Sicherheitstechnische Kurzbetrachtung –
eine praktische Anwendung zur Nutzung der SdT-Biliotek

Vorbereitungsprozess zur Auswahl der geeigneten Sicherheitsbetrachtung

Ausgangspunkt des Prozesses ist die Ermittlung und Beschreibung des Geschäftsprozesses. Zunächst wird festgelegt, worum es fachlich geht, welches Ziel mit dem Geschäftsprozess verfolgt wird und welches Ergebnis erreicht werden soll. Die Beschreibung soll so verständlich sein, dass auch Personen außerhalb des unmittelbar zuständigen Fachbereichs nachvollziehen können, welche Aufgabe erfüllt wird und welche Bedeutung der Prozess für die Organisation hat. Gleichzeitig werden die für den Geschäftsprozess zuständigen Stellen frühzeitig eingebunden. Hierzu können insbesondere Informationssicherheit, Datenschutz, Geheimschutz, Notfallmanagement und Geschäftsprozessmanagement gehören.

Im nächsten Schritt wird der „Betrachtungsgegenstand“ festgelegt. Dabei ist zu beantworten, welche technischen, organisatorischen und infrastrukturellen Bestandteile erforderlich sind, damit der Geschäftsprozess funktioniert. Dazu gehören beispielsweise Anwendungen, IT-Systeme, Netzkomponenten, Informationen, Räume, externe Dienste und weitere Abhängigkeiten. Ziel ist es, ein gemeinsames Verständnis darüber herzustellen, was tatsächlich betrachtet werden soll.

Ebenso wichtig ist die Abgrenzung zu nicht betrachteten Teilprozessen und Zielobjekten. Es wird dokumentiert, welche Bereiche bewusst außerhalb der Betrachtung liegen und welche Sachverhalte gegebenenfalls noch unbekannt sind. Damit wird verhindert, dass unklare oder nicht betrachtete Abhängigkeiten später unbemerkt Einfluss auf die Bewertung nehmen. Anschließend werden die für den Geschäftsprozess erforderlichen Zielobjekte systematisch erfasst. Es wird beschrieben, welche Geräte, Systeme, Software, Informationen, organisatorischen Einheiten oder Dienstleistungen genutzt werden und in welcher Beziehung sie zum Geschäftsprozess stehen.

Danach wird der Schutzbedarf (normal oder hoch) des gesamten Geschäftsprozesses betrachtet. Es ist zu bewerten, welche Auswirkungen eine Beeinträchtigung der Vertraulichkeit, Integrität oder Verfügbarkeit (ggf. auch Authentizität) auf den Geschäftsprozess haben könnte.

Auf Grundlage der Analyse werden anschließend logische und technische Netzpläne erstellt oder vorhandene Dokumentationen aktualisiert. Die Netzpläne sollen die wesentlichen Verbindungen und Abhängigkeiten nachvollziehbar darstellen. Gleichzeitig werden erneut diejenigen Zielobjekte und Teilbereiche dokumentiert, die nicht Bestandteil der weiteren Betrachtung sind.

Um ein besseres Verständnis über die bereits getätigten administrativen und organisatorischen Maßnahmen zu erhalten, ist eine Betriebsdokumentation erforderlich. Die Betreibdokumentation der ein ähnliches Dokument zeigt bereits erste Schwachstellen auf und erleichtert im weiteren Verlauf sog. „Quick-Wins“ zu ermitteln.

Am Ende der vorbereitenden Schritte steht eine Variantenentscheidung. Auf Basis des Geschäftsprozesses, des ermittelten Schutzbedarfs, der Anzahl und Komplexität der Zielobjekte, der vorhandenen Abhängigkeiten sowie der erkennbaren Risiken wird entschieden, welche Form der weiteren Sicherheitsbetrachtung angemessen ist.

Für überschaubare, klar abgegrenzte Geschäftsprozesse kann eine sicherheitstechnische Kurzbetrachtung gewählt werden. Sie dient als schnelle Methode, um anhand relevanter Gefährdungen, der betroffenen Schutzziele und der konkreten Zielobjekte die wesentlichen Risiken zu erkennen und geeignete Maßnahmen abzuleiten.

Ist der Geschäftsprozess dagegen komplexer, weist er zahlreiche technische oder organisatorische Abhängigkeiten auf oder ist eine umfassendere und nachvollziehbare Bewertung erforderlich, wird ein ausführliches Sicherheitskonzept erstellt. Dieses betrachtet die relevanten Anforderungen des Stand-der-Technik-Viewers umfassender und ermöglicht eine deutlich tiefere Bewertung und Dokumentation der Sicherheitsanforderungen.

Der vorbereitende Prozess endet somit mit einer begründeten Entscheidung:

- Kurzbetrachtung, wenn eine schnelle, risikoorientierte Bewertung für einen überschaubaren Geschäftsprozess ausreichend ist, oder
- ausführliches Sicherheitskonzept, wenn Umfang, Komplexität oder Schutzbedarf eine vertiefte Betrachtung erforderlich machen.

Risikoeinschätzung innerhalb der Sicherheitstechnischen Kurzbetrachtung

Die eigentliche Risikoeinschätzung beginnt nach der Festlegung des Betrachtungsgegenstands und der relevanten Zielobjekte. Ziel dieses Prozessabschnitts ist es, die für den Geschäftsprozess relevanten Gefährdungen systematisch zu erkennen, deren mögliche Auswirkungen zu bewerten und daraus einen angemessenen Umgang mit den identifizierten Risiken abzuleiten.

Zu Beginn wird der G0-Gefährdungskatalog des BSI geprüft. Maßgeblich ist nicht allein, ob eine Gefährdung theoretisch auftreten kann, sondern ob sie sich auf den betrachteten Geschäftsprozess tatsächlich negativ auswirken könnte. Für jede relevante Gefährdung wird deshalb geprüft, welches Schutzziel betroffen ist und welche Folgen sich für den Geschäftsprozess ergeben können. Neben den im Katalog enthaltenen Gefährdungen sind auch weitere, projektspezifische oder bisher nicht betrachtete Gefährdungen zu berücksichtigen. Werden solche Gefährdungen erkannt, werden sie ergänzend in die Betrachtung aufgenommen.

Wird festgestellt, dass eine Gefährdung für ein Zielobjekt tatsächlich wirksam werden kann, beginnt die konkrete Risikobewertung. Hierzu wird zunächst die Häufigkeit des Eintritts oder die Eintrittswahrscheinlichkeit eingeschätzt. Danach wird das mögliche Schadensausmaß bewertet. Entscheidend ist dabei die Auswirkung auf den gesamten Geschäftsprozess und nicht ausschließlich auf das einzelne technische Zielobjekt. Aus Eintrittswahrscheinlichkeit und Schadensausmaß wird anhand der festgelegten Risikomatrix das Risikoniveau bestimmt.

Das Ergebnis der Bewertung kann beispielsweise ein geringes, hohes oder sehr hohes Risiko sein. Ein geringes Risiko wird dokumentiert und kann grundsätzlich weiter beobachtet werden. Bei einem hohen oder sehr hohen Risiko wird dagegen ein Vorschlag zur Risikominimierung erarbeitet. Dieser beschreibt, mit welchen zusätzlichen technischen, organisatorischen oder personellen Maßnahmen das Risiko reduziert werden kann. Bei sehr hohen Risiken besteht ein entsprechend dringlicher Handlungsbedarf.

Auswahl und Zuordnung von Anforderungen im Stand-der-Technik-Viewer

Nach Abschluss der Gefährdungs- und Risikobewertung werden die für die Risikobehandlung geeigneten Anforderungen aus der BSI Stand-der-Technik-Bibliothek ausgewählt. Die Auswahl erfolgt für jedes relevante Zielobjekt einzeln. Ziel ist es, nachvollziehbar zu machen, welches Zielobjekt, welche Gefährdung und welches Schutzziel durch eine Anforderung adressiert werden. Als Arbeitswerkzeug wird der Stand-der-Technik-Viewer verwendet.
https://bsi-community.github.io/Stand-der-Technik-Viewer/
Die zugrunde liegenden maschinenlesbaren Inhalte werden in der öffentlichen BSI Stand-der-Technik-Bibliothek auf GitHub bereitgestellt.
https://github.com/BSI-Bund/Stand-der-Technik-Bibliothek

Der Viewer sollte möglichst in seiner aktuellen Online-Version genutzt werden. Für die Nachvollziehbarkeit sollten Bearbeitungsdatum, verwendeter Katalogstand und wesentliche Filter dokumentiert werden.

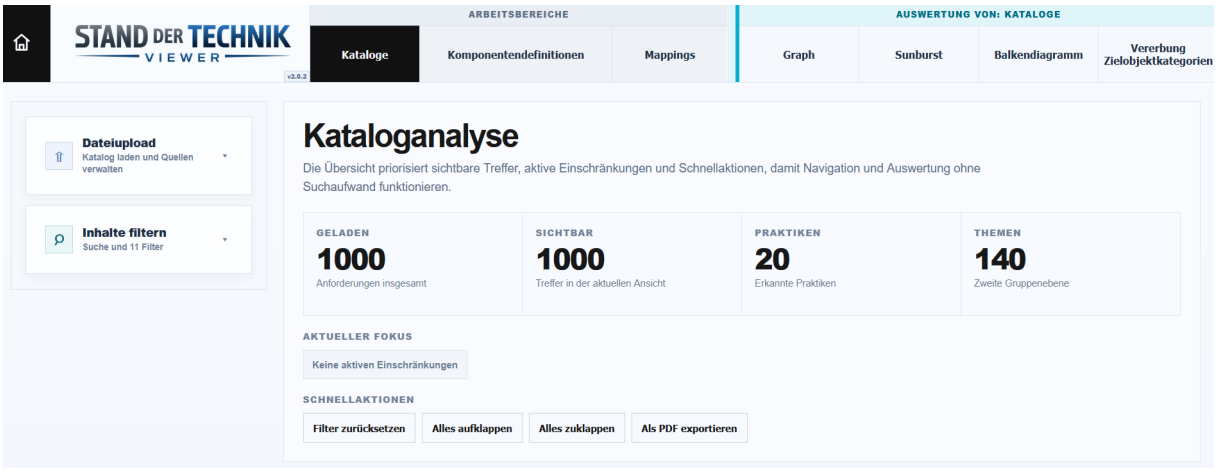

Abbildung 1 der Stand der Technik Viewer des BSI mit dem geladenen GS++- Katalog (Stand 14.08.2026)

Zielobjekt und Zielobjektkategorie bestimmen

Zu Beginn wird für jedes betrachtete Zielobjekt geprüft, welcher Zielobjektkategorie es fachlich zugeordnet werden kann. Zielobjekte können beispielsweise Anwendungen, IT-Systeme, Netze, Räume, Informationen oder externe Dienstleistungen sein. Die Zuordnung sollte nicht allein anhand des Namens erfolgen, sondern anhand der in der Bibliothek hinterlegten Definitionen. Für jedes Zielobjekt wird möglichst die spezifischste passende Kategorie ausgewählt. Im Viewer wird anschließend im Bereich „Inhalte filtern“ die passende Zielobjektkategorie aktiviert.

Vererbung berücksichtigen

Bei der Auswahl der Zielobjektkategorie ist die Vererbungshierarchie zu beachten. Eine spezifische Kategorie kann Anforderungen übergeordneter Kategorien übernehmen. Deshalb wird nicht nur die unmittelbar ausgewählte Kategorie betrachtet, sondern auch geprüft, welche darüberliegenden Kategorien fachlich relevant sind.

Der SdT-Viewer bietet automatisiert die Funktion der Vererbung und stellt alle vererbten Zielobjektkategorien übersichtlich dar.

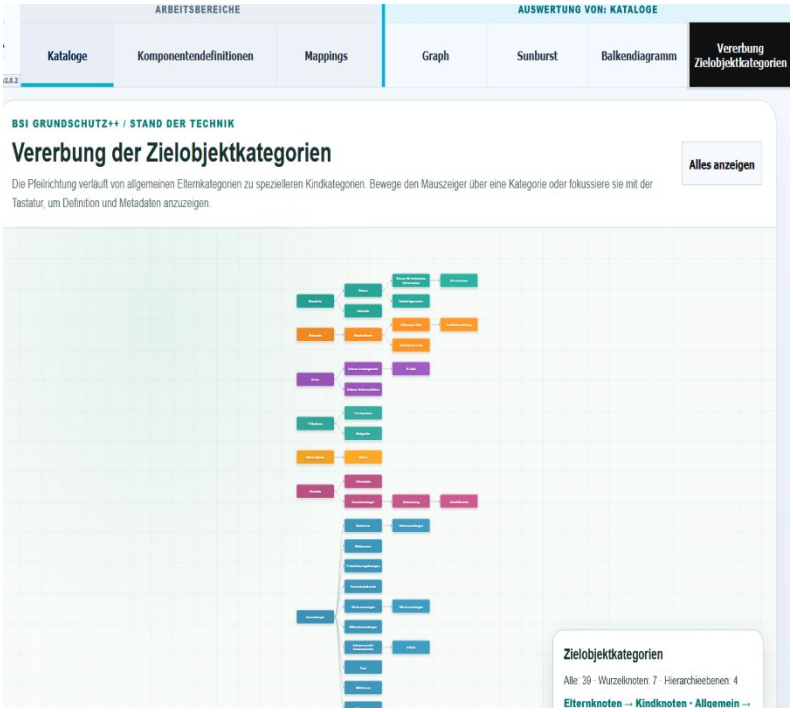

Abbildung 2 Zielobjektbaum

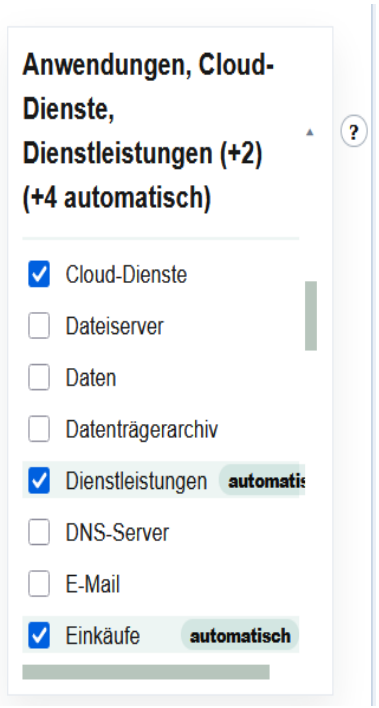

Abbildung 3
Vererbung des Zielobjektes Cloud-Dienste

Gefährdungen im Viewer eingrenzen

Nach der Auswahl der Zielobjektkategorien werden die zuvor ermittelten Gefährdungen in die Anforderungsauswahl einbezogen. Hierzu wird die Volltextsuche „Suche im Katalog“ verwendet. Gesucht werden kann insbesondere nach:

- der Nummer oder Bezeichnung einer G0-Gefährdung,
- einem relevanten technischen Begriff,
- dem betroffenen Zielobjekt.

Sind mehrere Gefährdungen für ein Zielobjekt relevant, können diese nacheinander oder mit der Mehrfachsuche betrachtet werden. Die Gefährdungssuche dient dazu, die grundsätzlich anwendbaren Anforderungen stärker auf die bereits festgestellten Risiken des Geschäftsprozesses einzugrenzen.

Schutzziele berücksichtigen

Zusätzlich werden die im Risikoszenario betroffenen Schutzziele berücksichtigt.

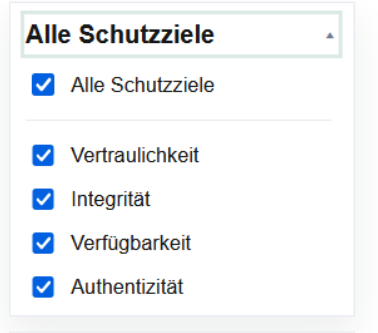

Abbildung 4 Schutzziele ggf. incl. Authentizität

Besondere Aufmerksamkeit erhält das Schutzziel, bei dem die größte Auswirkung auf den Geschäftsprozess festgestellt wurde.

Anforderungen fachlich prüfen

Die im Viewer angezeigten Anforderungen werden nicht automatisch übernommen. Jede Anforderung wird darauf geprüft, ob sie tatsächlich zum betrachteten Zielobjekt und zur Reduzierung des identifizierten Risikos passt.
Dabei sind insbesondere folgende Fragen zu beantworten:

- Passt die Anforderung zum Zielobjekt?
- Behandelt sie eine der ermittelten Gefährdungen?
- Unterstützt sie das betroffene Schutzziel?
- Ist sie für die konkrete technische oder organisatorische Ausprägung anwendbar?
- Ist die Anforderung bereits umgesetzt?
- Kann ihre Umsetzung das festgestellte Risiko tatsächlich reduzieren?

Der Viewer unterstützt somit die Recherche und Zuordnung. Die fachliche Bewertung bleibt Aufgabe der verantwortlichen Bearbeiter und beteiligten Fachstellen.

Umsetzungsstatus dokumentieren

Für jede ausgewählte Anforderung wird anschließend der Umsetzungsstatus festgestellt. Es werden drei Zustände verwendet:

- erfüllt
- nicht erfüllt
- nicht anwendbar

Erfüllte Anforderungen sollten möglichst durch einen geeigneten Nachweis belegt werden. Dies können beispielsweise Konfigurationen, technische Prüfungen, Netzpläne, Betriebsdokumentationen oder organisatorische Vorgaben sein.Eine Einstufung als „nicht anwendbar“ ist kurz zu begründen.

Anforderungen den Risiken zuordnen

Die ausgewählten Anforderungen werden anschließend den identifizierten Risiken zugeordnet.

Abbildung 5Rückverfolgbarkeit der Anforderung Auswahl

Dadurch bleibt nachvollziehbar, warum eine bestimmte Anforderung Bestandteil der Sicherheitsbetrachtung geworden ist. Eine Anforderung kann mehrere Risiken reduzieren. Ebenso können für ein einzelnes Risiko mehrere Anforderungen erforderlich sein.

Anforderungen priorisieren

Abschließend werden die offenen Anforderungen nach Risiko, Wirksamkeit und Aufwand priorisiert.
Dabei sollten insbesondere folgende Fragen berücksichtigt werden:

1. Welches Risiko wird reduziert?
2. Wie hoch ist das aktuelle Risiko?
3. Wie groß ist die erwartete Risikoreduktion?
4. Wie schnell kann die Anforderung umgesetzt werden?
5. Welcher personelle, technische oder finanzielle Aufwand entsteht?
6. Wirkt die Anforderung gleichzeitig auf mehrere Risiken?

Anforderungen mit hoher Sicherheitswirkung und geringem Umsetzungsaufwand eignen sich besonders als Quick Wins und sollten bevorzugt umgesetzt werden.

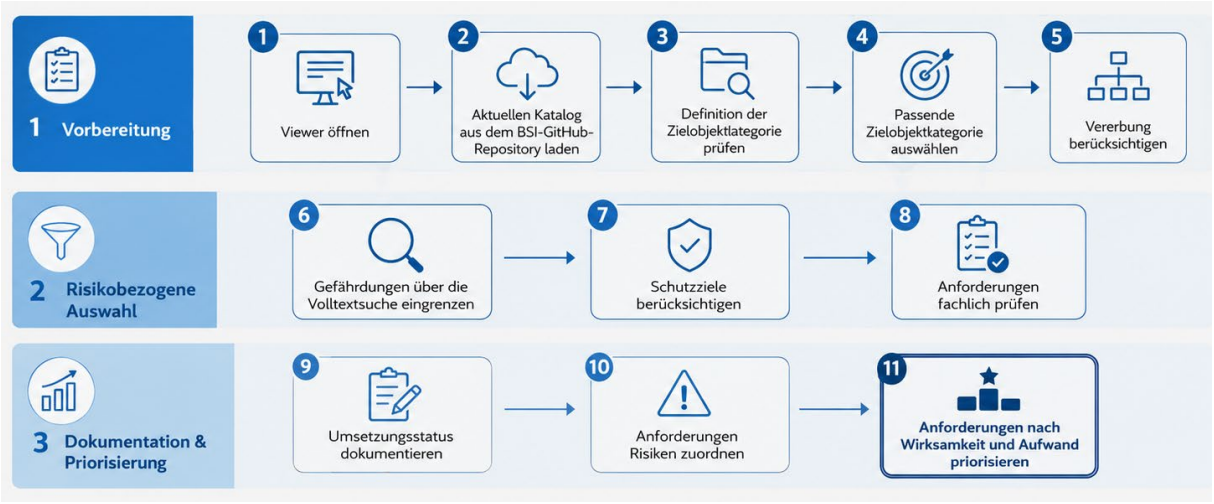

Abbildung 6 Zusammenfassender Überblick über den Kompakter Viewer-Ablauf

Managemententscheidung zum Abschluss der Sicherheitstechnischen Kurzbetrachtung

Ziel ist es, die Ergebnisse der Risikobewertung in eine kurze, nachvollziehbare Entscheidungsvorlage für die Organisationsleitung zu überführen, die Entscheidung zu dokumentieren und die daraus entstehenden Verpflichtungen verbindlich nachzuhalten.

Entscheidungsvorlage erstellen

Nach Abschluss der Gefährdungsanalyse, der Risikobewertung und der Auswahl geeigneter Anforderungen wird eine kompakte Entscheidungsvorlage erstellt. Sie enthält keine vollständige Wiederholung der technischen Detailanalyse, sondern konzentriert sich auf die für die Leitung entscheidungsrelevanten Punkte.

Die Vorlage sollte mindestens darstellen:

- welcher Geschäftsprozess beziehungsweise Scope betrachtet wurde,
- welche wesentlichen Risiken bestehen,
- welche Anforderungen bereits umgesetzt sind,
- welche Quick Wins bereits realisiert wurden,
- welche Anforderungen noch offen sind,
- welche Restrisiken verbleiben,
- welche weiteren Maßnahmen erforderlich sind,
- wer für deren Umsetzung verantwortlich ist und
- bis wann eine Umsetzung beziehungsweise Wiedervorlage erfolgen soll.

Das Muster der SiKu sieht ausdrücklich eine „Entscheidung der Organisationsleitung“ vor. Dabei werden drei grundsätzliche Entscheidungsmöglichkeiten unterschieden:

- sehr hohe Risiken führen grundsätzlich dazu, dass der Geschäftsprozess nicht in den Wirkbetrieb überführt und die Restrisiken nicht übernommen werden; Die Organisationsleitung kann den Geschäftsprozess damit außer Kraft setzen oder sie ordnet Maßnahmen zur Risikoreduzierung an. Hierzu sollen idealer Weise bereits Vorschläge erarbeitet worden sein, die der Organisationsleitung die Entscheidung erleichtert
- bei hohen Risiken kann ein Wirkbetrieb unter der Bedingung weiterer Risikoreduzierung erfolgen;
- bei geringen Risiken kann der Geschäftsprozess in den Wirkbetrieb überführt und das verbleibende Restrisiko übernommen werden.

Sachliche Einschätzung dokumentieren

Die Entscheidungsvorlage muss eine kurze fachliche Einschätzung enthalten. Diese soll der Organisationsleitung ermöglichen, die Tragweite der Entscheidung zu verstehen, ohne sämtliche technischen Einzelheiten der SiKu erneut nachvollziehen zu müssen.

Die fachliche Einschätzung beantwortet insbesondere folgende Fragen:

- Ist der Geschäftsprozess aus Sicht der Informationssicherheit grundsätzlich betreibbar?
  Hierbei werden die bereits umgesetzten Anforderungen und vorhandenen Sicherheitsvorkehrungen berücksichtigt.
- Welche wesentlichen Restrisiken verbleiben?
  Nicht jedes erkannte Risiko muss vollständig beseitigt werden. Entscheidend ist, dass die verbleibenden Risiken transparent dargestellt und einer bewussten Entscheidung zugeführt werden.
- Welche offenen Anforderungen sind für die Entscheidung besonders relevant?
  Anforderungen mit hoher Risikoreduktion oder unmittelbarer Bedeutung für die Betriebsfähigkeit sollten deutlich hervorgehoben werden.
- Welche Konsequenz hat eine Nichtumsetzung?
  Bei wesentlichen offenen Anforderungen sollte beschrieben werden, welches Risiko fortbesteht, wenn die Umsetzung unterbleibt.

Das SiKu-Muster sieht hierzu vor, bereits umgesetzte Sicherheitsvorgaben sowie die daraus verbleibenden Restrisiken gesondert zu dokumentieren.

Entscheidung der Organisationsleitung

Auf Grundlage der fachlichen Einschätzung trifft die Organisationsleitung eine dokumentierte Entscheidung. Dabei sind grundsätzlich drei Varianten möglich:

Freigabe:
Der Geschäftsprozess kann betrieben werden. Die verbleibenden Risiken werden akzeptiert.

Freigabe unter Auflagen:
Der Geschäftsprozess kann betrieben werden, jedoch müssen bestimmte offene Anforderungen innerhalb verbindlicher Fristen umgesetzt werden. Für diese Anforderungen werden Verantwortlichkeiten, Termine und gegebenenfalls Zwischenstände festgelegt.

Keine Freigabe:
Das vorhandene Risiko ist nicht vertretbar. Der Geschäftsprozess darf in der vorgesehenen Form nicht in den Wirkbetrieb überführt beziehungsweise nicht fortgeführt werden, bis eine ausreichende Risikoreduktion erreicht wurde.

Insbesondere bei einer Freigabe unter Auflagen sind die konkreten Anforderungen, die zuständige Stelle sowie Termine für die Vorlage der Umsetzung eindeutig zu benennen. Genau diese Elemente sind im Muster für die Leitungsentscheidung vorgesehen.

Entscheidung archivieren und Risikodokumentation aktualisieren

Nach der Entscheidung wird die schriftliche Freigabe beziehungsweise Ablehnung revisionssicher abgelegt. Dadurch bleibt nachvollziehbar, auf welcher Informationsgrundlage die Organisationsleitung entschieden hat und welche Restrisiken bewusst übernommen wurden.

Im Anschluss werden die Ergebnisse in die vorhandene Risikodokumentation übernommen. Der Risikokatalog muss insbesondere erkennen lassen,

- welches Risiko akzeptiert wurde,
- welches Risiko weiter reduziert werden muss,
- welche Anforderungen dazu umzusetzen sind,
- welche Fristen gelten und
- wer die Verantwortung trägt.

Damit wird verhindert, dass die Managemententscheidung vom operativen Risikomanagement getrennt bleibt.

Revisions- und Wiedervorlageplanung

Offene Anforderungen und akzeptierte Restrisiken müssen in die weitere Überwachung aufgenommen werden. Deshalb wird abschließend ein Revisions- beziehungsweise Wiedervorlageplan ergänzt.

Eine erneute Betrachtung ist insbesondere erforderlich, wenn

- vereinbarte Anforderungen nicht fristgerecht umgesetzt werden,
- sich der Geschäftsprozess oder der Scope wesentlich verändert,
- neue Zielobjekte oder Schnittstellen hinzukommen,
- neue Gefährdungen oder Schwachstellen bekannt werden,
- ein sicherheitsrelevanter Vorfall eintritt oder
- sich die Rahmenbedingungen der ursprünglichen Risikobewertung wesentlich ändern.

Mit der dokumentierten Managemententscheidung, der Aktualisierung des Risikokatalogs und der Festlegung der Wiedervorlage ist die Sicherheitstechnische Kurzbetrachtung formal abgeschlossen.

Kernaussage für die Organisationsleitung:
Die SiKu endet nicht mit einer technischen Bewertung, sondern mit einer bewussten Entscheidung darüber, welche Risiken akzeptiert werden, welche Anforderungen noch umzusetzen sind und unter welchen Bedingungen der Geschäftsprozess betrieben werden darf.

Als Beispiel der Anwendung wurde eine Videoüberwachungsanlage im öffentlichen Raum betrachtet. Des Weiteren befinden sich unausgefüllte Muster zur Bewertung der Gefährdungslage und für eine SiKu als Entscheidungsvorlage für die Leitung als Anlage.

Anlage sind folgende Datein:

- SiKu_Beispiel_Vido_ÜA
- Netzplan_Vidio_ÜA
- Beispiel_Gefähdungen_Vidio_ÜA
- Muster_SiKu
- Muster_Gefährungen