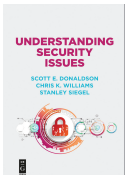
Stefan Beißel
Security Awareness

Weitere empfehlenswerte Titel

IT-Sicherheit, 10. Auflage
Konzepte - Verfahren - Protokolle
Claudia Eckert, 2018
ISBN 978-3-11-055158-7, e-ISBN 978-3-11-056390-0

IT-Sicherheit
Eine Einführung
Hellmann, Roland, 2018
ISBN 978-3-11-049483-9, e-ISBN 978-3-11-049485-3



Understanding Security Issues
Scott Donaldson / Chris Williams / Stanley Siegel, 2018
ISBN 978-1-5015-1523-1, e-ISBN 978-1-5015-0650-5

Intelligent Multimedia Data Analysis
Hrsg. v. Siddhartha Bhattacharyya / Indrajit Pan / Abhijit Das / Shibakali Gupta, 2019
ISBN 978-3-11-055031-3, e-ISBN 978-3-11-055207-2

Stefan Beißel

Security Awareness

Grundlagen, Maßnahmen und Programme
für die Informationssicherheit

DE GRUYTER

ISBN 978-3-11-066825-4
e-ISBN (PDF) 978-3-11-066826-1
e-ISBN (EPUB) 978-3-11-060826-7

Library of Congress Control Number: 2019946156

Bibliographic information published by the Deutsche Nationalbibliothek
The Deutsche Nationalbibliothek lists this publication in the Deutsche Nationalbibliografie; detailed bibliographic data are available on the Internet at http://dnb.dnb.de.

© 2019 Walter de Gruyter GmbH, Berlin/Boston
Cover image: monsitj / iStock / Getty Images Plus
Printing and binding: CPI books GmbH, Leck

www.degruyter.com

Vorwort

Security Awareness ist aufgrund der steigenden Bedrohung durch Social Engineering und immer strengerer Compliance-Anforderungen mittlerweile unverzichtbar. Die moderne Informationstechnik ist in fast jedem Unternehmen ein integraler Bestandteil und oft auch ein wesentlicher Erfolgsfaktor. IT-Systeme und -Daten müssen geschützt werden, um Beeinträchtigungen des Geschäftsbetriebs zu vermeiden. Nur wenn sich alle Mitarbeiter über die Risiken bei ihrer Arbeit bewusst sind und sich in sicherheitsrelevanten Situationen korrekt verhalten, kann im Unternehmen ein angemessenes Sicherheitsniveau geschaffen werden.

Viele Angriffe zielen auf die Unwissenheit oder Nachlässigkeit von Personen ab. Diese „Schwachstellen" kann man nur mit geeigneten Awareness-Maßnahmen beseitigen. Aber welche Maßnahmen sind geeignet und wie können unterschiedliche Maßnahmen in ein strukturiertes Konzept eingebettet werden? Wenn man hierauf eine Antwort finden möchte, sind fachliche Grundlagen zur Security Awareness und Informationen zu den Gestaltungsmöglichkeiten von Awareness-Maßnahmen äußerst hilfreich. Die infrage kommenden Medien, Inhalte und Umsetzungsmerkmale sind vielfältig. Die passende Kombination für eine Awareness-Maßnahme zu finden, ist nicht einfach und eine einzelne Maßnahme oft nicht ausreichend, um das Awareness-Niveau im Unternehmen nachhaltig zu erhöhen. Daher macht es Sinn, alle Aktivitäten rund um die Security Awareness in einem Programm zu organisieren. Die überlegte Bearbeitung von Programm-Phasen hilft dabei, eine Kombination geeigneter Maßnahmen zu planen und umzusetzen. Damit kann die Security Awareness am effektivsten erhöht werden.

Dieses Buch deckt das gesamte Spektrum von den Grundlagen der Informationssicherheit und der Security Awareness bis zur individuellen Gestaltung und Umsetzung von Awareness-Maßnahmen im Unternehmen ab. Die verschiedenen Kapitel verhelfen zu einer schnellen Orientierung und ermöglichen eine gezielte Fokussierung auf bestimmte Themenbereiche. Die Zusammenfassung bringt die Kernaussagen des Buchs in komprimierter Weise auf den Punkt und ermöglicht einen schnellen Einblick in die Phasen eines Awareness-Programms.

Bergisch Gladbach, im Juli 2019 Stefan Beißel

https://doi.org/10.1515/9783110668261-202

Inhalt

Abbildungsverzeichnis

https://doi.org/10.1515/9783110668261-204

1 Einführung

1.1 Gefahren

Die **Informationstechnik** (IT) hat sich in den letzten Jahrzehnten zu einem wesentlichen Bestandteil unserer Gesellschaft entwickelt. Sowohl im Privat- als auch im Berufsleben sind wir ständig von IT-Systemen umgeben. Informationen werden zunehmend elektronisch gespeichert, übertragen und verarbeitet. Von der elektronischen Rechnung bis zur Online-Videothek – die traditionellen Medien werden zunehmend durch IT-Lösungen ersetzt. Aus den Perspektiven der Effizienz und Umweltfreundlichkeit ist dies in der Regel sehr vorteilhaft.

Allerdings entsteht dadurch auch eine stärkere **Abhängigkeit** zur IT. Ein abgestürzter Computer hindert Berufstätige daran, ihre Arbeit auszuführen, und ein defektes Smartphone erschwert alltägliche Dinge, z. B. einen Einkaufszettel abzurufen oder eine Verkehrsroute zu finden. Die Durchdringung der IT, und damit auch die Abhängigkeit zur IT, erhöhen sich zunehmend. Die Budgets für neue IT-Investitionen in Unternehmen steigen entsprechend an.

Durch die immer stärkere Verknüpfung wesentlicher Abläufe mit unserer IT-Umgebung entstehen nicht nur neue Möglichkeiten, sondern auch neue **Gefahren**. IT-Systeme und elektronisch gespeicherte Informationen sind immer davon bedroht, kompromittiert, manipuliert oder beschädigt zu werden. Vertrauliche Informationen (z. B. Zahlungsdaten, Patientenakten oder geheime Geschäftsstrategien) sind bei Hackern heiß begehrt. Sie versuchen ständig und mit immer professionellerem Vorgehen, diese Daten einzusehen und für ihre Zwecke zu missbrauchen. Mit geschickten Manipulationen können Hacker ebenfalls persönliche Vorteile erlangen. Sie ändern Daten auf ihrem Übertragungsweg oder an ihrem Speicherort, z. B. durch die unerlaubte Änderung von Preisen in Online-Shops oder durch die Änderung von Finanztransaktionen. Durch die Beschädigung von Daten und Systemen können Personen und Unternehmen in ihrer Arbeit gestört und finanziell geschädigt werden. Unternehmen sind ohne IT oft kaum noch arbeitsfähig, was zu starken Umsatzeinbußen und hohen Reputationsschäden führen kann.

Dass die Gefahren rund um die IT immer stärker ansteigen, verdeutlicht auch der tendenzielle Anstieg an **Sicherheitsvorfällen** innerhalb der letzten Jahre. Obwohl die Anzahl neuer Sicherheitslücken zeitweise rückläufig ist, nimmt die Breite der bedrohten Systeme weiter zu, sodass sich die Sicherheitslage insgesamt verschärft.

Neue **Trends** im IT-Umfeld, welche in der Regel auf Effizienzerhöhungen durch neue IT-Lösungen ausgerichtet sind, erhöhen die bestehenden Gefahren zusätzlich. Die Geschäftsprozesse werden immer stärker durch die IT durchdrungen. Häufig werden auf diese Weise der Arbeitsaufwand und die Kosten gesenkt. Gleichzeitig werden Unternehmen aber oft mit einer erhöhten Komplexität und mit einer größe-

https://doi.org/10.1515/9783110668261-001

ren Menge an Angriffsmöglichkeiten konfrontiert. Je moderner und neuer eine IT-Lösung ist, desto schwerer kann sie beherrscht und vor Gefahren abgesichert werden. Aufgrund der starken Abhängigkeit vieler Geschäftsprozesse von einer funktionierenden IT-Umgebung, führen Sicherheitsvorfälle oft zur Behinderung des Geschäftsbetriebs und zu gravierenden Schäden. In den letzten Jahren konnten sich viele Trends durchsetzen, unter anderem mobile Geräte, soziale Netzwerke und Cloud Computing:

- **Mobile Geräte**, z. B. Notebooks, Smartphones und Tablets, ermöglichen eine immer größere Flexibilität bei der Aufgabenerfüllung. Die Integration dieser Geräte in den IT-Verbund eines Unternehmens birgt jedoch hohe Gefahren. Sie können aufgrund des ständigen Transports schneller verloren gehen oder gestohlen werden. Beim mobilen Arbeiten befinden sich die Mitarbeiter oft in weniger sicheren Umgebungen, z. B. an vielbesuchten öffentlichen Orten. Dort können Daten leichter ausgespäht werden als in einer kontrollierten Einrichtung des Unternehmens. **Bring Your Own Device** (BYOD) bezeichnet die Möglichkeit, dass die Mitarbeiter eines Unternehmens ihre eigenen Geräte mitbringen. Die Geräte werden von den Mitarbeitern privat beschafft und administriert. Sie werden auf Wunsch des Mitarbeiters mehr oder weniger stark in die IT-Umgebung des Unternehmens integriert. Da das Unternehmen allerdings nur eine beschränkte Kontrolle über diese Geräte besitzt, können viele sicherheitsrelevante Einstellungen und Installationen nicht ohne weiteres vorgenommen werden. Außerdem können die Mitarbeiter während ihrer privaten Nutzung uneingeschränkt auf schadhafte Dateien oder Webseiten zugreifen. Selbst wenn im Unternehmen spezielle Richtlinien über den Umgang mit den Geräten vorhanden sind, werden sie aufgrund von fehlendem Verständnis oder mangelndem Sicherheitsbewusstsein oft nicht befolgt. Sollte ein Gerät erfolgreich angegriffen worden sein, sind nicht nur die persönlichen Daten des Mitarbeiters, sondern auch Unternehmensdaten gefährdet. Um die Gefahren beim BYOD abzumildern, kann auch ein Kompromiss zwischen reinen Firmengeräten und BYOD-Geräten gefunden werden. Hierbei werden bedeutende Sicherheitseinstellungen der Geräte zwar zentral verwaltet, jedoch wird den Mitarbeitern eine maximal mögliche Flexibilität bei der Nutzung der Geräte eingeräumt. Voraussetzung ist, dass die Mitarbeiter vor der Anbindung ihrer Geräte ins Unternehmensnetzwerk ihre Erlaubnis dazu erteilen, dass ihre Geräte durch das Unternehmen verwaltet und überwacht werden. Unabhängig davon, ob unternehmenseigene oder private Geräte im Unternehmen eingesetzt werden, gehen mit mobilen Geräten viele **Gefahren** einher, die ein Unternehmen kennen und bewältigen sollte:
  - Aufgrund des häufigen Transports und mobilen Einsatzes können mobile Geräte schneller abhandenkommen als stationäre Geräte. **Verlust oder Diebstahl** können nicht nur dazu führen, dass Informationen nicht mehr verfügbar sind, sondern auch, dass sie unberechtigt ausgelesen und miss-

braucht werden. Insbesondere wenn Daten unverschlüsselt auf den mobilen Geräten gespeichert werden, können Angreifer mit geringem Aufwand an sensitive Daten gelangen.

- Die **Datenübertragung** muss aufgrund der Mobilität zeitweise über öffentliche Netze erfolgen. Eine Beschränkung der Datenübertragung auf das interne Unternehmensnetzwerk ist nicht mehr praktikabel. Dadurch ergeben sich Gefahren für die Daten auf ihrem Übertragungsweg. Wenn sie nicht geschützt werden, können sie während der Übertragung von Angreifern mitgelesen, manipuliert oder beschädigt werden. Zusätzliche Gefahren können entstehen, wenn Datenprotokolle eingesetzt werden, über die das Unternehmen noch wenig Erfahrung besitzt. Fehler in der Sicherheitskonfiguration und unbekannte Schwachstellen bieten Unbefugten zusätzliche Angriffsmöglichkeiten.
- Die **Komplexität** der eingesetzten mobilen Geräte nimmt ständig zu. Nicht nur die Betriebssysteme und Applikationen werden zunehmend umfangreicher und mächtiger, auch die Heterogenität der auf dem Markt erhältlichen Geräte steigt kontinuierlich. Insbesondere, wenn BYOD-Geräte genutzt werden, ist die Vielzahl an unterschiedlichen Geräten und Konfigurationsmöglichkeiten immer schwerer zu überschauen. Unerkannte Details, z. B. seltene Applikationen oder Datenschnittstellen, bieten neue Angriffsmöglichkeiten. Werkseinstellungen sind meist unsicher und müssen je nach Geräteversion individuell angepasst werden. Auch der technische Support wird gefordert, mit seltenen oder kaum bekannten Geräten umzugehen, was zu ungelösten Problemen und frustrierten Mitarbeitern – sowohl im Support als auch bei den Benutzern – führen kann. Aufgrund mangelnder Kompatibilität von Sicherheitsprogrammen besteht zudem die Gefahr, dass diese unbemerkt deaktiviert werden oder sogar vorsätzlich umgangen werden.
- Die Entwicklung und Überwachung von geeigneten **Kontrollmaßnahmen** gestalten sich bei mobilen Geräten schwieriger. Je heterogener die Geräte sind, desto zeitaufwändiger und problemanfälliger wird die Implementierung von Kontrollmaßnahmen auf den Geräten. Schlecht abgestimmte Sicherheitssoftware könnte die Bedienung der Geräte beeinträchtigen. In der Folge sind die Mitarbeiter unzufrieden und versuchen, Sicherheitsprogramme zu deaktivieren oder zu umgehen. Da die Geräte oft lange unterwegs sind, können Probleme teilweise nur schwer behoben werden. Datenlöschungen und intensive Geräteüberwachung aus der Ferne sind kompliziert, wenn die Mitarbeiter mit den Geräten persönliche Daten einsehen und speichern, was vor allem bei BYOD-Geräten der Fall ist.
- Die **Kompatibilität** der mobilen Geräte zu vorhandenen Geschäftsprozessen und im Unternehmen etablierten Applikationen und Dateiformaten kann durch bestimmte Geräte unter Umständen nicht hergestellt werden.

Folglich wird entweder die Arbeit der betroffenen Mitarbeiter gestört, was das Sicherheitsziel der Verfügbarkeit betreffen würde, oder es werden Workarounds gesucht, die bestehende Kontrollmaßnahmen womöglich ebenfalls umgehen.

- **Regulatorische Vorgaben** zum Umgang mit Daten und Systemen müssen natürlich auch beim Einsatz mobiler Geräte eingehalten werden. Darunter fallen z. B. die Verschlüsselung oder Archivierung von Daten. Aufgrund der technischen Restriktionen von mobilen Geräten können einzelne Vorgaben allerdings nur schwer implementiert und überwacht werden. Auch die Vermischung von privater und geschäftlicher Nutzung mobiler Geräte kann zu Problemen führen, vor allem bei der Einhaltung des Datenschutzes.

Der Einsatz mobiler Geräte sollte also gut überlegt sein. Das Unternehmen sollte sich der vorhandenen Gefahren bewusst sein und auf jeden Fall passende und funktionierende Kontrollmaßnahmen einsetzen. Mit diesen Kontrollmaßnahmen sollten die Gefahren so weit wie möglich beseitigt oder eingegrenzt werden. Wichtige Kontrollmaßnahmen für mobile Geräte sind unter anderem Verschlüsselung, Mobile Device Management und geeignete Sicherheitsrichtlinien.

- **Soziale Netzwerke**, wie Facebook, Twitter und Xing, haben sich in den letzten Jahren zu einem wichtigen Kommunikationsmedium entwickelt. Sowohl aus dem privaten als auch geschäftlichen Umfeld sind sie kaum noch wegzudenken. Durch die Erstellung und den Austausch von benutzergenerierten Inhalten konnte bei den Benutzern eine hohe Akzeptanz und Verbreitung erreicht werden. Mit den neuen Nutzungsmöglichkeiten gehen aber auch neue Risiken einher, wie Reputationsschäden durch negative Inhalte. Da vor allem die Veröffentlichung negativer Kommentare für jede Person mit Internetzugang sehr einfach ist, sollte das Unternehmen möglichst schnell darauf reagieren können. Um innerhalb des eigenen Unternehmens die Nutzung zu kontrollieren, kann unter anderem der dafür autorisierte Benutzerkreis mit technischen Maßnahmen eingeschränkt werden. Außerdem ist eine Nutzungsrichtlinie für soziale Netzwerke vorteilhaft. Die **Gefahren**, die mit sozialen Netzwerken in Verbindung stehen, sind in erster Linie:
  - Die **Vertraulichkeit** von sensitiven Informationen kann gefährdet werden, wenn Mitarbeiter Informationen in sozialen Netzwerken veröffentlichen. Aus mangelndem Sicherheitsbewusstsein wird oft nachlässig mit Informationen umgegangen. Selbst dann, wenn ein Verstoß gegen Sicherheitsvorgaben zeitnah erkannt wird und die Informationen wieder entfernt werden, können die Daten bereits von Unbefugten eingesehen und weiterverteilt worden sein. Durch die Veröffentlichung vertraulicher Daten werden oft auch verbindliche Regularien verletzt, was zu hohen Strafen, Schadensersatzforderungen und Imageverlusten führen kann. Insbesondere personenbezogene Daten und Zahlungsdaten sind hiervon betroffen. Wenn vertrauliche Daten über Reisepläne, Treffpunkte oder ähnliches öffentlich bekannt

gemacht werden, kann auch eine Gefahr für Leib und Leben hochrangiger Mitarbeiter bestehen: Anschläge könnten mit diesen Informationen zielgenauer geplant werden.

- **Imageschäden** können entstehen, wenn Personen, die dem Unternehmen Schaden möchten oder einen Groll gegen das Unternehmen hegen, negative oder sogar verleumderische Kommentare veröffentlichen. Dazu gehören z. B. verärgerte ehemalige Angestellte oder Konkurrenten. Auch ein unachtsamer Umgang mit sozialen Netzwerken kann dazu führen, dass ungünstig formulierte Kommentare oder andere Inhalte veröffentlicht werden. Sie können ein Grund für negative Reaktionen durch die Öffentlichkeit sein. Imageschäden ziehen meist auch finanzielle Verluste nach sich, da unter anderem die Höhe von Umsätzen oder Aktienkursen beeinträchtigt werden kann. Imageschäden betreffen nicht nur das Unternehmen im Gesamten. Auch das Ansehen einzelner Personen kann von negativen Äußerungen betroffen sein. Das Unternehmen sollte grundlegende Überlegungen anstellen, wie mit negativen Inhalten verfahren werden soll und welche unternehmenseigenen Reaktionen angebracht sind, um die Gefahr von Imageschäden zu reduzieren.

- **Cloud Computing** bietet eine bedarfsgerechte Bereitstellung von IT-Ressourcen durch einen Dienstleister über ein Netzwerk. Für den Kunden führt dies zu einer hohen Flexibilität und einer niedrigen Komplexität beim Abruf von Ressourcen. Durch den gesunkenen Investitionsbedarf in Hard- und Software kann der Kunde außerdem von einer Kostenersparnis profitieren. Allerdings ergeben sich daraus neue Bedrohungen, denn es werden mehr Daten über das Netzwerk übertragen und in einer externen Einrichtung eines Dienstleisters gespeichert. Die Absicherung der Daten sollte also überdacht werden. Sowohl auf dem Übertragungsweg als auch beim Dienstleister können geschäftskritische Daten und Systeme stärker von Bedrohungen betroffen sein. Große Teile der Sicherheit müssen je nach **Servicemodell** vom Dienstleister bereitgestellt oder zumindest unterstützt werden. Im Speziellen unterscheidet das National Institute of Standards and Technology (NIST) drei verschiedene Modelle:[1]
  - Beim **Software as a Service (SaaS)** kann der Kunde auf Applikationen, die der Dienstleister über die Cloud bereitstellt, zugreifen. Sie sind von verschiedenen Endgeräten zugänglich, z. B. über einen Web-Browser.
  - Beim **Platform as a Service (PaaS)** hat der Kunde die Möglichkeit, selbst erstellte oder beschaffte Applikationen in der Softwareumgebung des Dienstleisters zu betreiben.
  - Beim **Infrastructure as a Service (IaaS)** stellt der Dienstleister dem Kunden grundlegende IT-Ressourcen, wie Prozessorleistung, Speicherplatz und

1 Vgl. Mell u. Grance 2011, S. 2 f.

Netzwerke, bereit. Der Kunde kann darauf beliebige Software ausführen, inklusive selbst ausgewählter Betriebssysteme. Für die softwareseitige Administration der genutzten Systeme ist der Kunde selbst verantwortlich.

Daraus ergeben sich für den Kunden und den Dienstleister unterschiedliche **Verantwortlichkeiten** in Bezug auf die Administration.[2] Während beim SaaS der Kunde lediglich für die Daten und gegebenenfalls einige Schnittstellen verantwortlich ist, muss er beim IaaS das gesamte Spektrum von den Daten bis zur virtuellen Infrastruktur abdecken. Der Dienstleister verantwortet dann ausschließlich die physischen Geräte und Einrichtungen. Beim PaaS hingegen kümmert sich der Dienstleister zusätzlich um Betriebssysteme sowie virtuelle Systeme und Infrastruktur. Aus den verschiedenen Verantwortlichkeiten bei der Administration ergeben sich auch verschiedene Verantwortlichkeiten für die Umsetzung und Pflege von Kontrollmaßnahmen, die für eine angemessenen Sicherheit erforderlich sind. Während sich beim SaaS der Dienstleister selbstständig um Firewalls und die Härtung der Systeme kümmert, muss der Kunde beim PaaS und IaaS dabei mitwirken. Durch den Einsatz von Cloud Computing ergeben sich oft neue **Gefahren**, die zu gravierenden Schäden führen können, wenn man sich nicht mit ihnen auseinandersetzt:

- Die **Kontrollmaßnahmen** werden nicht mehr ausschließlich durch den Eigentümer der Daten entwickelt und betrieben. Wie oben bereits erwähnt geht die Verantwortung für viele Kontrollmaßnahmen auf den Dienstleister über. Der Kunde ist je nach Servicemodell gar nicht mehr dazu im Stande, bestimmte Kontrollmaßnahmen, z. B. die physische Zutrittskontrolle oder die Härtung von Betriebssystemen selbst durchzuführen. Der Kunde und der Dienstleister müssen nicht nur ein Bewusstsein darüber besitzen, welche Kontrollmaßnahmen erforderlich sind, sondern sich auch im Klaren darüber sein, wie die Verantwortlichkeiten aufgeteilt sind. Die bloße Annahme, dass sich der jeweils andere um bestimmte Kontrollmaßnahmen oder die Sicherheit im Allgemeinen kümmert, kann gravierende Folgen haben. Sollten nämlich fundamentale Kontrollmaßnahmen vernachlässigt oder sogar ganz übersehen werden, können das Sicherheitsniveau stark beeinträchtigt und sogar die gesamte Geschäftsfähigkeit gefährdet werden.
- Der Kunde sollte eine gewisse Skepsis gegenüber dem Dienstleister besitzen. Dieser kann aufgrund seiner privilegierten Zugriffsrechte grundsätzlich auf alle Daten in der Cloud zugreifen. Der Kunde sollte sich bewusst sein, dass keine betriebsfertigen technischen Barrieren gegen den **Missbrauch** der Daten durch den Dienstleister vorhanden sind. Zum einen sollte eine nachvollziehbare Vertrauensbasis vorhanden sein und zum anderen sollten Kontrollen entwickelt werden, welche dazu verhelfen, eventuellen

2 Vgl. PCI SSC 2013, S. 8.

Missbrauch zumindest zu erkennen. Unter anderem kann das Recht auf 2nd-Party-Audits (also Überprüfungen durch den Kunden) in der Dienstleistungsvereinbarung festgelegt werden. Nicht nur der beabsichtigte Missbrauch durch den Dienstleister sollte adressiert werden, sondern auch ein Missbrauch durch Dritte, der unter Umständen durch Unachtsamkeit oder mangelndes Sicherheitsbewusstsein beim Dienstleister ermöglicht wird. Sollte z. B. keine saubere Trennung der Daten verschiedener Kunden existieren, besteht die Gefahr, dass sich andere Kunden unberechtigten Zugriff auf Daten verschaffen oder dass Angriffe von Hackern die Daten mehrerer Kunden gleichzeitig gefährden.

- Die **Verfügbarkeit** der Daten kann beim Cloud Computing stark gefährdet werden. Im Fall von Störungen kann der Kunde womöglich wichtige Geschäftsprozesse nicht mehr ausführen – z. B. können wichtige Applikationen und Daten nicht mehr zugreifbar sein und Schnittstellen zu Geschäftspartnern und Kunden blockiert werden. Der Kunde sollte sich vor der Inanspruchnahme von Cloud-Services über die technische Zuverlässigkeit und Wiederherstellbarkeit informieren. Da nicht alle Arten von Störungen sinnvoll verhindert werden können, sollten Maßnahmen zur Wiederherstellung von Systemen und Daten entwickelt werden. Nur wenn Backups regelmäßig erstellt werden und bei Bedarf zuverlässig zurückgespielt werden können, kann ein dauerhafter Verlust von Daten verhindert werden. Aber auch die geschäftliche Überlebensfähigkeit des Dienstleisters sollte untersucht werden. Wenn der Dienstleister, z. B. wegen Zahlungsunfähigkeit, den Geschäftsbetrieb einstellen muss, müssen die Daten in angemessener Zeit an den Kunden zurückgegeben werden können.
- **Rechtliche und regulatorische Rahmenbedingungen** sollten ebenfalls nicht vernachlässigt werden. Rechtliche Folgen entstehen z. B. aus dem Standort und der Rechtsform des Dienstleisters. Darunter fallen z. B. der Gerichtsstand, die Haftbarkeit des Dienstleisters und eventuelle Konsequenzen aus einer landesüberschreitenden Datenübertragung. Der Dienstleister unterliegt womöglich weniger oder anderen Regularien als der Kunde. Dies könnte dazu führen, dass der Kunde eine falsche Vorstellung über das Sicherheitsniveau beim Dienstleister entwickelt oder dass er durch die Übertragung der Daten unbewusst gegen kritische Regularien verstößt. Der Kunde sollte sich im Vorfeld mit möglichen Problemen auseinandersetzen und die vorherrschenden Rahmenbedingungen bei der Auswahl des Cloud-Dienstleisters berücksichtigen.
- Zudem ergeben sich Risiken durch eine unkontrollierte Inanspruchnahme von öffentlich verfügbaren **Cloud-Diensten** durch die Mitarbeiter, insbesondere wenn die Cloud-Dienste im Unternehmen nicht zur Nutzung freigegeben wurden. Aufgrund des umfangreichen Angebots kostenloser Dienste könnten Mitarbeiter unüberlegt sensitive Daten in der Cloud spei-

chern, ohne dass zuvor die IT informiert oder über die Sicherheit nachgedacht wurde.

Heutzutage ist es unabdingbar, sich mit Maßnahmen auseinanderzusetzen, welche die steigenden Bedrohungen im IT-Umfeld beherrschbar machen. Hier besteht die Verknüpfung zur **Security Awareness** (im Folgenden kurz Awareness): Sie hilft, das Bewusstsein über die Notwendigkeit von Sicherheitsmaßnahmen zu erhöhen und Kenntnisse über deren Einsatz und Gestaltung zu vermitteln. Awareness ist – insbesondere vor dem Hintergrund der steigenden Abhängigkeit zur IT und den stärkeren Bedrohungen – ein wesentlicher Bestandteil der Informationssicherheit.

1.2 Bedeutung der Awareness

Awareness ist ein Mittel, um das **Sicherheitsniveau** eines Unternehmens zu erhöhen. Daher dient sie dem Interesse der Stakeholder. Gleichzeitig beeinflusst sie die Stakeholder, die im Unternehmen arbeiten. Sie führt nämlich zu einer Verhaltensanpassung, die darauf abzielt, Systeme und Informationen besser zu schützen.
Unternehmen werden von verschiedenen **Stakeholdern** beeinflusst. Der Begriff Stakeholder ist sehr weit gefasst und meint alle Personen und Personengruppen, die ein Interesse am Zustand oder Erfolg des Unternehmens besitzen. Im weiteren Sinne werden dabei auch Interessenhalter einbezogen, die nur indirekt oder temporär mit dem Unternehmen in Verbindung stehen, z. B. Laufkunden oder politische Interessengruppen.

Das Sicherheitsniveau eines Unternehmens – und damit auch das Awareness-Niveau – wird durch die Interessen der Stakeholder mehr oder weniger stark beeinflusst. Während einige Stakeholder, wie die Geschäftsleitung, direkten **Einfluss** auf die Ausgestaltung der Awareness besitzen, haben andere (z. B. Kunden) eher indirekten Einfluss darauf. Kunden beeinflussen die Umsatzzahlen eines Unternehmens und können ihren Interessen dadurch indirekt Bedeutung verleihen. Welchen Einfluss die Stakeholder in Bezug auf die Awareness eines konkreten Unternehmens besitzen, hängt von den individuellen Eigenschaften und Rahmenbedingungen des Unternehmens ab. Unternehmen, die z. B. in einem stark regulierten Sektor tätig sind, werden stärker von Kontrollorganen beeinflusst als andere. Unternehmen, die von Aktionären besessen werden, werden von ihren Eigentümern anders beeinflusst als Unternehmen in Familienbesitz.

Im Speziellen sind die individuellen Interessen und Machtpositionen der Stakeholder dafür ausschlaggebend, wie stark und in welcher Weise die Awareness in einem Unternehmen beeinflusst wird. Im Allgemeinen können die Stakeholder gemäß ihrer Einflussstärke geordnet werden (siehe Abb. 1.1). Dabei handelt es sich allerdings um pauschale Annahmen, die je nach Unternehmen auch davon abweichen können.

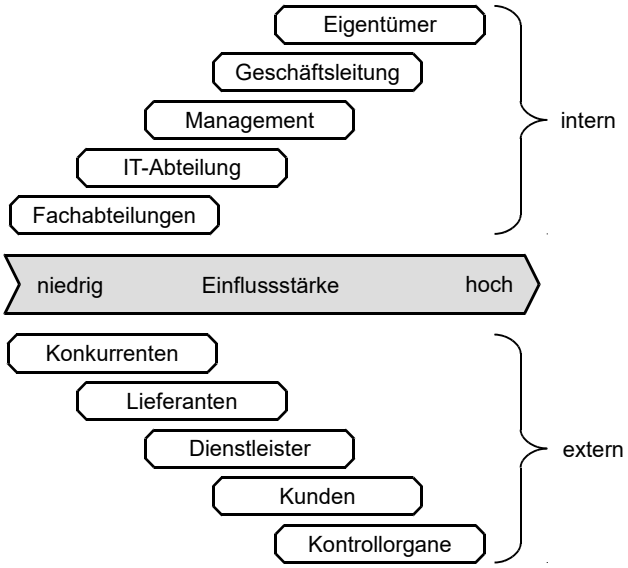


Abb. 1.1: Einflussstärke der Stakeholder auf die Awareness

Interne Stakeholder sind diejenigen Personen oder Gruppen, welche aufgrund ihrer Beziehungen zum Unternehmen wesentlich für die Geschäftstätigkeit sind und vom Erfolg des Unternehmens direkt betroffen sind. Hierzu gehören die Eigentümer und alle Mitarbeiter des Unternehmens:

– Die **Eigentümer** – auch Shareholder genannt – sind natürliche oder juristische Personen, die einen bestimmten Unternehmenserfolg anstreben. Dieser Erfolg muss nicht immer wirtschaftlich gemessen werden. Je nach Rechtsform des Unternehmens können auch ideelle, soziale oder kulturelle Erfolge angestrebt werden. Grundsätzlich kann ein Unternehmen von einer einzelnen natürlichen Person (dem Einzelunternehmer) oder von einem Zusammenschluss mehrerer Personen (z. B. in Form einer Gesellschaft bürgerlichen Rechts, offenen Handelsgesellschaft oder Kommanditgesellschaft) besessen werden. Hierbei haften die Eigentümer grundsätzlich mit ihrem Privatvermögen. Demgegenüber besitzt ein Unternehmen als juristische Person (z. B. in Form eines eingetragenen Vereins, einer Aktiengesellschaft, Gesellschaft mit beschränkter Haftung, Kommanditgesellschaft auf Aktien oder eingetragenen Genossenschaft) ihr eigenes Vermögen. Die Haftung weitet sich hier also nicht auf das Privatvermögen aus. Die Eigentümer haben den größten Einfluss auf die Awareness im Unternehmen. Durch die Finanzierung des gesamten Unternehmens können sie bestimmte Awareness-Maßnahmen oder -Programme beauftragen oder blockieren.

Selbst wenn sie das Unternehmen nur indirekt steuern, also andere Personen als Geschäftsführer eingestellt wurden, haben sie letztendlich, aufgrund der Besitzverhältnisse die entscheidende Machtposition. In der Regel befassen sich die Eigentümer allerdings nicht mit Detailfragen zur Awareness, sondern geben eher eine grobe Richtung vor.

- Die **Geschäftsleitung** ist mit der Führung der Geschäfte des Unternehmens betraut und vertritt es nach außen. Sie übernimmt die Steuerung und Regelung des gesamten Unternehmens, was auch als Governance bezeichnet wird. Dadurch ist sie direkt verantwortlich für grundlegende Strukturen, Prozesse und Vorgaben im Unternehmen. Auch auf die Awareness hat die Geschäftsleitung einen wesentlichen Einfluss. Zum einen gibt sie grob vor, welche Maßnahmen implementiert werden sollen und welches Sicherheitsniveau geschaffen werden soll, und zum anderen kontrolliert sie umfangreiche Programme oder Maßnahmen durch die Zuweisung von Ressourcen und ihre Befürwortung. Durch die Auswahl der zu befolgenden Regularien und Standards ergeben sich ebenfalls Einflüsse auf die Awareness. Regularien und Standards enthalten oft direkte oder indirekte Anforderungen an das Unternehmen. Diese Anforderungen bestimmen, ob und wie das Thema Awareness abgedeckt werden soll. Die Geschäftsleitung besitzt außerdem einen großen Einfluss auf die Unternehmenskultur. Mit ihrer Vorbildfunktion beeinflusst sie das Verhalten und die Einstellungen der Mitarbeiter, was sich wiederum auf das Sicherheitsniveau und die Awareness auswirkt.
- Das **Management** besteht aus allen Personen, die als Führungskräfte im Unternehmen eingesetzt werden. Sie befassen sich mit Führungsaufgaben, die zur Planung, Vorbereitung, Steuerung, Überwachung und Bewertung aller Tätigkeiten im Unternehmen wahrgenommen werden. Diese Führungsaufgaben lassen sich in fachliche und disziplinarische Aufgaben unterteilen: Fachliche Führungsaufgaben umfassen die Ausübung von Weisungsbefugnissen. Weisungen beziehen sich grundsätzlich auf den Arbeitseinsatz, also die geschäftlichen Tätigkeiten der geführten Mitarbeiter. Damit kann der Arbeitseinsatz zielgerichtet geplant und gesteuert werden und es kann auf Abweichungen reagiert werden. Disziplinarische Führungsaufgaben umfassen die Bewertung von Arbeitsergebnissen, die Förderung und Weiterentwicklung, die Maßregelung bei Verstößen sowie die Festlegung von Rahmenbedingungen (z. B. Arbeitszeit, Urlaub und Entlohnung). Awareness-Maßnahmen, an denen die Mitglieder des Managements teilnehmen, haben in der Regel nicht nur eine Verhaltensänderung der Manager zur Folge, sondern auch der geführten Personen. Manager haben eine Vorbildfunktion, welche sie bewusst oder unbewusst gegenüber ihren Mitarbeitern zur Wirkung bringen. Sicherheitsbewusstes Verhalten und der richtige Umgang mit sicherheitsrelevanten Informationen und Systemen können durch einen Manager vorgelebt werden. Außerdem können Manager ihr Wissen auch zielgerichtet weitergeben, indem sie z. B. kleinere Gruppen selbst beschulen.

Mit einem sogenannten Schneeballsystem können zunächst ausgewählte Personen geschult werden, die anschließend damit beauftragt werden, ihr erworbenes Wissen selbst weiterzugeben. Manager können das gewünschte Verhalten in sicherheitsrelevanten Situationen aktiv bei den Mitarbeitern einfordern und Verstöße mithilfe von disziplinarischen Maßnahmen direkt sanktionieren.

- Die **IT-Abteilung** besitzt aus Sicht der Sicherheit eine Doppelrolle: Einerseits ist sie interner Dienstleister und Lieferant für alle IT-Bedarfe im Unternehmen und andererseits beherbergt sie selbst Anwender und Nutzer von IT-Systemen. Die IT-Abteilung ist als Dienstleister und Lieferant in der Verantwortung, angemessene Sicherheitsmaßnahmen auszuwählen. Sie kombiniert physische, technische und organisatorische Maßnahmen, um eine ganzheitliche Sicherheit im Unternehmen zu schaffen. Dabei zählt die Awareness zum Bereich der organisatorischen Maßnahmen. Die IT-Abteilung besitzt also eine Schlüsselrolle bei der Auswahl und Umsetzung von Awareness-Maßnahmen. Mitglieder der IT-Abteilung sind auch selbst Teilnehmer an diesen Maßnahmen. Entwickler, Tester, Administratoren und andere Spezialisten arbeiten meist mit kritischen Systemen und Informationen. Ein verantwortungsvoller Umgang und ein sicherheitsbewusstes Verhalten können nicht als gegeben angesehen werden. Daher sollten gerade diese Personen mit zielgerichteten Awareness-Maßnahmen angesprochen werden. Die Vernachlässigung von Sicherheitsvorgaben kann insbesondere in der IT-Abteilung weitreichende Folgen haben, z. B. wenn neu entwickelte Software Sicherheitslücken besitzt oder Datenschnittstellen fehlerhaft sind.
- Die **Fachabteilungen** – also die Organisationseinheiten in einer Stab-Linien-Organisation, die mehrere gleichartige Stellen zusammenfassen und nicht zum IT-Bereich gehören – decken jeweils einen bestimmten, zusammenhängenden Aufgabenbereich im Unternehmen ab. Sie sind interner Auftraggeber von IT-Lösungen und Benutzer dieser Lösungen. Die Beauftragung erfolgt in der Regel durch ein – mehr oder weniger – formelles Fachkonzept, das alle funktionalen Anforderungen aus Sicht der jeweiligen Fachabteilung beschreibt. Im Rahmen der Aufgabenerfüllung werden die Mitglieder der Fachabteilungen mehr oder weniger stark mit sensitiven Informationen konfrontiert, sowohl in elektronischer als auch in papierbasierter Form. Eine hohe Awareness in den Fachabteilungen führt dazu, dass sich die Mitarbeiter bei ihrer täglichen Aufgabenerfüllung und auch bei der Beauftragung neuer IT-Lösung bewusst mit dem Thema Sicherheit auseinandersetzen. Dadurch kann ein unachtsamer Umgang mit sensitiven Systemen und Informationen vermieden werden und Änderungen oder Erweiterungen der eigenen Aufgaben können in Bezug auf eventuelle Sicherheitsprobleme kritisch betrachtet werden. Da einige Fachabteilungen ständig in Kontakt zu externen Kunden oder Geschäftspartnern stehen, haben viele Sicherheitsverletzungen eine direkte Außenwirkung. Vom ungewollten Datenabfluss bis zum nachhaltigen Imageschaden bestehen viele potenzielle Risiken,

die mit der Aufgabenerfüllung der Fachabteilungen zusammenhängen können. Mitarbeiter mit Kundenkontakt sollten z. B. darüber Bescheid wissen, welche Informationen ein Kunde erhalten darf, und Angreifer erkennen können, die mit Social Engineering vertrauliche Informationen erlangen möchten.

Externe Stakeholder sind vom Erfolg des Unternehmens in der Regel eher indirekt betroffen. Sie stehen zwar teilweise mit dem Unternehmen in einer Geschäftsbeziehung, sind aber an der eigentlichen Aufgabenerfüllung im Unternehmen und an dessen Geschäftsergebnis nicht beteiligt. Es handelt sich um Konkurrenten, Lieferanten, Dienstleister, Kunden und Kontrollorgane:

- **Konkurrenten** haben meist ein Interesse an einer Minderung des Unternehmenserfolgs. Insbesondere in gesättigten Märkten, in denen ein Verdrängungswettbewerb stattfindet, kann der Misserfolg eines Unternehmens durch die Umverteilung der Marktanteile dem Erfolg eines anderen Unternehmens gleichkommen. Wenn die Konkurrenten eher passiv gegenüber dem Unternehmen auftreten, sind zwar keine zielgerichteten Angriffe zu erwarten, allerdings können ungewollt oder unüberlegt veröffentlichte Informationen von Konkurrenten eingesehen und zum Nachteil des Unternehmens eingesetzt werden (z. B. Kundendaten oder Geschäftsstrategien). Demgegenüber ist ein aktives Vorgehen, das gezielt Daten abziehen soll oder das Unternehmen negativ beeinträchtigen soll, eine noch größere Gefahr. Obwohl dies in der Regel gegen geltende Gesetze verstößt (z. B. § 202a StGB – Verbot des Ausspähens von Daten), können diesbezügliche Angriffe aufgrund der teilweise schweren Nachverfolgbarkeit oder der Rechtssituation bei ausländischen Angreifern oft nicht geahndet werden. Awareness spielt also auch hier eine Rolle, und zwar nicht die Awareness der Konkurrenten, sondern die Awareness zum Umgang mit den Konkurrenten: Die Kenntnis darüber, wie Konkurrenten an sensitive Informationen gelangen können und wie dies verhindert werden kann, ist bei den Mitarbeitern des eigenen Unternehmens von großer Bedeutung.
- **Lieferanten** werden in der Regel aufgrund eines Kaufvertrags, der mit dem Unternehmen geschlossen wurde, tätig. Mit diesem Vertrag verpflichten sie sich zur Übergabe einer Sache (z. B. Arbeitsmittel oder Rohstoffe) und das Unternehmen zur Zahlung des geschuldeten Kaufpreises. Lieferanten haben ein Interesse an der Zahlungsfähigkeit des Unternehmens. In Bezug auf die Awareness ist eine angemessene Vorsicht beim Umgang mit Informationen angebracht. Auch wenn der Lieferant dem Unternehmen aufgrund der bestehenden Geschäftsbeziehung grundsätzlich nicht schaden möchte, können bestimmte Informationen (z. B. Preisinformationen) bei bestimmten Adressaten (z. B. anderen Kunden des Lieferanten) für Unmut sorgen. Sofern der Lieferant nicht gerade informationsverarbeitende Geräte liefert, spielt die Awareness beim Lieferanten für das eigene Unternehmen eine eher untergeordnete Rolle. Wenn jedoch derartige Geräte geliefert werden, könnte die Awareness beim Lieferanten

dazu führen, dass die Geräte vom Lieferanten z. B. bereits mit sicherheitsrelevanten Einstellungen oder Software-Updates versorgt wurden.

- **Dienstleister** haben oft eine tiefere Verbindung zum Unternehmen und kommen dadurch häufiger mit sensitiven Informationen in Berührung. Insbesondere wenn IT-Dienstleistungen ausgeführt werden, können unter Umständen große Datenmengen durch den Dienstleister eingesehen und verarbeitet werden. Die Awareness sollte also dahingehend im Unternehmen ausgeprägt sein, dass die Sicherheit auf Seiten des Dienstleisters hinterfragt und die Datenübertragung zum Dienstleister abgesichert wird. In Bezug auf die Sicherheit beim Dienstleister können verschiedene Maßnahmen durchgeführt werden, die z. B. von vertraglichen Vereinbarungen bis zu speziellen Sicherheitsaudits reichen. Unter anderem sollte eine Awareness darüber bestehen, welche Zertifizierungen (z. B. ISAE 3402 zum Thema interne Kontrollen) von Dienstleistern häufig vorgewiesen werden und welche Rückschlüsse man auf das Sicherheitsniveau des Zertifikatsinhabers ziehen kann. Die Datenübertragung zum und vom Dienstleister sollte ebenfalls aus Sicherheitsaspekten beurteilt werden. Vertrauliche Daten sollten z. B. nicht unverschlüsselt über öffentliche Netzwerke übertragen werden.
- **Kunden** sind als Erwerber von Dienstleistungen oder Waren grundsätzlich an niedrigen Preisen und hoher Qualität interessiert. Allerdings gerät auch der Schutz von Kundendaten zunehmend in den Fokus. Kunden reagieren sensibel darauf, wenn Unternehmen Kundendaten nicht ausreichend schützen. Da Kunden im Falle einer Kompromittierung ihrer Daten gemäß Bundesdatenschutzgesetz (§ 42a) benachrichtigt werden müssen, kommen Sicherheitsvorfälle von Unternehmen schnell an die Öffentlichkeit. Dies kann zu empfindlichen Umsatzeinbußen oder sogar zu Schadensersatzforderungen führen. Kunden agieren häufig kritisch bei der Auswahl von Unternehmen. Das Kriterium Sicherheit, das z. B. anhand von Zertifikaten oder guter Presse beurteilt werden kann, spielt dabei oft eine wichtige Rolle. Das Interesse eines Unternehmens, eine möglichst gute, werbewirksame Sicherheit zu etablieren, beeinflusst auch die Awareness. Mit einem hohen Awareness-Niveau und den resultierenden Sicherheitsvorteilen versuchen Unternehmen, den Kunden ein weiteres Qualitätskriterium zu liefern. Die Vermeidung von Sicherheitsvorfällen und schlechter Presse ist für kundenorientierte Unternehmen essenziell, um am Markt bestehen zu können.
- **Kontrollorgane** sind darin interessiert, dass das Unternehmen vorgegebene Regeln einhält. Welche Regeln für ein Unternehmen relevant sind, hängt von verschiedenen Faktoren ab. Unter anderem spielen die Geschäftstätigkeit und Branche eine Rolle. Z. B. sind Unternehmen, die mit Zahlungskarten arbeiten, an den Payment-Card-Industry-Datensicherheitsstandard (PCI DSS) gebunden. In den USA börsennotierte Unternehmen müssen den Sarbanes Oxley Act (SOX) befolgen. Aktiengesellschaften und GmbHs sind zur Einhaltung des Gesetzes zur Kontrolle und Transparenz im Unternehmensbereich (KonTraG) verpflichtet.

Alle Unternehmen, die mit personenbezogenen Daten in Berührung kommen, sind an das Bundesdatenschutzgesetz (BDSG) und die Datenschutz-Grundverordnung (DSGVO) gebunden. Daneben existieren unzählige Standards, Best Practices und Modelle, die das Unternehmen freiwillig einhalten kann, z. B. weil es sich davon einen Marketingerfolg oder eine Effizienzsteigerung verspricht. Dazu gehören unter anderem ISO 27001, IT-Grundschutz, IT Infrastructure Library (ITIL), ISO 9000 und Control Objectives for Information and Related Technology (COBIT). Die einzuhaltenden Regeln sind oft relativ allgemein formuliert (siehe auch Kapitel 3.8). Beispielsweise findet man im BDSG eine indirekte Forderung zur Implementierung von Awareness-Maßnahmen. Konkreter ist z. B. das PCI DSS, wo sogar die Häufigkeit und Vielseitigkeit der Awareness-Maßnahmen thematisiert werden. Wie die Erfüllung der Regeln im Detail ausgestaltet werden soll und inwiefern bestimmte Awareness-Maßnahmen zur Erfüllung einzelner Regeln genutzt werden sollen, hängt auch von der individuellen Unternehmenssituation ab. Beispielsweise sollte ein Unternehmen mit einem hohen Automatisierungsgrad anders mit Awareness-Maßnahmen versorgt werden als ein Unternehmen mit vielen individuellen Datenverarbeitungsprozessen.

Eine strukturierte **Stakeholderanalyse** kann eingesetzt werden, um die Interessen der Stakeholder transparent zu machen. Dadurch können kooperierende Stakeholder gegenüber konkurrierenden abgrenzt werden, was für den Erfolg eines Vorhabens (z. B. einer Awareness-Kampagne) von großem Vorteil sein kann: Nach der Identifizierung der Stakeholder und ihrer Interessen können wichtige Entscheidungsträger im Unternehmen vom Vorhaben überzeugt werden und konkurrierende Stakeholder können von Widerständen abgehalten werden. Bei der Stakeholderanalyse werden grundsätzlich sechs Schritte durchlaufen:[3]

1. Zunächst werden weitere Rahmenbedingungen für die Analyse festgelegt (Ziel der Analyse, Betrachtungsausschnitt und Abstraktionsgrad).
2. Anschließend werden Stakeholder identifiziert und relevante ausgewählt.
3. Dann werden die Stakeholder in Bezug auf ihre Einflussstärke priorisiert.
4. Als nächstes werden die Interessen der Stakeholder identifiziert.
5. Basierend auf den bisher gewonnenen Informationen wird eine Stakeholdermap erstellt. Mit dieser können die Prioritäten sowie die Kongruenzen und Konflikte zwischen den Interessen der Stakeholder visualisiert werden.
6. Abschließend können die gewonnenen Daten genutzt werden, um Stakeholderinteressen zielgerichtet zu berücksichtigen. Dabei können die Interessen befriedigt, neu ausgerichtet oder ausbalanciert werden.

3 Vgl. Resch 2012, S. 128 ff.

Die Awareness im Unternehmen beeinflusst das **Verhalten** der Mitarbeiter (siehe Abb. 1.2). Und das Verhalten hat wiederrum einen essenziellen Einfluss darauf, wie Systeme geschützt werden und ob die Sicherheit von Informationen angemessen ist oder von Sicherheitsverletzungen bedroht ist.

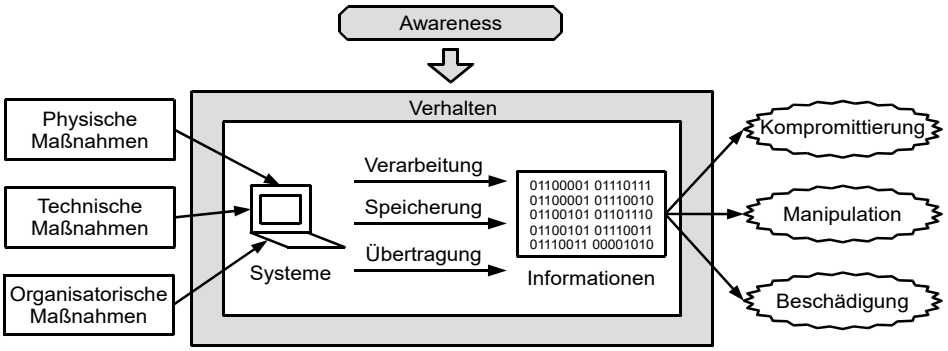


Abb. 1.2: Bedeutung der Awareness

Der Schutz von **Systemen** ist in zweifacher Hinsicht vom Verhalten der Mitarbeiter geprägt. Einerseits können Systeme nur dann umfassend geschützt werden, wenn passende Schutzmaßnahmen ausgewählt und implementiert werden. Nur wenn Mitarbeiter ein durchdachtes und strukturiertes Auswahlverfahren nutzen, können Schutzmaßnahmen mit einem angemessenen Kosten-Nutzen-Verhältnis gefunden werden. Andererseits ist die Akzeptanz der Maßnahmen und deren Unterstützung wichtig, um das Sicherheitsniveau dauerhaft aufrechtzuerhalten. Wenn Mitarbeiter aufgrund von Unwissenheit oder Bequemlichkeit Schutzmaßnahmen umgehen, kann die Sicherheit der Systeme stark gefährdet werden. Wenn physische Maßnahmen umgangen werden, sind Systeme ungeschützt gegenüber physischen Gefahren, z. B. Diebstahl oder Beschädigung von Systemen. Eine Zugangskontrolle kann keine Eindringlinge abhalten, wenn Mitarbeiter aus Bequemlichkeit Türen offenlassen. Auch technische Maßnahmen können ihre Wirkung verlieren, wenn Mitarbeiter sich nicht angemessen verhalten, z. B. wenn sie über Proxys auf gesperrte Webseiten zugreifen. Organisatorische Maßnahmen sind am stärksten vom Verhalten der Mitarbeiter abhängig. Im Gegensatz zu physischen und technischen Maßnahmen können sie nur funktionieren, wenn sie aktiv durch die Mitarbeiter innerhalb ihrer Tätigkeit umgesetzt werden. Z. B. kann eine Richtlinie nur eine Wirkung haben, wenn sie den Mitarbeitern bekannt ist und diese sich an die Inhalte halten.

Der Zweck von Systemen liegt darin, **Informationen** zu verarbeiten, zu speichern und zu übertragen: Informationen werden bei einer Speicherung auf einem Datenträger festgehalten. Grundsätzlich erfolgt dies in Form eines Binärcodes, der bei

Bedarf in Binär- oder Textdaten umgewandelt werden kann. Binärdaten müssen durch eine kompatible Applikation interpretiert werden. Textdaten können auch von Personen direkt interpretiert werden. Bei der Übertragung werden Informationen zwischen verschiedenen Systemen übermittelt. Je nach Standort der Systeme können lokale Netzwerke (engl. Local Area Networks), z. B. innerhalb eines Geschäftsgebäudes, und Weitverkehrsnetze (engl. Wide Area Networks), z. B. das Internet, für die Übermittlung genutzt werden. Die Verarbeitung dient der Überführung von Informationen in anders formatierte oder strukturierte Daten. Auf diese Weise werden Informationen z. B. zusammengeführt, verteilt, angereichert, abstrahiert oder transformiert. Oft ist die Verarbeitung ein wichtiger Bestandteil eines Geschäftsprozesses, z. B. die Aufbereitung von Informationen zur Bestellabwicklung bei einem E-Commerce-Händler. Das Verhalten beim Umgang mit Informationen ist ausschlaggebend dafür, ob Sicherheitsverletzungen ermöglicht und Informationen kompromittiert, manipuliert oder beschädigt werden können:

- Die **Kompromittierung** wird begünstigt, wenn Informationen unachtsam herausgegeben oder unsicher verarbeitet, gespeichert oder übertragen werden. Sobald Informationen weitergegeben werden, besteht die Gefahr, dass jemand unberechtigt von diesen Informationen Kenntnis erlangt. Die Bandbreite der Kompromittierung reicht von ungewolltem Aufschnappen von Informationen bis zur gezielten Ausspähung. Ein Verhalten der Mitarbeiter, bei dem die Sicherheit ständig berücksichtigt wird, führt zu einem sorgfältigen und vorsichtigen Umgang mit Informationen. Es sollte z. B. hinterfragt werden, wer Informationen mithören oder mitlesen kann und ob der vermeintliche Empfänger tatsächlich eine ausreichende Autorisierung besitzt. Systeme, die auf Informationen zugreifen, sollten zunächst in Bezug auf ein ausreichendes Sicherheitsniveau geprüft werden. Dabei sollte auch die Absicherung des Übertragungswegs (z. B. durch Verschlüsselung) berücksichtigt werden.
- Die **Manipulation** von Informationen kann dann auftreten, wenn Angreifer Zugriff auf Informationen an ihrem Speicherort oder während ihrer Übertragung erlangen können. Außerdem können Angreifer auch die Verarbeitung von Informationen manipulieren. Sie können dann Informationen zu ihrem Vorteil ändern, z. B. durch die Herabsetzung von Preisen in einem Online-Shop oder die Änderung von Zahlungsempfängern. Durch ein überlegtes Verhalten kann es Angreifern erschwert werden, an Anmeldedaten zu gelangen, z. B. sollten Passwörter niemals herausgegeben werden. Ein schnelles Reaktionsverhalten führt außerdem dazu, dass unberechtigt erlangte Zugriffe zeitnah erkannt und blockiert werden können.
- Die **Beschädigung** von Informationen kann ebenfalls durch unberechtigten Zugriff von Angreifern ermöglicht werden, aber auch durch unachtsames Verhalten von Mitarbeitern oder unkontrollierbare und teilweise unvorhersehbare Umweltereignisse. Mitarbeiter können durch unachtsames Verhalten die Gefahr erhöhen, dass Systeme und Informationen beschädigt werden. Zum einen kön-

nen sie durch unsicheres Verhalten (z. B. das Öffnen von Phishing E-Mails) Angreifern Zugriff auf Informationen verschaffen, was zur Beschädigung dieser Informationen führen kann. Zum anderen können sie selbst unbeabsichtigt Informationen oder Systeme physisch beschädigen, z. B. durch das Verschütten von Flüssigkeiten. Mittels einer bewussten Anpassung des Verhaltens können gefahrvolle Situationen vermieden werden.

Eine gute Awareness hat auch deswegen eine große **Bedeutung**, weil viele Angriffe auf die Unwissenheit oder Unachtsamkeit von Mitarbeitern ausgelegt sind. Diese Angriffe gehören meist zum Bereich des Social Engineerings, wobei Personen dazu beeinflusst werden, bestimmte Aktionen auszuführen (z. B. das Anklicken eines Weblinks) oder Informationen preiszugeben.

Viele zielgerichtete Angriffe auf Unternehmen werden mithilfe von Spear-Phishing-E-Mails ausgeführt. Spear Phishing ist im Gegensatz zum traditionellen Phishing ein gezielter Angriffsversuch, bei dem individuelle Informationen über das Opfer und seine Umgebung gesammelt und eingesetzt werden. Dadurch wirkt der getarnte Angriff authentischer und eine Erkennung wird erschwert.

Auch die Anfälligkeit gegenüber platzierten USB-Datenträgern ist in der Praxis sehr hoch. Viele platzierte USB-Datenträgern werden von unbedarften Mitarbeitern mitgenommen und darauf befindliche Dateien manchmal sogar geöffnet. Auf diese Weise können Angreifer Schadcode ins Unternehmen einschleusen.

Angreifer versuchen außerdem, das Prinzip der Reziprozität auszunutzen: Viele Personen, die vorab kleine Geschenke erhalten, geben im Gegenzug vertrauliche Informationen preis (z. B. ihr Passwort).

Da soziale Netzwerke häufig von Angreifern genutzt werden, um Erkenntnisse über Zugangsdaten und andere sensitive Informationen zu erlangen, ist auch der Umgang mit sozialen Netzwerken ohne eine gewisse Awareness gefährlich. Viele Mitarbeiter scheuen sich nicht, sich in sozialen Netzwerken mit Fremden zu verbinden, oder haben keine ausreichenden Zugriffsbeschränkungen auf ihren Social-Media-Profilen.

Der Mensch ist ein hoher Risikofaktor, da er oft leichter zu „hacken“ ist als ein IT-System. Das Verhalten von Personen ist daher in vielen Fällen die Ursache von aufgetretenen Sicherheitsvorfällen.

Eine höhere Awareness bei den potenziellen Opfern von Social-Engineering-Angriffen würde zu einem wirksamen Schutz führen. Die Angreifer zielen nämlich auf ein bestimmtes Verhalten der Opfer ab, das mithilfe von Awareness-Maßnahmen größtenteils verhindert werden kann. Aber auch andere Arten von Angriffen werden durch das Verhalten von Personen direkt oder indirekt beeinflusst. Unter anderem ist der Umgang mit technischen Sicherheitsmaßnahmen ausschlaggebend für ihre Effektivität. Wenn z. B. Antivirenprogramme nach Belieben deaktiviert werden, wird der Schutz gegen Schadcode erheblich beeinträchtigt.

1.3 Ausblick

Um die Hintergründe der Awareness für Informationssicherheit umfänglich verstehen zu können, ist eine Auseinandersetzung mit den relevanten **fachlichen Grundlagen** unumgänglich.

Daher wird im Kapitel 2 zunächst eine Einführung in die Informationssicherheit gegeben. Hierdurch wird verdeutlicht, was es bedeutet, die IT zu schützen, und welche Ziele man dabei in der Regel verfolgt. Die Informationssicherheit, über die eine Awareness geschaffen werden soll, muss vom Initiator der Awareness-Maßnahmen erstmal verstanden und eingegrenzt werden. Erst wenn die Informationssicherheit nicht nur im Allgemeinen, sondern auch im unternehmensspezifischen Kontext definiert wurde, können geeignete Awareness-Maßnahmen ausgewählt werden. Jedes Unternehmen besitzt andere Schwerpunkte und Präferenzen bezüglich Informationssicherheit. Während ein Unternehmen stark auf Vertraulichkeit fokussiert sein kann, ist es für ein anderes Unternehmen womöglich wichtiger, dass die angebotenen Dienstleistungen ständig verfügbar sind. Mithilfe von diversen Sicherheitsmaßnahmen können verschiedene Schutzziele erreicht werden. Um einen Überblick über verbreitete Sicherheitsmaßnahmen zu bieten, werden sie aus mehreren Perspektiven betrachtet und unterschiedlichen Kategorien zugeordnet. Grundsätzlich dienen alle Sicherheitsmaßnahmen (einschließlich Awareness-Maßnahmen) zur Reduzierung oder – im Idealfall – zur Eliminierung von Risiken. Daher wird auch der Begriff Risiko, inklusive verschiedener Methoden und Verfahren zur Identifizierung, Bewertung und Bewältigung von Risiken, beschrieben. Außerdem ist es wichtig, den Umfang schützenswerter Objekte und den resultierenden Sicherheitsbedarf genau eingrenzen zu können. Auf diese Weise können Awareness-Maßnahmen zielgerichteter angewendet werden. Z. B. muss nicht das gesamte Personal über sichere Softwareentwicklung geschult werden, wenn nur eine kleine Personengruppe mit der Softwareentwicklung beauftragt wurde. Eine fundamentale Frage, die sich bei jeder Art von Investition – auch bei Awareness-Maßnahmen – stellt, ist die Frage nach der Wirtschaftlichkeit. Nur wenn der erwartete Nutzen die notwendigen Kosten übersteigt, lohnt sich eine Investition wirtschaftlich. Daher wird ebenfalls in diesem Kapitel betrachtet, wie Kosten und Nutzen berechnet und gegeneinander abgewogen werden können.

Nach der Auseinandersetzung mit der Informationssicherheit werden anschließend die Grundlagen zur Awareness erläutert. Die Definition und Hintergründe zur Verhaltenssteuerung – dem grundlegenden Ziel der Awareness – werden aus psychologischer Sicht beschrieben. Dabei wird aufgezeigt, was Awareness im Detail bedeutet und wie Lernprozesse zur Awareness-Erhöhung erfolgreich gemacht werden können. Auch die Facetten der Unternehmenskultur und der Kommunikation sowie die Zusammenhänge zur Awareness werden betrachtet. Durch die Berücksichtigung verschiedener Kommunikationsformen zwischen Sender und Empfänger

kann ein Ansatz gefunden werden, der am besten zur individuellen Unternehmenssituation passt.

Die Governance der Awareness ist ein Teil der unternehmensweiten Governance, und somit ein Thema für die Unternehmensführung. Auch Awareness-Maßnahmen werden zur Steuerung und Regelung des Geschäftsbetriebs eingesetzt, weshalb eine Betrachtung aus der Governance-Sicht Sinn macht.

In Kapitel 3 werden **Awareness-Maßnahmen** umfassend betrachtet. Dabei werden die Ziele, die Adressaten, Medien, der Awareness-Zyklus, die Umsetzungsmerkmale, die Integration der Awareness ins Unternehmen, die Synergiemöglichkeiten und relevante Compliance-Vorgaben betrachtet.

Das grundlegende Ziel aller Awareness-Maßnahmen ist die Änderung des Verhaltens der Mitarbeiter. Daher wird zunächst erläutert, welche Verhaltensausprägungen aus Sicht der Informationssicherheit bedeutsam sind, welches Verhalten erwünscht ist und wie sich die Verhaltensausprägungen wechselseitig beeinflussen können.

Damit Awareness-Maßnahmen möglichst zielgerichtet gestaltet und umgesetzt werden können, müssen die Personen und Personengruppen, die durch die Maßnahmen adressiert werden sollen, bekannt sein. Es handelt sich nicht nur um Mitarbeiter, sondern auch um andere Stakeholder, die das Sicherheitsniveau des Unternehmens beeinflussen können.

Geeignete Medien sind das Fundament für die optimal gestaltete Awareness-Maßnahmen. Anhand der drei Bereiche Printmedien, audiovisuelle Medien und elektronischen Medien werden unterschiedliche Medien kategorisiert und im Hinblick auf ihren Einsatz in der Awareness beschrieben.

Der Awareness-Zyklus verdeutlicht, welche Stationen ein Mitarbeiter als Adressat von Awareness-Maßnahmen durchläuft. Vom Einstieg ins Unternehmen bis zu seinem Austritt wird er unterschiedlich mit Awareness konfrontiert.

Die Umsetzungsmerkmale zeigen auf, wie und warum Awareness-Maßnahmen umgesetzt werden können. Der Auslagerungsgrad entscheidet, inwieweit die erforderlichen Tätigkeiten mit externer Unterstützung erfolgen. Die Art der Auslösung von Awareness-Maßnahmen determiniert, was im Fokus der Umsetzung steht, z. B. Risiken oder Regularien. Außerdem stellt sich die Frage, wie die Adressaten der Awareness-Maßnahmen sinnvoll gruppiert werden können.

Die Integration beleuchtet, wie die Awareness im Unternehmen verankert werden kann, damit sie auch langfristig angemessen berücksichtigt wird. Dabei werden die institutionelle, funktionelle, instrumentelle und finanzielle Sicht thematisiert.

Die Synergiemöglichkeiten in der Awareness sind vor allem aus wirtschaftlicher Sicht interessant. Durch die Nutzung unterschiedlicher Ansätze können erhebliche Vorteile aus Kosten-, Zeit- und Qualitätssicht realisiert werden.

Aus dem Compliance-Bereich kommen viele Vorgaben, die sich mehr oder weniger direkt auf die Awareness im Unternehmen beziehen. Ein Unternehmen sollte wissen, welche Compliance-Vorgaben relevant sind, wenn Maßnahmen oder Pro-

gramme zur Awareness gestaltet werden. Daher werden verbreitete Gesetze, Standards und Best Practices sowie ihre Verbindung zur Awareness betrachtet.

Ein hohes Sicherheitsniveau zu schaffen, ist in den meisten Unternehmen je nach Ist-Situation eine herausfordernde und langwierige Aufgabe. Dies trifft auch in ähnlichem Maß auf die Schaffung einer hohen Awareness zu. In der Regel ist eine einzelne Awareness-Maßnahme kaum ausreichend, um eine dauerhaft merkliche Verbesserung zu erzeugen. Vielmehr muss die Awareness kontinuierlich und schrittweise im Unternehmen angegangen werden. Wie das grundsätzlich erreicht werden kann, zeigt das Kapitel 4. Hier wird beschrieben, wie die Awareness im Unternehmen durch **Awareness-Programme** in strukturierter und durchdachter Weise erhöht werden kann. Dabei werden neun verschiedene Phasen beschrieben: In der Orientierung wird erstmal ein Verständnis über die verschiedenen Phasen geschaffen. In der Initiierung wird gezeigt, wie interne oder externe Faktoren zum Start des Programms beitragen. Die Befürwortung befasst sich mit der Unterstützung des Senior Managements. In der Anforderungsanalyse werden interne und externe Anforderungen identifiziert und analysiert. In der Bedarfsanalyse werden die Anforderungen mit dem Status-quo abgeglichen, um den individuellen Bedarf an Awareness zu ermitteln. Die Planung dient der Auswahl und Gestaltung von Awareness-Maßnahmen. Mit der Genehmigung wird sichergestellt, dass die Arbeitsaktivitäten bewilligt werden und die erforderlichen Ressourcen bereitstehen. Die Implementierung beinhaltet unter anderem die Erstellung von Inhalten, den Einsatz von Medien und die Koordination des gesamten Programmablaufs. In der Beurteilung werden der Erfolg der Awareness-Maßnahmen untersucht sowie Probleme und Unzulänglichkeiten bei der Zielerreichung identifiziert.

Mit der **Zusammenfassung** in Kapitel 5 wird die Möglichkeit geboten, die Kernaspekte des Buchs nochmals zu wiederholen und wichtige Inhalte zu festigen. Auch eine schnelle Auffrischung oder ein erstmaliger Einblick in das Thema Awareness sollen damit vereinfacht werden. Zunächst werden die wichtigsten Elemente aus der Informationssicherheit und der Awareness kurz dargestellt und mit den Phasen eines Awareness-Programms in Verbindung gebracht. Dadurch gewinnt man schnell einen Eindruck darüber, welche Grundlagen und Hintergründe für welche Programmphasen relevant sind. Der Inhalt eines Awareness-Programms wird anschließend komprimiert dargestellt. Dabei wird erläutert, welche Ergebnisse die einzelnen Phasen erzeugen und auf welchen Grundlagen sie aufbauen. Diese Strukturierung verhilft nicht nur zu einem schnellen Überblick über die Phasen, sondern bietet auch eine zusätzliche Perspektive, um die Detailinformationen der vorhergehenden Kapitel gedanklich nochmals zu ordnen. Durch die Verwendung von Kapitelreferenzen erschließt sich dem interessierten Leser schnell, wo im Buch weitere Informationen zu den verschiedenen Themen gefunden werden können.

2 Fachliche Grundlagen

2.1 Informationssicherheit

2.1.1 Grundbegriffe

Bevor die Grundlagen rund um Informationssicherheit betrachtet werden, wird zunächst der Begriff an sich veranschaulicht. **Informationssicherheit** bedeutet, dass Informationen und IT-Systeme derartig abgesichert sind, dass sie nicht kompromittiert, manipuliert oder beschädigt werden. Mit anderen Worten soll gewährleistet werden, dass die primären und – bei Bedarf – die davon abgeleiteten sekundären Sicherheitsziele erfüllt werden (siehe Kapitel 2.1.3).

Informationssicherheit bezieht sich allgemein auf alle Aspekte rund um die Sicherheit von Informationen. Dabei werden alle Informationen unabhängig von der Art der Speicherung, Verarbeitung und Übertragung betrachtet. Informationen, die lediglich auf Papier niedergeschrieben werden oder z. B. sprachlich übermittelt werden, sind genauso betroffen wie Informationen, die mit IT-Geräten in Kontakt kommen, also unter Einbeziehung von elektronischen Hilfsmitteln gespeichert, übertragen oder verarbeitet werden. Die **IT-Sicherheit** konzentriert sich hingegen auf letztere – auf diejenigen Informationen, die mit der IT-Umgebung eines Unternehmens in Berührung kommen. Dadurch kommen auch informationsverarbeitende Systeme und Netzwerke in den Fokus. Aspekte außerhalb der IT, wie physische Sicherheitsmaßnahmen oder der Umgang mit papierbasierten Informationen, werden durch die IT-Sicherheit nicht abgedeckt. Die IT-Sicherheit ist also der Teilbereich der Informationssicherheit, der sich ausschließlich auf die IT konzentriert (siehe Abb. 2.1). Dieser Teilbereich ist gleichzeitig auch der größte Bereich, da heutzutage die meisten Informationen elektronisch erfasst werden.

Für den Begriff **Security Awareness** (kurz Awareness) – einem Teilgebiet der Informationssicherheit und IT-Sicherheit – gilt in Bezug auf die oben dargestellte Abgrenzung entsprechendes: Awareness für Informationssicherheit (engl. Information Security Awareness) deutet auf Awareness hin, die sich auf alle Informationen bezieht, und Awareness für IT-Sicherheit (engl. IT Security Awareness) auf Awareness, die sich ausschließlich auf elektronisch gespeicherte, übertragene oder verarbeitete Informationen bezieht. Awareness für IT-Sicherheit ist also ein Teilbereich der Awareness für Informationssicherheit. Die Inhalte dieses Buches beziehen sich auf letztere, und decken damit beide Bereiche ab. Im Folgenden wird (der einfachen Schreibweise zugunsten) lediglich der Begriff Awareness verwendet, wenn Awareness für Informationssicherheit gemeint ist. Der englische Begriff Awareness wird anstelle des deutschen Synonyms Bewusstsein verwendet, da sich dieser Begriff in der Praxis und Literatur der Informationssicherheit etabliert hat.

https://doi.org/10.1515/9783110668261-002

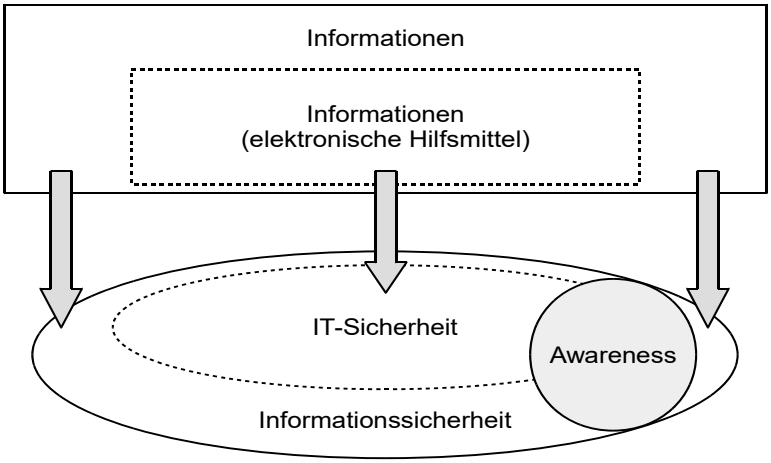


Abb. 2.1: Abgrenzung zwischen Informationssicherheit und IT-Sicherheit

Der Begriff **Awareness** bedeutet im Kontext der Informationssicherheit, dass eine Person oder eine Gruppe von Personen Wissen über Informationssicherheit besitzen – sich also über Informationssicherheit bewusst sind – und dieses Wissen bei ihrem Verhalten berücksichtigen.

In der Praxis verwendet man als Synonym für **Awareness-Maßnahmen** auch den Begriff Sensibilisierung, um die Erhöhung der Awareness von Mitarbeitern (also die Übermittlung von Informationen an Mitarbeiter zur Aneignung von Wissen über Informationssicherheit) zu beschreiben. Die sensibilisierten Personen werden sensibel, oder auch empfindlich, gegenüber sicherheitsrelevanten Reizen und Eindrücken gemacht.

Awareness-Maßnahmen werden von **Trainings- und Weiterbildungsmaßnahmen** abgegrenzt. Alle diese Maßnahmen dienen zwar der Aneignung von neuem Wissen mithilfe von Lernprozessen, allerdings besitzt das Wissen jeweils eine andere Fokussierung sowie andere Ausprägungen in Bezug auf den zeitlichen Rahmen, die Theorielastigkeit und das Anspruchsniveau.

Bei der Awareness geht es primär darum, allgemeines Wissen rund um die Informationssicherheit zu vermitteln und das Bewusstsein über die Bedrohungslage und Risikosituation des Unternehmens zu erhöhen. Es handelt sich in der Regel um eine zeitlich kurze Maßnahme, z. B. eine einstündige Präsentation oder sogar nur ein Blick auf ein Poster. Awareness-Maßnahmen sind oft sehr praktisch orientiert, also wenig theorielastig, und lerntechnisch wenig anspruchsvoll, da oft lediglich Anreize zur Bewusstseinserhöhung gegeben werden.

Trainingsmaßnahmen sind hingegen auf spezielle Technologien, Verfahren oder Fähigkeiten ausgerichtet. Der zeitliche Rahmen ist gering bis mittel, z. B. ein