Kassenärztliche Bundesvereinigung
Körperschaft des öffentlichen Rechts

Sicheres Netz der KVen

Richtlinie Security Incident Management

[KBV_SNK_RLEX_SIM]

Dezernat 6
Informationstechnik, Telematik und Telemedizin

10623 Berlin, Herbert-Lewin-Platz 2

Kassenärztliche Bundesvereinigung

Version	1.0
Datum:	31.10.2012
Klassifizierung:	Öffentlich
Status:	In Kraft

DOKUMENTENHISTORIE

Version	Datum	Autor	Änderung	Begründung	Seite
0.9	13.03.2012	KBV	Entwurfsfassung		

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.

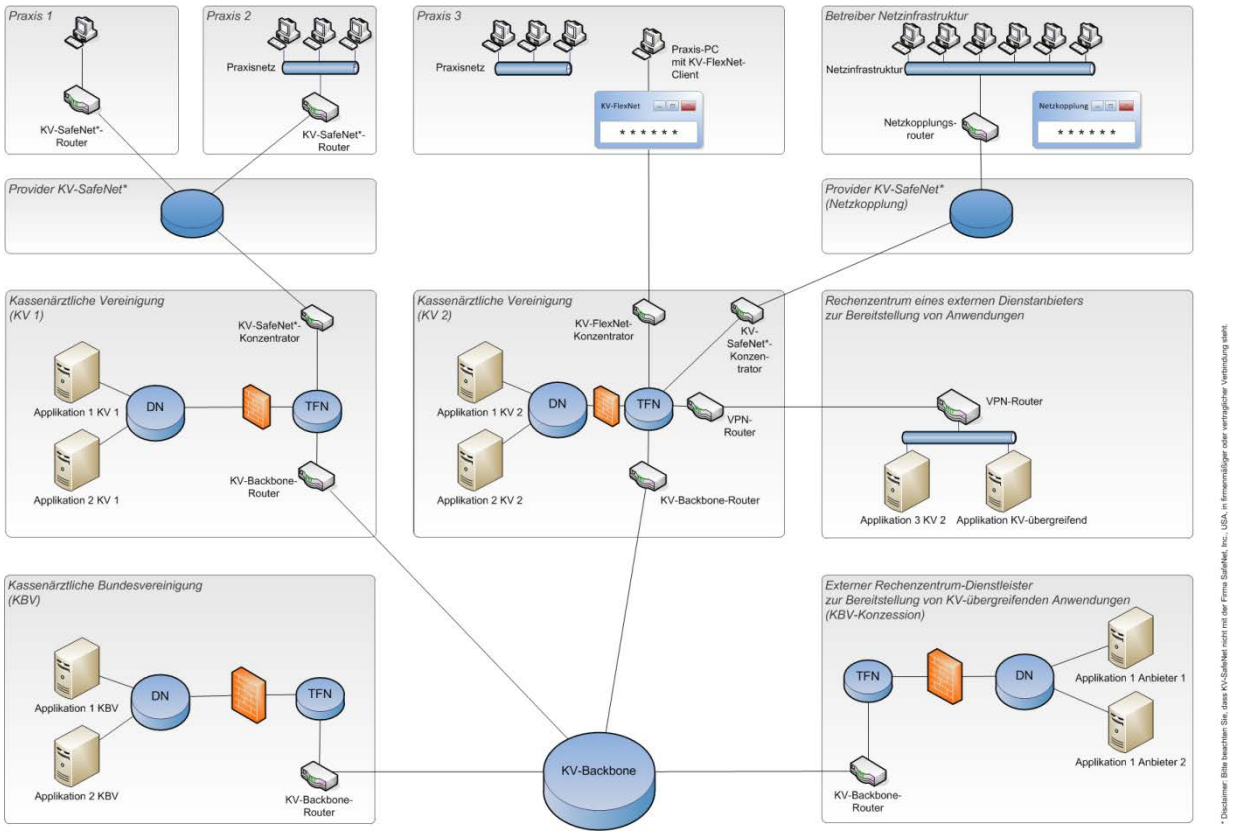

Abbildung 1: Beispielhafte Netztopologie

Teilnehmer am *Sicheren Netz der KVen* sind die Mitglieder der Kassenärztlichen Vereinigungen, also Vertragsärzte und –psychotherapeuten oder ein anderer nach den Richtlinien der KBV zugelassener Teilnehmer 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

Das Security Incident Management des *Sicheren Netzes der KVen* ist auf alle Verantwortungsbereiche und alle für diese Verantwortungsbereiche zuständigen Organisationen gemäß Richtlinie Informationssicherheit [KBV_SNK_RLEX_Informationssicherheit] im *Sicheren Netz der KVen* anzuwenden.

Dieses Dokument beschreibt die grundsätzliche Vorgehensweise zum Security Incident Management im *Sicheren Netz der KVen* und gibt konkrete Vorgaben, Empfehlungen und Beispiele für die organisationsspezifische Umsetzung für alle beteiligten Akteure.

Jede Organisation im *Sicheren Netz der KVen* soll für ihre Verantwortungsbereiche ein Security Incident Management etablieren und aufrechterhalten, welches den Maßgaben dieser Richtlinie entspricht. Die konkrete Form der Umsetzung obliegt der zuständigen Organisation.

Diese Richtlinie beschreibt

- den Security Incident Management Prozess,
- die Rollen und Verantwortlichkeiten im Rahmen des Prozesses,
- die einzelnen im Rahmen des Prozesses durchzuführenden Aktivitäten,
- die im Rahmen des Prozesses notwendigen Werkzeuge
- und die Schnittstellen des Prozesses zu anderen Prozessen eines Informationssicherheitsmanagementsystems (ISMS).

* 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.

Weiterhin werden in diesem Dokument im Abschnitt 2.4 „Monitoring“ Empfehlungen für die technische Umsetzung eines Monitorings einzelner Systeme im *Sicheren Netz der KVen* ausgesprochen.

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 KVen, Provider, Anbieter von Applikationen und durch die KBV oder KVen beauftragte externe Dienstleister.

2 Regelungen

Gemäß Richtlinie [KBV_SNK_RLEX_Informationssicherheit] ist Security Incident Management ein wesentlicher Baustein für die Informationssicherheit.

Security Incident Management behandelt das Management von Informationssicherheitsereignissen (Security Incidents). Ziel des Security Incident Managements ist es, mittels geeigneter Prozesse und Werkzeuge sicherzustellen, dass der Betrieb von Systemen und Dienstleistungen im Falle von Störungen innerhalb eines definierten Zeitraumes wiederhergestellt und die Störungsauswirkungen minimiert werden können.

Security Incidents 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

2.1 Zusammenarbeit zwischen den Organisationen

Grundlegend ist jede Organisation für den Betrieb des eigenen Security Incident Managements verantwortlich.

Security Incidents ohne Einfluss auf andere Verantwortungsbereiche und Organisationen müssen durch die verantwortliche Organisation selbst gelöst werden.

Security Incidents mit Einfluss auf andere Verantwortungsbereiche und Organisationen müssen an die KBV und die betreffenden Organisationen gemeldet werden und durch die verantwortliche Organisation selbst gelöst werden.

Falls durch eine Organisation Security Incidents bemerkt werden, die nicht im eigenen Verantwortungsbereich liegen, so müssen diese an die KBV und die verantwortliche Organisation gemeldet werden. Der Security Incident muss dann durch die verantwortliche Organisation selbst gelöst werden.

2.2 Aufbau und Betrieb des Security Incident Managements

Meldungen über Security Incidents müssen über definierte Schnittstellen

- angenommen,
- klassifiziert,
- priorisiert,
- an die jeweiligen Verantwortlichen zur Bearbeitung weitergeleitet
- abgeschlossen und bewertet werden.

Die folgenden Abschnitte definieren die Maßgaben, die für den Betrieb eines Security Incident Managements innerhalb einer Organisation notwendig und mindestens umzusetzen sind.

2.2.1 Sicherheitsorganisation, Rollen und Verantwortlichkeiten

Im Rahmen des Security Incident Managements soll die Organisation beschrieben sein. Hierbei sind die verantwortlichen Stellen und Aufgaben zu benennen.

Für den Prozess grundsätzlich wichtige Rollen und Verantwortlichkeiten werden im Folgenden kurz beschrieben.

Rolle	Aufgabe
Verantwortlicher für das Security Incident Management	• Betrieb und Weiterentwicklung der Prozesse des Security Incident Managements • Auswertung der Leistungsfähigkeit des Security Incident Managements anhand von Kennzahlen
1st Level Support (zentrale Meldestelle)	• Zentrale Meldestelle, die als erster Ansprechpartner für alle Incidents gilt, z.B. ein zentraler Helpdesk • Verantwortlich für die Erstlösung eines Incidents oder für die Weiterleitung an den nächstfolgende Support Level und weitere Beobachtung des Incidents
2nd Level Support, 3rd Level Support	• Instanzen für die weitere Behandlung und Lösung von Incidents, wenn durch den 1st Level Support keine Lösung erreicht werden konnte. • 2nd Level Support bzw. 3rd Level Support können sowohl durch organisationseigene Mitarbeiter als auch durch externe Dienstleister übernommen werden
Datenschutzbeauftragter	• Der Datenschutzbeauftragte ist bei allen Security Incidents hinzuzuziehen, bei denen personenbezogene Daten betroffen sind oder sein könnten.
Informationssicherheitsbeauftragter	• Der Informationssicherheitsbeauftragte ist bei allen Incidents zu informieren, bei denen Vertraulichkeit, Verfügbarkeit oder Integrität betroffen sind.
Verantwortlicher für das Risikomanagement	• Identifikation von Risiken, Bewertung und die Umsetzung von Risikomanagement-Maßnahmen entsprechend [KBV_SNK_RLEX_Risikomanagement] • Aus dem Prozess des Security Incident Managements erhält er Kennzahlen über bestehende Risiken und Hinweise zur Identifikation neuer Risiken
Verantwortlicher für das Business Continuity Management	• Der Verantwortliche für das Business Continuity Management ist verantwortlich für den gesamten Prozess des Business Continuity Managements entsprechend [KBV_SNK_RLEX_BCM]. Sollte sich ein Incident als Notfall erweisen, so ist der für diesen Fall definierte Prozess des Business

	Continuity Managements einzuleiten, d.h. insbesondere die Einleitung des entsprechenden Notfallplans.

2.2.2 Werkzeuge im Security Incident Management Prozess

Die im Security Incident Management einzusetzenden Werkzeuge sind in der folgenden Tabelle aufgeführt.

Werkzeug	**Erläuterungen**
Ticketsystem	Im Ticketsystem sind die einzelnen Security Incidents, der aktuelle Bearbeitungsstatus und wesentlichen Aktivitäten zu dokumentieren, die zur (vorübergehenden) Lösung führten.
Configuration Management Database (CMDB)	Die CMDB ist eine Datenbank, in der die Betriebsmittel der Organisation in Form sogenannter Configuration Items (CI's) hinterlegt sind. Die CMDB sollte u.a. eine Inventarisierung der Betriebsmittel, der Nutzer der jeweiligen Betriebsmittel und die Abbildung vertraglicher Abhängigkeiten wie z.B. Service- und Wiederherstellungszeiten bieten, sowie die Abhängigkeiten der einzelnen CI's voneinander darstellen können. Im Rahmen des Security Incident Management Prozesses kann die CMDB genutzt werden, um für jedes CI zu definieren • welche(s) System(e) im Falle eines Security Incidents betroffen sind und welche Abhängigkeiten diese voneinander haben, • welche Nutzer im Falle eines Security Incidents betroffen sind, • welche zugesagten Reaktions- und Wiederherstellungszeiten für das betroffene System bestehen und • wer der Verantwortliche für die Problemlösung ist.
Known Error Database (KEDB)	Die KEDB ist die Grundlage für die Dokumentation bekannter Probleme und deren Lösungen im Security Incident Management Prozess. Wurden im Rahmen des Security Incident Management Prozesses Lösungen gefunden, die noch nicht in der KEDB vorhanden waren, so sind diese Lösungen in der KEDB zu dokumentieren.

2.2.3 Prozess zur Sicherstellung des Incident Managements

Der Gesamtprozess des Security Incident Managements ist in 5 Phasen unterteilt. Diese Phasen gruppieren die Aktivitäten im Prozess thematisch und dienen der Übersichtlichkeit.

I. Erkennen, Melden und Erfassen

II. Klassifizierung, Priorisierung und Zuweisung

III. Herstellung des Soll-Zustandes / Eskalation
IV. Dokumentation und kontinuierliche Verbesserung
V. Reporting und Analyse

Die folgende Grafik stellt die Prozessphasen und einzelne Aktivitäten dar.

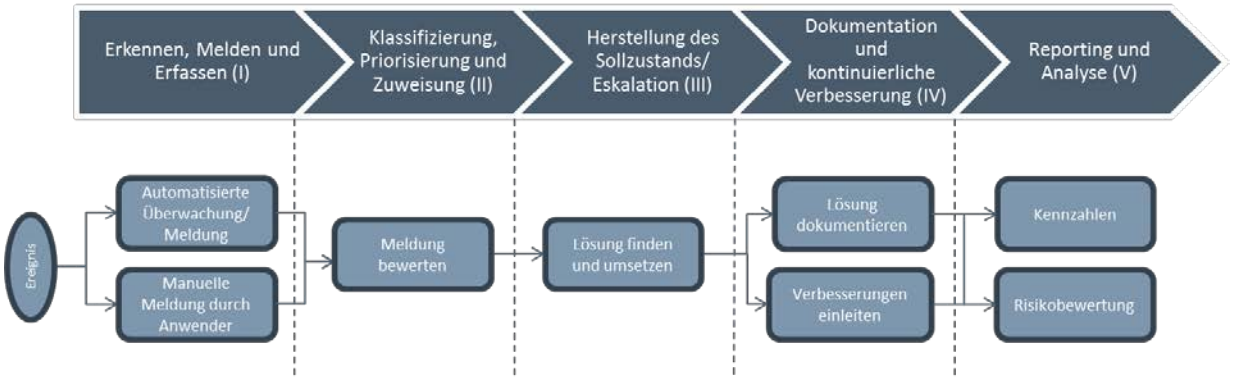

Abbildung 2: Überblick Incident Management Prozess

In den folgenden Abschnitten wird auf die einzelnen Phasen des Security Incident Management Prozesses und die jeweiligen Aktivitäten in den einzelnen Prozessphasen detaillierter eingegangen.

2.2.3.1 Erkennen, Melden und Erfassen (Phase I)

Die grundlegenden Aktivitäten dieser Phase sind:

- Vorfall erkennen,
- Vorfall melden und
- Vorfall erfassen.

Vorfall erkennen

Security Incidents müssen zuverlässig und korrekt durch Betroffene erkannt werden. Verhaltensregeln zum Umgang mit Security Incidents, insbesondere die Sensibilisierung im Umgang mit Security Incidents und die Definition der Meldewege, müssen vorliegen.

Weiterhin können durch die Implementierung eines Monitoring Systems bestimmte Security Incidents automatisiert bei Eintritt des Vorfalls oder evtl. bereits vor Eintritt des Vorfalls erkannt werden. Die grundlegende Konzeption eines solchen Monitoring Systems zur Überwachung bestimmter definierter Eigenschaften von Systemen ist in Abschnitt 2.4 „Monitoring“ beschrieben.

Vorfall melden

Ziel der Aktivität ist die Meldung von erkannten Security Incidents. Alle Vorfälle müssen unverzüglich an die zentrale Meldestelle gemeldet werden.

Die Meldewege müssen definiert sein. Mögliche Meldewege könnten u.a. eMail oder telefonisch Meldung, als auch der direkte Zugriff auf das Ticket System sein.

Vorfall erfassen

Der gemeldete Security Incident ist bezüglich der Vollständigkeit der Daten, Korrektheit und Plausibilität zu prüfen.

Der Incident ist in Form eines Tickets zu erfassen. Als Medium zur Erfassung und Dokumentation eines Security Incidents ist ein Ticket System zu nutzen.

2.2.3.2 Klassifizierung, Priorisierung und Zuweisung (Phase II)

Die grundlegenden Aktivitäten dieser Phase sind:

- Klassifizierung
- Priorisierung
- Zuweisung

Klassifizierung

Tickets müssen klassifiziert werden. Die einzelnen Klassen, die zur Klassifizierung genutzt werden, müssen definiert und den Betroffenen bekannt sein.

Mögliche Klassen für die Klassifizierung von Tickets sind z.B.

- Serviceanfrage,
- Beschwerde,
- Störung,
- Sicherheitsvorfall und
- Notfall.

Die Klassifizierung erfolgt im Ticket System durch den 1st Level Support oder ggf. durch andere erfahrene Personen.

Priorisierung

Die Priorisierung dient der Steuerung der Ticketbearbeitungsreihenfolge. Die Priorisierung ergibt sich aus den Auswirkungen und der Dringlichkeit des Incidents bzw. den vereinbarten Regelungen zur Reaktions- und Entstörzeit.

Die einzelnen Stufen, die zur Priorisierung genutzt werden können, müssen definiert sein, z.B.

- Hoch (Tickets mit kurzer notwendiger Entstörzeit, z.B. weniger als 8 Stunden)
- Mittel (Tickets mit mittlerer notwendiger Entstörzeit, z.B. zwischen 8 Stunden und 3 Werktagen)
- Niedrig (Tickets mit längerer notwendiger Entstörzeit, z.B. mehr als 3 Werktagen)

Die Priorisierung erfolgt durch den 1st Level Support oder ggf. durch andere erfahrene Personen.

Zuweisung

Das Ticket wird in Abhängigkeit von Klassifizierung und ggf. Priorisierung entsprechend qualifiziertem und berechtigtem Fachpersonal zugewiesen.

2.2.3.3 Herstellung des Soll-Zustandes / Eskalation (Phase III)

Die grundlegenden Aktivitäten dieser Phase sind:

- Erarbeitung und Diagnose einer Lösung
- Umsetzung der Lösung bzw. Durchführung eines Workarounds
- Ticketweiterleitung an andere Supportstufe bzw. Eskalation

Erarbeitung einer Diagnose und Lösung

Der Bearbeiter des Tickets analysiert den Incident und erarbeitet eine Lösung. Eine angemessene Form der IT-Dokumentation, vorzugsweise mittels der im Abschnitt 112.2.2 “Werkzeuge im Security Incident Management Prozess“ beschriebenen CMDB und KEDB, ist zu etablieren und zur Diagnose und Lösungserarbeitung zu nutzen.

Umsetzung der Lösung bzw. Durchführung einer temporären Lösung

Der Bearbeiter des Tickets setzt die erarbeitete Lösung um oder führt eine temporäre Lösung (Workaround) durch.

Ticketweiterleitung an andere Supportstufe bzw. Eskalation

Falls der Bearbeiter das Ticket nicht lösen kann, so muss sichergestellt sein, dass das Ticket an eine andere Supportstufe oder einen anderen Bearbeiter weitergeleitet wird. Hierzu gehören sowohl die Weiterleitung des Tickets an andere Bearbeiter innerhalb der Organisation oder externe Dienstleister als auch eine Weiterleitung an andere Verantwortungsbereiche des *Sicheren Netzes der KVen*.

Falls ein Incident nicht innerhalb einer definierten Zeit gelöst werden kann bzw. untypisch oder kritisch ist, muss ein Eskalationsprozess eingeleitet werden.

2.2.3.4 Dokumentation und kontinuierliche Verbesserung (Phase IV)

Die grundlegenden Aktivitäten dieser Phase sind:

- Dokumentation der Lösung und Änderung des Ticketstatus
- Meldung an den ursprünglich Meldenden des Incidents und die Betroffenen
- Schließen des Tickets

Dokumentation der Lösung und Änderung des Ticketstatus

Der Bearbeiter des Tickets dokumentiert die Lösung in der Known Error Database (KEDB) und ändert den Ticketstatus im Ticket System.

Meldung an den ursprünglich Meldenden des Incidents und die Betroffenen

Der Bearbeiter des Tickets informiert den ursprünglich Meldenden des Vorfalls und ggf. weitere Betroffene über die Lösung, z.B. telefonisch oder per eMail.

Schließen des Tickets

Nach Bestätigung durch den Meldenden oder automatisch nach Ablauf eines vordefinierten Zeitraumes wird das Ticket durch den Bearbeiter des Tickets im Ticket System geschlossen.

2.2.3.5 Reporting und Analyse (Phase V)

Eine Berichterstattung kann anlassbezogen oder nach einem definierten Zeitraum erfolgen.

Das Reporting sollte an den Verantwortlichen für das Security Incident Management, an den Risikomanager und die fachlich Verantwortlichen erfolgen.

Entsprechende Kennzahlen sind zu definieren und für definierte Zeiträume auszuwerten, z.B.:

- Anzahl der Security Incidents je Priorität
- Anzahl der Security Incidents je Gerät bzw. Gerätetyp
- Erstlösungsquote des 1st Level Supports
- Anzahl von Security Incidents, die vereinbarte Entstörfristen verletzen

Auf Basis dieser Kennzahlen sind die Reports und Analysen durchzuführen und an die Verantwortlichen zu schicken.

Insbesondere ist die Möglichkeit der Definition von Kennzahlen zur Identifikation von Risiken und der Risikoeinschätzung im Rahmen des Risikomanagements (Abschnitt 2.3.5) zu beachten.

2.3 Schnittstellen zu anderen Prozessen

Der Prozess des Security Incident Managements ist in die bestehenden Prozesse jeder Organisation einzubinden. Zu verschiedenen Prozessen existieren Schnittstellen, z.B. zum

- Problem Management,
- Change Management,
- Service Level Management,
- Business Continuity Management und
- Risikomanagement.

Diese Prozesse und deren Schnittstellen zum Security Incident Management werden im Folgenden beschrieben.

2.3.1 Problem Management

Das Problem Management dient der nachhaltigen Ermittlung von Ursachen, welche zu einem entsprechenden Incident geführt haben. Ist durch den Helpdesk ein Workaround, also eine temporäre Lösung für den betrachteten Incident erarbeitet worden, so ist es die Aufgabe des Problem Managements durch eine gezielte Analyse des Incidents eine nachhaltige und dauerhafte Lösung zu finden.

2.3.2 Change Management

Change Management hat das Ziel, dass alle Anpassungen an der IT-Infrastruktur kontrolliert, effizient und unter Minimierung von Risiken für den Betrieb bestehender Dienste durchgeführt werden.

Bei der Problemanalyse und Problemlösung eines Security Incidents sind daher zwingend die in der jeweiligen Organisation definierten Regelungen des Change Managements zu beachten. Eine entsprechende Schnittstelle im Security Incident Management Prozess ist hierfür vorzusehen.

2.3.3 Service Level Management

Das Service Level Management hat die Aufgabe, die Sicherstellung der vereinbarten Servicequalität zu gewährleisten. Die Service Qualität wird durch vertragliche Regelungen, den Service Level Agreements, geregelt.

In diesem Rahmen steuert das Service Level Management die internen und externen Leistungserbringer, um die Sicherstellung der vereinbarten Servicequalität zu gewährleisten. Die Berücksichtigung neuer Service Requests ist hierbei ebenso ein Inputfaktor, wie die Zusagen innerhalb der Service Level Agreements.

2.3.4 Business Continuity Management

Business Continuity Management (BCM), auch betriebliches Kontinuitätsmanagement genannt, beschäftigt sich mit der Vorsorge für Notfallsituationen 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. Business Continuity Management ist daher eine Strategie zur vorausschauenden Sicherstellung des Geschäftsbetriebs.

Der Prozess des Business Continuity Managements ist in [KBV_SNK_RLEX_BCM] beschrieben.

Das BCM umfasst einen proaktiven Teil, die Notfallvorsorge, und einen reaktiven Teil, der das Vorgehen in Notfällen beschreibt.

Im Rahmen der Notfallvorsorge wird eine Analyse der kritischen Geschäftsprozesse durchgeführt. Hieraus ergeben sich Schwellwerte und Kennzahlen, die im Incident Management für die Klassifizierung von Tickets sowie im Monitoring für die Systemüberwachung als Bewertungs-Maßstab herangezogen werden können.

Weiterhin muss im Security Incident Management im Prozessschritt Klassifizierung, Priorisierung und Zuweisung (Phase II) die Initiierung der BCM-Prozesse bei Eintritt eines Notfalls, z.B. die Einleitung eines Notfallplans, definiert werden.

2.3.5 Risikomanagement

Der Prozess des Security Incident Managements sollte auf Grundlage von Prozesskennzahlen und Schwellwerten die Steuerung des Risikomanagements unterstützen. Der Prozess des Risiko Managements ist in [KBV_SNK_RLEX_Risikomanagement] beschrieben.

Grundlage des Risikomanagements bilden die organisationseigenen Werte (Assets). Werte sind alle materiellen und immateriellen Güter, Informationen und Geschäftsprozesse, die einen Schutzbedarf haben. Alle organisationseigenen Werte sollen eindeutig identifiziert werden. Hierzu ist ein Inventar aller wichtigen Werte zu erstellen und zu pflegen. Es empfiehlt sich innerhalb dieser Liste die Werte in Wertegruppen zu gruppieren.

Der Prozess des Risikomanagements folgt einem Regelkreis. Die folgenden Prozessschritte werden für jeden identifizierten organisationseigenen Wert durchgeführt werden:

- Risikoidentifikation
- Risikoeinschätzung
- Risikobewertung
- Risikobehandlung

Diese Prozessschritte werden unterstützt durch die Risikoüberwachung und Risikokommunikation.

Verschiedene Kennzahlen des Security Incident Management Prozesses können für die einzelnen Schritte des Risikomanagement genutzt werden. Auf einzelne wird hier besonders eingegangen.

- Risikoidentifikation
    - Ein erhöhtes Aufkommen von Security Incidents kann als Indikator für neue, nicht hinreichend beachtete Risiken angesehen werden. Vermehrt auftretende Incidents bei bestimmten Werte oder Wertegruppen sind dann in die Risikoanalyse aufzunehmen.
- Risikoeinschätzung
    - Zur Einschätzung eines Risikos wird im Rahmen der Risikoeinschätzung die Wahrscheinlichkeit für das Eintreten eines Schadensereignisses und die Auswirkung bei Eintritt des Schadensereignisses geschätzt. Die Wahrscheinlichkeit des Eintritts eines Schadens z.B. bei bestimmten Werten und Wertegruppen wie IT-Systemen kann aus Kennzahlen des Security Incident Management abgeleitet werden.

Generell sollte für Risiken, bei denen aufgrund der Risikoeinschätzung und Risikobewertung ein potentiell hoher Schaden bei Eintritt des Schadensereignisses zu erwarten ist, eine höhere Priorisierung der entsprechenden Incidents im Incident Management und ggf. ein automatisiertes Monitoring wie in Abschnitt 2.4 beschrieben durchgeführt werden.

2.4 Unterstützung des Security Incident Managements durch automatisiertes Monitoring von Geräten und Diensten

Der Prozess des Security Incident Managements kann durch ein automatisiertes Monitoring von Geräten und Diensten unterstützt und verbessert werden.

Durch ein automatisches Monitoring kann ein (mögliches) Problem bereits bei der Entstehung und teilweise sogar vor der Entstehung erkannt und gemeldet werden. Durch diese frühzeitige Entdeckung und Meldung potentieller Probleme können Problemlösungen früher angegangen werden und Schadenswirkungen verringert werden.

Das Monitoring von Geräten und Diensten sollte in das Security Incident Management eingebunden werden. Hierzu sind grundlegend zwei Schritte notwendig. Einerseits müssen sinnvolle Schwellwerte und Kennzahlen im Monitoring System definiert werden, die festlegen, ab wann eine Störung eines Gerätes oder eines Dienstes vorliegt. Im nachfolgenden Schritt müssen die erkannten Störungen automatisiert über eine definierte Schnittstelle in den Prozess des Security Incident Managements aufgenommen werden, wie in Abschnitt 2.2.3.1 beschrieben, z.B. über eine definierte Schnittstelle zwischen dem Monitoring System und dem Ticket System.

Bei Erreichen des definierten Schwellwertes muss automatisch eine Benachrichtigung an das Ticket System erfolgen. Die Schwellwerte müssen sinnvoll eingestellt sein.

Die Benachrichtigung ist abhängig von den verwendeten Tools und sollte die zur Fehlerbehebung notwendigen Informationen beinhalten, u.a.

- Gerät, welches die Nachricht auslöst
- Zeitpunkt des Auftretens
- Status des Gerätes bzw. Dienstes
- Weitere Informationen, z.B. eine Problembeschreibung bzw. Error Codes

Die eingehende Nachricht muss vom Ticket System so automatisiert verarbeitet werden können, dass die Informationen in das Ticket System übernommen werden und der Prozess des Security Incident Managements aufgenommen werden kann.

In Anhang A werden für verschiedene Gerätegruppe und Dienste Empfehlungen ausgesprochen, die konkrete Umsetzung obliegt der jeweiligen Organisation.

Ein Monitoring sollte jede Organisation in ihrem Verantwortungsbereich etablieren. Dieses Monitoring sollte mindestens die kritischen Gerätegruppe bzw. Geräte und bestimmte Eigenschaften dieser Geräte umfassen.

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
Business Continuity Management (BCM)	Business Continuity Management, auch betriebliches Kontinuitätsmanagement genannt, beschäftigt sich mit der Vorsorge für Notfallsituationen 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. Business Continuity Management ist daher eine Strategie zur vorausschauenden Sicherstellung des Geschäftsbetriebs.
Business Continuity Management System (BCMS)	Managementsystem für ein BCM. Siehe Business Continuity Management (BCM).
Configuration Management Database (CMDB)	Eine Configuration Management Data Base beinhaltet die Gesamtheit aller für die Leistungserstellung erforderlichen Daten, inklusive der Beschreibung der einzelnen Configuration Items und deren Verbindungen untereinander.
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.
Informationssicherheitsmanagementsystem (ISMS)	Teil des gesamten Managementsystems, der auf der Basis eines Geschäftsrisikoansatzes die Entwicklung, Implementierung, Durchführung, Überwachung, Überprüfung, Instandhaltung und Verbesserung der Informationssicherheit abdeckt.
Known Error Database	Die Known Error Data Base enthält alle Fehler mit bekannter Ursache und zugehörige Workarounds.
KV-App	Siehe Applikation.

Begriff	Erklärung
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.
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*. 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.

4 Referenzierte Dokumente

Referenz	Dokument
KBV_SNK_RLEX_Informationssicherheit	Richtlinie Informationssicherheit
KBV_SNK_RLEX_Risikomanagement	Richtlinie Risikomanagement
KBV_SNK_RLEX_BCM	Richtlinie Business Continuity Management

A N H A N G

A Umsetzungsempfehlungen Monitoring

Wie an Abschnitt 2.4 beschreiben, unterstützt ein automatisiertes Monitoring von Geräten und Diensten den Prozess des Security Incident Managements.

In diesem Anhang werden für verschiedene Gerätegruppe und Dienste Empfehlungen ausgesprochen.

A.1 Gerätegruppen

Im *Sicheren Netz der KVen* kommen aufgrund der unterschiedlichen Verantwortungsbereiche und Aufgaben auch verschiedene Geräte und Gerätegruppen zum Einsatz, die jeweils eine heterogene Zusammenstellung von Hardware und Software darstellen.

In diesem Abschnitt erfolgt eine Kategorisierung der Geräte in Gerätegruppen. Für jede Gerätegruppe werden dann in den folgenden Abschnitten Empfehlungen getroffen.

Grundsätzlich wird für alle Geräte mindestens die Erreichbarkeit überwacht, für einzelne Geräte werden auch darüber hinaus gehende Parameter empfohlen, um z.B. frühzeitig und noch vor Erreichen eines Problems eine Meldung erzeugen zu können.

Die folgende Tabelle zeigt das Mapping zwischen Gerätegruppen und zu überwachenden Eigenschaften.

	Erreichbarkeit / Verfügbarkeit	Auslastung Schnittstelle	CPU/ RAM	Speicherplatz	AV + IDS/IPS Signaturen
Router	x	x	x		
Backbone-Router	x	x	x		
Switch	x				
Firewall	x	x	x		
IDS/IPS	x				x
Server	x		x	x	

A.1.1 Router und Backbone-Router

Router spielen generell eine zentrale Rolle in Netzwerken, da sie verschiedene Netzwerksegmente- und Netzklassen miteinander verbinden. Oft stellen sie auch externe Anbindungen zur Verfügung und sind daher von elementarer Wichtigkeit.

Im *Sicheren Netz der KVen* sind Router verschiedener Hersteller im Einsatz. Bei Routern sind generell die Möglichkeiten beschränkt, Informationen über den Zustand des Gerätes zu erhalten. Bei Routern ist die grundsätzliche Erreichbarkeit, aber auch die Auslastung der verschiedenen Verbindungen beziehungsweise Schnittstellen entscheidend. Hierbei sind die Schnittstellen, an denen eine konzentrierte Anzahl von Teilnetzen gebündelt wird diejenigen, die detailliert überwacht werden sollen.

Zusätzlich wird empfohlen bei kritischen Systemen - wie zum Beispiel Routern für externe Anbindungen - die CPU-Auslastung und die Speicher-Auslastung mit in die Überwachung aufzunehmen.

Die detaillierte Überwachung mit CPU und Speicherwerten hat den Vorteil, nicht nur Informationen über die Auslastung der einzelnen Verbindungen, sondern auch die Auslastung des Systems selbst zu erhalten. Hierdurch können frühzeitig Engpässe erkannt und gegebenenfalls die Notwendigkeit einer Reaktion bestimmt werden.

Bei Routern die im Netzwerk für logische Segmentierungen verantwortlich sind, die also keine externe Anbindung haben, genügt es, die Erreichbarkeit, die Auslastung und Verfügbarkeit der wichtigen Schnittstellen zu überwachen.

A.1.2 Switch

Zu den Eigenschaften, die bei Switchen zu überwachen sind, zählt die grundsätzliche Erreichbarkeit, aber auch die Verfügbarkeit verschiedener Schnittstellen beziehungsweise Netzwerkinterfaces.

Bei Switchen ist es im Allgemeinen nicht nötig, interne Eigenschaften des Gerätes wie die CPU oder Speichernutzung zu überwachen.

A.1.3 Firewall

Da Firewalls in Netzwerken nicht nur logisch, sondern auch physisch eine zentrale Rolle einnehmen, ist hier ein besonderes Augenmerk erforderlich. Wie bei kritischen Routern und Switches macht auch hier eine Überwachung der Schnittstellen Sinn, um einen Indikator über die Auslastung der Anbindung zu erhalten.

Ein weiterer wichtiger Wert, den es zu überwachen gilt, ist die Anzahl der geblockten Verbindungen.

Informationen über die Art der gesperrten Verbindungen sind im Normalfall nicht relevant, da von einer funktionsfähigen Firewall ausgegangen werden kann. Dies bedeutet im Umkehrschluss, dass die erlaubten Verbindungen analysiert werden müssten, um Rückschlüsse auf ein mögliches Eindringen eines Angreifers ziehen zu können.

Beides ist jedoch in der Praxis nicht realistisch umzusetzen. Da es einem Angreifer normalerweise nie gelingt sofort ein Einfallstor zu finden, sondern verschiedene Fehlversuche vorab stattfinden, sind diese ein indirekter Indikator darüber, ob ein gehäuftes Aufkommen an Angriffen zu verzeichnen ist. Dieser Wert der geblockten Verbindungen muss im Zuge der Umsetzung erarbeitet werden, da er sich von Standort zu Standort unterscheidet.

Zusätzlich ist es sinnvoll, bei Firewalls die Speicher und CPU-Auslastung zu überwachen. Firewalls haben eine Vielzahl an performancebeanspruchenden Eigenschaften. Zu diesen zählen unter anderem die Policy-Tabelle, anhand derer Pakete gefiltert werden. Weiter bieten Firewalls signaturbasierte IDS/IPS Funktionalität, die mit einem sehr großen Ressourcenbedarf einhergeht. All diese Faktoren wirken sich auf die Auslastung und den Betrieb des Systems aus und sind aufgrund dessen zu überwachen.

A.1.4 IDS / IPS

Im Allgemeinen sind Instrusion Detection/Instrusion Prevention Systeme im *Sicheren Netz der KVen* mit in die Firewall integriert und keine separate Hardware. Hierdurch sind die internen Systemeigenschaften bereits Bestandteil des Monitorings und werden überwacht.

Einzig die Auswertung des IDS/IPS Systems ist noch mit aufzunehmen. Da diese Alarme von IDS/IPS Systemen ereignisbasiert sind, ist von einer zyklischen Überprüfung abzusehen.

Beim Auftreten eines sicherheitsrelevanten Ereignisses muss die Benachrichtigung sofort erfolgen. Hierfür stellen IDS/IPS Systeme SNMP Traps zur Verfügung, die für die Informationsweiterleitung verantwortlich sind.

Diese Überwachung von SNMP Traps ist Teil des Monitorings.

A.1.5 Server

Bei Servern kommt es sehr auf die Nutzung an, um zu entscheiden, wie sie als Teil des Monitorings einzubinden sind und welche Parameter überwacht werden sollen.

Ein Fileserver hat im Hinblick auf die Überwachung sehr unterschiedliche Eigenschaften im Gegensatz zu einem HTTP-Server. Auch kommt es auf das installierte Betriebssystem an, welche Eigenschaften mit in die Überwachung aufgenommen werden. Schließlich ist auch der angebotene Dienst ein entscheidender Faktor bei der Bestimmung von zu überwachenden Parametern.

Aufgrund der sehr verschiedenen Eigenschaften kann hier keine grundsätzliche Aussage getroffen werden.

A.1.6 KV-SafeNet-Konzentrator

KV-SafeNet-Konzentratoren sind Hardware-VPN-Router in den Rechenzentren der KVen, die für Teilnehmer einen zentralen Punkt zum Anschluss an das *Sichere Netz der KVen* darstellen. Diese Zugangspunkte werden von den KV-SafeNet-Providern bereitgestellt.

Im eigentlichen Sinne sind KV-SafeNet-Konzentratoren Router für einen speziellen Zweck – eine gesicherte Verbindung. Aufgrund der gemeinsamen Eigenschaften mit Routern, die keine Verschlüsselung nutzen, sind auch die Überwachungsmöglichkeiten identisch und können Abschnitt 2.4.1.1 entnommen werden.

A.1.7 KV-FlexNet-Konzentrator

KV-FlexNet-Konzentratoren sind im *Sicheren Netz der KVen* VPN-Router, die für die VPN-Software-Clients in den Arztpraxen einen zentralen Einwahlpunkt darstellen. Diese Einwahlknoten stellen eine Dienstleistung einzelner KVen dar.

Die Funktion dieser KV-FlexNet-Konzentratoren entspricht der der KV-SafeNet-Konzentratoren. Der einzige Unterschied besteht darin, dass auf Seiten der Teilnehmer Software-Clients zum Einsatz kommen.

Aufgrund der gemeinsamen Eigenschaften gleicht auch hier der Ansatz der KV-SafeNet-Konzentratoren.

A.2 Services / Dienste

Wie im vorangegangenen Abschnitt der Gerätegruppen, werden in diesem Abschnitt die verschiedenen Eigenschaften der Dienste beschrieben, die Teil des Monitoring sind.

Folgende Dienste sollen näher betrachtet werden

- HTTP, HTTPS
- sFTP
- SSH
- DNS
- NTP
- Generische TCP-basierte Dienste

A.2.1 HTTP / HTTPS

Das Hyper Text Transfer Protokoll (HTTP) dient zur Übertragung von Inhalt, der von einem Web-Server generiert und versendet wird. Die Antworten enthalten dabei jeweils den Status des Web-Servers, sowie den im Browser darzustellenden Inhalt.

Die Status-Nachrichten als Teil der Antwort melden entweder den Normalbetrieb des Web-Servers, oder die jeweilige Störung im Ablauf. Dabei werden differenzierte Fehlerklassen gemeldet:

- HTTP Response Code 2xx (Service OK)
- HTTP Response Code 3xx (Service Warnung)
- HTTP Response Code 4xx or 5xx (Service Kritisch/Fehler)

Der zugestellte Inhalt kann ebenfalls auf Richtigkeit überprüft werden. Durch diese Eigenschaften - Zustellung von Inhalt und Status - ist es möglich, den Zustand des HTTP Dienstes an sich, sowie möglicher angeschlossener Datenbanken und Backend-Systeme zu prüfen.

Bei Webanwendungen wird die grundsätzliche Verfügbarkeit des Dienstes, aber auch der erwartete Inhalt kontrolliert. Zusätzlich kann bei SSL-Verbindungen die Gültigkeit des Zertifikates überprüft werden.

A.2.2 SFTP

Das Secure File Transfer Protocol (SFTP) dient zum sicheren Transfer von Daten über ungesicherte Verbindungen. Ein SFTP-Server stellt eine Verzeichnisstruktur und Dateien beziehungsweise Speicherplatz bereit, auf welche mittels entsprechender Clients zugegriffen werden kann.

Hierbei kann der Dienst selbst sowie die Möglichkeit, erfolgreich Daten zu übertragen, mit in das Monitoring integriert werden.

Im Zusammenhang mit diesem Dienst wird auch die Überwachung des verfügbaren Speicherplatzes empfohlen, da dieser Wert einen wichtigen Faktor für die Funktion des Dienstes darstellt.

Überprüft wird die Funktionalität eines SFTP Server durch das erfolgreiche Übertragen und Speichern im entfernten System.

A.2.3 SSH

Der Secure Shell (SSH) Dienst ist unter Unix-artigen Betriebssystemen der Dienst, durch den man eine gesicherte Terminalverbindung herstellen kann. Dieses Protokoll bietet entsprechende Funktionalität, um die Verbindung zu verschlüsseln, die Integrität der Daten sicher zu stellen und ein entferntes System zu bedienen.

Es kann die grundsätzliche Erreichbarkeit überprüft werden. Es kann der Dienst an sich, aber auch die Möglichkeit sich als bekannter Nutzer erfolgreich zu verbinden, überprüft werden.

A.2.4 DNS

Das Domain Name System (DNS) ist ein Service, der Namen zu Netzwerkadressen wandelt und somit den Zugriff auf Ressourcen erleichtert. Der DNS-Service liefert im Normalfall auf eine Anfrage zur Namensauflösung eine Antwort mit der zugehörigen IP-Adresse, die in der internen Konfiguration festgelegt wurde.

Diese Eigenschaft kann genutzt werden, um im Monitoring nicht nur die Verfügbarkeit des Dienstes an sich, sondern auch die Funktionalität zu überprüfen. Es wird die grundsätzliche

Erreichbarkeit sowie die gelieferte Antwort überprüft. Erwartete Ergebnisse können so kontrolliert und es kann auf mögliches Fehlverhalten reagiert werden.

A.2.5 NTP

Das Network Time Protocol dient einem Netzwerk mitsamt seinen verschiedenen Komponenten als Zeit-Synchronisations-Dienst. Es stellt die im Netzwerk allgemeingültige Zeit zur Verfügung und gilt als Referenz für alle weiteren Systeme. Die genaue Zeit aller Knoten im Netzwerk ist zum Beispiel für Log-Vergleiche zwischen verschiedenen Systemen von sehr großer Bedeutung.

Für den richtigen Betrieb des Dienstes ist unter anderem die Verfügbarkeit ausschlaggebend. Des Weiteren kann die Zeit-Differenz zum Monitoring-System selbst kontrolliert werden. Aufgrund der Relevanz dieses Dienstes ist es auch empfehlenswert, die Zeit des internen NTP Servers gegen einen externen zu prüfen.

Bei dem NTP Dienst wird die grundsätzliche Verfügbarkeit des Dienstes, aber auch die Zeitdifferenz zum eigenen System kontrolliert.

Somit sind die Verfügbarkeit des Dienstes, sowie die zur Verfügung gestellte Zeit sichergestellt.

A.2.6 Generische TCP-basierte Dienste

Das Transmission Control Protocol ist ein Netzwerkprotokoll, das vielen Diensten als Grundlage dient. TCP stellt unter anderem sicher, dass Datenpakete erfolgreich übertragen werden.

Es können auf dieser Basis alle nicht genauer spezifizierten Services, die auf TCP basieren, mit einer generischen Methode überwacht werden. Diese Methode ist ein so genannter TCP Handshake, der auf den entsprechenden Ports des Services durchgeführt wird.

Der zu überwachende Service wird so angesprochen und auf seine korrekte Reaktion hin überprüft. Wenn dieser TCP-Handshake funktioniert, ist der Service erreichbar und bestätigt die ankommende Anfrage.

Dadurch ist die Überwachung auf Erreichbarkeit eines auf TCP basierenden - und nicht genauer spezifizierten - Services möglich.