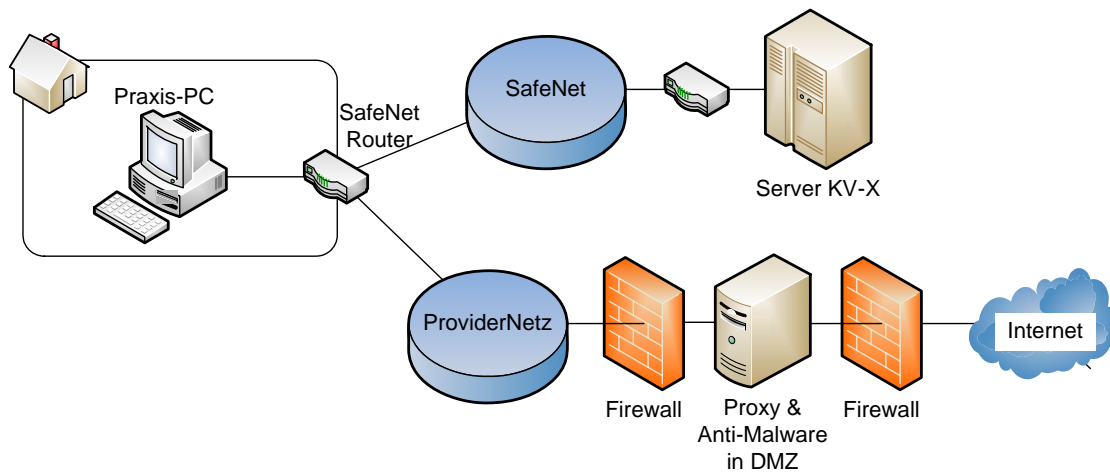
3.4.1 Proxy-, Gateway- und Sicherheitssysteme des Providers

Um das Gefährdungspotential bereits im Vorfeld von den angeschlossenen Praxen fernzuhalten, empfehlen wir, die Teilnehmer ausschließlich über ein gesichertes und vom Anbieter administriertes Transfer-Netzwerk⁵ ans Internet anzuschließen.

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

⁵ Das **Transfer-Netzwerk** besteht lediglich aus Teilnehmern des Anbieters und ist über ein Proxy-Gateway mit dem Internet verbunden.

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



3.4.2 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.

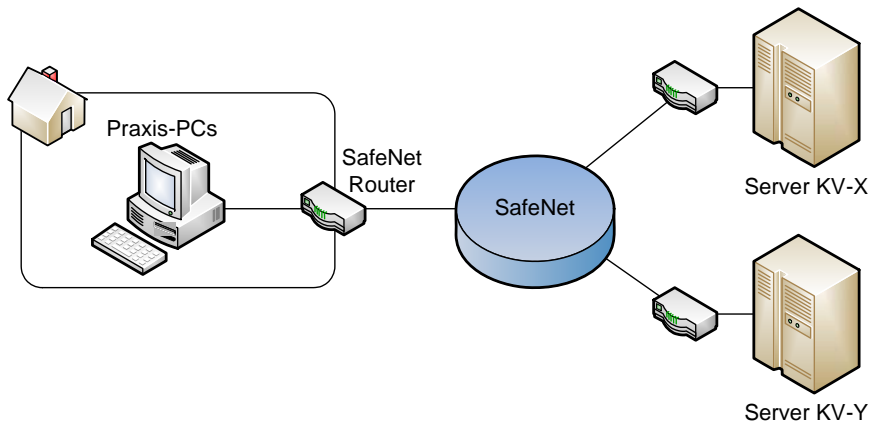
Bei fahrlässiger Unterlassung der Sicherheitsmaßnahmen behalten sich die KVen und KBV vor, den Zugang des einzelnen Teilnehmers oder sogar des Anbieters zu sperren.

4 Sicherheitsszenarien

Je nach Kommunikationspartner werden unterschiedliche Sicherheitsszenarien definiert.

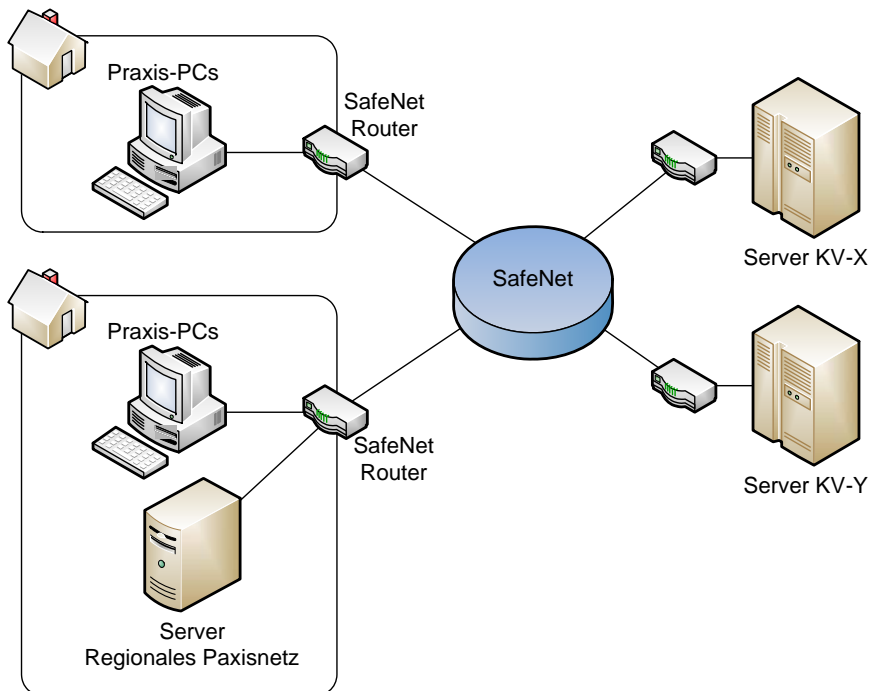
4.1 Szenario 1

Der Datenaustausch erfolgt ausschließlich innerhalb des KV-SafeNets und ausschließlich mit Servern der KVen. In diesem Szenario kann von einem sehr geringen Angriffspotential ausgegangen werden, zumal auch alle Teilnehmer bekannt sind.



4.2 Szenario 2

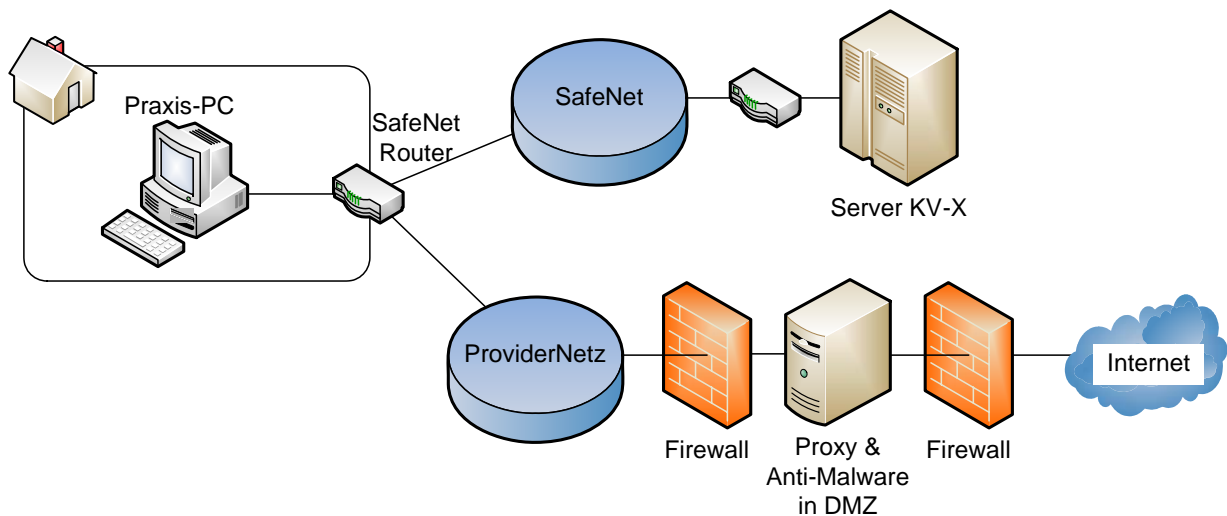
Der Datenaustausch erfolgt ausschließlich innerhalb des KV-SafeNets. Hier werden Datendienste benutzt, die nicht durch die KVen kontrolliert werden, wie z.B. der Mailserver eines Praxisnetzes oder Krankenhaus oder der gemeinsame Server eines (ortsübergreifenden) Versorgungszentrums. In diesem Szenario kann von einem mäßigen Angriffspotential ausgegangen werden.



4.3 Szenario 3

Der Datenaustausch erfolgt auch außerhalb des KV-SafeNets. Hier werden auch Datendienste aus dem Internet benutzt, wie z.B. öffentliche Mailserver oder weltweite Webseiten.

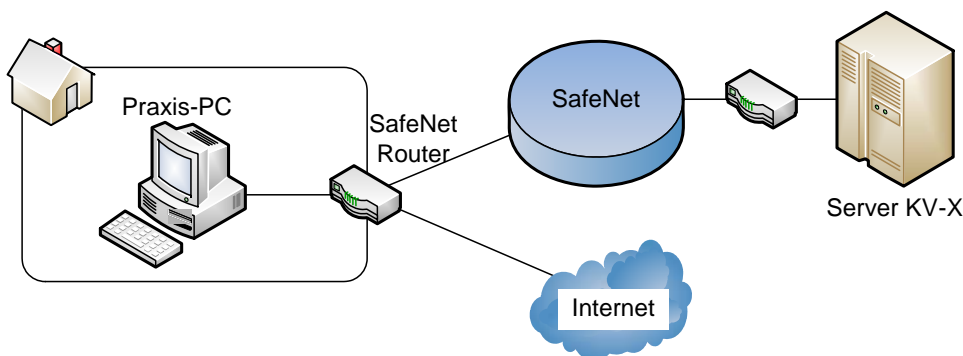
Da auf Seiten des Internets ein sehr großes Angriffspotential liegt, muss in diesem Szenario ebenfalls von einem großen Angriffspotential ausgegangen werden. Die Sicherheitsmaßnahmen des Providers können die Gefahr vor Angriffen aus dem Internet jedoch reduzieren.



4.4 Szenario 4

Der Datenaustausch erfolgt wie in Szenario 3 außerhalb des KV-SafeNets. 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 der Blackbox des KV-SafeNet-Routers zu implementieren.



5 Glossar

Begriff	Erklärung
Anbieter	Der Anbieter ist ein Unternehmen, welches nach der KV-SafeNet-Rahmenrichtlinie zertifiziert ist, und somit den Teilnehmern einen Zugang zum KV-SafeNet ermöglicht.
BÄK	Bundesärztekammer - ist die Arbeitsgemeinschaft der deutschen Ärztekammern und vertritt die berufspolitischen Interessen der Ärztinnen und Ärzte der Bundesrepublik Deutschland.
Blackbox	Eine Hardwarelösung, die grundsätzlich den Zugriff aus dem Transportnetz in das Netz des Teilnehmers verhindert. Zusätzlich wird durch den Aufbau eines VPNs eine sichere Verbindung zum Einwahlknoten hergestellt der mit dem KV-SafeNet verbunden ist.
BSI	Bundesamt für Sicherheit in der Informationstechnik. Das BSI ist der zentrale IT-Sicherheitsdienstleister des Bundes. Sie leistet Grundlagenarbeit im Bereich der IT-Sicherheit für Nutzer und Hersteller von Informationstechnik. Das sind in erster Linie die öffentlichen Verwaltungen in Bund, Ländern und Kommunen – aber auch Unternehmen und Privatanwender.
DÄB	Deutsches Ärzteblatt - ist eine Zeitschrift der Bundesärztekammer und der Kassenärztlichen Bundesvereinigung und veröffentlicht deren Bekanntgaben sowie Bekanntgaben von Institutionen, die im Einzelnen vom Herausgeber (BÄK, KBV) als Bekanntgeber benannt worden sind.
Desktop Firewall	siehe "Personal Firewall"
Diensteanbieter	Der Diensteanbieter ist eine KV, ein Ärztenetz, eine Arztpraxis oder ein anderer an das KV-SafeNet angeschlossener Teilnehmer, welcher Applicationen innerhalb des SafeNets für alle oder einen Teil der Teilnehmer zur Verfügung stellt.
Dienstleister	Der Dienstleister ist eine KV bzw. ein von ihr beauftragtes Unternehmen, welches den Anbietern die Möglichkeiten zur Verfügung stellt, ihre notwendige Technik für die Anbindung an das KV-SafeNet unterzubringen.
DMZ	Eine Demilitarized Zone (auch <i>ent- oder demilitarisierte Zone</i>) bezeichnet ein Computernetz mit sicherheitstechnisch kontrollierten Zugriffsmöglichkeiten auf die daran angeschlossenen Server.
Einwahlknoten	Der Einwahlknoten ist der Endpunkt des Anbieternetzes, der in der KV (Dienstleister) installiert ist, und den Übergang vom Anbieternetz zum KV-SafeNet darstellt.
IDS	Ein Intrusion Detection System (IDS) ist ein System zur Erkennung von Angriffen, die an ein Computersystem oder Computernetz gerichtet sind.
IP	Das Internet Protocol (IP) ist ein in Computernetzen weit verbreitetes Netzwerkprotokoll. Es ist die Implementierung der Vermittlungsschicht des TCP/IP-Modells bzw. der Vermittlungsschicht des OSI-Modells.
IP-Adresse	IP-Adressen werden in Computernetzen, die auf dem Internetprotokoll (IP) basieren, verwendet, um Daten von ihrem Absender zum vorgesehenen Empfänger transportieren zu können.
IP-SEC	IPsec (Kurzform für Internet Protocol Security) ist ein Sicherheitsprotokoll, das für die Kommunikation über IP-Netze die Schutzziele Vertraulichkeit, Authentizität und Integrität gewährleisten soll.
IT	Informationstechnik ist ein Oberbegriff für die Informations- und Datenverarbeitung sowie für die dafür benötigte Hard- und Software.
KBV	Kassenärztliche Bundesvereinigung - Körperschaft des öffentlichen Rechts ist die bundesweite Organisation der ärztlichen Selbstverwaltung

Begriff	Erklärung
KV	Kassenärztliche Vereinigung - Körperschaft des öffentlichen Rechts sind die bundeslandbezogenen Organisationen der ärztlichen Selbstverwaltung. Es gibt 17 KVen, die mit der KBV eine zentrale Organisation haben.
LAN	Abkürzung für "Local Area Network": lokal angelegtes Netzwerk. "Lokal" bezieht sich in diesem Sinne auf einen gemeinsamen Standort, wie beispielsweise ein Firmengelände oder einen Raum.
Personal Firewall	Eine Personal Firewall oder Desktop Firewall ist eine Software, die den ein- und ausgehenden Datenverkehr eines PCs auf dem Rechner selbst filtert.
PKI	Mit Public-Key-Infrastruktur bezeichnet man in der Kryptologie ein System, welches es ermöglicht, digitale Zertifikate auszustellen, zu verteilen und zu prüfen. Die innerhalb einer PKI ausgestellten Zertifikate werden zur Absicherung computergestützter Kommunikation verwendet.
Pre-shared Key	Mit Pre-Shared Key ("vorher vereinbarter Schlüssel") oder kurz PSK bezeichnet man solche Verschlüsselungsverfahren, bei denen die Schlüssel vor der Kommunikation beiden Teilnehmern bekannt sein müssen, also symmetrische Verfahren.
Proxy	siehe Application Layer Gateway
Reaktionszeit	Die Reaktionszeit ist der Zeitraum zwischen der ersten Störungsmeldung und der ersten qualifizierten Antwort durch den Anwendersupport des Anbieters. Die Antwort muss das Problem und seine Ursache klar beschreiben.
Sicherheits Gateway / Firewall	Eine externe (Netzwerk oder Hardware) Firewall stellt eine kontrollierte Verbindung zwischen zwei logischen Netzen her.
Teilnehmer	Ein Teilnehmer ist eine Arztpraxis, ein Krankenhaus, eine KV, ein Ärztenetz oder ein Anderes entsprechend der Rahmenrichtlinie vorgeschriebenes Mitglied des KV-SafeNets.
Teilnehmercomputer	Alle Rechner eines Teilnehmernetzwerkes, auf denen patientenbezogene Daten gespeichert bzw. verarbeitet werden und von denen aus über die Blackbox mittels VPN auf das KV-SafeNet zugegriffen werden kann.
Teilnehmernetzwerk	Die untereinander lokal vernetzten Teilnehmercomputer bilden das Teilnehmernetzwerk. In diesem Teilnehmernetzwerk können sich auch weitere über LAN vernetzte Endsysteme (z.B. Server, PC's, Drucker, Kartenleser) befinden.
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.
Update	Eine Aktualisierung, teils auch als Nachführung, Evidenthaltung oder Update bezeichnet, beschreibt den Vorgang, etwas bereits Vorhandenes auf einen neueren Stand zu bringen.
VPN	Virtual Private Network (dt. <i>virtuelles privates Netz</i> ; kurz VPN) dient der Einbindung von Geräten eines benachbarten Netzes an das eigene Netz, ohne dass die Netzwerke zueinander kompatibel sein müssen.
Wiederherstellungszeit	Die Wiederherstellungszeit ist der Zeitraum zwischen der ersten Störungsmeldung und der Beseitigung der gemeldeten Störung.
Zertifizierung	Durch die Zertifizierung wird dem Anbieter bestätigt, dass er alle Vorgaben, die in der zum Zertifizierungszeitpunkt gültigen Richtlinie festgelegt wurden, erfüllt. Im Ergebnis der Zertifizierung darf der Anbieter Teilnehmer an das KV-SafeNet anschließen.