1 Grundlagen des Testens der Sicherheit

»Man kann und darf wohl sein eigenes Leben für eine Sache riskieren, aber nie das Leben eines anderen.«
Sir Karl Raimund Popper

Eine maximale Sicherheit ist in den heutigen IT-Systemen wirtschaftlich sinnvoll nicht möglich und technisch höchst anspruchsvoll. Für das Abwägen, wie viel Sicherheit dennoch nötig ist und wie viel Restrisiko akzeptabel ist, spielt die Risikobewertung der wesentlichen Business-Assets eine fundamentale Rolle: In diese fließen unterschiedliche, möglichst alle Risiken abdeckende Parameter im Vorfeld von Sicherheitstests ein. Sie bestimmt nach Festlegen von Sicherheitsstufen pro Asset die Planung von Sicherheitsmaßnahmen und Sicherheitstests. Hierunter fallen auch proaktive Maßnahmen in Form von Sicherheitsrichtlinien, die klare Handlungsanweisungen vorgeben, um inhärent sichere Systeme zu erstellen. Die Wirksamkeit solcher Richtlinien muss allerdings alleine aufgrund stetig ändernder Sicherheitsgefährdungen regelmäßig mittels Sicherheitsaudits geprüft und bei Bedarf durch aktuelle Sicherheitstests nachgeschärft werden. Das gesamte prozessorale und technische Zusammenspiel aus Richtlinien, Sicherheitstests sowie dem Berücksichtigen zukünftiger möglicher Gefährdungen bei fortwährender Wirksamkeitsoptimierung wird durch Sicherheitsaudits analysiert und systematisch verbessert.

1.1 Sicherheitsrisiken

1.1.1 Die Rolle der Risikobewertung beim Testen der Sicherheit

Schon das klassische funktionale Testen basiert auf einer Vielzahl von projekt- und unternehmensspezifischen Elementen: So sind z. B. Anforderungen, Anwendungsfälle und mögliche Risiken hinter identifizierten Abweichungen von einem Soll individuell zu berücksichtigen: Eine angepasste Testplanung wird ihren Fokus meist auf solche Anwendungsfälle legen, deren Ausfall massiven Schaden (z. B. wirtschaftlicher Schaden durch entgangenen Umsatz) hervorrufen kann, oder auf solche, die besonders häufig genutzt werden (und bei denen eine Abweichung

eher effektiv wird). Die Testtiefe wird dann jeweils entsprechend diesem Fokus festgelegt.

Sicherheitstests verfolgen einen ähnlich risikobasierten Ansatz, fokussieren aber pro Anwendungsfall deren Sicherheitsaspekte und mögliche Gefährdungen: Diese müssen nicht nur technisch sein, sondern berücksichtigen auch

- Verhaltensmuster von Angreifern, wenn sich etwa Angriffshäufungen für bestimmte Industrien, Regionen oder Techniken abzeichnen,
- prozessorale Lücken, wenn etwa eingerichtete Zutrittskontrollen aus Bequemlichkeit umgangen werden, und
- organisatorische Unstimmigkeiten, wenn Anweisungen für z.B. Passwortrücksetzungen nicht zentral verantwortet werden.

Die Ziele von Sicherheitstests richten sich nach bestehenden Sicherheitsrisiken, also Risiken, die durch eine ungenügende Sicherheit auftreten können. Kann keinerlei direkter oder indirekter Schaden hervorgerufen werden, so sind Sicherheitstests aus wirtschaftlichen Gründen nicht angezeigt.

Sicherheitstests folgen einer Risikoanalyse, nicht umgekehrt.

Existierende Risiken sind also eine notwendige Vorbedingung für Sicherheitstests. Diese Risiken werden üblicherweise im Rahmen einer Sicherheitsrisikobewertung ermittelt. Allgemeine Risikomanagementtechniken werden bereits aus dem normalen, meist funktionalen Kontext heraus in [GTB CTFL 18] und [GTB CTAL TM 12] beschrieben: Denn auch dort gilt, dass ein Testen einer Funktionalität, deren Fehlverhalten oder vollständiges Ausfallen keinen Schaden anrichtet, wirtschaftlich nicht angezeigt ist.

International weit verbreitet sind die Risikomanagementtechniken der Standards ISO 31000 [ISO 31000] und ISO 27005 [ISO 27005] sowie der Richtlinie NIST 800-30 [NIST SP 800-30 02]. Während die ISO 31000 den allgemeinen Ablauf des Risikomanagements beschreibt, und damit auch außerhalb der IT angewendet wird, fokussiert die ISO 27005 speziell Informationssicherheitsrisiken. NIST 800-30 hat insbesondere für den nordamerikanischen Markt eine große Bedeutung.

1.1.1.1 ISO 31000

Die ISO 31000 (vgl. [ISO 31000]) bietet eine übersichtliche und gut verständliche Risikomanagementtechnik, die wie in Abbildung 1–1 dargestellt werden kann.

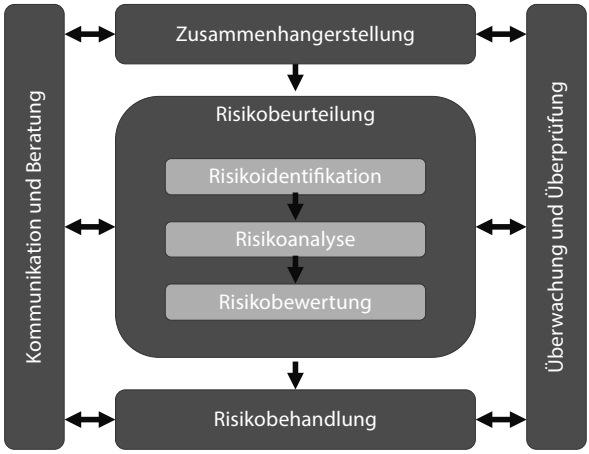


Abb. 1–1
Schematische Darstellung der ISO 31000

Sie ist dabei hinreichend generisch, um auch in tagtäglichen Situationen risikobasiert vorzugehen. Dies soll anhand eines Szenarios verdeutlicht werden.

Die ISO 31000 beschreibt einen eingängigen, universell einsetzbaren Risikomanagementprozess.

Beispiel: Risikomanagement

Beispiel: Risikomanagement

Das folgende Beispiel ist bewusst dem Nicht-IT-Bereich entnommen und soll den universellen Charakter des Risikomanagements aufzeigen. Im konkreten Beispiel geht es um die Abschätzung, ob man abends ein Bier trinken sollte, wenn man anschließend noch mit dem Auto selbst nach Hause fahren muss.

Eine allgemeingültige Sicht auf eine solche Risikoanalyse ist in Abschnitt 1.1.3 weiter unten beschrieben. Das konkrete Beispiel wird im Folgenden entlang des beschriebenen Risikomanagementprozesses betrachtet:

1. **Zusammenhangerstellung**
   Auch wenn die schädliche Wirkung der Zutat Bier außer Frage steht, gibt es weitere Parameter aus einem konkreten Kontext, die für die Folgeabschätzung relevant sind: Handelt es sich beim potenziellen Trinker um eine Schwangere, muss anschließend noch Auto gefahren werden, gibt es gruppendynamische Effekte und Einflüsse usw.
2. **Risikoidentifikation**
   In diesem Abschnitt werden für den konkreten Kontext (vgl. vorheriger Schritt) die einzelnen Risiken identifiziert. Die Abhängigkeit zum Kontext ist hier wichtig: Erzeugt eine Schwangere z. B. Risiken für sich und das ungeborene Kind, so gefährdet ein Mann ggf. nur sich (aber Achtung: Straßenverkehr).
3. **Risikoanalyse**
   In diesem Schritt werden die einzelnen Risiken detailliert analysiert: Wie groß ist der mögliche Schaden, welche Art ist der Schaden (monetär, gesundheitlich, reputationsbezogen usw.), wie wahrscheinlich ist er usw. Im konkreten Fall könnten medizinische Studien herangezogen werden, Ver-

kehrsstatistiken oder auch soziologische Studien für den Fall, dass ein Nicht-Trinken zur Gruppenisolation führt.

4. **Risikobewertung**
   In diesem Schritt findet ein Abgleich der Ergebnisse der Risikoanalyse mit dem eigenen Risikoappetit statt: So können zwei Menschen in einem sehr ähnlichen Kontext trotz sehr ähnlicher Risikoanalysen immer noch völlig unterschiedliche Bewertungen erzeugen; äußern kann sich das im nächsten Schritt der Risikobehandlung als ein unbekümmertes Trinken oder ein entsetztes Ablehnen des Getränkeangebotes.
5. **Risikobehandlung**
   Dieser Schritt bedeutet die eingeleitete Aktivität auf Basis der Bewertung. Die ISO sieht hier vier verschiedene Arten vor:
   - Das Risiko akzeptieren, was in dem konkreten Beispiel zum Trinken des Bieres führen würde.
   - Das Risiko vermeiden, was zum Ablehnen des Getränkes führen würde.
   - Das Risiko vermindern, was durch eine Reduktion der Trinkmenge oder des Alkoholgehaltes (Radler) erreicht werden kann.
   - Das Risiko delegieren, was im Falle des Autofahrers bedeuten könnte, den Autoschlüssel seinem ebenfalls mittrinkenden Kollegen zu geben.

Auch wenn dieser Prozess wenig komplex ist und damit evtl. eine einfache Anwendbarkeit suggeriert, so soll bereits hier nicht unerwähnt bleiben, dass eine Risikoanalyse eine höchst anspruchsvolle Aufgabe ist. Häufig werden hier bekannte Risiken vergessen, oder es dominieren eigene Gewohnheiten (»ich trinke immer ein Bier vor dem Nach-Hause-Fahren«) und eigene Risikobereiche (»nachts fahre ich sehr ungern«), oder die Risiken basieren auf unreflektierten Expertenmeinungen. Es benötigt meist sehr viel Erfahrung, wirklich vollständige und objektive Risikoanalysen durchzuführen.

Ohne Risiken bedarf es keiner Risikoanalyse.

Der Sicherheitstest, bei dem geprüft wird, wie sicher ein IT-System ist, lässt sich entlang dieses Standards im Bereich der Risikoidentifikation und der Risikoanalyse verorten. Der Sicherheitstest hilft also, existierende Risiken weiter zu analysieren, und zeigt ggf. weitere auf.

1.1.1.2 Das Risiko im Detail

Um eine detaillierte Risikoanalyse durchführen zu können, muss der Begriff Risiko weiter präzisiert werden:

Definition: Risiko

Ein Risiko ist ein Faktor, der zu negativen Konsequenzen in der Zukunft führen könnte, gewöhnlich ausgedrückt durch das Schadensausmaß und die Eintrittswahrscheinlichkeit. [GTB Glossar 18]

Beide Faktoren werden in der Praxis häufig quantifiziert (s. hierzu u. a. weiter unten Abschnitt 1.3.2) und für die Risikokalkulation multipliziert. So kann ein Risiko, das mit einer 1 %igen Wahrscheinlichkeit einen Schaden von 1.000 Euro bedeuten kann, als identisch zu einem anderen Risiko angesehen werden, bei dem mit einer 10 %igen Wahrscheinlichkeit ein Schaden von 100 Euro erzeugt werden kann. Das kalkulierte Risiko ist in beiden Fällen 10 Euro.

Beide Faktoren sind in der Praxis häufig nicht leicht und nachvollziehbar analysierbar:

- **Eintrittswahrscheinlichkeit**
  Häufig fehlen entsprechende Analysen, sie sind zueinander nicht konsistent oder lassen sich nur bedingt auf einen konkreten Kontext anwenden.
- **Schaden**
  Wie lassen sich Reputation, Marktdominanz oder auch gesundheitliche Schäden und Tod quantifizieren? Wie viel ist eine Beziehung »wert«, die z. B. aufgrund einer falsch zugestellten E-Mail zerbricht?

Um dennoch die Ermittlung von Eintrittswahrscheinlichkeit und Schaden durchführen zu können, existieren für den Bereich der IT-Sicherheit spezielle Risikomodelle (vgl. hierzu Abschnitt 1.3.2).

CIA der Security: Vertraulichkeit (Confidentiality=C), Integrität (Integrity=I) und Verfügbarkeit (Availability=A)

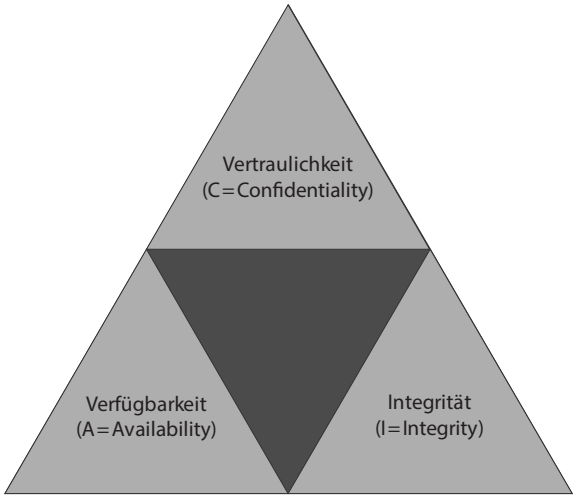
Informationssicherheitsrisiken sind nun solche Risiken, die die Sicherheit von Informationen eines Systems gefährden. Diese Definition ist eine Vereinfachung der Definition innerhalb der ISO 27001 [ISO 27001]:

Definition: Informationssicherheitsrisiko

»Als Informationssicherheitsrisiko wird das Potential bezeichnet, dass eine Bedrohung ausgenutzt werden kann und der Organisation so Schaden zugefügt wird.« [Klipper 15]

IT-Sicherheit ist folglich der Zustand, in dem Vertraulichkeit, Integrität und Verfügbarkeit von Informationen und Informationstechnik durch angemessene Maßnahmen geschützt sind (vgl. [BSI Glossar 13]).

Abb. 1–2
CIA-Dreieck der Sicherheit



Der Verlust der IT-Sicherheit bedeutet folglich den Verlust von Vertraulichkeit, Integrität oder Verfügbarkeit von Informationen oder Informationssystemen. Die Risiken hängen ganz wesentlich von den potenziellen schädlichen Auswirkungen auf betriebliche Vorgänge (z.B. Ziele, Funktionen, Image oder Reputation), betriebliche Assets, Individuen, andere Unternehmen sowie ein gesamtes Land ab [NIST SP 800-30 02]. Der Schaden wird dabei wiederum stark vom Kontext des Systems bestimmt:

Schadenshöhen hängen vom Kontext ab.

- Ist die Vertraulichkeit eines einfachen, öffentlichen Webservers verletzt, so ist der Schaden gering, da die Informationen per se für jeden gedacht waren. Bei einem internen Schadenssystem einer Versicherung ist ein solcher Verlust dagegen verheerend.
- Ist die Verfügbarkeit eines öffentlichen Warenbestellsystems nicht mehr gewährleistet, so beginnt direkt nach der ersten Sekunde der Nichtverfügbarkeit der Schaden durch Umsatzausfall zu wachsen. Die Nichtverfügbarkeit eines Druckers kann dabei bei Ausfällen von einigen Sekunden meist ignoriert werden.
- Ist die Integrität eines Wahrsageportals nicht gewährleistet, so kann dies – je nach Grad der Integritätsverletzung und der subjektiven Einstellung zu Wahrsagungen – durchaus vernachlässigt werden. Die Nichtintegrität von Systemen im medizinischen Bereich kann dagegen tödliche Folgen haben.

Im Rahmen einer Sicherheitsrisikobeurteilung, bestehend aus den drei Schritten der ISO 31000 – Risikoidentifikation, Risikoanalyse und Risikobewertung –, kann ein Unternehmen systematisch ermitteln, welche Bereiche und Assets einem Risiko ausgesetzt sind und welchen

Schweregrad die einzelnen Risiken haben. Für Sicherheitstester kann eine Sicherheitsrisikobewertung eine ergiebige Informationsquelle sein, auf deren Grundlage sich Sicherheitstests planen und konzipieren lassen. Idealerweise fokussieren Sicherheitstests dabei die besonders großen Risiken. Je größer ein Risiko, desto tiefer die Sicherheitstesttiefe. Die Sicherheitsrisikobewertung hilft also bei der Priorisierung von Sicherheitstests.

Ergebnisse der Sicherheitstests fließen dabei in eine verbesserte Sicherheitsrisikobewertung wieder ein. Sicherheitstests liefern also weitere wichtige Informationen, die für die Bewertung relevant sind.

Einen guten Überblick über die verschiedenen Möglichkeiten, wie Sicherheitsrisikobewertung und Sicherheitstesten sich im Rahmen einer umfassenden Sicherheitsbewertung ergänzen, erlauben die Norm ETSI 203-251 [ETSI 203-251 15] sowie ein technischer Bericht der ETSI mit einigen konkreten Fallbeispielen [ETSI TR 101 582 14].

1.1.1.3 Grenzen der Risikobewertung

Risikobewertung als eine fortwährende Aufgabe

Jede Risikobewertung (ob sicherheitsbezogen oder nicht) ist nur eine Momentaufnahme der berücksichtigten Parameter und fußt auf limitierten Informationen.

Beispiel: Geänderte Parameter einer Risikobewertung

Beispiel: Geänderte Parameter einer Risikobewertung

- **Geänderte Gesetze**
  Die Neufassung der Datenschutz-Grundverordnung kann dazu führen, dass eine Vielzahl von Risikobewertungen ungültig geworden ist.
- **Neue Nutzungsszenarien**
  Der zunehmende Einzug von meist unverschlüsselten Messenger-Diensten in kommerzielle Prozesse führt zu einer Neubewertung der Risiken.
- **Neue Marktanforderungen**
  Die zunehmende Sensibilisierung der Gesellschaft für Datenmissbrauch und die mit einem Sicherheitsvorfall aktuell verbundene negative Presse kann zu neuen Risikobewertungen führen.

Daher müssen Sicherheitsrisikobewertungen in regelmäßigen Abständen wiederholt werden. Das genaue Zeitintervall für die Durchführung von Sicherheitsrisikobewertungen variiert in Abhängigkeit vom Unternehmen und vom Grad der Veränderungen der Parameter. Manche Unternehmen führen alle drei bis sechs Monate Sicherheitsrisikobewertungen durch, andere einmal jährlich. Besondere Ereignisse wie z.B. die Einführung neuer Gesetze (vgl. die neue DSGVO 2016 [DSGVO 16]) sollte in jedem Fall zu einer flächendeckenden Neubewertung führen.

Die Anwendung und meist auch Dokumentation systematischer Risikobewertungen hat entgegen subjektiver Ad-hoc-Maßnahmen viele Vorteile:

- Nachvollziehbarkeit einer Entscheidung
- Bessere Vollständigkeit der Risiken sowie das Erkennen von Zusammenhängen zwischen Risiken. Grundsätzlich gilt, dass die gefährlichsten Risiken diejenigen sein können, die übersehen werden. Systematiken liefern hiergegen Hilfestellungen.
- Systematische Vorgehen lassen sich lernen und können zu Expertentum führen. Subjektivität wird dadurch reduziert, dass Hilfsmittel der Systematik wie Checklisten, Brainstorming, Modellierung oder Stakeholder-Management angewendet werden. Auch die bedarfsgerechte Verwendung formalisierter und formaler Techniken wie Fehlerbäume, Ursache-Wirkungs-Analysen oder Monte-Carlo-Simulationen zählen hierzu. Eine ausführliche Liste von Techniken zur Risikobewertung findet sich in der ISO 31010 [ISO 31010].

1.1.2 Ermittlung der Assets

Assets: wesentliche Güter in einem Unternehmen

Sicherheit bezieht sich vor allen Dingen auf die relevanten Güter eines Unternehmens, die sogenannten Assets: Diese Güter kommen heute im Wesentlichen in zwei Ausprägungen vor [Clement & Schreiber 13, S. 46]:

- **Non-digitale Güter**
  Hierzu zählen vor allen Dingen klassische physische Assets wie Maschinen, Gebäude oder IT-Hardware. Allerdings liegen auch viele informationsbasierte Assets heute non-digital vor: Beispiele hierfür sind kopierte Unterlagen, Verträge, Pläne, schriftliche Notizen, notierte Anmeldedaten und Passwörter. Da ihr Wert allerdings primär durch den Informationsgehalt der Träger (z.B. Papier, Mikrofilm) geprägt ist, werden sie auch als semiphysische Assets bezeichnet.
- **Digitale Güter**
  Diese Güter lassen sich vollständig »mit Hilfe von Informationssystemen entwickeln, vertreiben oder anwenden« (vgl. [Clement & Schreiber 13, S. 44]). Beispiele sind Dateien in der Cloud, Musikstücke auf dem Smartphone oder Wirtschaftspläne in Excel.

Ohne Assets keine systematische Risikoanalyse

Für eine Risikoanalyse gilt es, in einem ersten Schritt die relevanten Assets zu ermitteln, um dann jeweils anschließend festzustellen, welche davon in digitaler Form vorliegen und damit im Fokus eines möglichen Sicherheitstests liegen. Diese Gesamtsicht auf die Assets ist aber in jedem Fall wichtig, um überhaupt IT-Sicherheitstests zu motivieren:

Liegen die besonders relevanten Assets physisch vor (z. B. Maschinen und Materialien), so führt ein Risikomanagement zuerst zu physischen Maßnahmen wie Zutrittsschutz, bevor IT-Sicherheit betrachtet wird.

Es ist offenkundig, dass mit jeder Änderung der Menge betrachteter Assets auch die Risikoanalyse wiederholt werden muss. Aktuell verändert sich in der Industrie die Menge digitaler Assets am schnellsten, sodass diese Änderungen gleichzeitig Haupttreiber regelmäßiger Risikoanalysen sind:

> *»[…] für die einzelne Bank bringt die Digitalisierung neue Risiken. Denn die Zahl der schützenswerten Güter ist gewachsen; neben Geldvermögen sind inzwischen auch persönliche Daten und damit der Zugang zu Dienstleistungen im Cyberspace gespeichert.«* [Bundesbank 15]

Beispiele für digitale Güter sind:

- Kundendaten
- Businesspläne
- Proprietäre Software, die vom Unternehmen entwickelt wurde
- Systemdokumentation
- Bilder und Diagramme, die Eigentum des Unternehmens sind
- Geistiges Eigentum (z. B. Prozesse, Geschäftsgeheimnisse)
- Mitarbeiterdatensätze
- Steuererklärungen

Beispiel: Datenschutz-Grundverordnung

Beispiel: Datenschutz-Grundverordnung

Auch die aktuelle Datenschutz-Grundverordnung (DSGVO) legt für die dort mit dem Fokus auf personenbezogene Daten beschriebenen Sicherheitsrisiken einen Fokus auf Assets als ersten Schritt: Dabei wird dort angenommen, dass die wesentlichen Werte in heutigen Unternehmen durch die Kernprozesse gegeben sind. Dort heißt es konkret: *»Jeder Auftragsverarbeiter und gegebenenfalls sein Vertreter führen ein Verzeichnis zu allen Kategorien von im Auftrag eines Verantwortlichen durchgeführten Tätigkeiten der Verarbeitung.«* Das geforderte Verfahrensverzeichnis (Artikel 30 der DSGVO) ist also eine besondere Sicht auf digitale Assets, die im weiteren dann noch um die eigentlichen Daten-Assets, also insbesondere *»Kategorien personenbezogener Daten«*, verfeinert werden. Die DSGVO fordert für dieses Verfahrensverzeichnis eine Vollständigkeit, da dies die Ausgangsbasis für eine strukturierte Risikoanalyse darstellt [DSGVO 16].

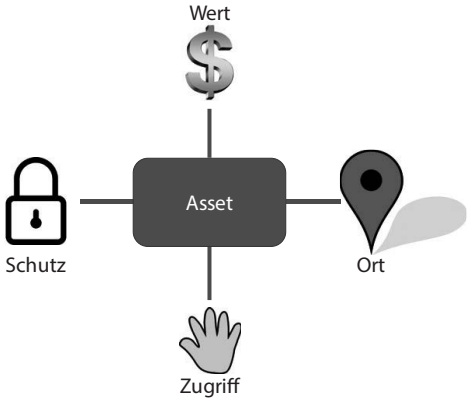


Abb. 1–3
Relevante Aspekte eines Assets für die Risikoanalyse

Für beide Arten von Assets, hier aber vor allen Dingen für digitale Assets, müssen grundsätzlich als Teil einer Risikobewertung folgende Fragen beantwortet werden:

- **Wert**
  Wie wertvoll ist das Asset?
- **Ort**
  Wo liegen die Assets?
- **Zugriff**
  Wie erfolgt der Zugriff auf die Assets?
- **Schutz**
  Wie sind die Assets geschützt?

1.1.2.1 Wert eines Assets

Assets: Je wertvoller, desto mehr Sicherheitsschutz ist notwendig.

Der Wert eines Assets entscheidet später ganz wesentlich, wie sicherheitsbedürftig es ist: Kaum werthaltige Assets stehen daher für einen Sicherheitstester meist viel weniger im Fokus als solche, die sehr wertvoll sind, zumindest, solange die Eintrittswahrscheinlichkeit eines Schadens ähnlich ist. Die Wertermittlung ist dabei häufig nicht leicht: Am einfachsten zu bestimmen sind hier noch materielle Werte, die vor allen Dingen für non-digitale Güter relevant sind: So hat eine Maschine einen Wert, der dadurch gekennzeichnet ist, wie teuer ihre Beschaffung war (häufig abzüglich eines Abnutzungsfaktors).

Schwieriger sind solche Assets zu beurteilen, deren Wert sich primär an den Kosten und Folgen ihres Verlustes orientiert. Dies gilt für manche non-digitalen Güter (z.B. Prototypen) und für alle digitalen Güter.

Beispiel: Ein digitales Angebot als Asset

Beispiel: Ein digitales Angebot als Asset

Ein schriftliches Angebot in Form eines PDF-Dokumentes hat keinen materiellen Wert, wohl aber einen Wert, der sich darin bemessen lässt, wie viel Umsatz möglicherweise verloren ginge, wenn das Angebot nicht pünktlich zum Ausschreibungsende vorhanden wäre. Ein anderer Wert für dasselbe Asset könnte dadurch bestimmt werden, was ein Mitbewerber für einen wirtschaftlichen Vorteil hätte, wenn er das Angebot bekäme.

Digitale Assets: schwierig in der Werteermittlung

Der Wert gerade für viele digitale Güter lässt sich meist nicht präzise bestimmen, sodass häufig grobe Abschätzungen oder vergleichbare Erfahrungswerte herangezogen werden.

Beispiel: Ermitteln des Wertes digitaler Assets

Beispiel: Ermitteln des Wertes digitaler Assets

Typische Fragen zu Informationen, im Folgenden wiederum bezogen auf den Verlust des digitalen Assets eines Angebotes – z. B. durch das Nutzen unverschlüsselter E-Mail-Kommunikation –, können bei der Wertermittlung des Assets helfen.

- Der zukünftige Umsatz, den das Asset verspricht, für das Angebot also der hinterlegte Angebotswert.
- Der Wert für einen Mitbewerber, der Kenntnis des Assets erhält und damit wirtschaftliche Vorteile gegenüber dem ursprünglichen Asset-Inhaber bekommt. Im Fall des Angebotes ist dies für Standardangebote entlang wohldefinierter Preistafeln (z. B. Kfz-Versicherungen) irrelevant. Im Fall von Angeboten, in denen individuelle Preisabsprachen, ggf. Umsetzungsdetails und Planungsdetails enthalten sind, kann diese Wertdimension durchaus erheblich sein.
- Der für die Erstellung oder die Neuerstellung des Assets aufgewendete bzw. nötige Zeit- und Aufwandsrahmen. Ein Angebot, für dessen Erstellung z. B. teure Experten hinzugezogen wurden, zeigt in dieser Wertedimension einen deutlichen Ausschlag.
- Strafen, die im Falle des Unvermögens, das Asset bei Bedarf vorweisen zu können, anfallen. Im Beispiel des Angebotes kann dies relevant werden, falls es – z. B. aufgrund des Verdachtes von Preisabsprachen oder datenschutzrechtlichen Befunden – nicht möglich ist, das Originalangebot für ein Audit oder Gerichtsverfahren vorzuzeigen.
- Strafen für den Verlust und vor allen Dingen die Weitergabe von datenschutzrechtlichen Daten. Sind im Angebot z. B. hochsensible Daten enthalten, kann die Offenlegung dieses Assets zu sensiblen Strafen führen, die letztlich auch als möglicher Wert des Assets herangezogen werden können.

1.1.2.2 Der Ort eines Assets

Nur bekannte Orte können geschützt werden.

Der Schutz eines Assets bedarf der Kenntnis, wo das Asset liegt. Dies gilt auch für digitale Assets, die klassischerweise auf Servern, Computern oder Speichermedien wie externen Festplatten oder CDs gespeichert werden. Es ist gerade für digitale Assets wichtig zu erkennen, dass ein Asset durchaus mehrere Orte haben kann. So hat jedes wertvolle Asset üblicherweise wenigstens zwei Orte: Einmal im produktiven Rechenzentrum und einmal in einem angeschlossenen Backup-System. Und selbst innerhalb des produktiven Rechenzentrums haben Assets meist mehrere Orte, da z.B. hochverfügbare Systeme in der Regel Daten fortwährend auf mehrere Festplatten und Systeme verteilen.

Die Menge von Orten nimmt aktuell aufgrund der Verbreitung von USB-Laufwerken, Smartphones und Tablets kontinuierlich zu. Wird einer der Orte im Kontext der Sicherheitsherstellung vergessen, besteht das Risiko, dass für diesen Ort das Sicherheitsniveau ungenügend ist. In der Vergangenheit haben sich gerade portable Orte alias Medien wie USB-Sticks und Speicherkarten als höchst riskant erwiesen. Als »Ort« von kritischen Assets werden sie zu schnell vergessen, obwohl der Wert ggf. außerordentlich hoch ist.

In 2018 wurden hochvertrauliche Daten des sächsischen Verfassungsschutzes, also einer Institution, der ein hohes Risikobewusstsein zugesprochen wird, auf einen USB-Stick kopiert. Dieser Stick als neuer Ort des Assets wurde von einem Mitarbeiter »aus Neugierde« mit nach Hause genommen und unterlag damit nicht mehr dem nötigen Schutz. [Leipziger Volkszeitung 18]

Der Ort von Assets, die in der Cloud abgelegt werden, ist je nach Cloud-Typ unterschiedlich schwer zu bestimmen. In öffentlichen Clouds obliegt der Ort häufig dem Cloud-Anbieter selbst und der konkrete Ort ist dem Asset-Besitzer nicht transparent. Hier kann dann nur die gesamte Cloud als Ort betrachtet (und später abgesichert) werden.

1.1.2.3 Der Zugriff auf ein Asset

Neben dem Wert und dem Ort ist eine weitere wichtige Frage, wie der Zugriff auf das Asset erfolgt. Grundsätzlich gilt hier, dass hierfür jeder Ort eines Assets betrachtet werden muss, da hier der Zugriff erfolgen muss. Während dies bei non-digitalen Gütern fast immer eine physische Präsenz voraussetzt – z.B. um Aktenordner einzusehen –, können digitale Assets deutlich mehr Zugriffsmöglichkeiten bieten:

Am verbreitetsten sind hierfür die folgenden Zugriffsmethoden:

- Zugriff per Computer über ein LAN- (Local Area Network), über ein Wi-Fi-Netz oder lokale Netze (Personal Area Network, PAN, z. B. via Bluetooth). Hierbei müssen sich der Zugriffsinitiator und der Asset-Ort im selben physischen Netz befinden.
- Zugriff aus der Ferne auf einen Asset-Ort, entweder über ein VPN- (Virtual Private Network) oder ein Cloud-Laufwerk. Der Zugriffsinitiator und der Asset-Ort befinden sich hierbei in unterschiedlichen physischen Netzen.
- Direkte Weitergabe physischer Datenspeicher (CDs, DVDs, USB-Laufwerke) von Person zu Person.
- Verschicken oder Teilen von Assets über unterschiedliche Plattformen (via E-Mail, WhatsApp, SnapChat usw.).

1.1.2.4 Der Schutz von einem Asset

Jeder Zugriff auf einen oder mehrere Orte eines Assets kann unterschiedlich geschützt sein. So kann der Zugriff auf ein digitales Asset auf einem USB-Stick dadurch erschwert werden, dass der Stick in einem Tresor eingeschlossen ist. Für die Zugriffsart des Auslesens des USB-Sticks kann wiederum Verschlüsselung eine wichtige Schutzrolle übernehmen.

Assets können durch eine angemessene Authentifizierung, Autorisierung und Verschlüsselung geschützt werden.

Der Schutz von Assets und ihren Zugriffen im Allgemeinen kann vor allen Dingen über drei Aspekte erfolgen (vgl. hierzu auch Kap. 5):

- **Authentifizierung**
  Jeder Zugriff ist nur nach einer Identifikation des Asset-Interessenten erlaubt. Der Fingerabdrucksensor eines modernen Smartphones ist eine typische Authentifizierungsmaßnahme, um den Anwender eindeutig zu identifizieren.
- **Autorisierung**
  Welche Berechtigungen hat ein authentifizierter Nutzer für das Asset? Darf er es nur lesen oder auch schreiben und löschen.
- **Verschlüsselung**
  Die Verschlüsselung bezieht sich vor allen Dingen auf die Form der Abspeicherung sowie die Form der Übertragung.

1.1.3 Analyse von Verfahren der Risikobewertung

Sicherheitsrisikobewertungen ähneln sehr stark einer standardmäßigen Risikobewertung.

Die Bewertung der speziellen Sicherheitsrisiken ähnelt sehr stark einer standardmäßigen Risikobewertung. Ergebnisse einer Sicherheitsbewertung fließen gerade in größeren Unternehmen in eine allgemeinere Risikobewertung ein. Beispiele allgemeinerer und damit nicht mehr in den Bereich der IT-Sicherheit fallender Risikobewertungen sind Währungsrisiken, Unwetterrisiken und politisch-gesellschaftliche Risiken.

Eine Sicherheitsrisikobewertung sollte die Perspektiven möglichst vieler interner und externer Stakeholder (Schlüsselpersonen) einnehmen. Je ganzheitlicher diese Perspektiven ausgewählt werden, desto vollständiger wird die Risikoidentifikation und -beurteilung sein.

Je mehr Perspektiven eine Sicherheitsbewertung berücksichtigt, desto ganzheitlicher ist sie.

Zu typischen Stakeholdern für eine Sicherheitsbewertung zählen neben der Organisation selbst, die die Assets verwaltet:

- **Kunden und Benutzer**
  Aus dieser Perspektive können typische Anwendungsfälle betrachtet werden, insbesondere IT-Infrastruktur (da z.B. gerade Privatkunden nicht die modernste IT verwenden) und fahrlässige Verhaltensweisen (z.B. ein und dasselbe Passwort für verschiedene Systeme). Diese Perspektive hilft auch bei der Risikobewertung, da gerade Kundendaten häufig im Fokus von Risikoanalysen stehen.
- **Öffentlichkeit und Gesellschaft**
  Auch die Öffentlichkeit und Gesellschaft kann für eine Analyse herangezogen werden. So sind z.B. regelmäßig geänderte Datenschutzbestimmungen technisch und juristisch problemlos möglich, werden aber von der Öffentlichkeit in der Regel als störend wahrgenommen. Hilfreich sind hier repräsentative Studien, die einen guten Eindruck über die Gesamtstimmung vermitteln. Ein plakatives Beispiel ist die teilweise sehr ernüchternde Wahrnehmung der Sinnhaftigkeit der neuen DSGVO (vgl. [Woll 18]). Auch die Planung von Kommunikation z.B. im Falle von Sicherheitsvorfällen muss diese Stakeholder berücksichtigen, da ansonsten trotz aller technischen und legalen Konformität die Reputation gefährdet sein kann.
- **Aufsichtsbehörden**
  Diese Stakeholder sind durch Vorgabe von Mindestanforderungen an das Sicherheitsmanagement ganz wesentlich. In Deutschland ist hier z.B. für den Bereich der Banken und Versicherungen die Bundesanstalt für Finanzdienstleistungen (BaFin) ein wichtiger Stakeholder, für kritische Infrastruktur ist das Bundesamt für Informationssicherheit (BSI) zuständig. Aufsichtsbehörden sind notwendig für die Gewährleistung der Konformität mit geltenden Gesetzen bezüglich der Informationssicherheit.

Der gesamte Prozess einer Risikobewertung und damit auch einer spezielleren Sicherheitsbewertung erfolgt in der Regel in drei Schritten, wie in Abbildung 1–4 dargestellt.

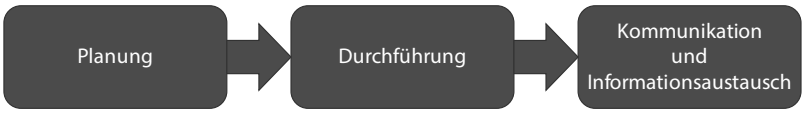


Abb. 1–4
Drei Schritte einer Risikobewertung

Diese High-Level-Darstellung lässt sich ebenfalls problemlos auf die ISO 31000 abbilden (vgl. Abb. 1–1): Die Planung wird dort als Zusammenhangerstellung, die Durchführung als Risikobeurteilung und der Schritt Kommunikation und Maßnahmen als Kommunikation und Beratung beschrieben.

Risikobewertung bedarf einer klaren Planung.

Die Planung (bzw. eben die Zusammenhangerstellung) besteht hierbei vor allen Dingen aus folgenden Aktivitäten und orientiert sich meist am organisatorischen Gesamtrahmen (in der Norm NIST 800-30 selbst als »Organizational Risk Frame« bezeichnet; für Deutschland ist hier häufig der sehr ähnliche BSI-Standard 200-3 maßgeblich [BSI 200-3 17]):

- Ermittlung des Zwecks der Bewertung: Erfolgt die Bewertung proaktiv, um das gesamte Gefährdungspotenzial abzuschätzen, oder reaktiv, um z.B. bei Bekanntwerden einer Sicherheitslücke das spezifische von dieser Lücke für ein Unternehmen ausgehende Risiko zu ermitteln.
- Ermittlung des Umfangs der Bewertung: Dies kann von einigen wenigen Stunden für einen Mitarbeiter bis hin zu Monaten und Jahren für ganze Teams reichen. Ein gutes Beispiel für einen großen Umfang ist z.B. das vom neuen Regulativ der Datenschutz-Grundverordnung [DSGVO 16] ausgehende Risiko im Falle der Nichteinhaltung. Hier haben einige Unternehmen mehrköpfige Teams über mehrere Jahre eingesetzt.
- Ermittlung der Annahmen und Randbedingungen im Zusammenhang mit der Bewertung. Möglich sind hier z.B. die Nennung von gültigen Gesetzen oder Annahmen über Nutzerprofile.
- Ermittlung der Informationsquellen, die als Eingangsquelle für die Bewertung genutzt werden. Möglich sind hier z.B. öffentliche Informationsquellen wie das BSI oder auch Analystenreports wie von Gartner und Forrester.
- Ermittlung des Risikomodells und der analytischen Konzepte (d.h. Bewertungs- und Analysekonzepte), die bei der Bewertung zu nutzen sind. Hier sind vor allen Dingen Angaben darüber zu machen,

wie die Werte der digitalen Assets ermittelt werden, wie die Risikowahrscheinlichkeiten abgeschätzt wurden, wie Aussagen über mögliche Schadensauswirkungen abgeleitet wurden und welche Risikotoleranz bzw. welchen Risikoappetit ein Unternehmen hat, wie also »*Ertrag und Risiko in der Vorbereitung unternehmerischer Entscheidungen gegeneinander abgewogen werden sollen*« [Gleißner & Wolfrum 17].

Die Durchführung von Risikobewertungen umfasst folgende spezifische Aufgaben und orientiert sich sehr eng an der ISO 31000 und den dort formulierten Schritten (vgl. Abschnitt 1.1.1.1, [NIST SP 800-30 02] und [BSI 200-3 17]):

- Ermittlung der Gefährdungsquellen, die für das Unternehmen relevant sind. Hierzu zählen grundsätzlich alle Quellen, die eine mögliche Gefährdung auf Assets darstellen. Möglich sind hier z.B. Eingangsbereiche, elektronische Zugänge (WLAN, VPN) oder auch Spionage eigener Mitarbeiter.
- Ermittlung der Gefährdungsereignisse, die von diesen Quellen ausgehen können. Der Eingangsbereich kann z.B. blockiert oder für Diebstähle missbraucht werden. Ein elektronischer Zugang kann z.B. gekappt oder abgehört werden.
- Ermittlung von Schwachstellen im Unternehmen, die von Gefährdungsquellen mittels konkreter Gefährdungsereignisse ausgenutzt werden könnten. Nicht jedes Gefährdungsereignis jeder Gefährdungsquelle kann tatsächlich zu einer Ausnutzung verwendet werden. Gibt es z.B. ein elektronisches Zutrittssystem, so kann ein unbefugter Zutritt je nach konkreter Umsetzung verhindert oder wenigstens gemindert werden. Auch eine Kappung des elektronischen Zugangs kann nur dann ausgenutzt werden, wenn keine Notfall-Stromversorgung existiert. In diesem Schritt geht es darum, solche Schwachstellen zu identifizieren, für die es konkrete Gefährdungsereignisse über bestimmte Gefährdungsquellen gibt.
- Ermittlung der Wahrscheinlichkeit, mit der ermittelte Gefährdungsquellen spezielle Gefährdungsereignisse initiieren, sowie der Erfolgswahrscheinlichkeit von Gefährdungsereignissen.
- Ermittlung von schädlichen Folgen (Auswirkungsanalyse, Impact-Analyse) für betriebliche Vorgänge und Assets, Einzelpersonen (z.B. auf ihre körperliche Unversehrtheit), andere Unternehmen/Organisationen und ggf. das gesamte Land, die aus der Ausnutzung von Schwachstellen durch die Gefährdung herrühren.

Die Kommunikation und der Informationsaustausch stellen in die eine Richtung sicher, dass die Ergebnisse der Risikobeurteilung auch entsprechend bekannt gemacht werden, um ggf. notwendige Maßnahmen zur Risikobewältigung abzuleiten. In die andere Richtung liefert sie wichtige Informationen für die Risikobewertung selbst.

Der konkrete Kommunikationsplan orientiert sich dabei eng an den Festlegungen des ersten Schrittes »Planung«. Erfolgt die Risikobeurteilung für den Zweck eines Gutachtens einer außenstehenden Instanz (z. B. im Kontext von Due-Diligence-Analysen oder zum Beleg bestimmter Compliance-Anforderungen), so beschränkt sich die Kommunikation ggf. auf den Informationsaustausch mit der außenstehenden Instanz. Erfolgt die Risikobeurteilung vor dem Hintergrund einer effektiven Ist-Stand-Erhebung mit anschließender Toleranzprüfung (im Sinne eines »ist dieses Gesamtrisiko für ein Unternehmen noch tragbar«), so wird dem Informationsaustausch ein konkreter Schritt folgen, um Maßnahmen zur Risikoreduktion abzuleiten.

1.2 Informationssicherheitsrichtlinien und -verfahren

1.2.1 Verstehen von Informationssicherheitsrichtlinien und -verfahren

Die Informationssicherheitsrichtlinien: ähnlich zur klassischen Testrichtlinie

Der Begriff der Richtlinie ist bereits aus dem klassischen funktionalen Testen bekannt:

Testrichtlinie

Ein Dokument, das auf hohem Abstraktionsniveau die Prinzipien, Vorgehensweisen und wichtigsten Ziele einer Organisation in Bezug auf das Testen zusammenfasst. [GTB Glossar 18]

Eine solche Richtlinie ist üblicherweise deutlich mehr als eine Sammlung von solchen Prinzipien und Vorgehensweisen: Anders als eine Leitlinie, die grundsätzlich eher empfehlenden Charakter hat, fordert eine Richtlinie normativ etwas. Während eine Leitlinie durchaus in begründeten Fällen explizit nicht angewendet wird, ist dies für Richtlinien in der Regel nicht möglich (vgl. [Huber 13]). Richtlinien sollten daher auch Aussagen darüber enthalten, was passiert, wenn sie nicht eingehalten werden.

Sicherheitsrichtlinien sind in Organisationen ähnlich positioniert: Sie geben für unterschiedliche Schlüsselrollen (z. B. IT-Nutzer, Administratoren oder Manager) verbindliche Prinzipien, Vorgehensweisen und die wichtigsten Ziele der Organisation hinsichtlich der Sicherheit vor.