



- Merkblatt -

Sicherheitsanforderungen an KV-SafeNet-Arbeitsplätze

Betreff: KV-SafeNet

Klassifizierung: **ÖFFENTLICH**

Version: **1.0**

Status: FREIGEgeben

Datum: **07.04.2016**

Autor: Thomas Kroh

Freigegeben durch: Robert Wölzlein

Freigabedatum: 07.04.2016

Prüfer: Tobias Drollinger

Prüfdatum: 16.12.2015

Brutus\daten\Vorlagen – Verträge - Formulare\KV-SafeNet\ IMO_DO_KV-SafeNet_Merkblatt-Sicherheitsanforderungen_V-1-0

Inhalt

Inhalt 1

1. Ziel und Zweck des Dokuments 2

2. Allgemeines zum KV-SafeNet 2

3. Sicherheitsmaßnahmen 3

 3.1. Benutzerrechte 3

 3.2. Softwareaktualisierung 3

 3.3. Webbrowser 3

4. Sicherheitssoftware 4

 4.1. Firewalls 4

 4.2. Malware- Schutzprogramme 4

5. Das Netzwerk in der Praxis 4

 5.1. Zugriffe über einen dedizierten Internet-PC 4

 5.2. Zugriffe über einen eigenen Proxy 5

 5.3. Parallele Zugänge zum Internet 5

6. Sicherheitsszenarien 5

 6.1. Szenario 1 – Ausschließliche KV-SafeNet-Nutzung 5

 6.2. Szenario 2 – Sicherheitsmaßnahmen durch Provider 6

 6.3. Szenario 3 – Sicherheitsmaßnahmen durch Teilnehmer 6

7. Quellverweis 6

Anlagen / Mitgeltende Dokumente: i

 - Antrag KV-SafeNet (Netzkopplung) i

 - Detaildaten KV-SafeNet (Netzkopplung) i

Abbildungsverzeichnis: ii

Versionsverzeichnis iii

1. Ziel und Zweck des Dokuments

Dieses Dokument ist eine Ergänzung für alle Teilnehmer am KV-SafeNet und soll als Merkblatt und Hilfestellung dienen, um einen verantwortungsvollen Umgang sensibler Daten, sowie deren Schutzbedarf einzuhalten.

Jeder Arzt ist verantwortlich für die Sicherheit seiner Praxis-IT und die ihm anvertrauten Patientendaten.

Da diese einen besonderen Schutzbedarf als personenbezogene Daten und Sozialdaten erfordern, ist hier ein erhöhter Schutz zur Absicherung bei der Nutzung von Onlinediensten außerhalb des KV-SafeNets nötig.

Die Gefahr durch Angriffe aus dem Internet muss durch den konsequenten Einsatz organisatorischer Maßnahmen und sicherheitstechnischer Vorkehrungen minimiert und Missbrauch durch verantwortungsvollen Umgang vermieden werden.

Dabei ist noch auf die Bekanntmachung im Deutschen Ärzteblatt (DÄB), Jg. 111, Heft 21 vom 23.Mai 2014 zum Thema [„Empfehlungen zur ärztlichen Schweigepflicht, Datenschutz und Datenverarbeitung in der Arztpraxis“](#) hinzuweisen.

2. Allgemeines zum KV-SafeNet

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.

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.

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.

Die Anbindung über einen Hardware-VPN erfolgt dabei über das KV-SafeNet, bei der neben der direkten Anbindung des Teilnehmers an das sichere Netz der KVen noch der Anschluss von Teilnehmern aus bereits in sich abgesicherten gesundheitsmedizinischen Netzinfrastrukturen an das Sichere Netz der KVen mittels KV-SafeNet (Netzkopplung) erfolgen kann.

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 Dienstleister die Möglichkeit, Dienste anzubieten, Voraussetzung hierfür ist eine Zertifizierung der betreffenden Applikation durch die KBV.

Erstellt: Thomas Kroh	Erstellt am: 07.04.2016	Betreff: KV-SafeNet
Freigegeben: Robert Wölzlein	Freigabedatum: 07.04.2016	Seite 2 / 6
Datei: IMO_DO_KV-SafeNet_Merkblatt-Sicherheitsanforderungen_V-1-0		

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.

3. Sicherheitsmaßnahmen

Grundsätzlich gilt für einen sicheren Zugang für Berechtigungen und alle Einstellungen die Regel

So wenig, wie möglich - so viel wie nötig!

3.1. Benutzerrechte

Während der täglichen Nutzung sollte darauf geachtet werden, dass vor allem beim Parallelbetrieb von KV-SafeNet und weiteren Onlinediensten auf einem Rechner, die Benutzerrechte am Arbeitsplatz nur auf die dafür unbedingt notwendigen Dienste beschränkt werden.

Ein Arbeiten mit Administratorrechten im täglichen Betrieb stellt damit ein erhöhtes Risiko dar und sollte unbedingt vermieden werden.

3.2. Softwareaktualisierung

Achten Sie auf eine zeitnahe Umsetzung empfohlener Programmupdates (Betriebssystem, Internetbrowser, E-Mail Clients, Virenschutz, Firewalls, etc.) durch Hersteller, da bekanntgewordene Sicherheitslücken so frühzeitig geschlossen und die Gefahr einer Ausnutzung dieser Lücken minimiert werden kann.

3.3. Webbrowser

Die Sicherheitseinstellungen der unterschiedlichen Webbrowser sind auf das höchstmögliche Niveau einzustellen. Dabei gilt auch Passwörter niemals zu speichern und attackierend gemeldete Seiten zu sperren.

Reduzieren Sie aktive Inhalte (Plugins, Web-Scripting) auf ein Minimum und versuchen Sie eine automatische Aktivierung nach Möglichkeit zu vermeiden.

Eine Einschränkung auf einzeln benötigte Seiten kann das Schutzniveau zusätzlich erhöhen.

Erstellt: Thomas Kroh	Erstellt am: 07.04.2016	Betreff: KV-SafeNet
Freigegeben: Robert Wölzlein	Freigabedatum: 07.04.2016	Seite 3 / 6
Datei: IMO_DO_KV-SafeNet_Merkblatt-Sicherheitsanforderungen_V-1-0		

4. Sicherheitssoftware

4.1. Firewalls

Grundsätzlich ist jeder an ein Netzwerk angeschlossene PC durch eine Desktop-Firewall vor unbefugtem Zugriff zu schützen.

Die Zugriffe sind dabei nur auf die für den Betrieb notwendigen Verbindungen zu begrenzen.

Die Firewall im KV-SafeNet-Router ersetzt **nicht** die lokalen Firewalls am PC!

4.2. Malware- Schutzprogramme

Als Malware bezeichnet man den Oberbegriff von Schadsoftware, die vom Benutzer unerwünschte oder schädliche Funktionen ausführen. Die verbreitetsten Klassen¹ stellen dabei Trojaner, Viren, Würmer und Adware dar.

Es ist daher dringend zu empfehlen geeignete Schutzprogramme zu installieren.

5. Das Netzwerk in der Praxis

Um die Gefährdung durch Schadcode zu minimieren dürfen Rechner mit Patientendaten generell nur dann mit dem Hausnetz verbunden werden, wenn dies unbedingt notwendig ist.

Sofern die Rechner keinen direkten Internetzugang benötigen, ist eine direkte Anbindung zu vermeiden.

5.1. Zugriffe über einen dedizierten Internet-PC

Eine Nutzung eines gesonderten Internet-PCs für die Nutzung von Mehrwertdiensten reduziert die Verletzbarkeit des Hausnetzes dabei erheblich.

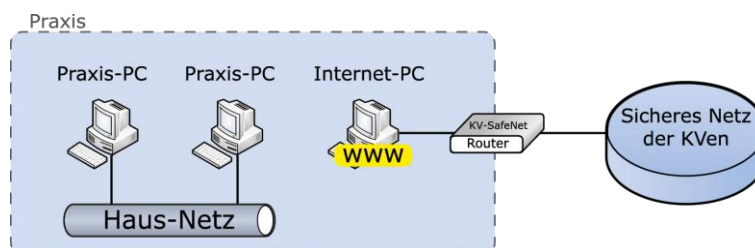


Abbildung 1 - Verwendung eines separaten Internet-PCs

¹ Es gibt je nach Zweck und Verhalten viele verschiedene Arten von Schadsoftware – s. auch <https://de.wikipedia.org/wiki/Schadprogramm>

Erstellt: Thomas Kroh	Erstellt am: 07.04.2016	Betreff: KV-SafeNet
Freigegeben: Robert Wölzlein	Freigabedatum: 07.04.2016	Seite 4 / 6
Datei: IMO_DO_KV-SafeNet_Merkblatt-Sicherheitsanforderungen_V-1-0		

5.2. Zugriffe über einen eigenen Proxy

Sollte keine Möglichkeit bestehen einen separaten Internet-PC zu betreiben, empfiehlt sich der Einsatz eines Proxys als „Vermittler“ der Anfragen der im Hausnetz angeschlossenen PCs ins Internet.

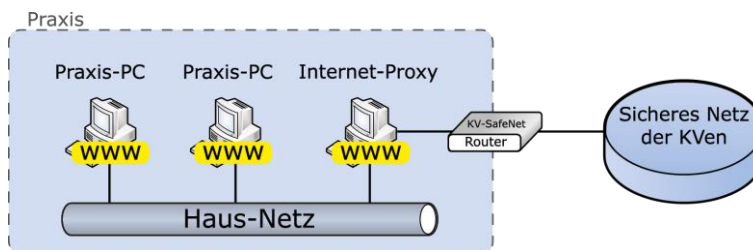


Abbildung 2 - Verwendung eines eigenen Proxy

5.3. Parallele Zugänge zum Internet

Neben dem KV-SafeNet-Zugang dürfen keine weiteren direkten Verbindungen (auch WLAN- oder andere Funkverbindungen) zum Internet bestehen. Schadsoftware und Unbefugte hätten sonst einen ungesicherten Zugang zum Praxis-EDV-System über einen „Seiteneingang“.

6. Sicherheitsszenarien

Es gibt unterschiedliche Möglichkeiten (Szenarien), um die Sicherheit für Ihre Daten beim Zugang mit dem KV-SafeNet zu erhöhen.

6.1. Szenario 1 – Ausschließliche KV-SafeNet-Nutzung

Ein hohes Sicherheitsniveau erreichen Sie, wenn Sie Ihre PCS in der Praxis ausschließlich an das Sichere Netz der KVen anbinden und keine weiteren Verbindungen zum Internet nutzen. IM KV-SafeNet sind nur die Teilnehmer des KV-SafeNet angebunden und alle bei der KBV bekannt.

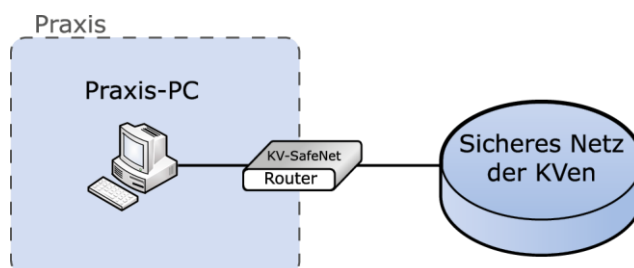


Abbildung 3 - Szenario 1 - nur KV-SafeNet

Erstellt: Thomas Kroh	Erstellt am: 07.04.2016	Betreff: KV-SafeNet
Freigegeben: Robert Wölzlein	Freigabedatum: 07.04.2016	Seite 5 / 6
Datei: IMO_DO_KV-SafeNet_Merkblatt-Sicherheitsanforderungen_V-1-0		

6.2. Szenario 2 – Sicherheitsmaßnahmen durch Provider

Neben dem KV-SafeNet wird auch das Internet zum Datenaustausch genutzt. Da hier die Anzahl und Art der Teilnehmer nicht kontrolliert werden kann, existiert hier ein hohes Angriffspotential. Sicherheitsmaßnahmen durch den Internetprovider können dieses Risiko reduzieren. Fragen Sie hierzu Ihren Provider.

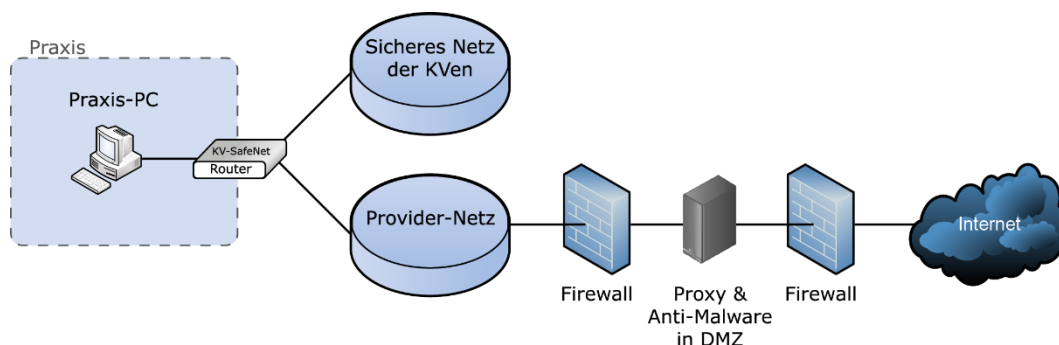


Abbildung 4 - Szenario 2 – Maßnahmen durch Provider

6.3. Szenario 3 – Sicherheitsmaßnahmen durch Teilnehmer

Auch hier besteht wie im Szenario 2 durch den direkten Anschluss des KV-SafeNet Routers an das Internet ein hohes Angriffspotential. Sämtliche Sicherheitsmaßnahmen gegen unerlaubte Zugriffe sind auf dem KV-SafeNet Router zu konfigurieren. Ferner wird der Einsatz von lokalen Firewalls (siehe 4.1), aktuellen Antiviren- & Antimalware-Programmen dringend empfohlen.

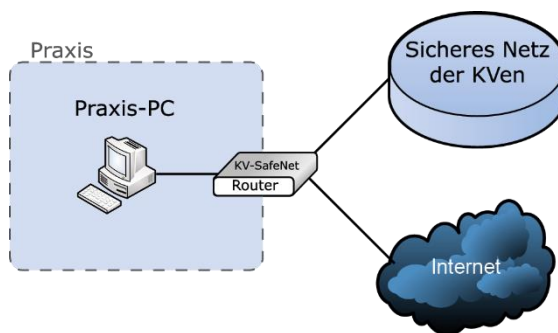


Abbildung 5 - Szenario 3 – Maßnahmen durch Teilnehmer

7. Quellverweis

Dieses Merkblatt beruht auf dem „Merkblatt Sicherheitsanforderungen KV-SafeNet-Arbeitsplätze“ der KBV in der zuletzt veröffentlichten Version 1.1 vom 31.10.2011.

Erstellt: Thomas Kroh	Erstellt am: 07.04.2016	Betreff: KV-SafeNet
Freigegeben: Robert Wölzlein	Freigabedatum: 07.04.2016	Seite 6 / 6
Datei: IMO_DO_KV-SafeNet_Merkblatt-Sicherheitsanforderungen_V-1-0		

Anlagen / Mitgeltende Dokumente:

- Antrag KV-SafeNet (Netzkopplung)
- Detaildaten KV-SafeNet (Netzkopplung)

Erstellt: Thomas Kroh	Erstellt am: 07.04.2016	Betreff: KV-SafeNet
Freigegeben: Robert Wölzlein	Freigabedatum: 07.04.2016	Anhang I
Datei: IMO_DO_KV-SafeNet_Merkblatt-Sicherheitsanforderungen_V-1-0		

Abbildungsverzeichnis:

Abbildung 1 - Verwendung eines separaten Internet-PCs.....4
 Abbildung 2 - Verwendung eines eigenen Proxy5
 Abbildung 3 - Szenario 1 - nur KV-SafeNet.....5
 Abbildung 4 - Szenario 2 – Maßnahmen durch Provider6
 Abbildung 5 - Szenario 3 – Maßnahmen durch Teilnehmer6

Erstellt: Thomas Kroh	Erstellt am: 07.04.2016	Betreff: KV-SafeNet
Freigegeben: Robert Wölzlein	Freigabedatum: 07.04.2016	Anhang II
Datei: IMO_DO_KV-SafeNet_Merkblatt-Sicherheitsanforderungen_V-1-0		

Versionsverzeichnis

Version	Datum	Kap	Änderung / Begründung	Autor
1.0	Dez.2015	-	Erstellung des Dokuments	t.kroh

Erstellt: Thomas Kroh	Erstellt am: 07.04.2016	Betreff: KV-SafeNet
Freigegeben: Robert Wölzlein	Freigabedatum: 07.04.2016	Anhang III
Datei: IMO_DO_KV-SafeNet_Merkblatt-Sicherheitsanforderungen_V-1-0		