Kassenärztliche Bundesvereinigung

Körperschaft des öffentlichen Rechts

Sicheres Netz der KVen

Richtlinie Risikomanagement

[KBV_SNK_RLEX_Risikomanagement]

Dezernat 6
Informationstechnik, Telematik und Telemedizin

10623 Berlin, Herbert-Lewin-Platz 2

Kassenärztliche Bundesvereinigung

Version	1.0
Datum:	12.12.2011
Klassifizierung:	Öffentlich
Status:	In Kraft

DOKUMENTENHISTORIE

Version	Datum	Autor	Änderung	Begründung	Seite
1.0	12.12.2011	KBV	Erstellung des Dokuments, QS und Freigabe		

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.

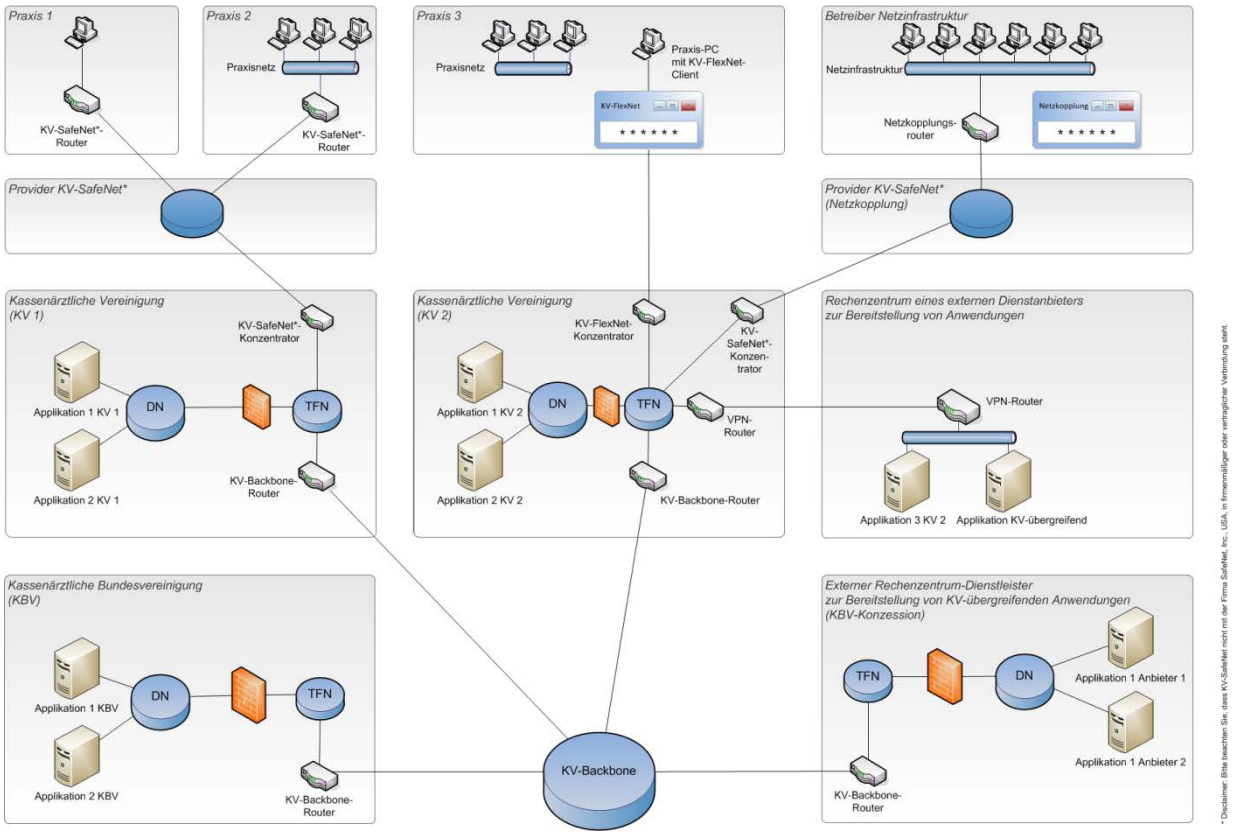


Abbildung 1: Beispielhafte Netztopologie

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

Gemäß Richtlinie [KBV_SNK_RLEX_Informationssicherheit] ist Risikomanagement ein wesentlicher Baustein für die Informationssicherheit. Dieses Dokument beschreibt die grundsätzliche Vorgehensweise zum Risikomanagement im *Sicheren Netz der KVen* und gibt konkrete Empfehlungen und Beispiele für die organisationsspezifische Umsetzung für alle beteiligten Akteure.

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.

* 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

2.1 Grundlagen und Einordnung

Ereignisse, die den Sicherheitszielen für das *Sichere Netz der KVen*[2] zuwiderlaufen, sollen im Einzelnen präventiv erkannt und das Ausmaß eines jeweiligen Risikos in qualitativer und falls erforderlich auch in finanzieller Hinsicht bewertet werden, um etwaige Gegenmaßnahmen einleiten zu können. Risikomanagement ist daher eine Strategie im Sinne einer vorausschauenden Schadensvermeidung.

Risikomanagement ist ein zentraler Baustein im Rahmen des Regelkreises zur Aufrechterhaltung und kontinuierlichen Verbesserung des Informationssicherheitsmanagements gemäß der Richtlinie [KBV_SNK_RLEX_Informationssicherheit]. Gleichzeitig ist das Risikomanagement eine methodische Voraussetzung für das betriebliche Kontinuitätsmanagemement (BCM) gemäß der Richtlinie [KBV_SNK_RLEX_BCM].

2.2 Management von Werten

Grundlage des Risikomanagements bilden die organisationseigenen Werte (Assets). Werte sind alle materiellen und immateriellen Güter, Informationen und Geschäftsprozesse, die einen Schutzbedarf haben.

2.2.1 Inventar der organisationseigenen Werte

Alle organisationseigenen Werte sollen eindeutig identifiziert werden. Hierzu ist ein Inventar aller wichtigen Werte zu erstellen und zu pflegen (Werteliste).

Es empfiehlt sich innerhalb dieser Liste die Werte zu gruppieren. Folgende Wertegruppen können dabei unterschieden werden[3]:

a) Informationen

Hierzu zählen alle Daten und Informationen wie zum Beispiel aus Datenbanken und Dateien, Verträgen und Vereinbarungen, Systemdokumentation, Forschungsinformationen, Benutzerhandbücher, Schulungsunterlagen, dokumentierte Betriebs- oder Supportverfahren, Sicherheitspläne, Auditprotokolle und archivierte Informationen.

b) Geschäftsprozesse

Unter Geschäftsprozesse wird die Abfolge von Tätigkeiten verstanden, die schrittweise ausgeführt werden, um das geschäftliche Ziel der eigenen Organisation zu erreichen.

c) Hardware

Hierzu zählen physische Werte wie zum Beispiel: Computeranlagen, Kommunikationsanlagen, Datenträger und andere technische Ausstattung wie Netzgeräte und Klimageräte.

[2] Siehe hierzu Richtlinie [KBV_SNK_RLEX_Informationssicherheit].
[3] Vgl. hierzu auch ISO/IEC 27005:2008 (E) – Information secutity risk management, Annex B. S. 30ff.

d) Software

Hierzu zählen zum Beispiel: Anwendungssoftware, Systemsoftware, Entwicklungstools und Dienstprogramme.

e) Netzwerk

Hierzu gehören Rechnernetze (lokale wie auch Weitverkehrsnetze) und Telekommunikationsnetze.

f) Personal

Hierzu zählen vor allem die Qualifikationen, Fähigkeiten und Erfahrungen der Mitarbeiter.

g) Standort

Hierzu gehören zum Beispiel Standorte, Gebäude und Gebäudeteile sowie Räumlichkeiten und Sicherheitszonen.

h) Organisation

Hierzu zählen die Struktur und Funktion der Organisation und ihr Image.

Informationen und Geschäftsprozesse sind *primäre Werte*. Hard- und Software, Netzwerk, Personal, Standort und Organisation sind *unterstützende Werte*, auf die die primären Werte vertrauen.

2.2.2 Bestimmung der Kritikalität

Gemäß der Richtlinie [KBV_SNK_RLEX_Informationssicherheit] steht im Mittelpunkt des Sicherheitsmanagements die Gewährleistung folgender Grundeigenschaften:

- Verfügbarkeit

  Eigenschaft von Werten, auf Verlangen zugänglich und nutzbar zu sein

- Integrität

  Eigenschaft der Absicherung von Richtigkeit und Vollständigkeit von Werten

- Vertraulichkeit

  Eigenschaft, dass Informationen unberechtigten Personen, Einheiten oder Prozessen nicht verfügbar gemacht oder enthüllt werden

Grundsätzlich sollen diese Grundeigenschaften für jeden einzelnen Wert eingeschätzt werden, um dessen Kritikalität zu bestimmen. Bei Bedarf können weitere Eigenschaften ergänzt werden. Verfügbarkeit, Integrität und Vertraulichkeit werden somit zu den Schutzzielen der einzelnen Werte.

Der Schutzbedarf kann je Schutzziel in Anlehnung an das BSI[4] in die folgenden drei Stufen definiert werden:

- Normal — Die Schadensauswirkungen sind begrenzt und überschaubar.
- Hoch — Die Schadensauswirkungen können beträchtlich sein.
- Sehr hoch — Die Schadensauswirkungen können ein existentiell bedrohliches, katastrophales Ausmaß erreichen.

Die einzelnen Schutzbedarfskategorien sind in ihrer Ausprägung und Abgrenzung exakt zu definieren. Dabei sind die organisationsspezifischen Anforderungen und Schutzbedarfe zu berücksichtigen. Eine mögliche Definition der Kategorien ist in Anhang A hinterlegt.

2.2.3 Verantwortung für organisationseigene Werte

Für alle organisationseigenen Werte sollen durch das Management Werteverantwortliche bestimmt werden. Werteverantwortliche haben dabei die vom Management zugewiesene Verantwortung für den sicheren Umgang mit diesem Wert. Folgende Verantwortung wird dabei in der Regel an den Verantwortlichen übertragen:

- Sicherstellung, dass Werte nach ihrem Schutzbedarf angemessen bewertet sind
- Definition und regelmäßige Überprüfung der Zutritts-, Zugangs- und Zugriffsbeschränkungen gemäß den entsprechenden Regelungen
- Unterstützung bei der Risikoidentifikation und -einschätzung
- Umsetzung von durch das Management festgelegten Maßnahmen zur Gewährleistung und Aufrechterhaltung der Sicherheit des Wertes

Die Umsetzung von Maßnahmen kann gegebenenfalls durch den Werteverantwortlichen delegiert werden. Die Verantwortung für den angemessenen Schutz des Wertes verbleibt jedoch beim Werteverantwortlichen.

2.2.4 Zulässiger Gebrauch von organisationseigenen Werten

Alle Mitarbeiter, Auftragnehmer und Dritte sollen den Regeln für den zulässigen Gebrauch von Informationen und organisationseigenen Werten in Verbindung mit informationsverarbeitenden Einrichtungen folgen. Diese Regeln sollen in Form von Verfahrensanweisungen dokumentiert werden und zur Verfügung stehen.

[4] Siehe BSI-Standard 100-2, IT-Grundschutz Vorgehensweise, Version 2.0, Abschnitt 4.3.1.

2.3 Risikomanagement

Der Prozess des Risikomanagements folgt einem Regelkreis. Die folgenden Prozessschritte sollen mindestens einmal im Jahr für jeden identifizierten organisationseigenen Wert durchgeführt werden:

a) Risikoidentifikation
b) Risikoeinschätzung
c) Risikobewertung
d) Risikobehandlung

Informationen und Ergebnisse des Risikomanagements sind zudem kontinuierlich zu kommunizieren. Die einzelnen Schritte, Aktivitäten und vor allem Risiken sind zu überwachen. Die folgende Abbildung verdeutlicht den Prozessablauf des Risikomanagements.

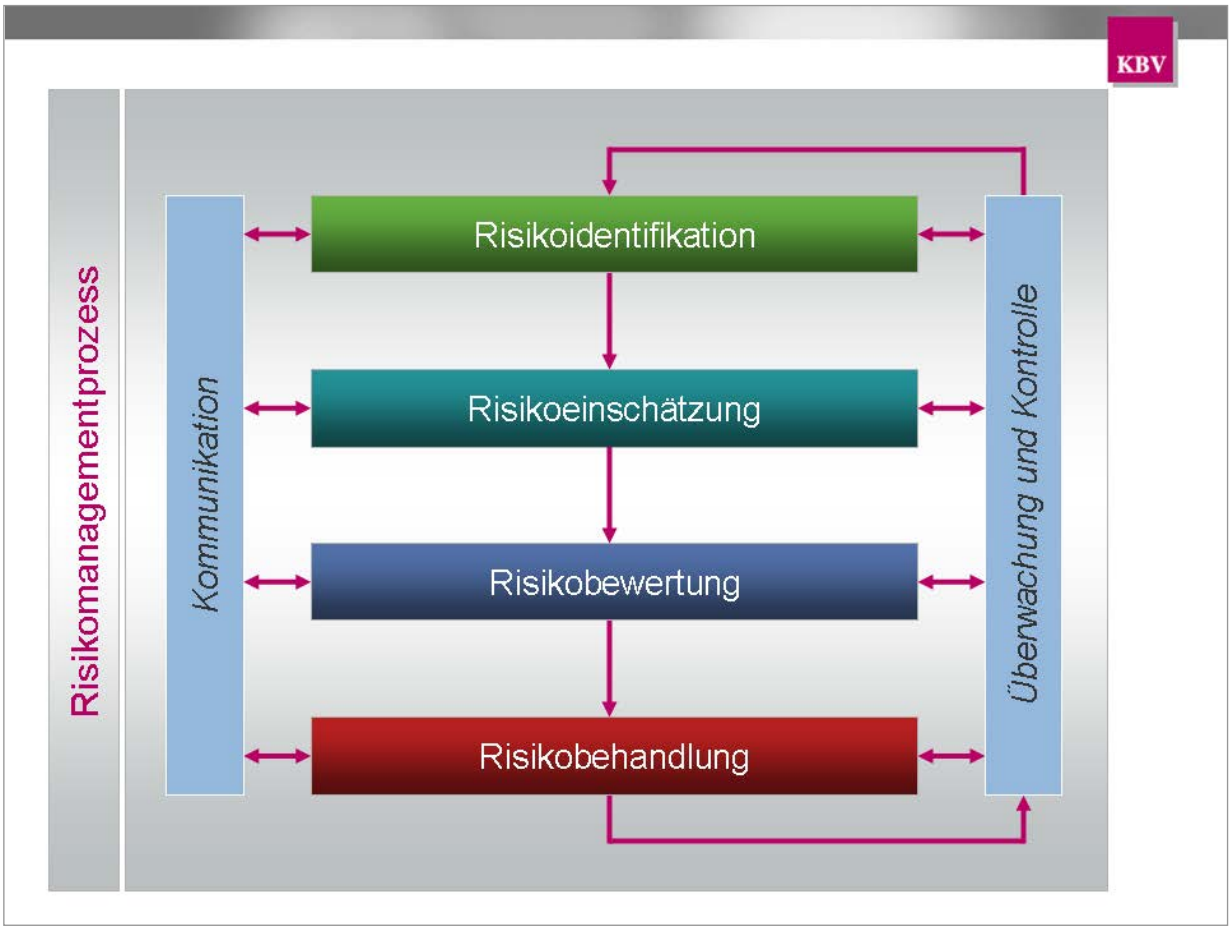


Abbildung 2: Schematische Darstellung des Risikomanagementprozesses[5]

[5] Vgl. hierzu auch ISO/IEC 27005:2008 (E) – Information secutity risk management, S. 5.

2.3.1 Risikoidentifikation

Grundlage für die Risikoidentifikation bilden die gruppierten *unterstützenden Werte* und ihre bestimmten Schutzbedarfe. Da die *primären Werte* (Informationen und Geschäftsprozesse) auf den unterstützenden Werten (Hard- und Software, Netzwerk, Personal, Standort und Organisation) aufbauen, sind sie bei der Identifikation der Risiken zweitrangig. Jedoch sollte dann die Referenz zwischen unterstützendem und primärem Wert dokumentiert werden. Zur Risikoidentifikation sind folgende Schritte erforderlich:

a) Identifikation der Bedrohungen

Je identifiziertem Wert sollen relevante Bedrohungen und ihre Quellen ermittelt werden. Dabei sind die Erfahrungen aus der Praxis und insbesondere vergangene Sicherheitsvorfälle auszuwerten.

Eine weitere Unterstützung bilden die Gefährdungskataloge des Bundesamts für die Sicherheit in der Informationstechnik (BSI). In Anlehnung daran können die ermittelten Bedrohungen wie folgt kategorisiert werden:

- Höhere Gewalt
- Organisatorische Mängel
- Menschliche Fehlhandlungen
- Technisches Versagen
- Vorsätzliche Handlungen

b) Identifikation bereits implementierter Maßnahmen

Bereits implementierte Maßnahmen sollen identifiziert und deren bisherige Wirkung berücksichtigt werden.

c) Identifikation der Schwachstellen

Je Bedrohung sollen die Schwachstellen identifiziert werden, die durch die Bedrohung ausgenutzt werden können und dem betroffenen Wert Schaden zufügen können. In folgenden Bereichen können Schwachstellen u.a. identifiziert werden:

- Organisation (Struktur)
- Geschäftsprozesse
- Personal
- Externe Dienstleistungen
- Physische Einrichtungen
- Systemkonfiguration
- Software
- Hardware
- Kommunikation

d) Ermittlung der Konsequenzen mit Bezug auf den Schutzbedarf

Ist eine Bedrohung identifiziert, die eine existente Schwachstelle ausnutzen kann, soll die Konsequenz beurteilt werden. Die Konsequenz ist in Bezug auf die definierten Schutzbedarfe des Wertes (siehe Abschnitt 2.2.2) zu ermitteln. Es muss ermittelt und begründet werden, welches Schutzziel (Verfügbarkeit, Vertraulichkeit bzw. Integrität) durch das Zusammentreffen von Bedrohung und Schwachstelle betroffen ist. Je nach Kritikalität (normal, hoch oder sehr hoch) des kompromittierten Schutzziels können die Folgen unterschiedlich sein.

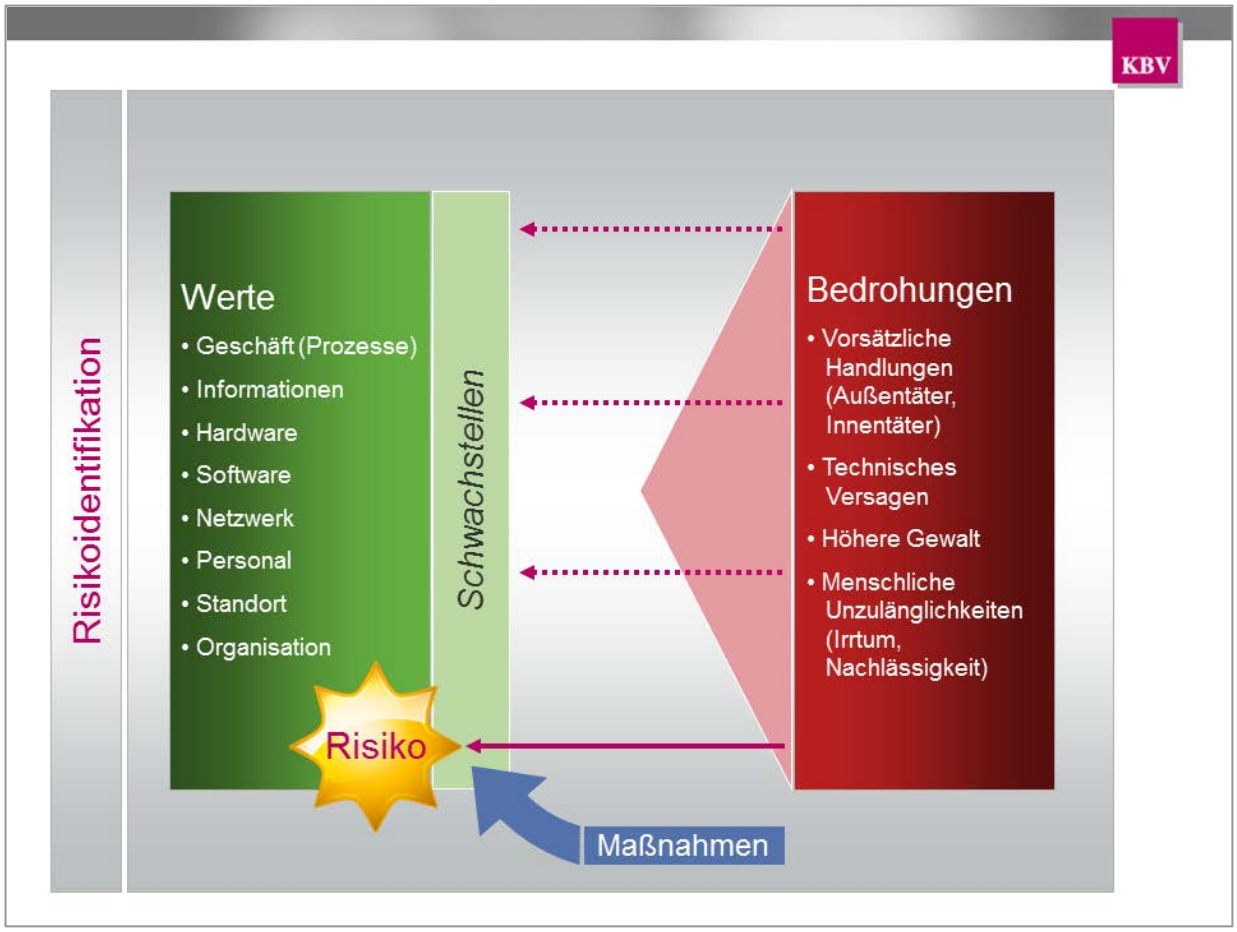


Abbildung 3: Schematische Darstellung der Risikoidentifikation

2.3.2 Risikoeinschätzung

Zur Einschätzung des Risikos sind zwei wesentliche Faktoren zu ermitteln:

a) Wahrscheinlichkeit

Die Wahrscheinlichkeit des Eintretens eines Schadensfalls kann in Stufen eingeschätzt werden. Hierbei ist insbesondere zu berücksichtigen, ob die zugrundeliegende Bedrohung zufällig oder absichtlich motiviert ist. Zur Einschätzung der Wahrscheinlichkeit sollten zudem Erfahrungswerte und der Rat von Experten berücksichtigt werden.

b) Auswirkung

Die Auswirkung, also der mögliche Schaden, kann ebenfalls gestuft eingeschätzt werden. Wenn möglich ist die Auswirkung monetär abzuschätzen. Dabei sind direkte und indirekte Kosten gleichermaßen zu berücksichtigen.

Wahrscheinlichkeit und Auswirkung sind in ihrer Ausprägung und Abgrenzung exakt zu definieren. Dabei sind die organisationsspezifischen Anforderungen und Bedarfe zu berücksichtigen. Eine mögliche Definition der Kategorien ist in Anhang B hinterlegt.

2.3.3 Risikobewertung

Im Rahmen der Risikobewertung soll der Risikograd berechnet werden. Er ist das Produkt der im Rahmen der Risikoeinschätzung ermittelten Wahrscheinlichkeit des Eintretens eines Schadensfalls und der geschätzten Schadensauswirkung (siehe Abschnitt 2.3.2).

Wurde im Zusammenhang mit der Risikoidentifizierung auch die Konsequenz ermittelt, die eine Bedrohung an einer ausnutzbaren Schwachstelle in Bezug auf die definierten Schutzbedarfe des Wertes haben kann (siehe Abschnitt 2.3.1, d)), so kann sie im Rahmen der Risikobewertung mit berücksichtigt werden. Je nach Kritikalität (normal, hoch oder sehr hoch) des kompromittierten Schutzziels können die Folgen unterschiedlich sein. Um dies im Rahmen der Risikobewertung zu berücksichtigen, ist der ermittelte Risikograd entsprechend zu gewichten (Gewichtung siehe Anhang B.3).

Damit ergibt sich die folgende Formel zu Berechnung eines Risikograde:

$$Risikograd = Wahrscheinlichkeit * Auswirkung * Konsequenz$$

Die so ermittelten gewichteten Risikograde lassen sich mit den Dimensionen Wahrscheinlichkeit und Auswirkungen in drei Matrizen darstellen (siehe Anhang C.1). Die gewichteten Risikograde können somit in folgende drei Risikoklassen (siehe Anhang C.2) gruppiert werden:

- Risikoklasse 1

  Das Risikoniveau ist gering und akzeptabel. Eine zusätzliche Maßnahme ist nicht zwingend erforderlich.

- Risikoklasse 2

  Es besteht ein mittleres Risiko. Eine zusätzliche Maßnahme ist erforderlich.

- Risikoklasse 3

  Es besteht ein hohes Risiko. Eine zusätzliche Maßnahme ist dringend erforderlich und mit hoher Priorität umzusetzen.

Das Ergebnis der Risikobewertung soll dokumentiert und dem Management als Bericht zur Verfügung gestellt werden.

2.3.4 Risikobehandlung

Auf der Grundlage der Risikobewertung erfolgt die Risikobehandlung. Risikobehandlung ist der Prozessschritt, der die Auswahl und Umsetzung von Maßnahmen zur Modifizierung des Risikos steuert. Dabei sind entsprechend der Höhe des ermittelten Risikograde die Prioritäten zu setzen. Grundsätzlich gilt: Das Risiko mit dem höchsten Risikograd hat die höchste Priorität in der Risikobehandlung. Folgende vier Optionen der Risikobehandlungen stehen grundsätzlich zur Verfügung:

a) Risikominderung

Die Behandlungsoption Risikominderung reduziert den Grad eines Risikos durch geeignete Maßnahmen. Maßgeblich sind dabei die Risikoklassen sowie weitere Anforderungen gesetzlicher, amtlicher oder vertraglicher Art. Maßnahmen müssen in einem wirtschaftlich vertretbaren Rahmen zu den ermittelten potenziellen Auswirkungen stehen. Ebenso sind bei den Maßnahmen der zeitliche Rahmen des Erfolgs sowie die benötigten personellen Ressourcen zu berücksichtigen.

b) Risikovermeidung

Die Risikovermeidung beseitigt alle Aktivitäten oder Bedingungen, die das betrachtete Risiko verursachen.

c) Risikoübertragung

Diese Behandlungsoption meint die Übertragung des Risikos auf Dritte. Hierbei ist sicherzustellen, dass der Auftragnehmer die entsprechende Fähigkeit und Kompetenz hat, das Risiko zu behandeln. Gegebenenfalls entstehen durch die Risikoübertragung neue Risiken. Diese sind einer erneuten Risikoeinschätzung und -bewertung zu unterziehen.

d) Risikobeibehaltung / Risikoakzeptanz

Anhand der priorisierten Risikograde (Risikoklassen) kann entschieden werden, ob das betrachtete Risiko akzeptiert wird.

Die anzuwendenden Maßnahmen zur Risikobehandlung sollen mit folgenden Merkmalen dokumentiert werden:

- Verantwortung für die Umsetzung (i.d.R. Werteverantwortlicher)
- Zeitliches und inhaltliches Ziel der Maßnahme
- Kosten der Maßnahme
- Metrik bzw. Indikator zur Messung des Erfolgs der Maßnahme
- Grad der Umsetzung

Das im Ergebnis der Risikobehandlung erwartete Restrisiko ist analog zu 2.3.2 und 2.3.3 einzuschätzen und zu bewerten sowie ggf. weiter zu behandeln.

2.3.5 Risikokommunikation

Der Prozess des Risikomanagements muss die Kommunikation von Risiken und ihre Behandlung zwischen Entscheidungsträgern und Interessengruppen gewährleisten. Entscheidungen im Rahmen des Risikomanagements sollen dokumentiert und mit den Fachverantwortlichen und Werteverantwortlichen kommuniziert werden. Ziele der Risikokommunikation sind u. a.:

- Sicherstellung, dass die Ergebnisse der Risikobewertung korrekt sind
- Vergewissern, dass die vorgeschlagene Risikobehandlung geeignet ist
- Zusammentragen von Informationen über Risiken
- Vermeidung von Sicherheitsvorfällen aufgrund mangelnder Kommunikation
- Sammeln neuer Erkenntnisse zur Informationssicherheit
- Verbesserung des Sicherheitsbewusstseins bei allen Beteiligten

2.3.6 Risikoüberwachung

Risiken und deren Attribute wie Auswirkung, Wahrscheinlichkeit, Bedrohung und Schwachstelle sind kontinuierlich zu überwachen und auf Veränderung zu prüfen. Dies gilt insbesondere auch für akzeptierte Risiken. Aspekte der Risikoüberwachung sind:

- Neue bzw. veränderte Werte
- Veränderung der Kritikalität von Werten
- Veränderte Bedrohungen und Schwachstellen
- Berücksichtigung von Informationssicherheitsvorfällen
- Veränderte Wahrscheinlichkeiten und Auswirkungen

Zudem ist die Überwachung des gesamten Risikomanagementprozesses erforderlich. Dies beinhaltet die regelmäßige Prüfung der definierten Kriterien im Risikomanagement.

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.
Informationssicherheit	Aufrechterhaltung der Vertraulichkeit, Integrität und Verfügbarkeit von Informationen; andere Eigenschaften wie Authentizität, Zurechenbarkeit und Verlässlichkeit können ebenfalls berücksichtigt werden.
Informationssicherheits-managementsystem (ISMS)	Teil des gesamten Managementsystems, der auf der Basis eines Geschäftsrisikoansatzes die Entwicklung, Implementierung, Durchführung, Überwachung, Überprüfung, Instandhaltung und Verbesserung der Informationssicherheit abdeckt.
Integrität	Eigenschaft der Absicherung von Richtigkeit und Vollständigkeit von Werten.
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.

Begriff	Erklärung
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.
Risiko	Möglichkeit, dass eine gegebene Bedrohung eine Schwachstelle eines Wertes oder eine Gruppe von Werten ausnutzt und dabei Schaden für die Organisation verursacht. Es wird als Kombination von Eintrittswahrscheinlichkeit und Auswirkung errechnet (Risikograd).
Risikomanagement	Gesamte Vorgehensweise des Identifizierens, Steuerns, Eliminierens oder Minderns unbestimmter Risiken, die Werte beeinträchtigen können.
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.
Verfügbarkeit	Eigenschaft von Werten, auf Verlangen zugänglich und nutzbar zu sein.
Vertraulichkeit	Eigenschaft, dass Informationen unberechtigten Personen, Einheiten oder Prozessen nicht verfügbar gemacht oder enthüllt werden.
Wert	Werte sind alle Informationen und Geschäftsprozesse (primäre Werte) sowie Hardware, Soft-ware, Netzwerk, Personal, Standorte und die Organisation (unterstützende Werte), die einen Schutzbedarf bezogen auf ihre Verfügbarkeit, Vertraulichkeit bzw. Integrität haben.
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_BCM]	Richtlinie Business Continuity Management

A N H A N G

A Mögliche Bewertung der Schutzbedarfe

A.1 Verfügbarkeit

Bewertung	Maßzahl	Erläuterung
Normal	1	Die Beeinträchtigung der Aufgabenerfüllung gefährdet nicht den gesamten Betrieb. Die tolerierbare Ausfallzeit ist größer als 24 Stunden und hat keinen oder nur begrenzten Schaden zur Folge.
Hoch	2	Hohe Verfügbarkeit über die normalen Geschäftszeiten muss gegeben sein. Kürzere Nichtverfügbarkeit (zwischen 1 bis 24 Stunden) ist tolerierbar und hat keinen oder nur geringen wirtschaftlichen Schaden zur Folge. Eine Ausfallzeit von mehr als 24 Stunden kann zu einem beträchtlichen Schaden führen.
Sehr hoch	3	Permanente Verfügbarkeit muss gegeben sein (24*7*365). Die maximal tolerierbare Ausfallzeit liegt bei einer Stunde. Schon durch eine Nichtverfügbarkeit von mehr als einer Stunde kann ein Schaden mit bedrohlichem Ausmaß entstehen.

A.2 Integrität

Bewertung	Maßzahl	Erläuterung
Normal	1	Die Verfälschung von Informationen und Daten hat keinen oder nur begrenzten Schaden zur Folge.
Hoch	2	Die Verfälschung von Informationen und Daten kann einen beträchtlichen Schaden zur Folge haben.
Sehr hoch	3	Die Verfälschung von Informationen und Daten kann einen Schaden mit existentiell bedrohlichem, katastrophalem Ausmaß zur Folge haben.

A.3 Vertraulichkeit

Bewertung	Maßzahl	Erläuterung
Normal	1	Betrifft Daten, Informationen und weitere Eigenschaften von Werten, deren Offenlegung zwar keinen oder nur begrenzten Schaden bedeuten würde, die aber dennoch nicht für die Öffentlichkeit bestimmt sind.
Hoch	2	Betrifft Daten, Informationen und weitere Eigenschaften von Werten, deren unbefugte Offenlegung einen beträchtlichen Schaden für die Interessen der Organisation und ihrer Mitarbeiter bedeuten würde.
Sehr hoch	3	Betrifft Daten, Informationen und weitere Eigenschaften von Werten, deren unbefugte Offenlegung einen Schaden mit existentiell bedrohlichem, katastrophalem Ausmaß für die Interessen der Organisation und ihrer Mitarbeiter bedeuten würde.

B Mögliche Einschätzung der Risiken

B.1 Wahrscheinlichkeit

Bewertung	Faktor	Erläuterung
Gering	1	Die Möglichkeit liegt in einem längeren Zeitraum (ca. ein Jahr und länger).
Mittel	2	Die Möglichkeit liegt in einem mittleren Zeitraum (ein Monat bis ein Jahr).
Hoch	3	Die Möglichkeit liegt in einem kurzen Zeitraum (kürzer als ein Monat).

B.2 Auswirkung

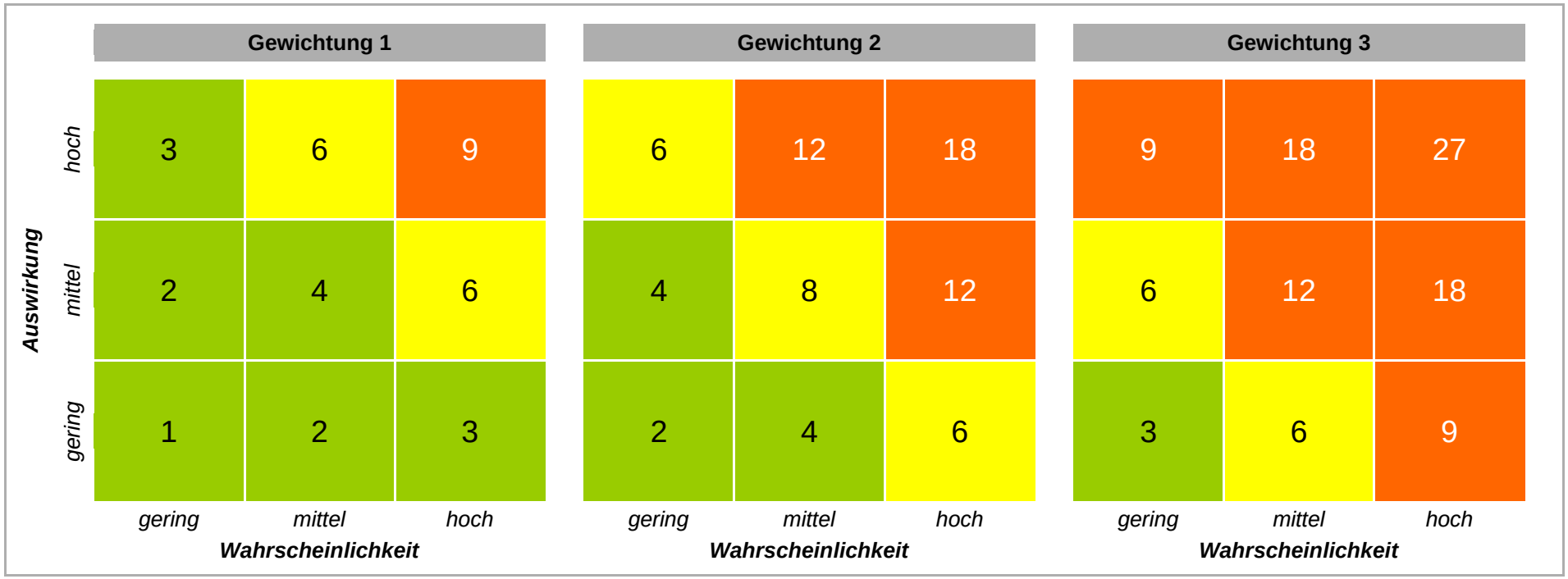
Bewertung	Faktor	Erläuterung
Gering	1	Das Schadenausmaß ist gering und tolerierbar (kleiner 5 T€).
Mittel	2	Das Schadensausmaß ist mittel bis hoch und nicht mehr tolerabel (zwischen 5 T€ und 50 T€).
Hoch	3	Das Schadensausmaß ist sehr hoch (größer 50 T€).

B.3 Gewichtung (Konsequenz)

Bewertung	Gewichtung	Erläuterung
Normal	1	Durch das Zusammentreffen von Bedrohung und Schwachstelle ist ein Schutzziel der Kategorie „Normal“ eines Wertes betroffen.
Hoch	2	Durch das Zusammentreffen von Bedrohung und Schwachstelle ist ein Schutzziel der Kategorie „Hoch“ eines Wertes betroffen.
Sehr hoch	3	Durch das Zusammentreffen von Bedrohung und Schwachstelle ist ein Schutzziel der Kategorie „Sehr hoch“ eines Wertes betroffen.

C Mögliche Bewertung der Risiken

C.1 Risikomatrizen



C.2 Risikoklassen

Bewertung	Risikograd	Erläuterung
Risikoklasse 1	1 - 4	Das Risikoniveau ist gering und akzeptabel. Eine zusätzliche Maßnahme ist nicht zwingend erforderlich.
Risikoklasse 2	5 - 8	Es besteht ein mittleres Risiko. Eine zusätzliche Maßnahme ist erforderlich und umzusetzen.
Risikoklasse 3	9 - 27	Es besteht ein hohes Risiko. Eine zusätzliche Maßnahme ist dringend erforderlich und mit hoher Priorität umzusetzen.