2 Vergleich der Begrifflichkeiten

Dass man auf der Basis schwammiger Begriffe hervorragend, kontrovers und lange *diskutieren* kann ist eine Binsenweisheit; dass man unter diesen Voraussetzungen kaum aussagekräftige *Ergebnisse* erzielen, aber beliebig viel Ressourcen investieren kann – ebenso.

Glossar

Wie auch immer – aus ökonomischer und aus methodischer Sicht erscheint es sinnvoll, in der eigenen Organisation ein Begriffsglossar zum Thema Informationssicherheit anzulegen und sich in jedem weiteren Dokument (Leitlinien, Konzepte,….) darauf zu beziehen.

Meist beginnt man allerdings als Sicherheitsverantwortlicher nicht auf der grünen Wiese, sondern muss sich in einer gewachsenen Management-Struktur bewegen, die den Standards mehr oder weniger entspricht. Ein Problem liegt zumeist schon in der verwendeten Terminologie, die von veröffentlichen Quellen abweicht. Strebt man die Konformität zu einem der Standards an, muss man sich aber zwangsläufig mit der Begriffswelt dieses Standards auseinander setzen.

Wir wagen deshalb hier den Versuch,

- die klassischen IT-Sicherheitsbegriffe aus der Praxis,
- die Begriffswelt der ISO 27001 (im Folgenden immer als „der Standard“ bezeichnet), sowie
- die Begrifflichkeiten des IT-Grundschutzes

unter einen Hut zu bringen bzw. für Vergleichbarkeit zu sorgen.

Wir werden diese Aufgabe angehen, indem wir den Sicherheitsprozess Revue passieren lassen und auf dieser Wegstrecke die anfallenden Begriffe aus den oben genannten Quellen einander näher bringen. In der Marginalien-Spalte deuten wir den Bezug wie folgt an:

(K)	Klassische IT-Sicherheitsbegriffe.
(ISO)	Begriffe aus der ISO 27000-Reihe.
(GS)	Begriffe des IT-Grundschutzes.

Wer sich in den Begrifflichkeiten bereits gut auskennt, kann die Abschnitte 2.1 bis 2.4 beim Lesen überspringen.

H. Kersten, J. Reuter, K.-W. Schröder,
IT-Sicherheitsmanagement nach ISO 27001 und Grundschutz, Edition <kes>,
DOI 10.1007/978-3-658-01724-8_2, © Springer Fachmedien Wiesbaden 2013

Werfen Sie jedoch auf jeden Fall noch einen Blick auf den wichtigen Abschnitt 2.5 aber der Seite 41.

2.1 Organisation, Werte und Sicherheitsziele

Organisation

Mit dem Wort *Organisation* meinen wir in diesem Buch jede Art von Institution wie z. B. Unternehmen, Behörde, Verband oder Verein – aber auch Teile derselben, ausgewählt z. B. nach organisatorischen Gesichtspunkten (Abteilung, Bereich, usw.), nach territorialen Gesichtspunkten (Niederlassung, Geschäftsstelle usw.) oder nach nationalen Gesichtspunkten (Landesorganisationen).

Informationswerte

Ausgangspunkt der Diskussion sind die *Werte* (Assets) einer Organisation, speziell *die Informationswerte* (Information Assets).

(K) Klassischerweise beschränkt man sich auf Informationswerte im engeren Sinne wie Informationen, Daten, Dateien, Datenträger. Hierfür definiert man Sicherheitsziele. Hinzu kommen meist IT-Systeme und Netze, innerhalb derer solche Informationswerte gespeichert, verarbeitet und übertragen werden. Auch für diese Systeme und Netze gibt man Sicherheitsziele vor.

(ISO) Der Standard versteht unter Werten alles, was aus Sicht der Organisation eine Bedeutung für die Geschäftstätigkeit hat. Beispiele:

- Typ *Information*[22]:
  - Informationen aus der Geschäftstätigkeit der Organisation, Daten, Dateien, Verzeichnisse, Datenbanken.
  - Eigene Dokumente wie Verträge, Verfahrens- und Arbeitsanweisungen, Schulungsmaterial, Notfall-Handbücher, Wiederanlaufpläne.
  - Externe Dokumente wie System-Beschreibungen und Nutzerhandbücher.
  - Alle Arten von Aufzeichnungen bzw. Protokollen.
- Typ *Software*[23]: Anwendungssoftware, System-Software, Entwicklungswerkzeuge.

---

22 In den meisten Quellen zum Thema Informationssicherheit wird nicht zwischen *Informationen* und *Daten* unterschieden.

- *Physische Werte*: Technische Komponenten wie Rechner, Firewalls, Gateways, Router, Netzwerk-Kabel, Datenmedien (z. B. Bänder, CD, DVD).
- *Infrastrukturen*: Server-Räume, Rechenzentren, Versorgungen aller Art.
- Typ *Dienstleistung,* und zwar solche, die man selbst erbringt, und auch solche, die man nutzt: RZ- und Telekommunikations-Services, Datenübertragung, Klimatisierung, Beleuchtung, Stromversorgung.
- *Mitarbeiter* mit Qualifikationen, Fähigkeiten, Erfahrungen und zugewiesenen Funktionen.
- *Sonstige („intangible") Werte* wie z. B. das Ansehen (Image) und die Kreditwürdigkeit einer Organisation.

Man erkennt, dass zu den Werten auch solche gerechnet werden, die nicht unmittelbar Informationen, Daten oder IT darstellen.

(GS) Beim IT-Grundschutz sind *IT-Anwendungen* Ausgangspunkt der Überlegungen: Sie werden zur Durchführung bestimmter Fachaufgaben (Geschäftsprozesse) eingesetzt und bedienen sich der IT-Systeme, Netzwerke und IT-Räume[24] und des Personals einer Organisation. Die Gesamtheit aus infrastrukturellen, organisatorischen, personellen und technischen Komponenten, die zur Erfüllung einer Fachaufgabe dienen, wird als *IT-Verbund* oder Informationsverbund bezeichnet und charakterisiert die Werte einer Organisation.

Fazit Vergleicht man die drei Quellen (K), (ISO) und (GS), stellt man fest, dass bei (ISO) der Begriff *Wert* am weitesten gefasst ist.

Sicherheitsziele

Für die Werte einer Organisation bestehen unterschiedliche Ziele, etwa

- die Ordnungsmäßigkeit der *Datenverarbeitung* (die IT läuft im Einklang mit allen geltenden Vorschriften und Richtlinien),

---

23 Diese Werte werden in der ISO 27002 separat aufgeführt, obwohl sie natürlich unter Werte vom Typ *Information* fallen.

24 Die benutzte räumliche Infrastruktur, in der die übrigen Werte installiert sind, betrieben oder aufbewahrt werden.

– die (Rechts-)Verbindlichkeit z. B. von Vereinbarungen bzw. *Dokumenten*,
– die Rechtsgültigkeit von elektronischen *Rechnungen* – und nicht zuletzt
– die Sicherheit der *Informationswerte*.

Unter die *Sicherheitsziele* für Informationswerte fallen unter anderem die bekannten Ziele der Vertraulichkeit, Integrität und Verfügbarkeit. Wir schicken voraus:

Als *Subjekte* bezeichnen wir Individuen, Organisationseinheiten, Geschäftsprozesse oder andere Entitäten, die auf Werte in verschiedenem Sinne zugreifen können: entwickeln, erstellen, speichern, lesen, verändern, löschen, übertragen, beschaffen, installieren, bereit stellen, nutzen, warten usw.[25]

(ISO) Wegen der sehr allgemeinen Begriffsbildung eines Wertes muss man die für die Informationssicherheit charakteristischen Ziele Vertraulichkeit, Verfügbarkeit und Integrität ebenfalls etwas allgemeiner fassen:

– Unter der *Verfügbarkeit* eines Wertes versteht der Standard die Eigenschaft des Wertes, für jedes autorisierte Subjekt bei Bedarf zugreifbar zu sein.
– Mit der *Integrität* eines Wertes ist im Standard die Eigenschaft der Richtigkeit und Vollständigkeit des Wertes gemeint, autorisierte Änderungen sind nur von befugten Subjekten durchzuführen.
– Die *Vertraulichkeit* eines Wertes vom Typ *Information* ist ihre Eigenschaft, nur autorisierten Subjekten bekannt zu sein.

(K) In der klassischen IT-Sicherheit sind zwei dieser Begriffe etwas enger gefasst: *Verfügbarkeit* und *Integrität* beziehen sich fast immer nur auf Daten, IT-Systeme und Netze.

(GS) Beim IT-Grundschutz werden die drei genannten Sicherheitsziele als *Grundwerte* der IT-Sicherheit bezeichnet – es wird allerdings keine Definition angegeben. Vielmehr wird im Zusammenhang mit *Vertraulichkeit* und *Integrität* meist von Daten bzw. Informationen und Programmen, bei der *Verfügbarkeit* von IT-Anwendungen und IT-Systemen gesprochen.

---

[25] Nicht jeder dieser Zugriffe ist für alle Arten von Werten sinnvoll definierbar; außerdem ist die Aufzählung nicht als abschließend anzusehen.

Sonstige Ziele

Generell ist festzustellen, dass an vielen Stellen in der Praxis weitere Sicherheitsziele hinzukommen können – wie z. B.

- die Authentizität von Subjekten,
- die Zuweisbarkeit von Handlungen zu Subjekten,
- die Nicht-Abstreitbarkeit von Zugriffen und
- die Zuverlässigkeit von Services.

Im Standard wird dies ausdrücklich akzeptiert, d. h. die Organisation ist bei Anwendung der ISO 27001 „berechtigt", Ziele so aufzuschreiben, wie es für die Organisation passt. Beim IT-Grundschutz dagegen ist man bei den Grundwerten auf die drei klassischen Ziele fixiert (wobei man davon ausgeht, dass alle anderen Ziele daraus abgeleitet werden können).

2.2 Risiken und Analysen

Dass Sicherheitsziele für die Werte einer Organisation nicht immer und ohne Weiteres erreicht werden, liegt daran, dass Risiken bestehen, die bei ihrem Eintritt einem Sicherheitsziel zuwiderlaufen können.

Risiko

Als *Risiko* wird nach ISO 27005[26] eine Kombination aus der

- Eintrittswahrscheinlichkeit eines (unerwünschten, unerwarteten, schädlichen) Ereignisses und
- dessen Konsequenzen definiert.

Die Eintrittswahrscheinlichkeit wird nicht im strengen mathematischen Sinne, sondern eher als *geschätzte Häufigkeit verstanden*.

In dieser Definition bleibt offen,

- welche Ereignisse zu analysieren sind,
- welche Konsequenzen betrachtet und wie diese bewertet werden,
- welche Kombination gemeint ist.

Ereignisse

Für unseren Kontext sind die folgenden *Ereignisse* unerwünscht, unerwartet oder schädlich und insofern wichtig für die weitere Betrachtung:

- *Gezielte Angriffe* von Personen (Innentäter, Hacker, Spione) auf Werte durch Ausnutzen von Schwachstellen in der verwendeten (Sicherheits-)Technik, in der Organisation oder der Schwachstelle „Mensch".

---

26 Auch nach dem älteren ISO Guide 73.

- *Ausfälle* von Geräten und Systemen, Personal und Prozessen.
- *Elementarereignisse* wie Erdbeben, Feuer, Wassereinbruch, Blitzeinschlag, usw., die sich auf Werte auswirken.
- *Fahrlässige Handlungen* und *Fehlbedienung von Systemen* durch Personen mit negativen Folgen für die Werte der Organisation.
- *Verstöße gegen Gesetze oder Verträge* mit finanziellen und anderen Konsequenzen für die Organisation.
- Potenzielle *Schädigung von Personen* (Ansehen, Gesundheit, Leben) und Organisationen (Ansehen, Kreditwürdigkeit etc.)

Im Standard werden solche Ereignisse als *Bedrohungen* (Threats) bezeichnet.

Konsequenzen

Die *Konsequenzen* solcher Bedrohungen können unmittelbar monetär einschätzbare Schäden sein – aber auch Imageverlust, Verlust der Kreditwürdigkeit, Entzug von Genehmigungen (etwa nach Gesetzesverstößen).

Kombination

Was ist nun mit *Kombination* gemeint? Sobald man Konsequenzen in Zahlen fassen kann – also etwa bei monetären Schäden –, besteht eine weit verbreitete Art der Kombination darin, das Risiko als *Produkt* aus Wahrscheinlichkeit und Schadenhöhe festzulegen. Das Risiko entspricht dann der *mittleren Schadenerwartung*.

Andere *probabilistische* Ansätze berücksichtigen dabei das Schadenausmaß stärker als die Häufigkeit. Dies stimmt mit der Motivation von Menschen überein, Versicherungen abzuschließen oder sich an Glücksspielen zu beteiligen.

Bei der Worst Case Methode, einem *possibilistischen* Ansatz, werden keine Werte für die Schadenhäufigkeit betrachtet, sondern das Risiko wird nur durch den größten denkbaren Schaden bestimmt.

Der Vollständigkeit halber sei darauf hingewiesen, dass in der *Portefeuilletheorie* das Risiko nicht durch die Erwartungswerte, sondern durch die Streuung der Verluste und Gewinne bestimmt wird.

Schließlich kommt bei der Bestimmung der Risikofunktion noch hinzu, dass die Einschätzung des Risikos subjektiven Präferenzen unterliegt. Eine sehr risikofreudige Organisation, die sich mit revolutionären, neuartigen Technologien beschäftigt, wird nicht die gleiche normierte Risikofunktion zur Begründung ihrer Ent-

scheidungen verwenden wie z. B. ein alt eingesessenes Versicherungsunternehmen.

Statistiken

Ein weiteres Problem liegt im Fehlen belastbarer Daten: Bei Elementarereignissen und beim Problem des Ausfalls von Geräten kann man in vielen Fällen aufgrund von Erfahrungen auf geschätzte Wahrscheinlichkeiten zurückgreifen und die (monetären) Konsequenzen können verhältnismäßig genau eingeschätzt werden. Dabei sind Statistiken von Versicherungsunternehmen oder deren Verbänden hilfreich; bei den Anbietern von Geräten wird vielfach für einzelne Geräte die bekannte MTBF = *Mean Time between Failure* angegeben. Für diese Art von Ereignissen existieren aus der Vergangenheit relativ verlässliche Schätzungen, die für die Zukunft extrapoliert werden können. Für viele andere Ereignisse in der Informationssicherheit (wie z. B. Hacker-Angriffe) gilt dieses Prinzip jedoch nicht, die Datenlage ist eher desolat.

Risikoklasse, Risikoindex

Ein weit verbreiteter Ansatz besteht deshalb darin, eine gewisse Unschärfe einzuführen und Risikoklassen (bzw. Risikoindizes) festzulegen. Jede Klasse (jeder Index) gibt eine gewisse Größenordnung oder Bandbreite vor. Die Folge ist, dass jedes Einzelrisiko einer Klasse (bzw. einem Index) grob zugeordnet wird, aber nicht mehr detailliert beziffert werden muss.

Zusammenfassend ist also der Begriff des Risikos aus ISO 27005 nicht unproblematisch, da wir

- in vielen uns interessierenden Fällen die Ereignisse (noch) nicht kennen und
- für bekannte Ereignisse nicht immer Wahrscheinlichkeiten ermitteln können.

Beispielsweise sind Hacker-Angriffe zwar in ihren Konsequenzen beschreibbar, eine halbwegs gesicherte Wahrscheinlichkeit für einen konkreten Angriff ist aber kaum zu ermitteln.

Vielfach sind uns die möglichen Angriffe noch nicht bekannt, weil sie z. B. Schwachstellen in Betriebssystemen ausnutzen, die noch nicht publiziert wurden.

In anderen Standards /CC/ und /ITSEC/ nutzt man eine Methode, die zwischen dem *Angriffspotenzial* der vermuteten Täter und der *Stärke* der vorhandenen Sicherheitsmaßnahmen abwägt.

Angriffspotenzial

Man bestimmt das Angriffspotenzial eines Täters, indem man

- seine technischen oder sonstigen *Fachkenntnisse*,
- seine verfügbaren *Ressourcen* (wie z. B. die für den Angriff benötigte Zeit sowie erforderliche Spezialwerkzeuge), und

– die sich ihm bietende *Gelegenheit* (wie z. B. Kenntnis über besondere Umstände, Mitarbeit von Insidern)

anhand von Tabellen (vgl. /ITSEM/) auswertet und auf diese Weise das Angriffspotenzial einer von drei Klassen NIEDRIG, MITTEL oder HOCH zuweist.

Stärke von Maßnahmen

Sicherheitsmaßnahmen werden nun danach bewertet, welches Angriffspotenzial – eine der drei genannten Stufen – sie gerade noch abwehren können. Dieser Mindestwert wird *Stärke* der Maßnahme genannt.

Die Frage, ob man einem Angriff standhalten kann, ist bei dieser Betrachtungsweise eine Frage der Abwägung zwischen Angriffspotenzial und Stärke der vorhandenen Sicherheitsmaßnahmen. Wahrscheinlichkeiten für einen Angriff oder seine Schadenfolgen spielen in diesem Rahmen jedoch keine Rolle.

Die Stärke von (technischen) Sicherheitsmaßnahmen in IT-Produkten wird meistens bei der Zertifizierung solcher Produkte nach /ITSEC/ oder /CC/ ermittelt und im jeweiligen Zertifizierungsreport angegeben. Dass dabei Wahrscheinlichkeiten oder Schadenfolgen keine Rolle spielen können, ist erklärlich, da solche Abschätzungen immer nur bezogen auf konkrete Organisationen möglich sind – nicht aber bei Typ-Prüfungen bzw. Typ-Zertifizierungen von IT-Produkten.

Schließen wir die generelle Betrachtung ab und widmen wir uns wieder den drei Begriffsquellen:

(K)

In der klassischen IT-Sicherheit geht man meist nach der Regel *Risiko = Produkt aus Häufigkeit und Schadenhöhe* vor und legt dabei mehr oder weniger (un)sichere Schätzungen für die Häufigkeiten und Schadenhöhen zugrunde oder verwendet gleich ein System mit Risiko-Indizes oder Risiko-Klassen.

(ISO)

Im Standard wird *keine* detaillierte Methode zur Ermittlung von Risiken vorgeschrieben. Eine solche festzulegen wird vielmehr der betreffenden Organisation aufgegeben. In der ISMS-Leitlinie muss die Organisation beschreiben, welches Verfahren der Risikoanalyse sie anzuwenden gedenkt. Dazu zählt auch die Definition von Risikoklassen und Akzeptanzschwellen. Letzteres meint, dass Risiken unterhalb eines bestimmten Schwellenwertes ohne weitere Maßnahmen „ausgesessen“ werden, über den Schwellenwert hinausgehende Risiken jedoch den Einsatz von Gegenmaßnahmen erzwingen.

Der Standard beschränkt sich auf Mindestanforderungen und gibt eine grobe Prozessbeschreibung. Beispiele für mögliche Analysemethoden finden sich in der ISO 27005.

Kurz zusammengefasst sieht das Vorgehen so aus:

Schritt 1: Risiko-Identifizierung

Bei der *Risiko-Identifizierung werden für die Informationswerte des ISMS*

- Ursachen bzw. Quellen für Bedrohungen von Informationswerten identifiziert und
- vorhandene (Gegen-)Maßnahmen ermittelt;
- es wird geprüft, ob hierbei Schwachstellen existieren.

Nach ISO 27005 ist das Zusammentreffen einer Bedrohung und einer Schwachstelle *Voraussetzung* für ein Risiko – nur dann ist man einem Risiko ausgesetzt (Risiko-Exposition).

Schwachstellen können darin bestehen, dass vorhandene Maßnahmen ausnutzbare Sicherheitslücken beinhalten, etwa in den technischen Prinzipien, der Umsetzung oder auch der Anwendung der Maßnahme. Gibt es erst gar keine Gegenmaßnahmen gegen eine Bedrohung, so ist dies natürlich erst recht eine Schwachstelle.

Schritt 2: Risikoabschätzung

Ist man gegenüber einzelnen Bedrohungen tatsächlich exponiert, muss eine *Risikoabschätzung* durchgeführt werden, d. h.

- für jede solche Bedrohung ist die Höhe des Risikos abzuschätzen bzw. zu klassifizieren.

Im Ergebnis dieses Schrittes liegt also eine Liste von Bedrohungen vor, denen gegenüber man exponiert ist und die man entsprechend abgeschätzt bzw. klassifiziert hat.

Schritt 3: Risikobewertung

Was versteht man unter Risikobewertung?

Da die Höhe eines Risikos nicht isoliert, sondern immer im Bezug zur Geschäftstätigkeit der Organisation gesehen werden muss, ist die Höhe des Risikos an einer Bewertungsskala zu spiegeln: Man braucht eine Einschätzung dafür, welche *Bedeutung* das betreffende Risiko für die Organisation hat. Diesen Vergleichsprozess nennt man *Risikobewertung*.

Als Beispiel sei ein Verlustrisiko von 1 Mio. € genannt, das für ein mittelständisches Unternehmen eine Katastrophe, für eine Großbank vielleicht nur Peanuts bedeutet. Erst die *Bewertung* des Verlustes durch die betreffende Organisation führt zu einer

Einordnung des Risikos. Im ersten Fall würde sich EXISTENZBEDROHEND ergeben, im zweiten Fall nur GERINGFÜGIG.

Arbeit man also bspw. mit Risikoklassen, muss man diesen eine Bewertungsskala zuordnen – ausgedrückt durch Attribute wie z. B. GERINGFÜGIG, BETRÄCHTLICH, GRAVIEREND und EXISTENZBEDROHEND.

Synthese

In der Normenreihe ISO 27000 wird der Prozess bestehend aus Risiko-Identifizierung und Risikoabschätzung als *Risikoanalyse* bezeichnet. Risikoanalyse und Risikobewertung werden gemeinsam als *Risikoeinschätzung* benannt.

Risikoanalyse = Risiko-Identifizierung + Risikoabschätzung

Risiko-Einschätzung = Risikoanalyse + Risikobewertung

Das von einer Organisation ausgewählte Vorgehensmodell bei den drei Schritten der Risikoeinschätzung ist zu beschreiben, und zwar typischerweise in der ISMS-Leitlinie! Dazu zählt auch die Festlegung von Risikoklassen und Bewertungsstufen.

Wendet man nun dieses Vorgehensmodell auf die einzelnen Risiken der Organisation an, erhält im Ergebnis eine Liste mit exponierten Bedrohungen, deren Risiko jeweils beziffert oder klassifiziert und im Hinblick auf ihre Bedeutung für die Organisation bewertet ist. Die Analyseschritte und die Ergebnisse sind schriftlich festzuhalten.

Sowohl das Vorgehensmodell als auch die konkreten Ergebnisse sind regelmäßig zu überprüfen und ggf. zu aktualisieren.

(GS)

Eine Motivation beim IT-Grundschutz war es dagegen, möglichst auf detaillierte individuelle Risikoanalysen der zuvor skizzierten Art zu verzichten: Man geht von so genannten *Gefährdungen* aus, die bei ihrem Eintreten zu Schäden für die Organisation führen können. Solche Gefährdungen werden im Gefährdungskatalog zahlreich und detailliert beschrieben.

Schäden können unterschiedlicher Natur sein, sie werden deshalb beim IT-Grundschutz zu *Schadenkategorien* gruppiert, nämlich

– Verstoß gegen Gesetze[27], Vorschriften oder Verträge,

[27] Einschließlich Verstöße gegen das Recht auf informationelle Selbstbestimmung.

- Beeinträchtigung der persönlichen Unversehrtheit,
- Beeinträchtigung der Aufgabenerfüllung,
- negative Außenwirkung,
- finanzielle Auswirkungen.

Für jede IT-Anwendung und jede Schadenkategorie wird nun ermittelt, welche *Auswirkungen* Schäden dieser Kategorie auf die Organisation haben können; dabei wird eine Klassifizierung mit drei Stufen

- TOLERABEL bzw. GERINGFÜGIG,
- BETRÄCHTLICH,
- KATASTROPHAL

zugrunde gelegt; die Abgrenzung dieser Stufen untereinander legt die jeweilige Organisation selbst fest – ein gewisses Analogon zur Risikobewertung im Standard.

Schutzbedarf

Jeder IT-Anwendung ordnet man schließlich einen *Schutzbedarf* zu, der sich aus der Schadenauswirkung wie folgt ergibt:

Tabelle 3: Definition des Schutzbedarfs

Schadenauswirkung	Schutzbedarf
TOLERABEL bzw. GERINGFÜGIG	NORMAL[28]
BETRÄCHTLICH	HOCH
KATASTROPHAL	SEHR HOCH

Der Schutzbedarf einer IT-Anwendung *vererbt* sich nach bestimmten Regeln auf die von der IT-Anwendung „genutzten" IT-Systeme, Netzwerke und IT-Räume, so dass man allen beim IT-Grundschutz betrachteten Werten einen Schutzbedarf zuordnen kann.

Alle weiteren methodischen Schritte beim IT-Grundschutz basieren auf dieser Feststellung des Schutzbedarfs.

Die Maßnahmen aus den Maßnahmenkatalogen für den normalen Schutzbedarf sollen beim IT-Grundschutz aus einer (allerdings nicht publizierten) Risikoanalyse abgeleitet worden sein.

Man beachte: Im Vergleich zu ISO 27005 haben wir es bei den Gefährdungen des IT-Grundschutzes nicht automatisch mit exponierten Bedrohungen zu tun. Es werden auch keine Angaben

28 Frühere Bezeichnung: GERING BIS MITTEL.

zu Wahrscheinlichkeiten oder Schadenhöhen gemacht – also sind es auch keine Risiken im Sinne des Standards.

Eine Bestimmung von individuellen *Risiken* hat beim IT-Grundschutz lediglich für den Bereich hohen und sehr hohen Schutzbedarfs zu erfolgen. Der BSI-Standard 100-3 beschreibt diese Thematik.

Fazit

Bei aller Methodendiskussion sollte generell bedacht werden, dass die erreichbare Genauigkeit bei Risikoanalysen aufgrund der Natur von Informationsrisiken begrenzt ist, andererseits sehr detaillierte Methoden auch einen erhöhten Aufwand nach sich ziehen.

Weiterhin: Nehmen wir einmal an, dass alle Einzelrisiken exakt berechenbar wären. Da die Einzelrisiken oft aber nicht unabhängig voneinander und nicht zueinander disjunkt sind, ist eine Zusammenfassung der Einzelrisiken zu einem Gesamtrisiko nur auf dem Wege der intuitiven Schätzung möglich.

Man beachte außerdem, dass wir im Bereich der Informationssicherheit eher selten die *Verkettung* von (Schaden-)Ereignissen analysieren.

2.3 Maßnahmenauswahl und Risikobehandlung

Maßnahmenauswahl

(K)

Beim klassischen Vorgehen priorisiert man zunächst die Risiken und beginnt mit der höchsten Klasse, um jedem Einzelrisiko einen geeigneten Satz von Maßnahmen zuzuordnen, mit dem das verbleibende Risiko unter eine noch akzeptierte Grenze fällt.

Die Beurteilung der Risiken, der Eignung von Maßnahmen und der Einschätzung des verbleibenden Risikos erfolgt dabei nach bestem Wissen der Analysten der Organisation (ggf. verstärkt um externe Sicherheitsberater).

(ISO)

Der Standard fordert eine ähnliche Vorgehensweise: Für jeden Informationswert sind bezüglich Verfügbarkeit, Vertraulichkeit und Integrität und ggf. weiterer Ziele die Risiken zu identifizieren, abzuschätzen und zu bewerten. Dabei gehen die Bedrohungen, Schwachstellen, sowie die Einschätzung von Ausmaß und Häufigkeit der Schäden ein.

Maßnahmenziele

Sodann sind die so genannten *Maßnahmenziele* aus dem Anhang A des Standards für jeden Informationswert anzuwenden. Dabei handelt es sich um Ziele für bestimmte thematische Berei-

che, wie z. B. die Zugriffskontrolle oder die Behandlung von Sicherheitsvorfällen.

Anwenden bedeutet dabei zu entscheiden, ob ein Maßnahmenziel für die Organisation bzw. den betrachteten Wert relevant ist, und dann entsprechende Maßnahmen zuzuordnen. Neben den Maßnahmenzielen des Standards können natürlich organisationsspezifische Maßnahmenziele eingeführt und analog behandelt werden.

Begriff Maßnahme

Hinsichtlich des Begriffs der Maßnahme ist anzumerken, dass zwischen *Maßnahmen im Sinne des Standards* und *Einzelmaßnahmen der Organisation* unterschieden werden muss: Mit *Maßnahmen* sind im Anhang A des Standards Anforderungen gemeint, die durch Einzelmaßnahmen von der Organisation abzudecken bzw. zu erfüllen sind (vgl. zu dieser Begriffsverwirrung auch Abschnitt 2.5).

Die Maßnahmen im Sinne des Standards betreffen

- Leitlinien und Regelwerke,
- vertragliche Gestaltung,
- Prozeduren und Praktiken,
- Organisationsstrukturen und
- administrative, personelle, infrastrukturelle oder technische Anforderungen.

Einzelmaßnahmen für den letzten Aufzählungspunkt sind die klassischen Sicherheitsmaßnahmen, die Gegenmaßnahmen zu Bedrohungen, etc.

Nach Anwendung der Maßnahmenziele und nach Zuordnung geeigneter Einzelmaßnahmen sind die verbleibenden Risiken („Restrisiken“) nach Umsetzung der Maßnahmen entsprechend einem vorher festgelegten Plan weiter zu behandeln.

(GS)

Als *IT-Verbund* einer Organisation wird beim IT-Grundschutz die Gesamtheit von Infrastruktur, Personal und IT bezeichnet, die der Erfüllung der betrachteten Fachaufgaben dienen.

Bei der *Modellierung* des IT-Verbunds werden passende *Bausteine* aus dem Handbuch ausgewählt, und zwar aus den Bausteingruppen *Übergreifende Aspekte* (Organisation), *Infrastruktur*, *IT-Systeme*, *Netze* und *Anwendungen*. Die Auswahl hat so zu erfolgen, dass die Kombination der gewählten Bausteine ein der Realität möglichst nahe kommendes Modell des IT-Verbunds ergibt.

Zu jedem ausgewählten Baustein gehört eine spezifische priorisierte Liste von Einzelmaßnahmen, die vom BSI als geeignet für den *normalen* Schutzbedarf angesehen werden und folglich von der Organisation umzusetzen sind. Hier legt man im Gegensatz zum Standard also eine Grundmenge von (Einzel-)Maßnahmen verbindlich fest, von der nur begründet abgewichen werden darf.

Die Maßnahmenkataloge des IT-Grundschutzes bilden auch eine Basis für Maßnahmen für den hohen und sehr hohen Schutzbedarf, werden jedoch vom BSI hierfür nicht automatisch als vollständig und ausreichend stark angesehen.

Für den Schutzbedarf HOCH oder SEHR HOCH ist die Vorgehensweise so, dass zunächst der IT-Verbund nach IT-Grundschutz modelliert wird und alle entsprechenden Sicherheitsmaßnahmen für den normalen Schutzbedarf umzusetzen sind. Dann wird in einer ergänzenden Analyse dem höheren Schutzbedarf Rechnung getragen. Dieses Verfahren ist im BSI-Standard 100-3 beschrieben, betrachtet jedoch keine Risiken im engeren Sinne des Standards.

Man beachte, dass beim Grundschutz zunächst die Werte mit normalem Schutzbedarf betrachtet – grob gesagt also die mit dem eher geringen Risiko – und hierfür Maßnahmen vorschreibt, die der Anwender umzusetzen hat. Erst danach kommen die Werte mit dem Schutzbedarf HOCH und SEHR HOCH an die Reihe, die einer zusätzlichen Analyse zu unterziehen sind. Dies ist eine durchaus bedenkliche Abkehr von der üblichen Vorgehensweise, sich zunächst um die sehr hohen und hohen Risiken zu kümmern.

Risikobehandlung

Bei der *Risikobehandlung* hat man generell eine Reihe von Alternativen bzw. Optionen:

- Einstellung risikoträchtiger Geschäftstätigkeiten.
- Akzeptanz von einzelnen Risiken, d. h. man akzeptiert sie, ohne weitere Maßnahmen vorzusehen (*Risiko-Akzeptanz*).
- Verlagerung von Risiken (Verlagerung der Geschäftstätigkeiten an einen sichereren Ort, Versicherung von Risiken, Outsourcing risikobehafteter Geschäftstätigkeiten[29]).

29 Soweit dabei eine Risikoverlagerung überhaupt möglich ist.

– Auswahl und Implementierung geeigneter Maßnahmen, mit denen das verbleibende Risiko[30] unter eine von der Organisation noch akzeptierte Grenze rutscht.

Risiko-behandlungsplan

Wichtig ist, einen Risikobehandlungsplan aufzustellen, in dem die zulässigen Optionen für die Behandlung von Risiken festgelegt werden und für jedes Risiko eine Behandlungsoption ausgewählt wird.

Im Standard wird diese Vorgehensweise explizit gefordert.

Beim IT-Grundschutz wird vom Restrisiko gesprochen, dies allerdings eher in einem qualitativen Sinne:

– Für den normalem Schutzbedarf sind die Restrisiken bei Anwendung der Katalogmaßnahmen nach Aussagen des BSI *grundsätzlich* als gering einzustufen. Ist die Umsetzung dieser Maßnahmen nicht oder unvollständig erfolgt (z. B. aus Budget-Gründen), können Restrisiken entstehen, die jedoch nicht näher beziffert oder klassifiziert werden.
– Bei höherem Schutzbedarf wird untersucht, ob die auswählten – ggf. verstärkten – Maßnahmen geeignet sind, die betrachteten Bedrohungen abzuwehren oder nicht. Im Negativfall liegen Restrisiken vor, die aber auch hier nicht näher beziffert oder klassifiziert werden.

Im Falle solcher „Restrisiken“ ist eine Entscheidung der Leitungsebene über deren Akzeptanz herbeizuführen

2.4 Sicherheitsdokumente

Beschäftigen wir uns noch kurz mit zwei grundlegenden Begriffen, hinter denen sich Dokumente verbergen: Sicherheitsleitlinie und Sicherheitskonzept.

Gelegentlich wird statt *Sicherheitsleitlinie* auch der Begriff *Sicherheitspolitik* verwendet – möglicherweise aufgrund einer nicht korrekten Übersetzung von *(Security)* P*olicy*.

---

30 Für das englische *residual risk* (verbleibende Risiken) wird im deutschen Sprachraum und im Kontext der Informationssicherheit vielfach der Begriff *Restrisiko* verwendet. Eine abweichende Definition von *Restrisiko* wurde im Jahre 1978 durch das Bundesverfassungsgericht im Rahmen des „Kalkar-Urteils“ getroffen: Demnach werden hierunter die „hypothetischen Risiken, die nach dem Stand der Wissenschaft unbekannt, aber nicht auszuschließen“ sind, verstanden. Wir schließen uns dieser Definition im Einklang mit ISO 27001 an.

Sicherheitsleitlinie

(K)

In der *Sicherheitsleitlinie* wird zumeist die Organisation mit ihrem Geschäftszweck, dem internen Aufbau und den Standorten, den Informationswerten und der verwendeten Technik *im Überblick* dargestellt. Anschließend werden die relevanten externen und internen Vorgaben summarisch aufgeführt bzw. referenziert. Dann wird die Bedeutung der Informationssicherheit für die Organisation beschrieben, indem die Gefährdungslage skizziert und die möglichen Folgen für die Organisation behandelt werden. Schlussendlich werden grundsätzliche Regeln für die IT-Sicherheit aufgeführt.

(ISO)

Auch beim Standard gibt es eine Sicherheitsleitlinie im Grunde sogar zwei: die *ISMS-Leitlinie* und die *Informationssicherheitsleitlinie*.

ISMS-Leitlinie und Informationssicherheitsleitlinie dürfen in *einem* Dokument zusammenfassend dargestellt werden – weshalb in vielen realen Beispielen nicht genau zwischen den beiden Aspekten unterschieden wird. Die Autoren empfehlen aber eine Aufteilung in zwei Dokumente.

Die *Informationssicherheitsleitlinie* einer Organisation definiert, wie Informationssicherheit individuell verstanden wird, d. h.

- welche grundsätzlichen (Informations-)Werte und welche grundsätzlichen Sicherheitsziele für diese Werte seitens der Organisation bestehen,
- welchen grundsätzlichen Risiken sich die Organisation hinsichtlich dieser Werte ausgesetzt sieht und welche Auswirkungen diese Risiken auf die Organisation haben können,
- wie die Verantwortung für die Sicherheit organisiert ist und durch welche Verfahren die Organisation diese Risiken steuert,
- welchen weiterführenden Dokumenten Details zur Sicherheit entnommen werden können.

Beispiel

Im Anhang dieses Buches ist ein Beispiel (!) für eine Informationssicherheitsleitlinie (im Sinne des Standards) angegeben, in der diese Informationen aufgeführt sind.

Die *ISMS-Leitlinie* wird im Standard als Erweiterung[31] der Informationssicherheitsleitlinie verstanden. Hinzu treten nämlich die

[31] Diese Erweiterung ist in unserem Beispiel im Anhang nicht vorgenommen worden.

Rahmenbedingungen für das Management der Informationssicherheit, insbesondere

- die Methode der *Risikoeinschätzung* (*Risikoanalyse* und *Risikobewertung)*, die von der Organisation einheitlich angewendet werden soll,
- die Kriterien der *Risikobehandlung* inkl. Festlegung von Risikoschwellen bzw. Risikoklassen,
- die Optionen der *Risikobehandlung* inkl. Festlegung von Akzeptanzschwellen.

Bei beiden Formen der Leitlinie handelt es sich vorwiegend um summarische Aussagen.

Gründe für diese (letztlich vernünftige) Aufteilung in zwei Bestandteile sind:

- Es sollen Vorgaben zum *Management* der Sicherheit und Vorgaben zum *Gegenstand* der Sicherheit voneinander getrennt werden.
- Der Adressatenkreis: Die ISMS-Leitlinie richtet sich an das Sicherheitsmanagement, die Informationssicherheitsleitlinie dagegen an die von der Informationssicherheit Betroffenen.

(GS) Bei Anwendung des IT-Grundschutzes ist eine *IT-Sicherheitsleitlinie* zu erstellen, in der neben dem *Stellenwert* der IT-Sicherheit und der Bedeutung der IT für die Aufgabenerfüllung insbesondere die IT-Sicherheitsziele und die *Strategie* zu ihrer Umsetzung zu beschreiben sind.

Bei den IT-Sicherheitszielen ist der Bezug zu den Geschäftserfordernissen der Organisation herzustellen und das angepeilte Sicherheitsniveau festzulegen. Optional kann auf wichtige Gefährdungen, gesetzliche und vertragliche Anforderungen sowie Sensibilisierungs- und Schulungsmaßnahmen eingegangen werden.

Bei der *Strategie* geht es um die Art und Weise der Umsetzung bzw. Durchsetzung (z. B. die angemessene Organisationsstruktur) und der Erfolgskontrolle.

Man erkennt, dass sich die IT-Sicherheitsleitlinie beim IT-Grundschutz nahe an der Informationssicherheitsleitlinie des Standards bewegt.

Sicherheitskonzept

(K) Das *Sicherheitskonzept* enthält (hoffentlich) eine präzise Festlegung des Betrachtungsgegenstands und sodann verschiedene Analysen (Anforderungen, Gefahren, Bedrohungen, Schwachstel-

len, Risiken). Anschließend werden „passende“ Maßnahmen ausgewählt und validiert; schlussendlich werden verbleibende Risiken ermittelt und beschrieben.

(ISO)

Das klassische Sicherheitskonzept gibt es in dieser Form im Standard nicht. Die entsprechenden Inhalte sind auf separate Arbeitspakete verteilt, die gemeinsam in *einem* Dokument oder *getrennt* dokumentiert werden können:

- Die *Festlegung des Anwendungsbereichs* – was der Gegenstand des ISMS ist und wofür die Analysen durchgeführt werden – ist aus Sicht des ISO 27001 ein separater Schritt, der allen anderen vorausgeht.
- Die Erfassung bzw. Festlegung der Informationswerte (Assets) im Anwendungsbereich.
- Die *Risikoanalyse* und *Risiko-Bewertung* für den Anwendungsbereich
- Die *Erklärung zur Anwendbarkeit.*

Beim letzten Aufzählungspunkt geht es um die bereits auf der Seite 34 f. erläuterten Maßnahmenziele und Maßnahmen, mit denen die bewerteten Risiken gesteuert werden. Der Anhang A der ISO 27001 gibt eine bestimmte Systematik vor, nach der Maßnahmenziele und Maßnahmen aus- oder abgewählt werden können. Kriterium für die Abwahl ist immer, ob ein Maßnahmenziel oder eine Maßnahme für die Organisation und ihre Werte ungeeignet oder aus anderen Gründen nicht anwendbar ist.

Die Organisation ist grundsätzlich frei, ergänzend eigene Maßnahmenziele und Maßnahmen hinzuzufügen und damit analog zu verfahren.

Bei den Entscheidungen und Begründungen spielen die Ergebnisse der Risikoeinschätzung und der Risikobehandlung eine Rolle, aber auch die in der Leitlinie enthaltenen Angaben zu gesetzlichen Anforderungen, vertraglichen Verpflichtungen und Geschäftsanforderungen der Organisation.

SoA

Die so entstandene Liste von Maßnahmenzielen, (umgesetzten bzw. noch umzusetzenden) Einzelmaßnahmen und entsprechenden Erklärungen bzw. Begründungen erhält die Überschrift *Erklärung zur Anwendbarkeit* (abgekürzt: *SoA*[32]).

Oft findet man als SoA lediglich ein Blatt vor, das von zuständigen Personen der Organisation unterzeichnet ist und in dem

32 SoA = Statement of Applicability (vgl. auch Abschnitt 2.5).

erklärt wird, dass die zuvor genannte Liste abgesegnet ist, zur Anwendung freigegeben wird oder Ähnliches mehr. Ein solches Vorgehen ist in Ordnung (wenn auch im Standard so nicht gefordert).

(GS)

Als Sicherheitskonzept wird beim IT-Grundschutz die Gesamtheit der Informationen aus folgenden Schritten bezeichnet:

- Strukturanalyse: Erfassen der IT-Anwendungen, IT-Systeme und Netzwerke, IT-Räume.
- Schutzbedarfsanalyse.
- Modellierung: Auswahl geeigneter Bausteine mit spezifischen Maßnahmen.
- Basis-Sicherheits-Check.
- Ergänzende Sicherheitsanalyse bei hohem und sehr hohem Schutzbedarf.
- Realisierungsplanung.

Die sich als Ergebnis der Modellierung ergebenden Maßnahmen werden nach „Maßnahme vorhanden“ bzw. „Maßnahme noch nicht vorhanden, Umsetzung vorsehen“ klassifiziert. Diese Prüfung heißt *Basis-Sicherheits-Check*.

Die *Gefährdungskataloge* des IT-Grundschutzes eignen sich als Fundstelle für Gefährdungen und Schwachstellen der Informationssysteme und können somit Input für alle weiteren Schritte liefern.

Die sehr konkreten *Maßnahmenkataloge* können in Ergänzung zur ISO 27002 als Quelle für das Auffinden von erprobten Sicherheitsmaßnahmen verwendet werden – auch für die im Sinne des Standards *organisationsspezifischen* Maßnahmenziele und Maßnahmen.

2.5 Übersetzungsprobleme bei der deutschen Ausgabe des Standards

Zwischen englischen und deutschen Normtexten besteht immer das Problem einer möglichst präzisen Übersetzung. Wir wollen in diesem Abschnitt einige Punkte zusammentragen, die bei der deutschen Fassung der ISO27001 übersetzungsbedingt zu Fragen Anlass geben.

Statement of Applicability

Beginnen wir mit dem *Statement of Applicability* (SoA), das immer als *Erklärung zur Anwendbarkeit* übersetzt wird. Warum sollten die darin aufgeführten Inhalte nicht anwendbar sein? Viel wichtiger ist die Frage, ob die Inhalte *geeignet* sind, die von der

Organisation gewünschte Sicherheit herzustellen. Man beachte, dass das englische Wort *applicability* neben *Anwendbarkeit* auch die Bedeutung *Eignung* besitzt; somit wäre *Erklärung zur Eignung* eine bessere Übersetzung.

Control — Zu mancher Verwirrung hat die Übersetzung des Wortes C*ontrol* mit *Maßnahme* geführt. Inspiziert man die Texte im Anhang A des Standards – also die Controls –, so stellt man fest, dass es sich stets um (Sicherheits-)*Anforderungen* handelt. Dann wird auch klar, warum in einer konkreten Organisation den Controls erst noch (Einzel-)*Maßnahmen* zugeordnet werden müssen, um die jeweilige Anforderung zu erfüllen.

Control Objective — Es geht weiter mit C*ontrol Objective*, das mit *Maßnahmenziel* übersetzt wurde. Dies geht nun völlig schief, weil eine Maßnahme für sehr unterschiedliche Ziele eingesetzt werden kann, also mitnichten eine Maßnahme ein Ziel besitzt. Gemeint ist natürlich, dass die in einem Control beschriebene Anforderung (!) einem bestimmten Ziel dient. Eine bessere Übersetzung wäre einfach *Ziel der Anforderung*.

Policies — Der englische Begriff S*ecurity Policy* wird bekanntlich (richtigerweise) mit *Sicherheitsleitlinie* übersetzt. Wenn das Wort *policy* oder *policies* allein auftaucht, sind damit jedoch Regeln, Regelwerke oder Richtlinien gemeint. Leider wird in der deutschen Fassung der Norm an solchen Stellen immer mit *Leitlinie(n)* übersetzt. Dies trägt, wie wir aus Erfahrung wissen, zur Verwirrung bei, weil Leser annehmen, die gemeinten Vorgaben müssten in der Sicherheitsleitlinie stehen – was mitnichten der Fall ist.

Authority — In englischen Texten dieser Art kommt häufig das Wort *authority* vor, was je nach Kontext *Behörde*, aber einfach auch *Autorität* meinen kann. Dass man *relevant authorities* kontaktieren soll, kann deshalb bedeuten, einschlägige sachverständige Stellen zu kontaktieren – was nicht zwangsläufig Behörden sein müssen.

Measure — Der Standard spricht an vielen Stellen von *messen* als Übersetzung von *measure*. Dieses englische Wort hat allerdings auch die Übersetzung *abschätzen*, was zutreffender ist, weil eine Messung im präzisen Sinne bei den relevanten Anforderungen ohnehin nicht möglich ist.

Access Control — Da haben es Übersetzer in der Tat schwer: Der Terminus A*ccess Control* kann wörtlich übersetzt *Zugangskontrolle, Zutrittskontrolle* oder *Zugriffskontrolle* bedeuten. In der neuen Ausgabe der ISO 27000 wird Access Control immer mit Bezug auf alle Arten von Assets verstanden, die ja sehr unterschiedlicher Natur sein können:

- Daten: Hier wäre *Zugriffskontrolle* die richtige Übersetzung.

- Bei physischen Orten (Räumlichkeiten, Sicherheitszonen) wäre es dann die *Zutrittskontrolle*[33].
- Wenn jemand Services, Anwendungen, Netzdienste nutzen kann, sprechen wir oft davon, dass der Betroffene Zugang zu diesen Objekten hat: *Zugangskontrolle*.

Wenn Sie in unseren deutschen Normtexten der ISO 27000-Reihe das Wort *Zugangskontrolle* finden, prüfen Sie besser anhand des Kontextes, was genau gemeint ist!

Audit Logging

Im Anhang A kommt der Begriff *Audit Logging* vor – in der deutschen Fassung übersetzt als *Auditprotokolle*. Dies hat (fast) nichts mit unseren internen bzw. externen Audits zu tun, sondern meint die Aufzeichnungen diverser Kontroll- und Überwachungseinrichtungen (z. B. Log-Protokolle bei IT-Systemen, Aufzeichnungen über Zutritte zu Sicherheitszonen etc.), die aufbewahrt werden, um zu einem späteren Zeitpunkt Auswertungen über mögliche Sicherheitsverletzungen und andere Vorkommnisse durchführen zu können.

33 An einigen Stellen in der Normenreihe ist hier auch von *entry controls* die Rede.

http://www.springer.com/978-3-658-01723-1

IT-Sicherheitsmanagement nach ISO 27001 und Grundschutz

Der Weg zur Zertifizierung

Kersten, H.; Reuter, J.; Schröder, K.-W. - Kersten, H.; Wolfenstetter, K.-D. (Hrsg.)

2013, XIII, 377 S. 4 Abb., Softcover
ISBN: 978-3-658-01723-1