WHITEPAPER

Informationswerte & Schutzbedarf

Schutz beginnt beim Wert

Carsten Beck
Cybersecurity Auditor | ISO/IEC 27001, ISO 22301 & ISO/IEC 42001 Lead Auditor
MAS Information Systems Management
November 2026 · Version 1.0

Executive Briefing

Viele Organisationen kennen ihre Systeme, aber nicht den Wert ihrer Informationen. Welche Informationen wirklich kritisch sind, wer für sie verantwortlich ist und wo sie überall liegen, wissen sie oft nicht. Ohne dieses Wissen schützen sie nach Gewohnheit, nach Budget oder nach dem, was ein Projekt gerade verlangt.

Das Ergebnis ist ein Fehlschutz in zwei Richtungen. Teils wird der Schutzbedarf zu hoch eingestuft und aufwendig umgesetzt, etwa mit einer Hochverfügbarkeit für eine Anwendung, auf deren Informationen der Betrieb tagelang verzichten könnte. Gleichzeitig bleiben Informationen mit hohem Wert ungeschützt, bis hin zu Geschäftsgeheimnissen, die offen im Internet zu finden sind. Beides hat oft dieselbe Ursache. Niemand hat bewusst bestimmt, was die Informationen wert sind und wie stark Leistungen von ihnen abhängen.

Selbst wo der Wert bekannt ist, bleibt ein zweites Problem. Business-Impact-Analyse, Prozessanforderungen, Klassifizierung, Datenschutz, Verträge und die Schutzbedarfsanalysen einzelner Anwendungen stellen Anforderungen an dieselben Schutzobjekte, also an Anwendungen, Plattformen und Dienstleister. Jede dieser Analysen kann für sich plausibel sein, zusammen können sie trotzdem ein falsches Bild ergeben. Dieses Whitepaper führt deshalb zwei Blickrichtungen zusammen, Top-down von der Geschäftsleistung und Bottom-up vom Wert der Information. Wo sie sich am Schutzobjekt treffen, entsteht ein Schutzbedarfsprofil je Schutzziel, also für Vertraulichkeit, Integrität, Verfügbarkeit und Nachvollziehbarkeit.

Eine Organisation, die den Wert ihrer Informationen nicht kennt, kann ihren Schutzbedarf nicht vollständig begründen. Belastbar wird der Schutzbedarf erst, wenn Informationswert und Bedeutung der Leistungen am Schutzobjekt zu einem Profil zusammengeführt werden. Wirksam wird er erst, wenn daraus Sicherheitsanforderungen folgen, deren Erfüllung nachgewiesen ist oder deren Abweichung bewusst entschieden wurde. Eine Schutzlücke darf nicht verdeckt werden, indem man die Einstufung dem Istzustand anpasst. Sie verlangt einen Entscheid der zuständigen Ebene.

Den Wert zu bestimmen, beginnt nicht mit einem vollständigen Inventar, sondern mit den kritischsten Informationsbeständen. Für jeden wird ein Informationseigner benannt und geprüft, wo die Informationen tatsächlich liegen, auch bei Dienstleistern, und ob etwas davon öffentlich zugänglich ist.

Dieses Papier richtet sich an Leitungs- und Aufsichtsgremien sowie Verantwortliche in Fachbereichen, Informationssicherheit, Datenschutz, IT, Business Continuity Management und Audit. Viele Abschnitte enthalten einen Prüfnachweis, Kapitel 10 schliesst mit Leitfragen.

1 Ausgangslage: Der Wert ist oft unbekannt

Informationssicherheit beginnt nicht bei einer Massnahme, sondern bei der Frage, was für eine Organisation von Wert ist. In vielen Organisationen wird diese Frage nie ausdrücklich gestellt. Geschützt werden Systeme, Netze und Arbeitsplätze, meist einheitlich und ohne zu unterscheiden, welche Informationen besonders schutzwürdig sind. Dieses Papier vertieft damit eine Querschnittsfrage der Informationssicherheit, die in Projekten, im Betrieb und in Audits gleichermassen auftaucht, nämlich den Wert von Informationen und ihren Schutzbedarf. Es greift zugleich das Prüffeld «Informationswerte & Schutzbedarf» aus dem Beitrag «Typische Audit-Prüffelder» dieser Reihe auf und knüpft an den Beitrag zum Business Continuity Management an, der den fehlenden Zusammenführungspunkt zwischen Business-Impact-Analyse und Schutzbedarfsanalyse als Bruchstelle beschreibt.

Informationssicherheit umfasst viele Handlungsfelder, von der Steuerung über technische Massnahmen bis zu den Schnittstellen zu Datenschutz, Recht und Business Continuity Management (Abbildung 1). Quer durch diese Felder stellt sich dieselbe Frage. Was ist zu schützen, wie stark und mit welchem Nachweis?

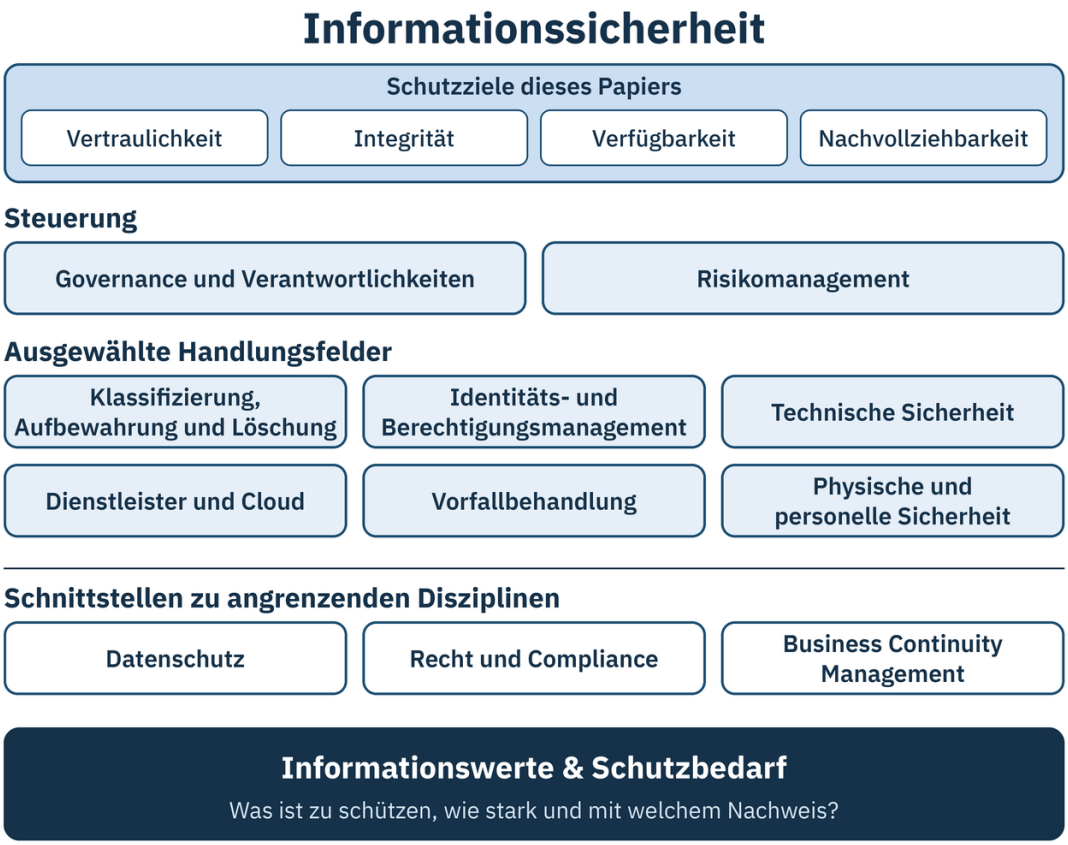


Abbildung 1: Informationswerte und Schutzbedarf als Querschnitt ausgewählter Handlungsfelder und Schnittstellen (eigene Darstellung)

1.1 Warum der Wert unbekannt bleibt

Die Ursachen sind selten Nachlässigkeit. Sie liegen in der Art, wie Informationen entstehen, wie Organisationen ihre IT verwalten und wann sie die Frage überhaupt stellen.

- **Informationen entstehen nebenbei.** Selten wird ausdrücklich entschieden, dass ein Geschäftsgeheimnis oder besonders schützenswerte Personendaten entstehen. Sie entstehen in einer Kalkulation, einem Arztbericht oder einer Fallnotiz zu einem Gesuch und liegen oft verteilt über viele Ablagen.

- **Inventare listen Systeme, nicht Informationen.** Das zentrale Verzeichnis der IT-Komponenten, oft eine Configuration-Management-Datenbank (CMDB), kennt Server, Anwendungen und Lizenzen. Welche Informationen darin liegen und was sie wert sind, steht dort meist nicht.
- **Der Informationseigner (Data Owner) fehlt.** Gemeint ist die Person, die für eine Information verantwortlich ist. Die IT betreibt, der Fachbereich nutzt, aber niemand ist benannt, der den Wert beurteilt und dafür einsteht.
- **Schutzbedarf wird vom System her ermittelt.** Jedes Projekt bewertet «seine» Anwendung. Informationen, die über mehrere Anwendungen verteilt sind, beurteilt niemand als Ganzes.
- **Es fehlt der Anlass.** Solange nichts passiert, stellt niemand die Frage nach dem Wert. Nach einem Vorfall kommt die Antwort zu spät.

Aufsicht und Vorfälle zeigen dieses Muster. Die Eidgenössische Finanzmarktaufsicht (FINMA) stellte 2024 fest, dass viele Institute nicht klar definiert hatten, was für sie kritische Daten sind (Aufsichtsmitteilung 03/2024). Beim Cyberangriff auf den IT-Dienstleister Xplain im Jahr 2023 lagen dort umfangreiche, teils sensible Daten mehrerer Bundesstellen und kantonaler Behörden, deren Umfang und Sensitivität nicht ausreichend bekannt waren. Beide Beispiele zeigen, wie wichtig Werttransparenz ist, also das Wissen, welche Informationen welchen Wert haben, wer für sie verantwortlich ist und wo sie liegen. Wo sie fehlt, lassen sich angemessene Schutzanforderungen kaum ableiten und weitergeben, schon gar nicht bis zum Dienstleister.

1.2 Fehlschutz in zwei Richtungen

Wenn der Wert der Informationen nicht bekannt ist, kann der Schutz zu gering oder unnötig hoch ausfallen. Abbildung 2 zeigt die vier möglichen Lagen.



Abbildung 2: Fehlschutz in zwei Richtungen, wenn der Wert unbekannt ist (eigene Darstellung)

Überschutz entsteht, wenn Anforderungen ohne fachliche Begründung zu hoch angesetzt werden. Typisch ist die Verfügbarkeit. Wer nicht weiss, wie lange ein Prozess ohne bestimmte Informationen auskommt, verlangt im Zweifel Hochverfügbarkeit, Pikettdienst und teure Service Levels. Ein anderes Beispiel ist eine aufwendige Verschlüsselung mit eigenem Schlüsselmanagement für Daten, die bereits öffentlich sind.

Dieser Schutz wird umgesetzt, betrieben und bezahlt, obwohl der geschützte Wert den Aufwand nicht rechtfertigt. Überschutz ist kein harmloser Sicherheitsüberschuss. Er bindet Mittel, die anderswo fehlen, und er untergräbt die Glaubwürdigkeit von Anforderungen.

Dass Schutz in einem vertretbaren Verhältnis zum Aufwand stehen muss, ist für die Bundesverwaltung ausdrücklich geregelt. Das Bundesgesetz über die Informationssicherheit beim Bund (Informationssicherheitsgesetz, ISG) gilt für die Bundesbehörden und, soweit sie Informationen oder Informatikmittel des Bundes bearbeiten, auch für weitere Stellen. Die verpflichteten Behörden und Organisationen haben bei der Informationssicherheit den Grundsätzen der Zweckmässigkeit, der Wirtschaftlichkeit und der Benutzerfreundlichkeit Rechnung zu tragen (Art. 6 Abs. 4 ISG). Der Gedanke gilt nicht nur für den Bund. Auch das Datenschutzgesetz verlangt eine dem Risiko angemessene Datensicherheit (Art. 8 DSG), und gängige Standards wie ISO/IEC 27001 und 27005 oder der BSI-Standard 200-2 richten die Massnahmen am Risiko aus.

Unterschutz entsteht, wenn Informationen mit hohem Wert nicht als solche erkannt werden. Sie werden dann wie gewöhnliche Informationen behandelt, manchmal sogar nachlässiger. In der Praxis finden sich Geschäftsgeheimnisse in Präsentationen, die auf der eigenen Website zum Download stehen, Kalkulationen oder Falldossiers in öffentlich geteilten Freigabelinks, interne Angaben in den Metadaten veröffentlichter Dokumente, unvollständig geschwärzte Dokumente oder Zugangsdaten in öffentlichen Code-Repositories. Niemand hat entschieden, diese Informationen zu veröffentlichen. Oft hat schlicht niemand gewusst, dass sie schutzwürdig sind.

> **Was ein falsch eingeschätzter Wert bewirken kann**
>
> **Integrität:** Sind in der Patientenakte Allergie- oder Medikationsangaben falsch, wird die Person auf dieser Grundlage falsch behandelt. Wurde die Integrität dieser Daten nur als «normal» eingestuft, können zusätzliche Plausibilisierungen und Vier-Augen-Freigaben fehlen. Hier geht es nicht um Daten, sondern um Patientensicherheit.
>
> **Vertraulichkeit:** Eine Kalkulation für eine öffentliche Ausschreibung liegt auf einer Kollaborationsplattform, auf die auch externe Partner Zugriff haben. Gelangt sie zu einem Mitbewerber, kann nicht nur der Auftrag verloren sein, sondern auch der oft erhebliche Aufwand für die Offerte, ohne dass ein System kompromittiert wurde.
>
> **Verfügbarkeit:** Die Alarmierungsdaten von Einsatzkräften liegen in einer als unkritisch eingestuften Anwendung der Verwaltung. Fällt sie bei einem Unwetter aus, zeigt sich erst dann, dass ohne sie niemand aufgeboten werden kann.
>
> **Nachvollziehbarkeit:** Ein Bewilligungsentscheid wird angefochten. Die Behörde kann nicht belegen, wer die Entscheidgrundlagen wann verändert hat. Die Überprüfung und Verteidigung des Entscheids werden erschwert, auch wenn er inhaltlich richtig war.

Überschutz und Unterschutz zeigen, dass der Schutz nicht am Wert ausgerichtet ist. Massnahmen richten sich nicht nach den möglichen Auswirkungen, sondern nach Gewohnheit, Budget oder dem Zufall eines Projekts. Häufig haben beide dieselbe Ursache, nämlich den unbekannten Wert. Wer den Wert seiner Informationen kennt, kann gezielt handeln. Wo Schutz fehlt, lässt er sich erhöhen. Wo Schutz über das Erforderliche hinausgeht, lässt er sich abbauen.

Prüfnachweis: Für eine Stichprobe der aufwendigsten Sicherheitsmassnahmen ist zu zeigen, auf welche Anforderung und auf welche Einstufung im Schutzbedarfsprofil sie zurückgehen. Lässt sich eine aufwendige Massnahme auf keine begründete Anforderung zurückführen, ist das ein Hinweis auf Überschutz.

1.3 Ein Leitbeispiel: plausible Einzelbefunde, falsches Gesamtbild

Auch wo der Wert bekannt ist, entsteht nicht automatisch ein stimmiges Bild. Anforderungen an dasselbe Schutzobjekt entstehen im Business Continuity Management, in der Informationssicherheit, im Datenschutz, in der Beschaffung und im Fachbereich, der seine Informationen klassifiziert. Fehlt der Abgleich, bleiben Lücken unentdeckt, obwohl jedes Verfahren für sich plausible Ergebnisse liefert. Ein Beispiel ist eine Fachanwendung, die Bewilligungsentscheide unterstützt. Tabelle 1 zeigt, was die einzelnen Verfahren für sie ergeben.

Verfahren / Sicht	Ergebnis
Business-Impact-Analyse	Prozess zwei Arbeitstage unterbrechbar; keine erhöhte Verfügbarkeitsanforderung.
Prozessverantwortung	Bewilligungsentscheide berühren Rechte von Personen. Fehler fallen oft erst im Rechtsmittelverfahren auf. Anforderungen an Integrität und Nachvollziehbarkeit werden nicht ausdrücklich formuliert.
Schutzbedarfsanalyse der Anwendung	Vertraulichkeit hoch; Integrität, Verfügbarkeit und Nachvollziehbarkeit normal.
Datenschutz	Besonders schützenswerte Personendaten. Die Folgenabschätzung ergibt ein hohes Risiko für die Persönlichkeit.
Klassifizierung	Ein Teil der Dossiers ist VERTRAULICH klassifiziert.
Architektur	Monatlicher Export in eine Auswertungsplattform, die nur für INTERN freigegeben ist.
Outsourcing	Der Betreiber hat privilegierten Datenbankzugriff. Änderungen werden nicht protokolliert.

Tabelle 1: Ergebnisse der einzelnen Verfahren im Leitbeispiel (eigene Darstellung)

Jede Aussage kann innerhalb ihres jeweiligen Verfahrens entstanden sein. Erst in der Zusammenführung werden drei Lücken sichtbar. Die Integrität wurde als normal eingestuft, obwohl falsche Daten zu falschen Entscheiden über Personen führen können, bis hin zu einer zu Unrecht entzogenen Bewilligung. Die Klassifizierung endet an der Anwendungsgrenze, und der Export bringt VERTRAULICH klassifizierte Dossiers in eine Umgebung, die dafür nicht vorgesehen ist. Und auch die Nachvollziehbarkeit wurde als normal eingestuft, obwohl bei einem angefochtenen Entscheid belegt werden muss, wer die Entscheidgrundlagen wann verändert hat. Gerade das ist nicht gewährleistet, denn der Betreiber kann Entscheidgrundlagen über seinen privilegierten Zugang verändern, ohne dass dies protokolliert oder fachlich freigegeben wird. Die Lücken sind unterschiedlicher Art. Bei Integrität und Nachvollziehbarkeit ist bereits die Einstufung zu tief, und zusätzlich erreicht die Umsetzung das erforderliche Niveau nicht. Beim Export liegt die Lücke in der Umsetzung (Abschnitt 6.3). Eine Business-Impact-Analyse, die sich wie üblich auf die Folgen einer Unterbrechung konzentriert, hätte keine dieser Lücken aufgedeckt, denn keine davon betrifft die Verfügbarkeit.

Mehrere plausible Einzelanalysen können zusammen ein falsches Sicherheitsbild ergeben. Die Qualität liegt nicht nur in der Einzelanalyse, sondern in der Konsistenz ihrer Schnittstellen.

2 Begriffe trennen

Vier Begriffe werden in der Praxis oft vermischt, obwohl sie unterschiedliche Fragen beantworten. Ihre Trennung ist die Voraussetzung dafür, sie später sauber zusammenzuführen.

Begriff	Kernfrage	Bedeutung für die Steuerung
Informationswert	Warum ist eine Information für die Organisation, Betroffene oder Dritte schutzwürdig?	Ausgangspunkt für fachliche, rechtliche und risikobezogene Anforderungen.
Klassifizierung	Welche Einstufung und welche Behandlungsvorgaben gelten für eine Information?	Formelle Vorgabe für Umgang, Kennzeichnung, Weitergabe und Ablage.
Kritikalität	Wie schnell werden die Folgen einer Beeinträchtigung einer Leistung oder eines Prozesses untragbar?	Treibt Priorisierung, Unterbrechungstoleranz und Kontinuitätsanforderungen.
Schutzbedarf	Welches Schutzniveau braucht ein Schutzobjekt je Schutzziel?	Bündelt alle Anforderungen und ist Grundlage für Sicherheitsanforderungen und Risikobehandlung.

Tabelle 2: Vier Begriffe und die Fragen, die sie beantworten (eigene Darstellung)

Das folgende Glossar definiert diese und weitere Begriffe, die im Papier wiederkehren. Es dient zugleich als Nachschlagehilfe für die späteren Kapitel.

Begriffe und Abkürzungen

Informationswert: Die Bedeutung einer Information für die Organisation, für betroffene Personen oder für Dritte, gemessen an den Folgen ihrer Offenlegung, Veränderung, Nichtverfügbarkeit oder fehlenden Nachvollziehbarkeit. Schutzpflichten aus Klassifizierung, Datenschutz, Geheimhaltung und Verträgen sind Teil dieses Werts, denn sie legen fest, welche Folgen rechtlich oder vertraglich nicht hingenommen werden dürfen.

Bedeutung der Leistung: Alle Anforderungen, die sich aus Zweck und Folgen einer Geschäftsleistung oder eines Prozesses ergeben, je Schutzziel. Die Kritikalität ist ihr zeitbezogener Teil und wird in der Business-Impact-Analyse erhoben. Anforderungen an Vertraulichkeit, Integrität und Nachvollziehbarkeit formulieren die Prozessverantwortlichen (Kapitel 4).

Werttransparenz: Das Wissen, welche Informationen welchen Wert haben, wer für sie verantwortlich ist und wo sie liegen.

Schutzobjekt: Das abgegrenzte Objekt, für das Schutzbedarf festgestellt wird. Das kann ein einzelnes IT-System sein, häufig ist es eine Fachanwendung mit ihren Daten, Komponenten und Schnittstellen, die einem gemeinsamen Zweck dient. Plattformen, die anderen Schutzobjekten Leistungen bereitstellen, etwa ein Identitätsdienst, eine Virtualisierungsumgebung oder ein Cloud-Dienst, sind eigene Schutzobjekte. Das gilt auch für ausgelagerte Leistungen eines Dienstleisters.

Informationsgruppe: Sinnvoll zusammengefasste Informationen innerhalb eines Schutzobjekts, die gleich bewertet werden können, etwa «Falldossiers» oder «Stammdaten Kundschaft».

Schutzobjekt-Verantwortliche (SO-V): Die für ein Schutzobjekt verantwortliche Person. In der Bundesverwaltung wird die Rolle als SO-V bezeichnet. Sie ist nicht identisch mit dem Informationseigner, der für die Information verantwortlich ist.

Informationsbestand: Organisationsweit zusammengehörende Informationen, unabhängig davon, in welchen Schutzobjekten sie bearbeitet werden, etwa «Kalkulationen» oder «Falldossiers». In den einzelnen Schutzobjekten erscheinen sie als Informationsgruppen.

Schutzziel: Die Eigenschaft einer Information, die geschützt werden soll. Dieses Papier verwendet vier Schutzziele, die jeweils beschreiben, was gewährleistet sein muss, nämlich Vertraulichkeit (nur Berechtigte haben Zugang), Integrität (Informationen sind korrekt und vollständig), Verfügbarkeit (sie stehen zur Verfügung, wenn sie gebraucht werden) und Nachvollziehbarkeit (es lässt sich belegen, wer sie wann bearbeitet hat).

Schutzbedarf: Das erforderliche Schutzniveau je Schutzziel, gemessen an den möglichen Folgen einer Beeinträchtigung. Bewertet wird er zunächst für Informationsgruppen. Verbindlich festgestellt wird er für das Schutzobjekt, das sie bearbeitet, zusammen mit den Anforderungen aus den unterstützten Leistungen. Wo dieses Papier vom Schutzbedarf einer Information oder Informationsgruppe spricht, ist diese erste Bewertung gemeint.

Schutzbedarfsprofil: Die Einstufung eines Schutzobjekts je Schutzziel, mit Begründung und Herkunft jeder Anforderung.

Schutzbedarfsfeststellung: Der Schritt, in dem alle Anforderungen an ein Schutzobjekt aus beiden Blickrichtungen zu einem Schutzbedarfsprofil zusammengeführt werden (Kapitel 6). Eine Schutzbedarfsanalyse leistet das nur, wenn sie die Ergebnisse von Business-Impact-Analyse, Klassifizierung, Datenschutz und Verträgen einbezieht. Bleibt sie auf die einzelne Anwendung beschränkt, ist sie eine Quelle unter mehreren (Tabelle 1). In anderen Beiträgen dieser Reihe steht dafür vereinfachend «Schutzbedarfsanalyse».

Vererbung: Übertragung der Anforderungen einer Leistung oder eines Schutzobjekts auf die Schutzobjekte, die sie unterstützen, je Schutzziel und im Umfang der tatsächlichen Abhängigkeit (Abschnitte 4.1 und 6.2).

Erhöhter Schutzbedarf: Mindestens ein Schutzziel ist hoch oder sehr hoch eingestuft. Welche Auswirkungen den Stufen normal, hoch und sehr hoch entsprechen, legt die Organisation fest.

Sicherheitsanforderung: Konkrete, überprüfbare Vorgabe, was an einem Schutzobjekt erreicht sein muss, um das erforderliche Schutzniveau zu gewährleisten, ohne Festlegung auf eine bestimmte Lösung (Kapitel 7).

Wirksamkeitsnachweis: Beleg, dass eine Sicherheitsanforderung durch Massnahmen erfüllt wird, die im Betrieb wirken. Ist eine Anforderung bewusst nicht vollständig erfüllt, tritt der dokumentierte Risikoentscheid an seine Stelle. Er belegt einen Entscheid, keine Erfüllung.

Informationseigner (Data Owner): Die für eine Information verantwortliche Person, in der Regel eine Führungsperson im Fachbereich. Sie verantwortet die Beurteilung des Werts und die daraus folgenden Schutzanforderungen und steht für Zugriffs- und Risikoentscheide ein. Sie ist nicht identisch mit dem Systembetreiber.

Überschutz / Unterschutz: Umgesetzter Schutz, der deutlich über beziehungsweise unter dem liegt, was der Wert der Information und die Bedeutung der Leistung erfordern.

Unterbrechungstoleranz und Wiederanlaufziel: Die Unterbrechungstoleranz ist das Ausmass und die Dauer einer Unterbrechung, die die Leitung für eine Leistung zu akzeptieren bereit ist. Das Wiederanlaufziel ist die Frist, in der eine Tätigkeit nach einer Unterbrechung wieder auf dem Mindestleistungsniveau laufen soll, also im Mindestumfang, der dann noch akzeptabel ist. Aus ihm und der gewählten Kontinuitätslösung ergeben sich die technischen Wiederanlaufziele der Schutzobjekte (vgl. Beitrag zum Business Continuity Management dieser Reihe).

«Dienstleister» schliesst in diesem Papier interne Leistungserbringer ein. Rollenbezeichnungen wie Informationseigner und SO-V gelten für alle Geschlechter.

2.1 Klassifizierung ist nicht Schutzbedarf

In der Bundesverwaltung werden Informationen als INTERN, VERTRAULICH oder GEHEIM klassifiziert (Art. 13 ISG). Massstab ist die unberechtigte Kenntnisnahme, also die Vertraulichkeit. Die Wirkung der Klassifizierung reicht aber weiter, denn sie ist mit den Sicherheitsstufen für Informatikmittel verknüpft. Das ISG kennt drei solche Stufen, den Grundschutz, den hohen Schutz und den sehr hohen Schutz (Art. 17 ISG). Der Grundschutz gilt, sofern keine höhere Stufe erforderlich ist.

Die Verordnung über die Informationssicherheit in der Bundesverwaltung und der Armee (Informationssicherheitsverordnung, ISV) ordnet einem Informatikmittel die Stufe «hoher Schutz» zu, wenn eine Verletzung der Informationssicherheit Beeinträchtigungen jener Art zur Folge haben kann, die auch die Klassifizierungsstufe VERTRAULICH definieren. Für «sehr hoher Schutz» gilt dasselbe mit Bezug auf GEHEIM (Art. 28 in Verbindung mit Art. 19 und 20 ISV). Der Leitfaden des Bundesamts für Cybersicherheit (BACS) zur Schutzbedarfsanalyse zieht daraus den Schluss, dass bei der Bearbeitung VERTRAULICH klassifizierter Informationen mindestens «hoher Schutz» gilt, bei GEHEIM klassifizierten «sehr hoher Schutz». Zudem ist die Bearbeitung solcher Informationen eine sicherheitsempfindliche Tätigkeit (Art. 5 ISG), mit Folgen für Personal, Betrieb und Dienstleister. Im Sicherheitsverfahren des Bundes gibt die Bearbeitung klassifizierter Informationen damit eine Mindest-Sicherheitsstufe für das betroffene Informatikmittel vor.

In der Privatwirtschaft fehlt diese Trennung oft. Die Norm ISO/IEC 27001 sieht vor, Informationen nach den Sicherheitsbedürfnissen der Organisation zu klassifizieren, gestützt auf Vertraulichkeit, Integrität, Verfügbarkeit und die Anforderungen interessierter Parteien (Anhang A, Control 5.12). In der Praxis sind solche Schemata jedoch meist auf die Vertraulichkeit ausgerichtet und werden trotzdem als Schutzbedarf behandelt. «Streng vertraulich» sagt dann viel über den Umgang mit einem Dokument, aber nichts darüber, wie lange die Anwendung ausfallen darf oder wie Änderungen nachgewiesen werden müssen.

In beiden Welten müssen Klassifizierung und Schutzbedarf aufeinander bezogen werden, dürfen aber nicht ineinander aufgehen. Die Klassifizierung kann das Schutzniveau eines Schutzobjekts anheben. Eine auf Vertraulichkeit ausgerichtete Klassifizierung kann auch Anforderungen an andere Schutzziele auslösen, etwa an die Nachvollziehbarkeit von Zugriffen. Sie ersetzt aber nicht die eigene Beurteilung von Verfügbarkeit, Integrität und Nachvollziehbarkeit. Eine Anwendung mit nicht klassifizierten Informationen kann sehr hohe Integritätsanforderungen haben, und eine klassifizierte Information kann in einer Anwendung liegen, deren Ausfall kaum ins Gewicht fällt.

2.2 «Das ist vertraulich» – ist es das wirklich?

Dieser Satz fällt schnell, in Projekten, Sitzungen und Audits. Oft fehlt eine klare Definition, was «vertraulich» in der Organisation überhaupt bedeutet. Der Satz ist selten falsch gemeint, aber oft ungeprüft. Dahinter steht eine Vorsichtsmassnahme, eine Gewohnheit oder eine Einstufung ohne nachvollziehbare Schadensbetrachtung. Das ISG zieht hier eine klare Linie. Klassifizierungen sind auf das erforderliche Mindestmass

zu beschränken und nach Möglichkeit zeitlich zu begrenzen (Art. 11 Abs. 2 ISG). Der Gedanke gilt weit über die Bundesverwaltung hinaus.

Auch Überklassifizierung hat ihren Preis. Sie macht die Behandlungsvorgaben zur Last, die im Alltag oft umgangen wird, und lässt die wirklich schutzwürdigen Informationen in der Masse untergehen. Wer alles als vertraulich kennzeichnet, nimmt dem Begriff seine Unterscheidungskraft und bezahlt Schutz, der in keinem Verhältnis zum Wert steht. Das Gegenstück ist das reflexhafte «ist ja nur intern», das Geschäftsgeheimnisse unter Wert behandelt.

Prüfbar wird die Aussage durch drei Fragen.

- Welcher konkrete Schaden entstünde, für wen und in welchem Szenario?
- Erreicht dieser Schaden die Schwelle, die die Organisation für «vertraulich» festgelegt hat?
- Wie lange gilt die Einstufung, und wer hat sie vorgenommen?

Hilfreich sind dafür vorab festgelegte Schadensszenarien, wie sie der IT-Grundschutz des deutschen Bundesamts für Sicherheit in der Informationstechnik (BSI) verwendet. Sie fragen nach Verstössen gegen Gesetze oder Verträge, nach Folgen für betroffene Personen, für die Aufgabenerfüllung und das Ansehen sowie nach finanziellen Auswirkungen. Für jedes Szenario legt die Organisation selbst fest, ab wann ein Schaden als erheblich gilt. Eine Einstufung ohne nachvollziehbare Begründung ist keine belastbare Klassifizierung.

Prüfnachweis: Vorab ist zu prüfen, ob die Stufen und ihre Schwellen festgelegt sind. Für eine Stichprobe als vertraulich eingestufter Informationen ist dann die Begründung vorzulegen, also Schadensszenario, Schwelle und, wo möglich, Befristung. Fehlt sie bei einem grossen Teil, sind die Einstufungen nicht belastbar. Ob tatsächlich überklassifiziert wurde, zeigt erst die fachliche Nachprüfung.

2.3 Datenschutz und Geheimhaltung: Quellen von Anforderungen

Der BACS-Leitfaden zur Schutzbedarfsanalyse (Kapitel 2, Schritt 2) führt den Datenschutz neben Vertraulichkeit, Integrität, Verfügbarkeit und Nachvollziehbarkeit als fünftes Schutzziel. Das ist für die Bundesverwaltung folgerichtig, weil die datenschutzrechtliche Beurteilung dort ein eigener Prüfschritt ist. Dieses Papier behandelt Datenschutz in der Schutzbedarfsfeststellung als Quelle von Anforderungen. Datenschutzrechtliche Anforderungen werden dort in die Schutzziele übersetzt, wo sie Anforderungen an die Informationssicherheit begründen.

Das gilt vor allem für die Datensicherheit. Sie bildet die Schnittmenge zwischen Datenschutz und Informationssicherheit. Das Bundesgesetz über den Datenschutz (Datenschutzgesetz, DSG) verlangt technische und organisatorische Massnahmen (TOM), die eine dem Risiko angemessene Datensicherheit gewährleisten (Art. 8 DSG). Die Verordnung über den Datenschutz (Datenschutzverordnung, DSV) nennt dafür dieselben vier Schutzziele wie dieses Papier. Personendaten müssen ihrem Schutzbedarf entsprechend vertraulich, verfügbar, integer und nachvollziehbar bearbeitet werden (Art. 2 DSV). Die datenschutzrechtlichen Anforderungen an die Datensicherheit werden in der Schutzbedarfsfeststellung den Schutzzielen zugeordnet. Die TOM folgen daraus als Massnahmen (Kapitel 7).

Datenschutz ist aber mehr als Datensicherheit. Zweckbindung, Verhältnismässigkeit, Transparenz oder Profiling können problematisch sein, ohne dass ein Schutzziel verletzt ist. Diese Fragen beantwortet die Datenschutzbeurteilung, nicht die Schutzbedarfsfeststellung.

Das DSG unterscheidet Personendaten und besonders schützenswerte Personendaten (Art. 5 DSG). Den festen Begriff verwendet dieses Papier nur für diese gesetzliche Kategorie. Auch gewöhnliche Personendaten können je nach Umfang und Kontext hohe Risiken für Betroffene erzeugen. Der Verantwortliche prüft

deshalb zunächst in einer Vorprüfung, ob die vorgesehene Bearbeitung ein hohes Risiko für die Persönlichkeit oder die Grundrechte der betroffenen Personen mit sich bringen kann. Ist dies der Fall, ist grundsätzlich eine Datenschutz-Folgenabschätzung zu erstellen (Art. 22 DSG).

Daneben bestehen Schutzpflichten unabhängig vom Datenschutz, etwa Amts- und Berufsgeheimnisse (Art. 320 und 321 StGB), Geschäftsgeheimnisse, spezialgesetzliche Verschwiegenheitspflichten, regulatorische Vorgaben und vertragliche Vertraulichkeitszusagen. Eine Information kann deshalb in hohem Mass schutzwürdig sein, ohne klassifiziert zu sein und ohne Personendaten zu enthalten. Wird nur nach Klassifizierung und Personendaten gefragt, fallen gerade Geschäftsgeheimnisse leicht durch alle Raster.

2.4 Vier Schutzziele, auch die Nachvollziehbarkeit

Dieses Papier führt die Nachvollziehbarkeit als eigenständiges Schutzziel und folgt damit dem Informationssicherheitsgesetz (Art. 6 Abs. 2 ISG) und der Datenschutzverordnung (Art. 2 DSV, vgl. Abschnitt 2.3 dieses Papiers), die sie beide ausdrücklich nennen. ISO/IEC 27001 und der BSI-Grundschutz stellen Vertraulichkeit, Integrität und Verfügbarkeit in den Mittelpunkt. Der BSI-Grundschutz zählt Authentizität und Nichtabstreitbarkeit zur Integrität, lässt aber weitere Grundwerte ausdrücklich zu und unterstützt die Nachvollziehbarkeit durch Anforderungen an die Protokollierung (Baustein OPS.1.1.5).

Die Nachvollziehbarkeit als eigenes Schutzziel zu behandeln, ist sinnvoll, weil zwei verschiedene Fragen dahinterstehen, nämlich ob Daten richtig sind und ob sich nachweisen lässt, wer sie wann bearbeitet, insbesondere verändert hat. Beide verlangen unterschiedliche Massnahmen. Wer sie in einem Feld zusammenfasst, bewertet meist nur die erste. Im Datenschutz ist die Nachvollziehbarkeit ebenfalls zentral. Bearbeiten umfasst dort jeden Umgang mit Personendaten, vom Beschaffen über das Speichern, Verwenden, Verändern und Bekanntgeben bis zum Löschen oder Vernichten (Art. 5 DSG). Die DSV verlangt unter bestimmten Voraussetzungen eine Protokollierung, die festhält, wer welche Daten wann und auf welche Art bearbeitet hat und an wen sie gegebenenfalls bekanntgegeben wurden (Art. 4 DSV). Protokollierung ist damit eine Massnahme, die Informationssicherheit und Datenschutz gemeinsam dient.

3 Zwei Blickrichtungen auf dasselbe Schutzobjekt

Das Grundmodell dieses Papiers lässt sich in einem Satz fassen. Anforderungen erreichen dasselbe Schutzobjekt aus zwei Richtungen (Abbildung 3).

Top-down trägt die Anforderungen der Geschäftsleistung über den Prozess zum Schutzobjekt, Bottom-up die Anforderungen aus dem Wert der Information, einschliesslich der für sie geltenden Schutzpflichten. Beide Richtungen können dasselbe Schutzziel betreffen. Gerade deshalb müssen sie am Schutzobjekt zusammengeführt werden. Das Schutzobjekt ist dafür der geeignete Ort, weil viele Anforderungen erst dort konkret werden. Es bündelt Informationsgruppen mehrerer Eigner und unterstützt oft mehrere Prozesse, und Klassifizierung, Datenschutz und Verträge greifen dort, wo Informationen tatsächlich bearbeitet werden. Dort zeigen sich auch die Widersprüche zwischen den Quellen. Erst daraus entsteht das Schutzbedarfsprofil, und erst aus ihm folgen Anforderungen, Massnahmen, Entscheide und Nachweise. In Abbildung 3 zeigen die durchgezogenen Pfeile Herkunft, Vererbung und Umsetzung der Anforderungen, der gestrichelte Rückweg den Wirksamkeitsnachweis, also den Beleg, dass die Anforderungen im Betrieb tatsächlich erfüllt werden (Kapitel 9).

Die Top-down-Richtung ist aus dem Business Continuity Management bekannt (ISO 22301). In der dort üblichen Form erkennt sie Verfügbarkeitsanforderungen gut, Vertraulichkeitsanforderungen aber kaum. Methodisch ist auch die Bottom-up-Richtung angelegt, im BSI-Grundschutz ebenso wie im Sicherheitsverfahren des Bundes mit seinem Informationsverzeichnis je Schutzobjekt (vgl. Abschnitte 6.2 und 5.2 dieses

Papiers). Sie reicht aber über das einzelne Schutzobjekt hinaus, denn dieselben Informationen können in mehreren Anwendungen, in Exporten und bei Dienstleistern liegen (Abschnitt 1.1). Deshalb wird sie ausführlicher behandelt.



Abbildung 3: Top-down und Bottom-up treffen sich am Schutzobjekt; Plattformen und Dienstleister sind ihrerseits Schutzobjekte, für die dieselbe Kette gilt (Arbeitsmodell, eigene Darstellung)

4 Top-down: von der Geschäftsleistung nach unten

Die Top-down-Sicht beginnt bei den Leistungen, die eine Organisation erbringen muss. Für die Verfügbarkeit ist diese Logik aus dem Business Continuity Management bekannt (ISO 22301, Abschnitt 8.2 Business-Impact-Analyse und Risikobeurteilung). Die Leitung legt fest, wie lange eine Leistung ausfallen darf. Daraus folgt, wie schnell die unterstützenden Anwendungen, Plattformen und Dienstleister wieder verfügbar sein müssen.

Die Bedeutung einer Leistung prägt aber nicht nur die Verfügbarkeit. Bei einem Abrechnungssystem sind falsche Buchungen oft gravierender als ein kurzer Ausfall. Ein Ausfall fällt sofort auf, eine Verfälschung womöglich erst Monate später. Ein Entscheidprozess, der Rechte von Personen berührt, muss auch bei geringer zeitlicher Kritikalität belegen können, auf welcher Grundlage entschieden wurde. Und der Zweck eines Prozesses kann Informationen vertraulich machen, die für sich unkritisch wären, etwa wenn sie einer laufenden Übernahmeprüfung oder Untersuchung zugeordnet sind. Die Business-Impact-Analyse fragt in der Regel nur nach den Folgen einer Unterbrechung über die Zeit. Diese Anforderungen erfasst sie deshalb meist nicht.

Zuständig für diese Anforderungen sind die Prozessverantwortlichen. Sie beurteilen für ihre Leistung, welche Folgen falsche, offengelegte oder nicht nachvollziehbare Informationen hätten, und bringen diese Beurteilung in die Schutzbedarfsfeststellung ein (Kapitel 6). Der BSI-Grundschutz sieht dafür ausdrücklich eine Schutzbedarfsfeststellung für Geschäftsprozesse vor (vgl. Abschnitt 6.2 dieses Papiers). Wo sie fehlt, bleibt die Top-down-Richtung auf die Verfügbarkeit beschränkt.

4.1 Vererbung folgt der tatsächlichen Abhängigkeit

Die Anforderungen einer Geschäftsleistung werden auf die Schutzobjekte übertragen, die sie unterstützen. Man spricht von Vererbung. Sie erfolgt nicht pauschal, sondern je Schutzziel und im Umfang der tatsächlichen Abhängigkeit.

Beispielsweise liefert eine Anwendung einem kritischen Prozess nur Referenzdaten wie Tarife oder Postleitzahlen. Ihre Integrität ist hoch einzustufen, denn falsche Tarife verfälschen den Prozess. Vertraulich sind diese Daten aber kaum, und ein kurzer Ausfall lässt sich mit den zuletzt gelieferten Daten überbrücken. Würde die Anwendung in allen Schutzzielen so hoch eingestuft wie der Prozess, wäre das Überschutz. Diese pauschale Übernahme ist eine häufige Quelle dafür.

Weil sich Abhängigkeiten selten vollständig im Voraus erheben lassen, gilt im Zweifel die Anforderung der unterstützten Leistung, je Schutzziel getrennt. Eine tiefere Einstufung des Schutzobjekts ist zulässig, wenn sie sich mit der tatsächlichen Abhängigkeit begründen lässt. Die Begründung wird dokumentiert. So lässt sich Überschutz gezielt vermeiden, und es bleibt nachvollziehbar, ob eine tiefere Einstufung begründet ist oder still herabgesetzt wurde.

Prüfnachweis: Für eine kritische Geschäftsleistung sind die unterstützenden Anwendungen und Plattformen mit ihrem Schutzbedarfsprofil vorzulegen. Abweichungen von den aus der Geschäftsleistung abgeleiteten Anforderungen müssen je Schutzziel begründet sein.

5 Bottom-up: von der Information nach oben

Die Bottom-up-Sicht beginnt bei der Information. Nicht der Ablageort steht am Anfang, sondern die Frage, warum eine Information geschützt werden muss und welche Folgen eine Beeinträchtigung hätte. Erst danach folgen die Fragen, wo sie liegt, wo sie bearbeitet wird und welche Leistungen von ihr abhängen. Bottom-up ist damit mehr als ein Dateninventar. Es ist die Rückverfolgung des Informationswerts in den betrieblichen Kontext.

5.1 Der erste Schritt: den Wert erkennen

Wer den Wert seiner Informationen bisher nicht kennt, sollte nicht mit einem vollständigen Inventar beginnen. Ein solches Vorhaben dauert lange, liefert zuerst Masse statt Erkenntnis und verliert oft unterwegs die Unterstützung der Fachbereiche. Wirksamer ist ein Einstieg über die kritischsten Informationsbestände, die «Kronjuwelen» der Organisation. Er beginnt mit vier Fragen an Leitung und Fachbereiche, eine je Schutzziel. Massstab ist jeweils, ob die Auswirkungen noch tragbar wären.

1. Bei welchen Informationen wäre eine Offenlegung nicht tragbar?
2. Bei welchen Informationen wäre eine unbemerkte Veränderung nicht tragbar?
3. Wie lange könnten wir ohne eine bestimmte Information arbeiten, bevor ihr Fehlen nicht mehr tragbar ist?
4. Bei welchen Informationen wäre es nicht tragbar, wenn sich nicht belegen lässt, wer sie wann eingesehen oder verändert hat, auch wenn alle Zugriffe berechtigt waren?

Die Antworten sollten zunächst zu einer bewusst begrenzten Liste der kritischsten Informationsbestände führen. Für jeden Bestand braucht es zweierlei, nämlich den Fachbereich, der den Wert beurteilen kann, und einen Informationseigner, der als verantwortliche Person dafür einsteht. Anschliessend wird verfolgt,

wo diese Bestände heute tatsächlich liegen. Dazu gehört ausdrücklich die Aussensicht. Was davon ist öffentlich zugänglich, auf der eigenen Website, in geteilten Links, in Code-Repositories oder über Dienstleister?

Genauso wichtig ist die Gegenfrage, welche Informationen ausdrücklich nicht kritisch sind. Wer das festhält, schafft die Grundlage, um Überschutz abzubauen und die freiwerdenden Mittel dorthin zu lenken, wo sie wirken. Danach wird der Kreis schrittweise erweitert, bis für die relevanten Schutzobjekte Informationsverzeichnisse vorliegen (Abschnitt 5.2).

Prüfnachweis: Vorzulegen ist die Liste der kritischsten Informationsbestände, jeweils mit Informationseigner und Ablageorten, ebenso die Festlegung, was ausdrücklich nicht kritisch ist. Zu zeigen ist, wann die Liste zuletzt geprüft wurde und ob dabei auch öffentlich zugängliche Quellen einbezogen wurden.

5.2 Das Informationsverzeichnis als Grundlage

Das Sicherheitsverfahren des Bundes zeigt, wie ein solches Vorgehen methodisch aussehen kann. Es ist im ISG und in der ISV geregelt (Art. 16 ISG, Art. 27 bis 29 ISV).

Das Verfahren umfasst sechs Schritte, nämlich Schutzobjekt identifizieren, Schutzbedarf ermitteln, Sicherheitsanforderungen festlegen, Schutzmassnahmen umsetzen, Restrisiken beurteilen und vor der produktiven Nutzung freigeben. Der Schutzbedarf wird mithilfe einer Schutzbedarfsanalyse (Schuban) ermittelt. Dafür stehen ein Leitfaden und eine Vorlage zur Verfügung.

Nach dem Leitfaden wird zuerst das Schutzobjekt beschrieben und dann ein Informationsverzeichnis erstellt. Es umfasst alle Informationen, die das Schutzobjekt erzeugt, speichert, verarbeitet oder überträgt oder für den eigenen Betrieb benötigt. Je Informationsgruppe werden Klassifizierung, Kreis der Berechtigten und Personenbezug festgehalten, erst dann die Auswirkungen je Schutzziel. Bewertet werden Informationsgruppen, nicht einzelne Dokumente oder Datensätze. Das hält den Aufwand in Grenzen. Der Leitfaden verlangt, die Informationen sinnvoll zu gruppieren. Zweckmässig ist, Informationen mit deutlich abweichendem Schutzbedarf als eigene Gruppe zu führen. Auch das amerikanische National Institute of Standards and Technology (NIST) ordnet den Schutzbedarf nach Informationstypen (FIPS 199, SP 800-60).

Zwei Eigenschaften sind über die Bundesverwaltung hinaus lehrreich. Der Ansatz bewertet die möglichen Auswirkungen einer Verletzung, unabhängig von Bedrohungen. Wie wahrscheinlich ein Schaden ist, gehört in die Risikoanalyse. Und er zählt auch die Informationen, die nur für den Betrieb nötig sind, etwa Schlüssel, Konfigurationen, Protokolle und Zugangsdaten. Sie fehlen in fachlich geführten Inventaren oft.

5.3 Der Informationseigner verantwortet, der Betreiber setzt um

Schutzbedarf beruht auf einer fachlichen Beurteilung, braucht aber auch klar verteilte Verantwortung. Der Fachbereich beurteilt mit seinem Fachwissen, was eine Information wert ist. Der Informationseigner verantwortet diese Beurteilung ebenso wie die daraus folgenden Schutzanforderungen. Er steht für Zugriffs- und Risikoentscheide ein, unabhängig davon, in wie vielen Schutzobjekten seine Information liegt. Ein Schutzobjekt kann dagegen Informationen mehrerer Eigner bündeln. Nach dem hier vorgeschlagenen Rollenmodell führt in diesem Fall die Schutzobjekt-Verantwortliche (SO-V) deren Beurteilungen für das Schutzobjekt zusammen (Kapitel 6). Der Eigner ist also für die Information zuständig, die SO-V für das Schutzobjekt.

Die Informationssicherheit prüft, ob die Einstufung plausibel und begründet ist. Wo Personendaten betroffen sind, wird die Datenschutzberatung beigezogen. Sie berät und prüft, die Verantwortung für die Einhaltung des Datenschutzes bleibt aber beim Verantwortlichen im Sinne des DSG. Verbindlich wird die Einstufung durch die Genehmigung der dafür vorgesehenen Stellen. Die Organisation legt fest, wer dazu befugt

ist, etwa Auftraggeber und Prozessverantwortliche. Erst dann setzt die IT um. Sie betreibt die Systeme, entscheidet aber nicht über den Wert der Informationen der Fachbereiche. Für Informationen, die sie selbst für den Betrieb benötigt, etwa Schlüssel, Konfigurationen, Protokolle und Zugangsdaten (Abschnitt 5.2), ist sie selbst der Fachbereich, der den Wert beurteilt.

In der Praxis füllt häufig die Projektleitung das Formular der Schutzbedarfsanalyse aus, und der Informationseigner unterschreibt. Nicht selten bestimmt der Fachbereich die Projektleitung auch zur SO-V, ohne dass gefragt wird, ob sie das nötige Fachwissen für die Beurteilung mitbringt. Zudem endet die Projektleitung mit dem Projekt, die Verantwortung für das Schutzobjekt aber nicht. Entscheidend ist deshalb weniger die Unterschrift als die Frage, ob die Begründungen erkennbar aus fachlicher Kenntnis stammen und ob die SO-V über das Projekt hinaus benannt ist.

5.4 Datenflüsse: Schutzanforderungen müssen mitwandern

Eine Information ist nur dann geschützt, wenn ihre Anforderungen in allen Bearbeitungskontexten gelten. Das betrifft die Fachanwendung, aber auch Schnittstellen, Exporte, Auswertungsplattformen, Kollaborationswerkzeuge, Test- und Entwicklungsumgebungen, Datensicherungen, Dienstleister und die Grenze zur Öffentlichkeit. Am Ziel des Datenflusses gelten die Anforderungen an die Vertraulichkeit weiter, jene an Integrität und Nachvollziehbarkeit überall dort, wo mit den Daten gearbeitet oder entschieden wird. Die Verfügbarkeit bemisst sich am jeweiligen Kontext. Eine Kopie in einer Testumgebung muss nicht so verfügbar sein wie die Produktion, wohl aber ebenso vertraulich. Wo Daten zusammenfliessen, kann der Schutzbedarf am Ziel sogar höher liegen (Abschnitt 5.5). Ohne Übersicht über die Datenflüsse bleibt Bottom-up ein Inventar ohne Wirkung. Der eingangs erwähnte Fall Xplain verdeutlicht, weshalb Schutzanforderungen auch externe Bearbeitungskontexte und Dienstleister einbeziehen müssen.

Prüfnachweis: Für ein ausgewähltes Schutzobjekt sind das Informationsverzeichnis und die Datenflüsse vorzulegen. Zu prüfen ist, ob jede Informationsgruppe mit erhöhtem Schutzbedarf an jedem Ziel ihres Datenflusses je Schutzziel angemessen, hinsichtlich der Vertraulichkeit mindestens gleichwertig geschützt ist oder ob eine Ausnahme dokumentiert entschieden wurde.

5.5 Der Wert ist nicht statisch: Aggregation und Zeit

Der BSI-Grundschutz kennt den Kumulationseffekt bei Systemen. Für Informationen gibt es ein Gegenstück, das in Schutzbedarfsanalysen selten ausdrücklich bewertet wird. Viele für sich wenig sensible Datensätze können zusammengeführt deutlich schutzwürdiger sein. Einzelne Adressen sind wenig heikel, ein vollständiges Verzeichnis aller Kundinnen und Kunden mit Vertragsstatus dagegen sehr wohl. Durch die Verknüpfung vieler für sich wenig sensibler Personendaten kann ein deutlich höheres Risiko für betroffene Personen entstehen.

Aggregation entsteht dort, wo Daten zusammenfliessen, etwa in Data Warehouses und Data Lakes, in Exporten für Auswertungen, in Suchindizes und zunehmend in Anwendungen der künstlichen Intelligenz (KI) mit Zugriff auf breite Datenbestände. Diese Plattformen müssen eigenständig bewertet werden. Es genügt nicht, die Einstufung der Quellsysteme zu übernehmen. Die ISV verlangt dasselbe für klassifizierte Informationen. Werden sie zu einem Sammelwerk zusammengefasst, ist die Klassifizierung neu zu beurteilen (Art. 16 Abs. 2 ISV).

Auch die Zeit verändert den Wert. Ein Beispiel sind die Krankenkassenprämien für das Folgejahr. Sie dürfen bis zu ihrer offiziellen Bekanntgabe im Herbst nicht vorzeitig bekannt werden, danach sind sie für alle öffentlich einsehbar. Hier ist der Zeitpunkt des Wertwechsels bekannt. Bei anderen Informationen hängt er von einem Ereignis ab. Ausschreibungsunterlagen können nach dem Zuschlag an Schutzbedarf verlieren, Untersuchungsakten nach Abschluss des Verfahrens, Zugangsdaten nach ihrer Rotation. Ein Wertverlust

tritt aber nicht zwangsläufig ein. Die Kalkulation einer abgeschlossenen Ausschreibung kann für künftige Offerten weiterhin wertvoll sein. Für Personendaten setzt das Gesetz dem Lebenszyklus eine Grenze. Sie sind zu vernichten oder zu anonymisieren, sobald sie für den Zweck der Bearbeitung nicht mehr erforderlich sind und keine Aufbewahrungspflicht entgegensteht (Art. 6 Abs. 4 DSG). Für klassifizierte Informationen verlangt das ISG, Klassifizierungen nach Möglichkeit zu befristen (Art. 11 Abs. 2 ISG, vgl. Abschnitt 2.2 dieses Papiers). Die ISV schreibt zudem vor, ihren Schutzbedarf mindestens alle fünf Jahre zu überprüfen (Art. 25 ISV). Schutzbedarf braucht deshalb neben Änderungsereignissen auch einen Bezug zum Lebenszyklus der Information. Wann steigt oder sinkt ihr Wert, und wer passt die Einstufung dann an?

6 Zusammenführung zum Schutzbedarfsprofil

Top-down und Bottom-up treffen bei Anwendungen, Systemen, Plattformen und Dienstleistern zusammen. Dort müssen die Anforderungen aus der Bedeutung der Geschäftsleistung und aus dem Wert der Information, einschliesslich der Schutzpflichten, in ein stimmiges Profil überführt werden. Ein Einzelwert wie «Schutzbedarf hoch» ist dafür zu grob. Er verdeckt, dass die Schutzziele unterschiedlich ausgeprägt sind und unterschiedliche Massnahmen verlangen. Für die Fachanwendung aus dem Leitbeispiel (Abschnitt 1.3) könnte ein zusammengeführtes Profil so aussehen, wie in Tabelle 3 dargestellt. Bei der Zusammenführung leiten die Prozessverantwortlichen die bisher nicht ausdrücklich formulierten Anforderungen an Integrität und Nachvollziehbarkeit aus dem Entscheidprozess ab. Die SO-V führt sie in das Schutzbedarfsprofil über.

Schutzziel	Einstufung	Quelle der Anforderung	Begründung
Vertraulichkeit	hoch	Bottom-up: Informationswert (Klassifizierung, Datenschutz)	VERTRAULICH klassifizierte Dossiers, besonders schützenswerte Personendaten.
Integrität	hoch	Top-down: Prozessverantwortung (Entscheidverfahren); Bottom-up: Datenschutz (Folgenabschätzung)	Verfälschte Daten führen zu falschen Entscheiden über Personen, etwa zu einer zu Unrecht entzogenen Bewilligung. Fehler fallen spät auf. Der Entscheid wird oft erst im Rechtsmittelverfahren korrigiert, die Folgen bis dahin nicht. Als Schwelle für «hoch» sind erhebliche, nur schwer rückgängig zu machende Folgen für Betroffene angenommen.
Verfügbarkeit	normal	Top-down: Business-Impact-Analyse	Prozess zwei Arbeitstage unterbrechbar. Keine Hochverfügbarkeit nötig.
Nachvollziehbarkeit	hoch	Top-down: Prozessverantwortung (Entscheidverfahren); Bottom-up: Datenschutz (Art. 4 DSV)	Wird ein Entscheid angefochten, muss belegt werden können, wer die Entscheidgrundlagen wann verändert hat. Fehlt dieser Beleg, sind Überprüfung und Verteidigung des Entscheids erheblich erschwert (Beispiele in Abschnitt 1.2). Das erreicht die angenommene Schwelle für «hoch». Zusätzlich Protokollierung nach Art. 4 DSV, sofern die gesetzlichen Voraussetzungen erfüllt sind.

Tabelle 3: Schutzbedarfsprofil der Fachanwendung aus dem Leitbeispiel (eigene Darstellung)

Die Einstufungen sind keine allgemeingültigen Schwellenwerte. Entscheidend sind die Spalte «Quelle» und die Begründung. Sie machen sichtbar, welche Quelle, also welches vorgelagerte Verfahren oder welche Prozessanforderung, eine Anforderung ausgelöst hat, und damit, wo eine spätere Änderung eine Neubewertung auslösen muss. Das Profil zeigt zudem, wo bewusst nicht hoch eingestuft wurde. Auch das ist eine Aussage, die Kosten sparen kann.

Diese Zusammenführung braucht eine verantwortliche Stelle. Der Informationseigner kann sie allein kaum leisten, weil ein Schutzobjekt meist Informationsgruppen mehrerer Eigner bündelt und zusätzlich Anforderungen aus Prozessen, Datenschutz und Business Continuity Management trägt. Zweckmässig ist deshalb, die Zusammenführung der Beurteilungen mehrerer Eigner und Fachbereiche der SO-V zuzuweisen. In anderen Organisationen bietet sich dafür die entsprechend benannte Rolle an. Die Informationssicherheit plausibilisiert das Ergebnis. Widersprechen sich Anforderungen aus verschiedenen Quellen, sollte die SO-V die Differenz der zuständigen Entscheidungsinstanz vorlegen. Der Beitrag zum Business Continuity Management dieser Reihe beschreibt diese Lücke für die Verfügbarkeit. Business-Impact-Analyse und Schutzbedarfsanalyse entstehen getrennt, und ihre Werte werden erst über eine Übersetzungsregel zwischen Verfügbarkeitsstufe und Wiederanlauffrist vergleichbar. In der Bundesverwaltung sind die Verantwortlichkeiten für die Schutzobjekte im Inventar festzuhalten (Art. 7 Abs. 3 Bst. b ISV).

6.1 Gesamtbewertung: was eine Verdichtung verdecken kann

Viele Verfahren und Bewertungsschemata fassen das Profil am Ende zu einem Gesamtergebnis zusammen, etwa «erhöht» oder «nicht erhöht». Davon hängt in vielen Verfahren ab, ob eine vertiefte Risikoanalyse folgt. Problematisch wird es, wenn die Regel ein einzelnes kritisches Schutzziel überstimmt. In der Praxis zu beobachten sind etwa Regeln, nach denen bei der Vertraulichkeit ein einzelnes kritisches Kriterium genügt, bei Verfügbarkeit, Integrität und Nachvollziehbarkeit aber mehrere zusammenkommen müssen. Eine Anwendung mit sehr hohem Integritätsbedarf wird dann im Gesamtergebnis als «nicht erhöht» geführt. Die Risikoanalyse unterbleibt, es gelten nur die Mindestanforderungen (Kapitel 7), und das Risiko wird weder analysiert noch von der zuständigen Ebene entschieden.

Der BACS-Leitfaden geht strenger vor. Die Sicherheitsstufe «hoher Schutz» gilt, sobald an mindestens einer Stelle erhebliche Auswirkungen ausgewiesen sind. Damit bestimmt die höchste einzelne Auswirkung die Sicherheitsstufe, unabhängig davon, bei welchem Schutzziel sie auftritt. Ebenso verlangt die Methodik Grundschutz++ eine explizite Risikobetrachtung, sobald ein Geschäftsprozess bei mindestens einem Schutzziel hohen Schutzbedarf hat (BSI-Standard 300-1, Kapitel 2.11). Das hier vorgeschlagene Modell folgt dieser strengeren Regel. Auch die Definition von «Erhöhter Schutzbedarf» in Kapitel 2 beruht auf ihr. Eine weichere Regel würde dazu führen, dass die Risikoanalyse trotz sichtbarer Einzelwerte entfällt. Die Gesamtstufe steuert dabei das Verfahren, also ob eine Risikoanalyse oder ein Sicherheitskonzept erforderlich ist. Die Anforderungen selbst folgen weiterhin dem Profil je Schutzziel, sonst entsteht in den übrigen Schutzzielen Überschutz. Die Stufen des Profils legt die Organisation fest. In der Bundesverwaltung sind sie an die Schwellen der ISV für die Sicherheitsstufen anzubinden.

6.2 Vererbung ist eine Regel, kein Automatismus

Der BSI-Grundschutz bestimmt zuerst den Schutzbedarf der Geschäftsprozesse und Informationen und überträgt ihn dann auf Anwendungen, IT-Systeme, Räume und Kommunikationsverbindungen. Er verbindet damit Top-down und Bottom-up bereits auf der Ebene von Prozessen und Informationen. Auch die Methodik Grundschutz++ setzt beim Geschäftsprozess an und zieht dabei die darin verarbeiteten Informationen heran (BSI-Standard 300-1, Kapitel 2.5 und 2.6). Sie betrachtet Vertraulichkeit, Integrität und Verfügbarkeit und unterscheidet die Kategorien «normal» und «hoch». Eigene Kategorien sind zulässig, müssen aber

diesen beiden zugeordnet werden. Die Nachvollziehbarkeit führt dieses Papier darüber hinaus als eigenständiges Schutzziel. Das hier beschriebene Modell ergänzt diesen Ansatz, weil viele Anforderungen und Widersprüche erst am Schutzobjekt konkret werden (Kapitel 3). Für die Ableitung helfen vor allem die Denkprinzipien in Tabelle 4, die sich an den BSI-Grundschutz anlehnen.

Prinzip	Wirkung	Typischer Fall
Maximumprinzip	Das Zielobjekt übernimmt je Schutzziel den höchsten Schutzbedarf der Anwendungen, die es benötigen.	Server, auf dem mehrere voneinander unabhängige Fachanwendungen mit unterschiedlichem Schutzbedarf laufen.
Abhängigkeiten	Ist eine Anwendung auf die Ergebnisse einer anderen angewiesen, überträgt sich ihr Schutzbedarf je Schutzziel und im Umfang der tatsächlichen Abhängigkeit auf die liefernde Anwendung (Abschnitt 4.1).	Dienst für Referenzdaten, zentrale Schnittstellenplattform.
Kumulationseffekt	Fallen mehrere Anwendungen gleichzeitig aus, können sich ihre Einzelschäden zu einem grösseren Gesamtschaden summieren. Der Schutzbedarf des Zielobjekts liegt dann höher als der jeder einzelnen Anwendung.	Virtualisierungsplattform, Identitätsdienst, zentrales Netz.
Verteilungseffekt	Eine einzelne Komponente erhält einen tieferen Schutzbedarf als die Anwendung, wenn sie nur weniger kritische Teile bedient oder wenn andere Komponenten ihren Ausfall übernehmen. Das betrifft in der Regel nur die Verfügbarkeit.	Einer von mehreren gleichwertigen Servern einer Anwendung.

Tabelle 4: Denkprinzipien für die Vererbung des Schutzbedarfs (in Anlehnung an BSI-Standard 200-2, Kapitel 8.2)

Diese Prinzipien sind Denkmodelle, keine Rechenregeln. Vor allem der Verteilungseffekt verlangt eine Begründung, weil er tiefere Einstufungen erlaubt. Er gilt nur für die einzelne Komponente, nicht für die Anwendung oder die Leistung.

Prüfnachweis: Für eine gemeinsam genutzte Plattform, etwa eine Virtualisierungsumgebung, ist vorzulegen, welche Anwendungen auf ihr laufen und wie ihr Schutzbedarf daraus abgeleitet wurde. Wird eine einzelne Komponente wegen Redundanz tiefer eingestuft, ist zu belegen, dass die Redundanz funktioniert, etwa mit einem Umschalttest.

6.3 Abweichungen müssen entschieden, nicht geglättet werden

Bei der Zusammenführung zeigen sich zwei Arten von Differenzen.

Die erste liegt zwischen Anforderungen aus verschiedenen Quellen. Im Leitbeispiel stuft die Schutzbedarfsanalyse der Anwendung die Integrität als normal ein, aus dem Entscheidprozess folgt «hoch» (Tabellen 1 und 3). Solche Widersprüche entscheidet die zuständige Instanz bei der Einstufung selbst.

Die zweite liegt zwischen erforderlichem und erreichtem Schutz, wie die folgenden Beispiele zeigen.

- Das Profil verlangt hohe Integrität, und daraus folgt die Anforderung, Veränderungen zu verhindern oder zu erkennen (Kapitel 7). Die Anwendung prüft Eingaben aber nicht auf Plausibilität, und Änderungen an Entscheidgrundlagen brauchen keine Freigabe.

- Eine Information ist VERTRAULICH klassifiziert, die eingesetzte Kollaborationslösung erfüllt die Behandlungsvorgaben jedoch nicht.
- Der Dienstleister sichert weniger zu, als das Profil verlangt.
- Umgekehrt wird eine Anwendung hochverfügbar betrieben, obwohl kein Prozess das verlangt.

Abweichungen zwischen erforderlichem und erreichtem Schutz dürfen nicht durch eine stillschweigend angepasste Einstufung verschwinden. Sie sind als Lücke sichtbar zu machen und auf der zuständigen Ebene zu entscheiden. Betrifft eine Abweichung Informationen mehrerer Eigner, legt die SO-V sie dieser Ebene vor, und die betroffenen Eigner werden beigezogen. Zur Wahl stehen, die Anforderung umzusetzen, eine Alternative zu wählen, eine ausgleichende Massnahme zu treffen oder das Restrisiko bewusst zu akzeptieren. Zwingende rechtliche Vorgaben und nicht abdingbare Anforderungen des gewählten Verfahrens bleiben dabei einzuhalten. Im Grundschutz++ etwa lassen sich MUSS-Anforderungen nicht durch eine Risikoakzeptanz ersetzen (BSI-Standard 300-1, Kapitel 4.1.2). Das ISG verlangt ausdrücklich, dass getragene Risiken nachweislich akzeptiert werden (Art. 8 Abs. 3 ISG). Kosten und Aufwand sind legitime Argumente. Sie gehören aber in den Risikoentscheid und nicht in die Einstufung. Umgekehrt ist auch ein deutlicher Überschutz eine Abweichung, die eine Entscheidung verdient. Sie lautet entweder beibehalten, weil es gute Gründe gibt, oder abbauen.

Eine Schutzbedarfsfeststellung ist wirksam, wenn Widersprüche und Abweichungen einen nachvollziehbaren Entscheid auslösen, statt zu verschwinden.

Prüfnachweis: Für ein Schutzobjekt mit einer bekannten Abweichung zwischen erforderlichem und erreichtem Schutzniveau ist der Entscheid vorzulegen, mit der gewählten Option, der entscheidenden Ebene und, bei akzeptiertem Restrisiko, der Begründung.

7 Vom Schutzbedarf zur Sicherheitsanforderung

Eine Einstufung allein schützt nichts. Ihre Wirkung entsteht dort, wo aus ihr konkrete und überprüfbare Anforderungen folgen. Im Sicherheitsverfahren des Bundes gilt der IT-Grundschutz der Bundesverwaltung für jedes Schutzobjekt als Mindestniveau. Bei nicht erhöhtem Schutzbedarf genügt er. Bei erhöhtem Schutzbedarf folgen ein Informationssicherheits- und Datenschutzkonzept mit Risikoanalyse, schutzobjektspezifische Massnahmen, die Beurteilung der Restrisiken und die Freigabe vor dem Betrieb.

Unabhängig vom gewählten Verfahren lässt sich die Wirkung als Kette beschreiben (Abbildung 4). Sie macht den Wirksamkeitsnachweis, den das Bundesrecht an anderer Stelle verlangt (Kapitel 9), zum festen Glied je Schutzobjekt. Die Kette besteht aus sechs Gliedern.

1. **Schutzbedarf:** Profil je Schutzziel, mit Quelle und Begründung.
2. **Sicherheitsanforderung:** die konkrete, überprüfbare Vorgabe, was am Schutzobjekt erreicht sein muss, ohne Festlegung auf eine bestimmte Lösung.
3. **Massnahme:** die gewählte technische oder organisatorische Umsetzung.
4. **Restrisiko:** was trotz Massnahme verbleibt und beurteilt werden muss.
5. **Entscheid und Freigabe:** durch die zuständige Ebene, vor dem Betrieb.
6. **Wirksamkeitsnachweis:** Beleg, dass die Massnahme im Betrieb wirkt und die Anforderung erfüllt.



Abbildung 4: Die Kette vom Schutzbedarf zum Wirksamkeitsnachweis, am Leitbeispiel (eigene Darstellung)

7.1 Anforderungen sind nicht dasselbe wie Massnahmen

Hohe Vertraulichkeit bedeutet nicht automatisch Verschlüsselung, und hohe Verfügbarkeit nicht automatisch Redundanz. Die Anforderung beschreibt das Ziel, die Massnahme den gewählten Weg dorthin. Nur wer beides trennt, kann prüfen, ob eine weniger aufwendige Alternative das Ziel ebenso erreicht oder ob eine Massnahme es verfehlt. Tabelle 5 zeigt die Übersetzung je Schutzziel.

Schutzziel	Mögliche Sicherheitsanforderung	Mögliche Massnahmen und Nachweise
Vertraulichkeit	Zugriff nur für berechtigte Rollen. Weitergabe und Veröffentlichung nur über freigegebene Kanäle und an freigegebene Ziele.	Identitäts- und Berechtigungsmanagement (IAM), Need-to-Know-Prinzip, Verschlüsselung, Data Loss Prevention (DLP), Freigabeprozess für Publikationen, Vertragsklauseln, Rezertifizierung der Berechtigungen.
Integrität	Veränderungen, die unberechtigt oder unbeabsichtigt erfolgen, werden verhindert oder erkannt.	Freigaben, Funktionstrennung, Plausibilisierungen, Change-Management, Hash- und Signaturverfahren, Abstimmungen.
Verfügbarkeit	Das Schutzobjekt ist innerhalb seines technischen Wiederanlaufziels und mit Daten bis zum festgelegten Wiederherstellungspunkt wieder verfügbar, sodass die Leistung auf dem Mindestleistungsniveau fortgeführt werden kann.	Redundanz, Datensicherung und Wiederherstellung, Notbetrieb, Tests mit gemessener Wiederanlaufzeit, Service Level Agreements (SLA) mit Dienstleistern.

Schutzziel	Mögliche Sicherheitsanforderung	Mögliche Massnahmen und Nachweise
Nachvollziehbarkeit	Sicherheitsrelevante Handlungen und Bearbeitungen der Informationen sind einer Identität und einem Zeitpunkt zuzuordnen, auch bei privilegiertem Zugriff.	Protokollierung, manipulationsgeschützte Protokolle, verlässliche Zeitquelle, Auswertung, Aufbewahrung.

Tabelle 5: Übersetzung des Schutzbedarfs in Anforderungen und Massnahmen (eigene Darstellung)

Am Leitbeispiel aus Abschnitt 1.3 lässt sich die Kette für eine der drei Lücken vollständig nachzeichnen (Abbildung 4).

Vom Befund zum Wirksamkeitsnachweis im Leitbeispiel

Befund. Der Export bringt VERTRAULICH klassifizierte Dossiers in eine Auswertungsplattform, die nur für INTERN freigegeben ist (Tabelle 1).

Anforderung und Massnahme. Exportierte Inhalte müssen für die Zielumgebung zulässig sein. Die Auszüge werden deshalb vor dem Export anonymisiert und auf weitere Geheimhaltungsgründe geprüft. Die Anonymisierung allein genügt nicht, denn eine Klassifizierung kann auch auf Inhalten ohne Personenbezug beruhen, etwa auf Geschäftsgeheimnissen von Gesuchstellern. Ob die Auszüge für die Zielumgebung zulässig sind, beurteilt der Informationseigner (Abschnitt 5.3).

Restrisiko, Entscheid und Nachweis. Durch Verknüpfung mit anderen Daten auf der Auswertungsplattform können die Auszüge wieder einen Personenbezug erhalten oder weitere schutzwürdige Informationen offenlegen (Abschnitt 5.5). Die zuständige Ebene akzeptiert dieses Restrisiko und gibt den Export frei, mit den Bedingungen, dass die Anonymisierung wirksam ist und die Auszüge höchstens INTERN klassifiziert sind. Exportstichproben über einen festgelegten Zeitraum und eine periodische Prüfung der Verknüpfbarkeit in der Zielumgebung belegen die Anonymisierung und die Einhaltung der Freigabebedingungen. Als Orientierung für eine wirksame Anonymisierung dient der TOM-Leitfaden des EDÖB.

Die anderen beiden Lücken. Für die Integrität folgen Plausibilisierungen und Freigaben. Für die Nachvollziehbarkeit gilt die Anforderung aus Tabelle 5, wonach Bearbeitungen einer Identität und einem Zeitpunkt zuzuordnen sind, auch bei privilegiertem Zugriff. Der privilegierte Zugang des Betreibers ist für den Betrieb nötig und als solcher keine Abweichung. Die Lücke liegt darin, dass Änderungen an Entscheidgrundlagen über diesen Zugang weder protokolliert noch fachlich freigegeben werden. Eine manipulationsgeschützte Protokollierung, deren Einträge ausserhalb des Einflussbereichs des Betreibers aufbewahrt werden, schliesst die Nachvollziehbarkeitslücke. Der Wirksamkeitsnachweis hat drei Teile. Eine Teständerung über einen privilegierten Zugang wird vollständig und zurechenbar protokolliert. Ein Versuch, den Eintrag mit den Rechten des Betreibers nachträglich zu verändern oder zu löschen, scheitert. Und die regelmässige Auswertung dieser Protokolle ist für einen festgelegten Zeitraum belegt. Solange die Lücke besteht, entscheidet die zuständige Ebene über das Restrisiko (Abschnitt 6.3).

8 Schnittstellen: Schutzbedarf als Bindeglied

Seine Wirkung entfaltet der Schutzbedarf an den Schnittstellen. Dort entscheidet sich, ob eine fachliche oder rechtliche Anforderung in der Sicherheitssteuerung ankommt. Tabelle 6 zeigt für die wichtigsten Schnittstellen, was der Schutzbedarf dort liefert und woran sich erkennen lässt, ob die Verbindung funktioniert.

Schnittstelle	Was der Schutzbedarf liefert	Erkennbar an
Risikoanalyse	Welche Schutzziele wie wichtig sind und welche Abweichungen einen Risikoentscheid verlangen. Je nach Verfahren löst erhöhter Schutzbedarf eine vertiefte Risikoanalyse aus, etwa nach BSI-Standard 200-3 oder ISO/IEC 27005.	Wo das Verfahren es vorsieht, liegt für jedes Schutzobjekt mit erhöhtem Schutzbedarf eine aktuelle Risikoanalyse vor.
Identitäts- und Berechtigungsmanagement	Anforderungen an die Prüfung von Identitäten, an das Rollenmodell, an privilegierte Zugriffe, an die regelmässige Überprüfung von Berechtigungen und an die Protokollierung.	Häufigkeit der Berechtigungsüberprüfung und Umfang der Protokollierung entsprechen dem Profil.
Architektur und Change	Das verbindliche Schutzbedarfsprofil und die Sicherheitsanforderungen, aber keine fertige Lösung für Netzzonen, zulässige Datenflüsse oder die Wahl der Plattform. Wesentliche Änderungen an Architektur, Datenflüssen oder Funktionen lösen eine Neubewertung aus.	Daten mit erhöhtem Schutzbedarf fliessen nur in Zonen, die die mitwandernden Anforderungen erfüllen (Abschnitt 5.4), oder die Ausnahme ist entschieden. Changes mit Auswirkung auf den Schutzbedarf sind neu bewertet.
Kommunikation und Publikation	Welche Informationen nicht öffentlich werden dürfen, auch nicht in Präsentationen, Downloads oder Metadaten.	Ein Freigabeprozess für Veröffentlichungen besteht. Stichproben auf der Website zeigen keine unbeabsichtigt veröffentlichten schutzwürdigen Inhalte. Festgestellte Abweichungen werden bereinigt.
Outsourcing und Cloud	Anforderungen für Verträge, Nachweise, Berichterstattung, Standorte, Subunternehmer und Ausstieg. Grundlage dafür, Dienstleister nach dem Schutzbedarfsprofil der ausgelagerten Leistung zu kategorisieren, also nach Kritikalität und Wert der bearbeiteten Informationen (vgl. Beitrag IT-Outsourcing & Governance dieser Reihe).	Vertragliche Zusagen sind dem Profil gegenübergestellt. Abweichungen sind durch einen Risikoentscheid geklärt.
Business Continuity Management	Verbindet Kritikalität und Wiederanlauf mit der Frage, ob Daten nach einer Wiederherstellung noch integer und vollständig sind.	Wiederherstellungstests prüfen auch Integrität und Vollständigkeit der Daten, nicht nur den Start der Anwendung.
Datenschutz und Aufbewahrung	Sicherheitsrelevante Ergebnisse aus Datenschutz-Folgenabschätzung und Verzeichnis der Bearbeitungstätigkeiten (Art. 12 DSG) sowie Aufbewahrungs- und Löschfristen als Teil des Profils.	Sicherheitsmassnahmen aus der Folgenabschätzung sind im Sicherheitskonzept wiederzufinden.

Schnittstelle	Was der Schutzbedarf liefert	Erkennbar an
KI-Anwendungen	Welche Informationen ein KI-System lesen, verknüpfen und weitergeben darf, einschliesslich des Risikos der Aggregation. Vgl. Beitrag KI-Governance dieser Reihe.	Für KI-Anwendungen sind die zugänglichen Datenbestände nach Schutzbedarf begrenzt, und die Zugriffe sind nachvollziehbar.
Berichterstattung und Eskalation	Welche Abweichungen zwischen Soll und Ist die Leitung kennen und entscheiden muss.	Offene Abweichungen bei erhöhtem Schutzbedarf erscheinen im Bericht an die Leitung.

Tabelle 6: Schnittstellen des Schutzbedarfs und mögliche Prüfnachweise (eigene Darstellung)

Ob diese Verbindungen im Betrieb tatsächlich tragen, lässt sich nicht aus Vorgaben und Konzepten ablesen. Das zeigt erst der Wirksamkeitsnachweis (Kapitel 9).

9 Nachweis der Wirksamkeit: Rückweg und Verfahren

Ein dokumentierter Schutzbedarf sagt, was eine Organisation für erforderlich hält. Entscheidend ist aber, ob er im Betrieb tatsächlich erreicht wird. Wirksamkeit ist dabei auf zwei Ebenen nachzuweisen. Am Schutzobjekt wird die Erfüllung der abgeleiteten Anforderungen belegt. Auf Ebene des Verfahrens wird gezeigt, dass die Schutzbedarfsfeststellung selbst dauerhaft funktioniert.

Anforderungen werden von oben nach unten weitergegeben. Ob sie erfüllt sind, muss in umgekehrter Richtung belegt werden. Auf diesem Rückweg wird zuerst abgeglichen, ob die Zusagen der unteren Glieder, etwa die vertraglichen Zusagen eines Dienstleisters, zu den Anforderungen passen. Dann wird nachgewiesen, dass sie tatsächlich erfüllt werden. Der Abgleich ist Voraussetzung für den Nachweis, ersetzt ihn aber nicht (vgl. Beitrag zum Business Continuity Management dieser Reihe). Dieser Rückweg ist erst geschlossen, wenn das unterste Glied, an das Anforderungen weitergegeben wurden, etwa eine Plattform oder ein Dienstleister, belegen kann, dass es das geforderte Schutzniveau tatsächlich trägt. Ist eine Anforderung bewusst nicht vollständig erfüllt, tritt am Schutzobjekt der dokumentierte Risikoentscheid an die Stelle des Erfüllungsnachweises. Er belegt einen Entscheid, keine Erfüllung, und bleibt deshalb als offene Abweichung sichtbar (Abschnitt 6.3).

In der Bundesverwaltung ist jährlich zu prüfen, ob eine wesentliche Änderung eingetreten ist, die das Sicherheitsverfahren erneut auslöst (Art. 27 Abs. 5 und 6 ISV). Die Wirksamkeit der Massnahmen wird über einen jährlichen Kontroll- und Auditplan risikobasiert überprüft (Art. 13 ISV). Bei der Zusammenarbeit mit Dritten sind die Massnahmen vertraglich festzuhalten und ihre Umsetzung angemessen zu überprüfen (Art. 9 ISG). Für Informatikmittel der Stufe «sehr hoher Schutz» schreibt das ISG eine periodische Prüfung der Wirksamkeit ausdrücklich vor (Art. 18 Abs. 3 ISG).

Für die Ebene des Verfahrens hilft die in der Prüfpraxis übliche Unterscheidung zweier Fragen, die auch die anderen Beiträge dieser Reihe verwenden. Design Effectiveness fragt, ob das Verfahren geeignet gestaltet ist. Operating Effectiveness fragt, ob es über einen Zeitraum tatsächlich angewendet wird und ob sich das belegen lässt.

Design Effectiveness	Operating Effectiveness
Die kritischsten Informationsbestände sind mit benanntem Informationseigner erfasst. Ebenso ist festgelegt, was ausdrücklich nicht kritisch ist.	Die Liste ist aktuell. Stichproben bestätigen die dokumentierten Ablageorte, auch mit Blick auf öffentlich Zugängliches. Festgestellte Abweichungen werden erfasst und bereinigt.
Schutzobjekte, Informationseigner, SO-V und Schutzziele sind definiert. Top-down- und Bottom-up-Anforderungen werden in einem definierten Schritt durch eine benannte Stelle, etwa die SO-V, zusammengeführt.	Neue und geänderte Schutzobjekte werden fachlich begründet bewertet. Business-Impact-Analyse, Schutzbedarf, Klassifizierung und Datenschutzbeurteilung sind stimmig, oder Abweichungen sind entschieden.
Die Gesamtbewertung überstimmt kein einzelnes kritisches Schutzziel. Kriterien für die Anwendung von Vererbung, Kumulations- und Verteilungseffekt sowie Aggregation sind festgelegt.	Wo das gewählte Verfahren bei erhöhtem Schutzbedarf eine Risikoanalyse verlangt, ist diese durchgeführt worden, auch wenn nur ein einzelnes Schutzziel erhöht eingestuft ist. Gemeinsame Plattformen und Orte, an denen Daten zusammenfliessen, sind auf gebündelte Abhängigkeiten geprüft.
Erhöhter Schutzbedarf löst definierte Anforderungen oder Risikoentscheide aus. Hohe Einstufungen sind begründet.	Für erhöhte Einstufungen bestehen zusätzliche Schutzmassnahmen oder dokumentierte Restrisikoentscheide. Aufwendige Massnahmen lassen sich auf eine Anforderung zurückführen.
Wesentliche Änderungen und absehbare Wertwechsel im Lebenszyklus der Information lösen eine Neubewertung aus.	Changes, neue Anbieter, geänderte Datenflüsse oder Wertwechsel im Lebenszyklus führen nachweisbar zu überprüften und bei Bedarf angepassten Einstufungen.

Tabelle 7: Design und Operating Effectiveness der Schutzbedarfsfeststellung (eigene Darstellung)

Prüfnachweis: Für ein Schutzobjekt mit erhöhtem Schutzbedarf sind drei Unterlagen nebeneinanderzulegen, nämlich das Schutzbedarfsprofil, die abgeleiteten Anforderungen und für jede betrachtete Anforderung der jüngste geeignete Beleg ihrer Wirksamkeit. Beispiele sind eine Rezertifizierung der Berechtigungen für die Vertraulichkeit oder eine Auswertung der Protokolle für die Nachvollziehbarkeit. Festzuhalten ist, ob alle Anforderungen oder eine begründete Auswahl geprüft werden. Bei wiederkehrenden Kontrollen muss der betrachtete Zeitraum erkennbar sein. Für bewusst nicht erfüllte Anforderungen tritt der dokumentierte Risikoentscheid an die Stelle des Belegs. Fehlt für eine Anforderung sowohl der Beleg als auch der Risikoentscheid, ist weder die Erfüllung belegt noch die Abweichung entschieden. Die Lücke ist dann nicht gesteuert.

10 Leitfragen für Leitungs- und Aufsichtsgremien

Die folgenden Fragen eignen sich für eine Standortbestimmung. Sie zielen nicht auf das Formular, mit dem der Schutzbedarf erhoben wurde, sondern darauf, ob die Organisation erklären kann, warum sie welche Informationen wie schützt.

Zum Wert der Informationen

- Wissen wir, welche Informationen für uns am kritischsten sind, wer für sie verantwortlich ist und wo sie liegen, auch bei Dienstleistern, in der Cloud und öffentlich zugänglich?
- Wissen wir, wo wir zu wenig und wo wir mehr als nötig schützen, und was uns beides kosten kann?

Zur Zusammenführung

- Sind die Anforderungen aus Geschäftsleistungen und Prozessen mit dem Schutzbedarf der unterstützenden Anwendungen für alle Schutzziele abgeglichen, nicht nur die zeitbezogene Kritikalität aus der Business-Impact-Analyse mit der Verfügbarkeit?
- Werden die Anforderungen einer Leistung je Schutzziel und im Umfang der tatsächlichen Abhängigkeit auf unterstützende Schutzobjekte übertragen, statt pauschal?
- Ist für jedes Schutzobjekt benannt, wer die Anforderungen zusammenführt, und auf welcher Ebene Widersprüche entschieden werden?
- Werden Klassifizierung, Datenschutz, Amts-, Berufs- und Geschäftsgeheimnisse sowie vertragliche Zusagen als eigene Quellen von Anforderungen berücksichtigt?
- Gelten diese Anforderungen auch dort, wohin die Informationen fliessen?
- Verhindert unser Verfahren, dass ein einzelnes kritisches Schutzziel durch eine Gesamtbewertung relativiert wird?

Zu Entscheid und Nachweis

- Werden Abweichungen zwischen erforderlichem und erreichtem Schutzniveau sichtbar gemacht und auf der zuständigen Ebene entschieden, statt durch eine geänderte Einstufung aufgelöst?
- Wird der Schutzbedarf neu beurteilt, wenn sich Systeme, Datenflüsse, Anbieter oder der Wert der Information selbst ändern?
- Können wir für unsere kritischsten Schutzobjekte mit einem Wirksamkeitsnachweis belegen, dass die abgeleiteten Anforderungen im Betrieb erfüllt sind?

Wo diese Fragen offenbleiben, sind Leitung und Aufsicht gefordert, Klarheit zu schaffen, die notwendigen Entscheide herbeizuführen und sich die Wirksamkeit des Schutzes nachweisen zu lassen.

Fazit

Schutz beginnt beim Wert. Wer nicht weiss, welche Informationen für die Organisation wirklich zählen, schützt oft nach Gewohnheit, nämlich zu viel dort, wo es wenig bewirkt, und zu wenig dort, wo der Schaden gross wäre. Am Anfang steht deshalb nicht ein besseres Formular für die Schutzbedarfsanalyse, sondern Klarheit darüber, welche Informationen kritisch sind.

Schutzbedarf entsteht aus mehreren Perspektiven. Top-down werden Anforderungen aus der Bedeutung von Geschäftsleistungen und Prozessen abgeleitet, Bottom-up aus dem Wert der Information einschliesslich Klassifizierung, Datenschutz und weiterer Schutzpflichten. Beide Perspektiven müssen bei Anwendungen, Systemen, Plattformen und Dienstleistern zu einem konsistenten Schutzbedarfsprofil zusammengeführt werden. Dieses Profil ist nicht statisch. Es ist neu zu beurteilen, wenn sich Leistungen, Informationen, Abhängigkeiten oder der Wert der Information selbst ändern.

Der Nutzen der Schutzbedarfsfeststellung liegt nicht in der Einstufung, sondern in den Entscheidungen, die sie auslöst. Ein hoher Schutzbedarf ohne nachvollziehbare Konsequenz für Anforderungen oder Risikoentscheide hat kaum Steuerungswirkung. Eine Anforderung ohne Umsetzung bleibt Absicht. Eine Massnahme ohne Wirksamkeitsnachweis bleibt Behauptung. Vom Informationswert zur wirksamen Sicherheitsanforderung führt deshalb eine durchgängige Kette (Abbildungen 3 und 4). Der Wert wird erkannt, Anforderungen werden zusammengeführt und abgeleitet, Massnahmen umgesetzt, Risiken entschieden und die Wirksamkeit nachgewiesen.

Quellen

Bundesamt für Cybersicherheit BACS, Leitfaden zur Schutzbedarfsanalyse, Version 1.0 vom 14. Oktober 2024 (P041), publiziert durch das SEPOS.

Bundesamt für Cybersicherheit BACS, Bericht zu den Datenanalysen nach dem Cyberangriff auf die Firma Xplain, 7. März 2024.

Bundesamt für Sicherheit in der Informationstechnik BSI, BSI-Standard 200-2 IT-Grundschutz-Methodik, insbesondere Kapitel 8.2 (Schutzbedarfsfeststellung, Schadensszenarien, Vererbung), und BSI-Standard 200-3 Risikoanalyse auf der Basis von IT-Grundschutz. Ergänzend: IT-Grundschutz-Kompendium, Edition 2023, Baustein OPS.1.1.5 Protokollierung.

Bundesamt für Sicherheit in der Informationstechnik BSI, BSI-Standard 300-1 Methodik Grundschutz++, Version 1.0 vom 20. Oktober 2026, insbesondere Kapitel 2.5, 2.6, 2.11 und 4.1.2.

Bundesgesetz über den Datenschutz (Datenschutzgesetz, DSG, SR 235.1) vom 25. September 2020, insbesondere Art. 5, 6 Abs. 4, 8, 12 und 22.

Bundesgesetz über die Informationssicherheit beim Bund (Informationssicherheitsgesetz, ISG, SR 128) vom 18. Dezember 2020, insbesondere Art. 5, 6, 8, 9, 11, 13, 16, 17 und 18.

Eidgenössische Finanzmarktaufsicht FINMA, Aufsichtsmitteilung 03/2024 zu Erkenntnissen aus der Cyber-Risikoaufsicht, 7. Juni 2024.

Eidgenössischer Datenschutz- und Öffentlichkeitsbeauftragter EDÖB, Leitfaden zu den technischen und organisatorischen Massnahmen des Datenschutzes (TOM), 15. Januar 2024, insbesondere Abschnitt 5.3 (Anonymisierung).

Informationssicherheitsverordnung (ISV, SR 128.1) vom 8. November 2023, insbesondere Art. 7, 13, 16, 19, 20, 25 und 27 bis 29.

ISO 22301:2019 mit Amendment 1:2024, Business continuity management systems – Requirements. Eine dritte Ausgabe befindet sich in Entwicklung.

ISO/IEC 27001:2022 mit Amendment 1:2024 und ISO/IEC 27002:2022, insbesondere Control 5.12 (Klassifizierung).

ISO/IEC 27005:2022, Information security risk management.

National Institute of Standards and Technology NIST, FIPS 199 Standards for Security Categorization of Federal Information and Information Systems (2004), und NIST SP 800-60 zur Kategorisierung nach Informationstypen.

Schweizerisches Strafgesetzbuch (StGB, SR 311.0), Art. 320 (Amtsgeheimnis) und Art. 321 (Berufsgeheimnis).

Staatssekretariat für Sicherheitspolitik SEPOS, Sicherheitsverfahren (sepos.admin.ch/de/sicherheitsverfahren), Stand August 2026.

Verordnung über den Datenschutz (Datenschutzverordnung, DSV, SR 235.11) vom 31. August 2022, insbesondere Art. 2 und 4.

Hinweis

Dieses Whitepaper gibt meine persönliche fachliche Einschätzung wieder, nicht die einer Behörde oder Aufsicht. Es beruht auf öffentlichen Quellen, ohne nicht öffentliche Informationen. Unverändert weitergeben und mit Quellenangabe zitieren erlaubt; kommerzielle Verwertung und Bearbeitung nur mit vorheriger Zustimmung.



Fragen und Austausch willkommen

carsten@carsten-beck.ch

Alle Beiträge der Reihe

carsten-beck.ch/publikationen

linkedin.com/in/carstenbeck-grc