Forschungsprogramm 2021

Vertrauen in Datenverarbeitung

Kurzstudie

Pirmin Puhl
Jana Stuck
Saskja Schäfer
Annette Hillebrand (Projektleiterin)

Bad Honnef, Dezember 2021

wik Wissenschaftliches Institut für Infrastruktur und Kommunikationsdienste

Impressum
WIK Wissenschaftliches Institut für
Infrastruktur und Kommunikationsdienste GmbH
Rhöndorfer Str. 68
53604 Bad Honnef
Deutschland
Tel.: +49 2224 9225-0
Fax: +49 2224 9225-63
E-Mail: info@wik.org
www.wik.org

Vertretungs- und zeichnungsberechtigte Personen
Geschäftsführerin und Direktorin
Dr. Cara Schwarz-Schilling
Direktor Alex Kalevi Dieke
Direktor Abteilungsleiter Netze und Kosten Dr. Thomas Plückebaum
Direktor Abteilungsleiter Regulierung und Wettbewerb Dr. Bernd Sörries
Leiter der Verwaltung Karl-Hubert Strüver
Vorsitzende des Aufsichtsrates Dr. Daniela Brönstrup
Handelsregister Amtsgericht Siegburg, HRB 7225
Steuer-Nr. 222/5751/0722
Umsatzsteueridentifikations-Nr. DE 123 383 795
Dezember 2021

Inhalt

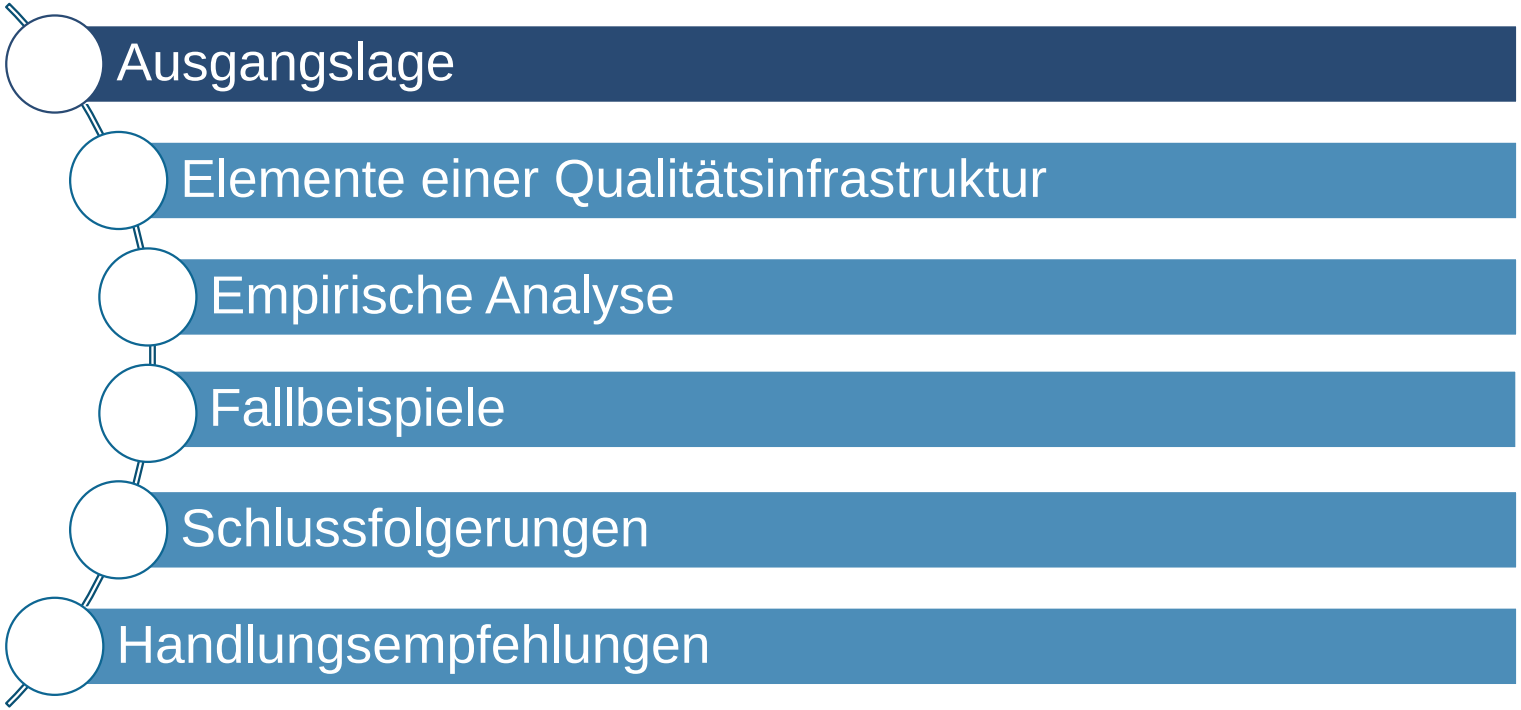
Ziel der Studie

Die Kurzstudie „Vertrauen in Datenverarbeitung“ entstand im Rahmen Forschungsprogramms des WIK - Wissenschaftliches Institut für Infrastruktur und Kommunikationsdienste in Bad Honnef. Das Ziel dieser Kurzstudie ist die Identifikation von Faktoren, die eine Qualitätsinfrastruktur und Siegel oder Zertifizierungen mit hohem Vertrauen ausmachen sowie eine Begriffsklärung und -definition. Die Kurzstudie ist zusätzlich in einem „WIK-Schlaglicht“ für kleine und mittlere Unternehmen (KMU) zusammengefasst.
WIK-Studie_Schlaglicht_Vertrauen_in_Datenverarbeitung_2021.pdf

Methodik

- Auswertung der relevanten Literatur im Bereich IT-Sicherheit und Gütezeichen
- Bestandserhebung und Analyse von 49 relevanten Siegeln und Zertifizierungen im Bereich Informationssicherheit in Deutschland und fünf Siegeln und Zertifizierungen für Rechenzentren (Desk Research)
- Interviews mit 15 Expertinnen und Experten von relevanten Akteuren auf dem Gebiet der Informationssicherheit, Qualitätsinfrastruktur, KMU, IT-Beratung, Verbände und Forschungseinrichtungen (ergänzend: Online-Umfrage per Survey Monkey bei KMU)

Inhalt


Ausgangslage
Elemente einer Qualitätsinfrastruktur
Empirische Analyse
Fallbeispiele
Schlussfolgerungen
Handlungsempfehlungen

Vertrauen

Vertrauen

„… ist die Erwartung, nicht durch das Handeln anderer […] geschädigt zu werden; als solches stellt es die unverzichtbare Grundlage jeder Kooperation dar, die sich immer dort ergibt, wo Akteure (Vertrauensnehmer), die Einfluss auf andere (Vertrauensgeber) haben, über die Freiheit verfügen, in ihrem Handeln die Interessen anderer zu berücksichtigen oder nicht.“ [1]

In anderen Worten: Vertrauen basiert auf transparenter Information und Kommunikation, nachprüfbaren Fakten und gegenseitig verfügbaren Sanktionsinstrumenten.

Digitaler Wandel gelingt, wenn Technologien, Lösungen und Dienste akzeptiert und genutzt werden. Dies hängt entscheidend davon ab, in welchem Maß ihnen begründetes Vertrauen entgegengebracht wird. Vertrauen zu den betreffenden Technologien, Lösungen und Diensten kann durch Reputationssysteme oder Konformitätsbewertungen entstehen und verstetigt werden.[2] In dieser Studie wird die Wirkung von Akkreditierung und Konformitätsbewertungen, also Gütezeichen (Siegel und Zertifikate), auf Vertrauen in Datenverarbeitung näher untersucht.

Eine „*Konformitätsbewertung ist eine Darlegung, dass festgelegte Anforderungen bezogen auf ein Produkt, einen Prozess, ein System, eine Person oder eine Stelle erfüllt sind*“.[3] Siegel und Zertifikate garantieren, dass zum Prüfungszeitpunkt Konformität zu den Prüfkriterien der festgelegten Anforderungen besteht, die den Siegeln und Zertifikaten zugrunde liegen. Dies entspricht dem funktionalistischen Ansatz eines Vertrauenskonzeptes.[4] Vertrauen dient nach diesem Ansatz „*der Reduktion von Komplexität. […] Der Mensch […] kann nur handlungsfähig werden, wenn es ihm gelingt, angemessene Formen der Informationsreduktion zu entwickeln.*“[5] Siegel und Zertifikate stellen somit ein probates Mittel zur Reduktion von Komplexität sowie Informationsasymmetrien und damit Entscheidungsunsicherheiten potenzieller Kunden von KMU dar.[6]

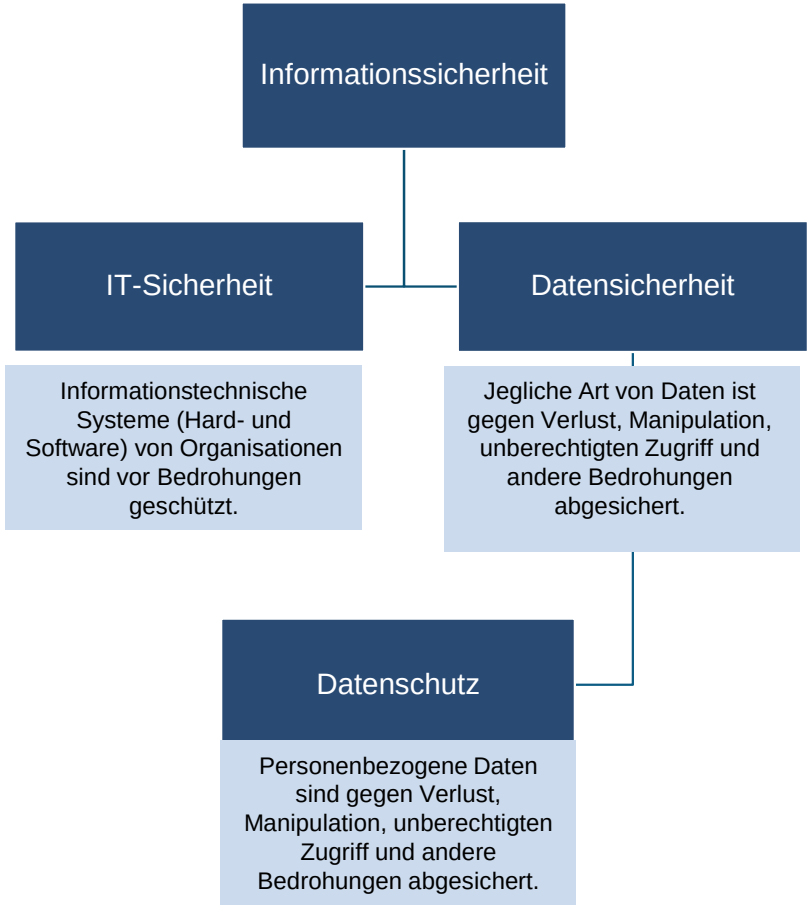
Definition Informationssicherheit

Vertrauen in Datenverarbeitung ist dann gegeben, wenn die Überzeugung besteht, dass die allgemeinen Schutzziele der Informationssicherheit ausreichend sichergestellt und Risiken minimiert werden. Informationssicherheit umfasst alle Maßnahmen in technischen und nicht technischen Systemen mit folgenden Schutzzielen:

- **Vertraulichkeit:** Daten dürfen nur von befugten Personen (mit Rollen- und Rechtezuweisungen) eingesehen, bearbeitet und verwaltet werden.
- **Integrität**: Daten können nicht unerkannt verändert oder manipuliert werden.
- **Verfügbarkeit**: Auf Daten kann in zugesicherter Art und Weise zugegriffen werden.

IT-Sicherheit, Datensicherheit und Datenschutz sind dabei als Teilbereiche der Informationssicherheit (Abb. 1) zu sehen.

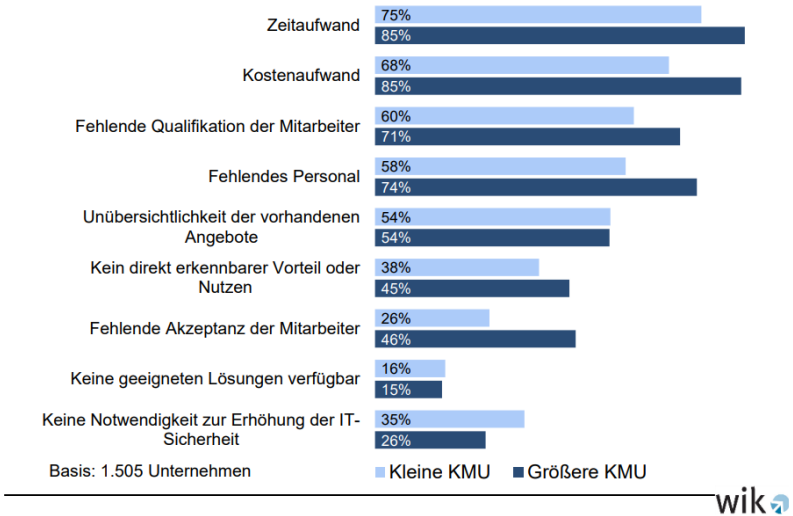
Abbildung 1: Definition Informationssicherheit



Quelle: WIK Recherche

Die Situation der IT-Sicherheit in KMU

Abbildung 2: Hemmnisse bei der Verbesserung der IT-Sicherheit aus Sicht der KMU nach Unternehmensgröße



Quelle: Hillebrand, A., Niederprüm, A., Thiele, S., Schäfer, S. (2017): Aktuelle Lage der IT-Sicherheit in KMU, WIK-Studie im Auftrag des BMWi, S. 76 (kleine KMU < 50, größere KMU 50-499 Mitarbeiter)

* Definition des BMWi nach Institut für Mittelstandsforschung (IfM) Bonn, <500 MA, <50 Million Umsatzerlös/ Jahr

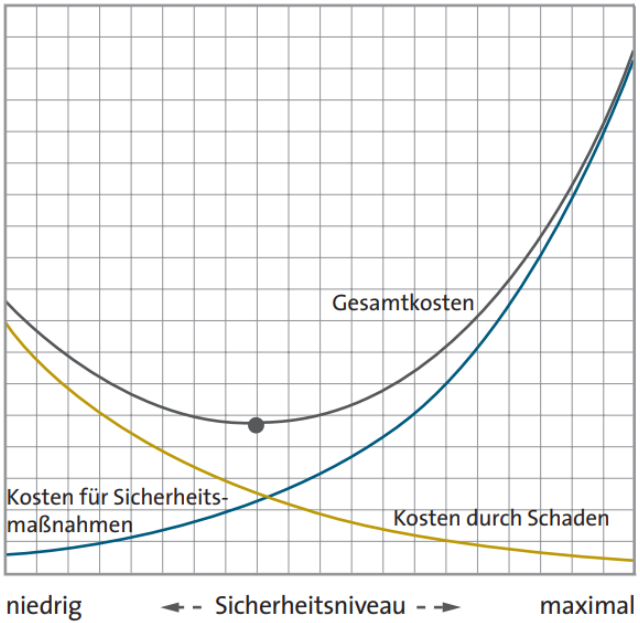
In vielen kleinen und mittleren Unternehmen (KMU)* wird Informationssicherheit, nach eigenen Aussagen, eine hohe Bedeutung beigemessen.[7] Am Bewusstsein für IT-Sicherheit mangelt es aber weiterhin. Risiken werden zwar erkannt, notwendige Maßnahmen unterbleiben jedoch allzu oft.[8] Die mangelnde Bereitschaft, die Umsetzungslücke zu schließen, darf nicht als „Vertrauen“ in die eigene Datenverarbeitung missverstanden werden.

Verbesserungen in der IT-Sicherheit bedeuten für die KMU einen hohen Zeitaufwand (Abb. 2). Qualifiziertes Personal oder Mitarbeiter fehlen häufig. Für jedes zweite KMU sind die vorhandenen Angebote zu unübersichtlich und kleinteilig. Die Folge ist eine abwartende Haltung der KMU.[9] KMU wissen oftmals nicht, in welche (sichere) Hardware, Software oder Dienstleistung sie investieren und welchem Dienstleister sie vertrauen können. Vielmehr herrscht eine „Augen zu und durch“-Mentalität.[10] Stehen Kaufentscheidungen an, wird Sicherheit letztlich oft hintangestellt: Datensicherheit ist nur für ein Fünftel der Entscheider in KMU ein zentraler Faktor beim Softwarekauf.[11]

Das Handeln der KMU deckt sich demnach nicht immer mit den Einstellungen und Aussagen der in der WIK-Studie befragten KMU-Geschäftsführer und -Sicherheitsexperten. Sie erklären, bestmöglich die IT-Sicherheit im Betrieb zu erhöhen, auf der anderen Seite unterbleibt dies aus Gründen der Risikofehleinschätzung, Unübersichtlichkeit der Angebote oder fehlender (personeller) Ressourcen.

Risikoabschätzung in KMU

Abbildung 3: Wirtschaftlich vertretbares Sicherheitsniveau in Abhängigkeit der Gesamtkosten



Quelle: Rumpel, R. et. al. (2011): Zertifizierung von Informationssicherheit in Unternehmen – ein Überblick, S. 6

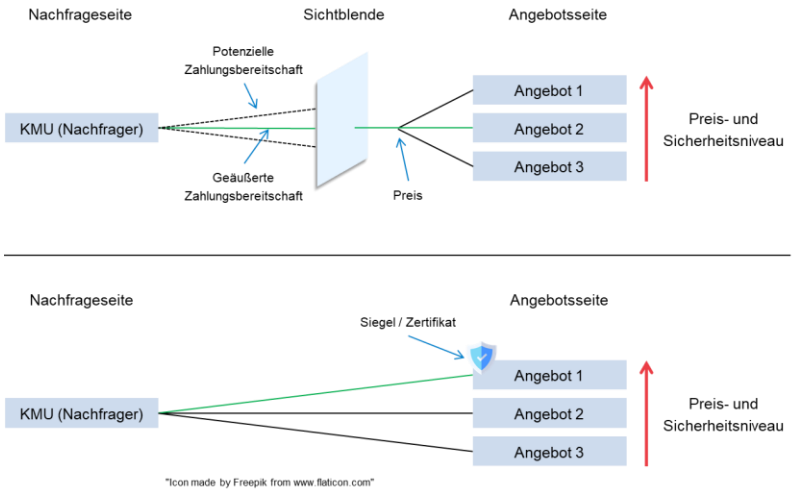
KMU wird zunehmend bewusst, dass die relevanten Schutzziele Vertraulichkeit, Integrität und Verfügbarkeit prioritär verfolgt werden müssen, um Risiken zu minimieren. Viele KMU sind jedoch mit Entscheidungen darüber, welche Systeme angeschafft werden, um ihre Werte ausreichend zu schützen überfordert. Anforderungen an Datensicherheit und Datenschutz sowie Komplexität und mangelnde Kenntnisse zur IT-Sicherheit führen dazu, dass Entscheider bei Investitionen zurückhaltend sind.[12]

Auf der anderen Seite fehlen Anreize für Hersteller und Anbieter von Produkten und Dienstleistungen, Informationssicherheit von sich aus zu integrieren. Nutzer und Kunden können das IT-Sicherheitsniveau kaum beurteilen.[13] Bei neu bekannt gewordenen Sicherheitslücken kann zudem nicht eingeschätzt werden, ob und wie schnell Hersteller reagieren. Nutzer und Kunden fokussieren sich bei der Auswahl eher auf Preis und Funktionalität.[14] Hinzu kommt, dass Hersteller bei einem Sicherheitsvorfall meist nicht für Schäden aufkommen müssen. Die Kosten tragen stattdessen die betroffenen Dienstleister und deren Nutzer.[15]

KMU schätzen IT-Risiken als (zu) niedrig ein und IT-Anbieter investieren nur so viel, wie Kunden bereit sind zu zahlen. Nach Einschätzung der befragten Experten bleiben die Investitionen hinter den Risiken zurück: Unternehmerische Entscheidungen stimmen nicht mit dem wirtschaftlich optimalen Sicherheitslevel überein[16] (Abb. 3) und Informationssicherheit wird vom Markt kaum honoriert.[17]

Risikoabschätzung in KMU

Abbildung 4: Effekt von Siegeln und Zertifikaten auf die Zahlungsbereitschaft der Kunden



Quelle: WIK Recherche, angelehnt an Fritsch, M. (2018) Marktversagen und Wirtschaftspolitik. Mikroökonomische Grundlagen staatlichen Handelns. München, 10. A: Vahlen., S. 252

Die Schwierigkeit besteht für die Kunden darin, mit geringem Aufwand herauszufinden, welches Angebot vertrauenswürdig ist und Sicherheitsversprechen hält. Für IT-Anbieter besteht die Herausforderung darin sichtbar zu machen, dass ihre Produkte und Dienstleistungen dem gewünschten Sicherheitsniveau entsprechen.

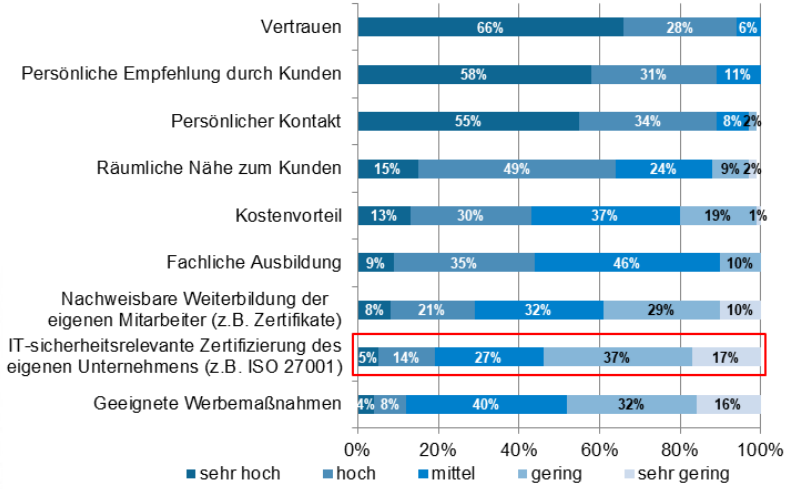
Um Vertrauenswürdigkeit zu belegen und zu visualisieren, haben sich darum in den vergangenen Jahrzehnten Standards für Audits und Zertifikate etabliert. Neben der Möglichkeit im eigenen Betrieb Audits vorzunehmen, um dort ein nachprüfbares Qualitätsniveau (inkl. sicherer Datenverarbeitung) zu gewährleisten, können Unternehmen auf zertifizierte Anbieter oder Produkte bauen. Kunden sehen dann anhand der Siegel und Zertifikate „auf einen Blick“, ob (Sicherheits-) Anforderungen eingehalten werden (Abb. 4, untere Darstellung).

Siegel und Zertifikate erlauben somit eine Reduktion der Komplexität der Angebote, beugen möglichen Informationsasymmetrien vor und sind ein geeignetes Mittel, um adverse Selektion aufgrund verborgener Eigenschaften zu verhindern (Prinzipal-Agent-Theorie). Herstellern und Dienstleistern wird darüber hinaus ein Anreiz geboten, Sicherheits-maßnahmen umzusetzen, um dies als Wettbewerbsvorteil auszuspielen (Signalling).[18]

Bei Verbrauchern haben z. B. in den Bereichen Tierwohl und Fairtrade Zertifikate und Gütesiegel bereits erfolgreiche Signalwirkungen und gesellschaftlich erwünschte Änderungswirkungen auf angebotene Produkte gezeigt.[19]

Risikoabschätzung in KMU

Abbildung 5: Faktoren einer erfolgreichen Akquise aus Sicht der IT-Dienstleister



Quelle: Klemeschov et. al. (2014): IT-Dienstleister und IT-Sicherheit in KMU, S. 15

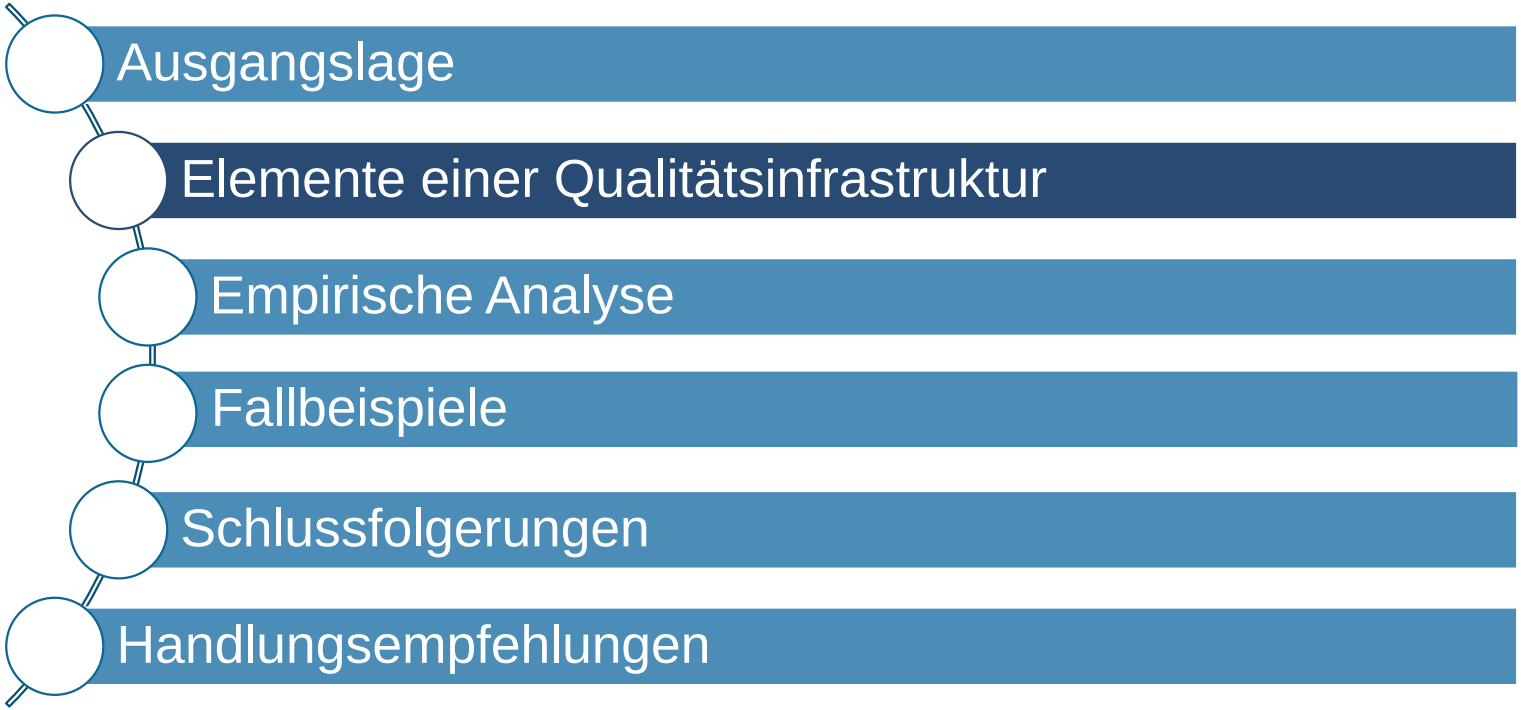
Es zeigt sich bei der Analyse des Marktes für IT-Dienstleistungen und Produkte, dass KMU vor großen Hürden stehen.

Fast drei Viertel der KMU arbeiten mit IT-Dienstleistern zusammen.[20] Dabei haben KMU Schwierigkeiten, überhaupt Anbieter für IT-Leistungen zu finden. Dies deckt sich mit Aussagen vieler IT-Dienstleister, die zumeist auf Unternehmenskunden ab einer gewissen Größe spezialisiert sind und für kleine KMU (bis etwa 100 Mitarbeitende) erweiterte Privatkundenangebote bereithalten.[21]

In der Kundenakquise kommen eher kleinere Anbieter mit KMU zusammen. Oft geschieht dies durch persönliche Empfehlungen.[22] Die IT-Dienstleister geben an, dass Vertrauen das wichtigste Kriterium dabei sei, allerdings nicht durch Zertifikate belegt sein müsse[23] (Abb. 5).

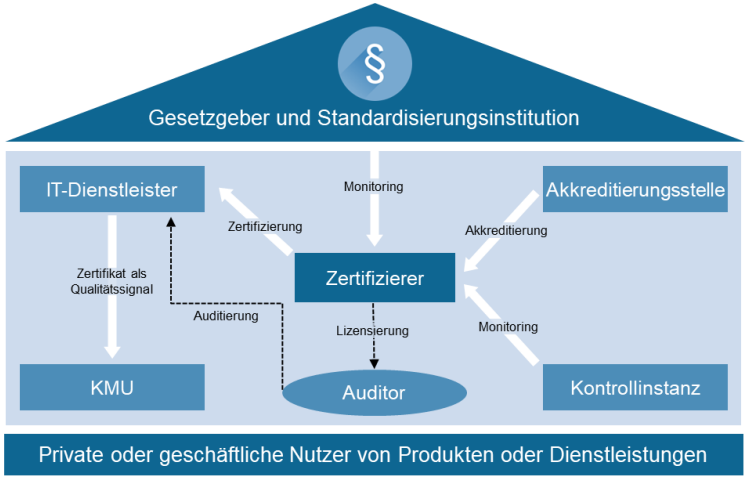
KMU dagegen halten Zertifikate für relevante Eignungs- und Auswahlkriterien. Für drei Viertel der KMU sind Kennzeichnungen zur IT-Sicherheit beim Kauf von Produkten und Dienstleistungen wichtig bis sehr wichtig; deutlich wichtiger als bei Individualverbrauchern.[24] Komplexität und Individualität von IT-Lösungen und Dienstleistungen erschweren die Entscheidungen in KMU. Die Bereitstellung von mehr Informationen hilft bei der Auswahl.[25] Vertrauen (ohne Zertifizierung), persönliche Kontakte und Empfehlungen sind für KMU wichtig. Häufig können IT-Dienstleister von KMU ohnehin nur in räumlicher Nähe gewählt werden, damit die Implementierung, Schulung und ggf. Wartung vor Ort durchgeführt werden kann.[26]

Inhalt


Ausgangslage
Elemente einer Qualitätsinfrastruktur
Empirische Analyse
Fallbeispiele
Schlussfolgerungen
Handlungsempfehlungen

Qualitätsinfrastruktur in Deutschland

Abbildung 6: Schematische Darstellung eines möglichen Zertifizierungsprozesses



Quelle: WIK Recherche, angelehnt an Jahn, Schramm, & Spiller (2005): Zur Glaubwürdigkeit von Zertifizierungssystemen: Eine ökonomische Analyse der Kontrollvalidität, S. 60 sowie enisa (2013): Auditing Security Measures - An Overview of schemes for auditing security measures, S. 34

Eine verlässliche Qualitätsinfrastruktur basiert, neben (ggf. gesetzlich vorgeschrieben) Normen und Standards auf einer Konformitätsbewertung und einer Akkreditierung (Abb. 6). Internationale oder nationale Gremien legen die Anforderungen fest. Ob die Anforderungen auch eingehalten werden, prüfen unabhängige Prüfstellen (Auditoren) mittels Konformitätsbewertungen. Zertifizierungsstellen bescheinigen die Prüfung. Diese Zertifizierungsstellen wiederum erbringen einen Kompetenznachweis, wenn sie durch unabhängige Stellen akkreditiert wurden.[27]

Normen und Standards können auch von Unternehmen selbst festgelegt werden und sich als proprietäre Standards im Markt etablieren. Darüber hinaus können (Bestandteile von) Normen und Standards kombiniert oder ergänzt werden. Diese kann dann der Herausgeber selbst oder (lizenzierte) Dritten überprüfen und zertifizieren.

Akkreditierte öffentliche sowie private, gemeinnützige oder gewinnorientierte Institutionen können mit Güte- und Prüfbestimmungen, die auf anerkannten Normen und Standards beruhen, Vertrauen durch Zertifizierungen schaffen. Die Einhaltung kann zusätzlich durch unabhängige Auditoren geprüft werden. Es können allerdings auch Gütezeichen mit weniger strengen Vorgaben genutzt werden. Es ist oft nicht ohne weitere Recherchen ersichtlich, welche Ansprüche an ein Gütezeichen bestehen. Dies bedeutet einen hohen Aufwand und Unsicherheiten für KMU.

DIN

„Der Unique Selling Point der deutschen Wirtschaft ist die Qualität und das Vertrauen in unsere Produkte und Dienstleistungen. Normung ist ein zentraler Baustein der Qualitätsinfrastruktur in Deutschland.“

Alexandra Horn, DIN e. V.

Norm

„eine technische Beschreibung oder ein anderes Dokument, das für jedermann zugänglich ist und unter Mitarbeit und im Einvernehmen oder mit allgemeiner Zustimmung aller interessierten Kreise erstellt wurde. Sie beruht auf abgestimmten Ergebnissen von Wissenschaft, Technik und Praxis“.[28]

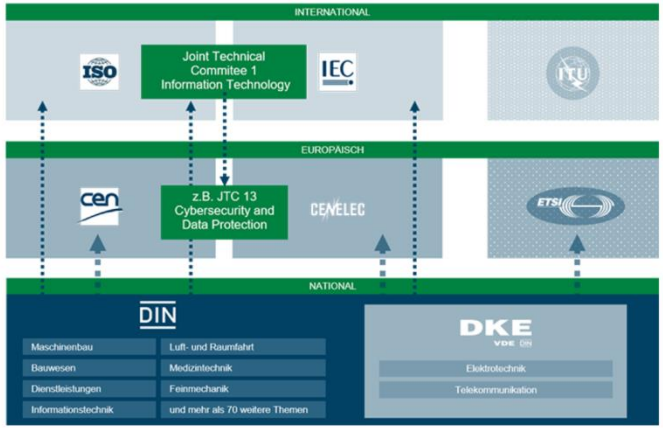
Seit über 100 Jahren entwickelt das Deutsche Institut für Normung e.V. (DIN) Normen und Standards. Diese konkretisieren den mit Gesetzen und Verordnungen geschaffenen gesetzlichen Rahmen, ohne selbst verpflichtend zu sein. Sie bilden die Grundlage für hohe Qualität und Interoperabilität von Technologien. Das DIN wurde 1975 im „Normenvertrag“ mit der Bundesrepublik Deutschland als einzige nationale Normungsorganisation in Deutschland anerkannt.

Der gemeinnützige Verein finanziert sich zu großen Teilen aus eigenen Erträgen (61,8 %) über den Verkauf von Normen, anderen Verlagsprodukten und Dienstleistungen über den Beuth Verlag. Der andere Teil stammt aus Projektmitteln der Wirtschaft (19,4 %), Mitgliedsbeiträgen (9,9 %) und Projektmitteln der öffentlichen Hand (8,9 %).[29]

Das DIN hat die Aufgabe, alle wichtigen Akteure in die Normung miteinzubeziehen. Nachdem der zuständige Ausschuss den Bedarf in der Branche geprüft hat, erarbeiten die Interessengruppen die Norm im Konsens. Das Netzwerk des DIN umfasst insgesamt 32.000 Expertinnen und Experten aus Wirtschaft, Forschung, Politik und von Verbraucherseite. Auch Kommentare der Öffentlichkeit werden in den Prozess einbezogen. Nach Veröffentlichung wird die Norm spätestens alle fünf Jahre überprüft. Die 2008 gegründete Kommission Mittelstand (KOMMIT) unterstützt KMU in der Normung und Standardisierung. Außerdem fördert das Bundesministerium für Wirtschaft und Energie (BMWi) eine breite Beteiligung von KMU in der Normung über das Technologieförderprogramm WIPANO.

DIN

Abbildung 7: Zusammenarbeit der nationalen und internationalen Normungsorganisationen



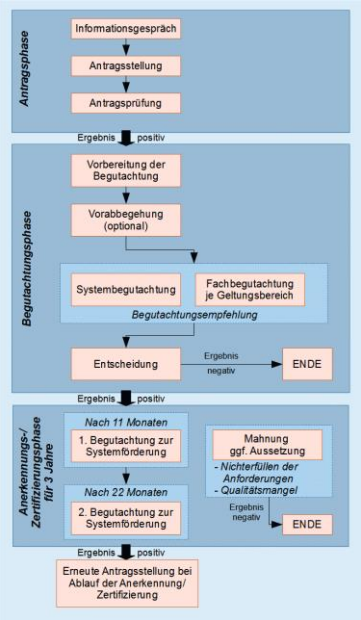
Quelle: DIN (2021): Internationale Normung

DIN vertritt die deutschen Interessen in europäischen und internationalen Normungsorganisationen und bildet ein wichtige Element der internationalen Normung (Abb. 7). Das CEN (Europäisches Komitee für Normung) erarbeitet europäische Normen mit dem Ziel, die in Europa geltenden Normen zu vereinheitlichen. Europäische Normen müssen unverändert als nationale Norm übernommen werden. Dies stützt das übergeordnete Ziel: Die Vereinfachung des freien Verkehrs von Waren und Dienstleistungen, der Interoperabilität und technologischen Entwicklung stärkt die Wettbewerbsfähigkeit von Unternehmen.[30] In der ISO (Internationale Organisation für Standardisierung) erarbeiten Vertreter und Vertreterinnen aus 165 Ländern internationale Normen. Deren Übernahme als nationale Norm ist hingegen nicht verpflichtend. Eine breite Akzeptanz der internationalen Normung erhöht jedoch den Druck, diese als nationale Normen zu übernehmen. Dies führt zu einem kontinuierlichen Wettbewerb zwischen Normen.[31] Laut Angaben des DIN sind 85 % aller Standardisierungsprojekte international[32].

Im DIN Normenausschuss Informationstechnik und Anwendungen (NIA) erarbeiten über 500 Expertinnen und Experten Normen auf dem Gebiet der Informationstechnik und ausgewählter IT-Anwendungsbereiche. IT-Normen sollen u. a. die Leistungsfähigkeit und Qualität von IT-Systemen verbessern sowie die Sicherheit von IT-Systemen und Daten erhöhen. NIA ist das Spiegelgremium zu zahlreichen Gremien auf europäischer und internationaler Ebene, die sich mit Informationssicherheit befassen.[33]

BSI

Abbildung 8: Schematischer Ablauf eines Anerkennungs- und Zertifizierungsverfahrens beim BSI



Quelle: BSI (2021): Anerkennung von Stellen und Zertifizierung von IT-Sicherheitsdienstleistern

Das Bundesamt für Sicherheit in der Informationstechnik (BSI) ist die deutsche Cyber-Sicherheitsbehörde und der „Gestalter einer sicheren Digitalisierung in Deutschland“. Das BSI hat u. a. nach dem BSI-Gesetz die Aufgabe zur Zertifizierung von informationstechnischen Produkten, Komponenten und (Management-)Systemen. Die Prüfungen (Audits) für diese Zertifizierungen führt das BSI nicht selbst, sondern die vom BSI anerkannten Prüfstellen durch. Das BSI zertifiziert IT-Sicherheitsdienstleister und erkennt Prüfstellen an. Für diese Aufgaben gibt die Behörde Zertifizierungsprogramme heraus, in denen Regeln, Verfahren sowie das Management zur Durchführung der Zertifizierung festgelegt und beschrieben sind.[34]

Im Bereich Zertifizierung ist das BSI in den folgenden Bereichen tätig: Die Zertifizierung nach ISO 27001 auf der Basis von IT-Grundschutz bietet einen De-Facto-Standard für Informationssicherheit. Produkt-Zertifizierungen sind durch das BSI entweder durch die Common Criteria oder nach verschiedenen technischen Richtlinien möglich. Mit dem freiwilligen IT-Sicherheitskennzeichen, das auf Grundlage des IT-Sicherheitsgesetz 2.0 entstanden ist, soll künftig Transparenz für Verbraucher über grundlegende Sicherheitseigenschaften digitaler Produkte erkennbar werden.

Neben der Zertifizierung bietet das BSI auch Anerkennungsprogramme an (Abb. 8). Die Anerkennung einer Prüfstelle über die Norm DIN EN ISO/IEC 17025 bestätigt deren Fachkunde und Eignung.

Akkreditierung (DAkkS)

Akkreditierung

Gemäß Art. 2 Nr. 10 VO (EG) 765/2008 ist „Akkreditierung“ die behördliche Bestätigung, dass eine Konformitätsbewertungsstelle die in harmonisierten Normen festgelegten Anforderungen und, gegebenenfalls, zusätzliche Anforderungen, einschließlich solcher in relevanten sektoralen Akkreditierungssystemen, erfüllt, um eine spezielle Konformitätsbewertungstätigkeit durchzuführen.

Die Akkreditierung wurde 2010 durch die EU-Verordnung 765/2008 zu einer hoheitlichen Aufgabe, seitdem muss jeder Mitgliedsstaat eine nationale Akkreditierungsstelle haben. So wurde das Akkreditierungswesen länderübergreifend harmonisiert und sichergestellt, dass es im öffentlichen Interesse erfolgt. In der Europäischen Kooperation für Akkreditierung (EA) überprüfen und beurteilen sich die nationalen Akkreditierungsstellen gegenseitig. Die Deutsche Akkreditierungsstelle (DAkkS) ist als nationale Akkreditierungsbehörde für die Akkreditierung von Konformitäts-bewertungsstellen mit Sitz in Deutschland zuständig. Neben der Akkreditierung von Konformitätsbewertungsstellen werden auch Konformitätsbewertungsprogramme akkreditiert. Diese stehen hinter einem Gütezeichen und legen die Anforderungen an das zertifizierte Produkt fest. Andere Behörden dürfen Konformitätsbewertungsstellen die Befugnis erteilen, tätig zu werden35, wenn dies durch Rechtsvorschriften geregelt ist. So erkennt das BSI sachverständige Stellen für die Zertifizierung von IT-Sicherheit an36.

Für die Tätigkeit der „Konformitätsbewertung“ in Form von Prüfung/Inspektion/Zertifizierung, etc. bestehen international harmonisierte ISO/IEC-Normen. Sie definieren den absoluten Mindeststandard an diese Organisationen und für deren Prüftätigkeiten. Damit wird zugleich der berufliche Mindeststandard an solche Tätigkeiten im Binnenmarkt beschrieben. Wer die harmonisierten Normen der Reihe 17000 unterschreitet, prüft, nach Aussage der DAkkS, nicht lege artis und missachtet den Stand der Technik, was eine Gefährdung der öffentlichen Sicherheit darstellt und von den Behörden der Mitgliedsstaaten zu unterbinden ist.

Akkreditierung (DAkkS)

Grundsätzlich ist eine Akkreditierung für die Ausstellung eines Siegels oder eine Zertifizierung nicht erforderlich, fördert allerdings das Vertrauen in die Zertifizierungsstelle und das Zertifikat. Ausnahmen bilden Konformitätsbewertungen, für die eine Rechtsvorschrift die Akkreditierung der Bewertungsstelle anordnet (§ 3 Abs. 2 AkkStelleG), z. B. die Datenschutzgrundverordnung (DSGVO).

Unabhängig davon, ob die Akkreditierung obligatorisch ist oder nicht, müssen die Mitgliedstaaten der EU gemäß Art. 3 VO (EG) Nr. 765/2008 sicherstellen, dass die Anforderungen der Akkreditierung in Bezug auf die Bewertung der Konformität eingehalten werden. Der mit der Verordnung eingerichtete Akkreditierungsrahmen gilt ausdrücklich sowohl für den reglementierten als auch für den freiwilligen Bereich. Der Grund dafür ist, dass die Grenze zwischen beiden fließend sein kann, weil Konformitätsbewertungsstellen in beiden Bereichen tätig sind und Produkte in beiden Bereichen verwendet werden. Eine getrennte Behandlung würde deshalb für die öffentlichen Behörden und Marktakteure unnötigen Aufwand verursachen und zu Widersprüchen zwischen dem reglementierten und nicht reglementierten Bereich führen[37].

Die Kosten der Akkreditierung durch die DAkkS sind in der Allgemeinen Gebührenverordnung (AGebV) festgelegt. Eine Studie des Deutschen Verbandes Unabhängiger Prüflaboratorien e. V. (VUP) analysierte die Kosten einer Akkreditierung im Verhältnis zum Umsatz der Prüflabore.

Die Kosten der Akkreditierung für Laborunternehmen mit einem Umsatz unter zwei Millionen € belaufen sich auf 0,85 % ihres Umsatzes. Große Laborunternehmen ab 20 Mio. € Umsatz bezahlen hingegen nur 0,06 % ihres Umsatzes für die Akkreditierung.[38]

Laut dem Geschäftsführer des VUP ziehen sich KMU aus dem Markt zurück oder reduzieren den Umfang, da sie sich die Akkreditierung nicht mehr im bisherigen Umfang leisten können.[39]

Exkurs: Fairtrade-Siegel

Das **Fairtrade-Siegel** hat einen hohen Bekantheitsgrad in der breiten Öffentlichkeit. Es vereint zentrale Merkmale von Gütezeichen. Es dient hier als Beispiel für ein erfolgreich eingeführtes, allgemein verständliches Siegel

Bildquelle: TransFair e.V.

- Das Fairtrade-Siegel vereint zentrale Merkmale, die auch auf komplexere Gütezeichen zutreffen. Es kann als Beispiel für ein vertrauenswürdiges, bekanntes Siegel gelten, wie es für Informationssicherheit in dieser Form fehlt
- Es kennzeichnet Produkte aus fairem Handel
- 90 % der Bevölkerung bekannt, 92 % aller Käufer von Fairtrade-Produkten vertrauen dem Siegel (GlobeScan-Studie 2021)
- Identifizierte vertrauensbildende Faktoren:
  - Unabhängige Organisation
  - Strenge Prüfung
  - Regelmäßige Kontrollen
  - Aktuelle Standards
  - Transparenz

Exkurs: Fairtrade-Siegel

Fairtrade Labelling Organizations International (FLO) steht als Dachverband hinter dem Fairtrade-System. FLO verbindet nationale Fairtrade-Organisationen und Produzenten-Netzwerke und entwickelt die Fairtrade-Standards.

Das Fairtrade-Siegel kennzeichnet seit 2003 Produkte aus fairem Handel, bei deren Herstellung soziale, ökologische und ökonomische Kriterien in der gesamten Wertschöpfungskette eingehalten wurden. Die ISO 17065 akkreditierte Tochtergesellschaft FLOCERT führt die Audits für das Fairtrade-Siegel durch. Mit einer Bekanntheitsquote von 90 % ist das Fairtrade-Siegel laut GlobeScan Studie 2021 das bekannteste Nachhaltigkeitssiegel in Deutschland und 92 % aller Käufer von Fairtrade-Produkten vertrauen ihm. Welche Faktoren führen zu dem hohen Vertrauen in das Siegel?

1.	**Unabhängige Organisation** Mehr als 30 Organisationen aus verschiedenen Bereichen sind Mitglieder von Fairtrade Deutschland.
2.	**Strenge Prüfung** Ein Erstaudit dauert mehrere Tage, in denen neben der Auswertung verschiedener Informationsquellen Produktionsanlagen inspiziert und Interviews mit Angestellten durchgeführt werden.
3.	**Regelmäßige Kontrollen** Nach der Erst-Zertifizierung werden die Produzenten-Organisationen innerhalb des dreijährigen Zertifizierungszyklus mindestens zwei weitere Male und auch durch unangekündigte Audits überprüft.
4.	**Aktuelle Standards** Die Fairtrade-Standards werden mindestens alle fünf Jahre überarbeitet und aktualisiert.
5.	**Transparenz** Die Entwicklung der Standards erfolgt nach den Vorgaben der ISEAL und unter Einbindung aller wichtigen Akteure. Über Beschwerdemechanismen können alle Verstöße gemeldet werden.

Inhalt

- Ausgangslage
- Elemente einer Qualitätsinfrastruktur
- **Empirische Analyse**
- Fallbeispiele
- Schlossfolgerungen
- Handlungsempfehlungen

Empirische Analyse: Zertifikate und Siegel

Die Ergebnisse und Aussagen beruhen auf Desk Research und Experteninterviews. Es wurden nach bestem Wissen alle öffentlich verfügbaren Informationen der Herausgeber und Zertifizierer auf deren Webseiten sowie Informationen aus öffentlich zugänglichen Stellen ausgewertet.

Im Rahmen dieser Studie haben wir mittels Desk Research **49 Siegel und Zertifizierungen aus dem Bereich Informationssicherheit** identifiziert, die für KMU potenziell relevant sind.*

Die Siegel und Zertifikate wurden folgendermaßen kategorisiert:

- Herausgeber: Wer definiert die Normen und Standards für Siegel und Zertifizierungen? Wer führt die Siegelvergabe / Zertifizierung durch?
- Prüfgegenstand: Gelten die Siegel und Zertifizierungen generisch für Informationssicherheit oder für spezifische Teilbereiche? Für welche Bereiche und Produktkategorien sind sie anwendbar?
- Kosten: Sind die Kosten für Siegelverleihung und Zertifizierung veröffentlicht? Wie berechnen sich diese und wie hoch fallen schätzungsweise sie aus?
- Akzeptanz für und Vertrauen in Siegel und Zertifizierungen: Was ist die Grundlage der Prüfkriterien? Werden sie offengelegt? Wie ist die Gültigkeitsdauer der Siegel und Zertifikate? Ist der Auditor unabhängig? Ist eine Akkreditierung der Zertifizierungsstelle notwendig?

Die Untersuchung beschränkt sich auf Siegel und Zertifizierungen, die in Deutschland bekannt und gebräuchlich sind.

* In der Untersuchung wurden Zertifikate auf Grundlage von Normen und Standards von ISO, DIN und IEC nur einfach gezählt, obwohl die Zertifizierung selbst von mehreren Prüforganisationen durchgeführt wird, sich die Prüfung der Kriterien im Detail unterscheiden kann und damit faktisch (mehrere) unterschiedliche Zertifikate vorliegen. Fünf weitere IT-sicherheitsrelevante Zertifizierungen für Rechenzentren wurden in einer Fallstudie betrachtet.

Zertifikate und Siegel

49 Zertifikate / Siegel im Bereich Informationssicherheit:

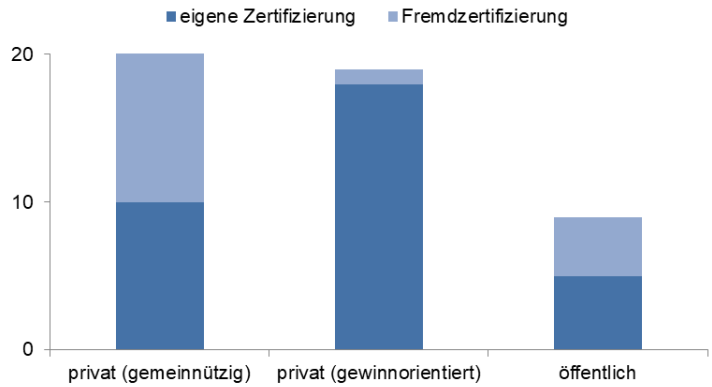
- ADCERT-Datenschutzsiegel
- BITMi-Gütesiegel für mittelständische Softwarehersteller
- BITMi-TÜV-SÜD-Zertifikat für Softwarequalität
- BNT - Geprüfter Datenschutz
- Check 28 Datenschutzaudit
- CIF - cloud industry forum code of practice
- Cloud Computing Compliance Criteria Catalogue - C5
- CSA Trusted Cloud Provider
- Cybersecurity Made In Europe
- Datenschutz für KMU (VdS 10010)
- EDAA-OBA
- ePrivacycert
- ePrivacyseal EU
- Eurocloud Star Audit
- European Privacy Seal (EuroPriSe)
- GoodPriv@cy
- IEC 62443
- IITR CERT
- Informationssicherheit für KMU (VdS 10000)
- ISIS12 / CISI12
- ISO/IEC 15408 Common Criteria
- ISO/IEC 21964-1 - DIN 66399
- ISO/IEC 27001
- ISO/IEC 27001 auf Basis des BSI-Grundschutz
- ISO/IEC 27017
- ISO/IEC 27018
- ISO/SAE 21434 "Road Vehicles – Cyber Security Engineering"
- ISO27701
- IT Security made in EU (ITSMIE)
- IT Security made in Germany (ITSMIG)
- IT-Sicherheitskatalog
- IT-Sicherheitskennzeichen
- KOMMUNALE IT-SICHERHEIT
- Software Hosted in Germany
- Software Made in Germany
- Technische Richtlinien des BSI - BSI TR-01201 (De-Mail), BSI-TR-03108 (Sicherer E-Mail-Transport), BSI TR-03132 (Sichere Szenarien für Kommunikationsprozesse im Bereich hoheitlicher Dokumente)
- Technische Richtlinien des BSI - BSI TR 03124 (eID-Client)
- Technische Richtlinien des BSI - BSI TR-03148 (Sichere Breitband Router), TR BSI TR-03119 (Chipkartenleser)
- TISAX
- Trust in Privacy (TIP)
- Trusted App
- Trusted App by Appvisory
- Trusted Cloud Datenschutz-Profil für Cloud-Dienste (TCDP)
- Trusted Cloud Label für Cloud Services
- Trusted Cloud Service – TÜV
- Trusted Site Privacy
- TÜV geprüfter Datenschutz / überwachter Datenschutz
- VdS SecIoT (VdS 3836)
- Zertifizierter Datenschutz - inois Datenschutz-Zertifikat

Fünf Zertifikate / Siegel für Rechenzentren (Fallstudie):

- Betriebssicheres Rechenzentrum gem. DIN EN 50600
- Data Center Star Audit
- Reliable Data Center
- Trusted Site Infrastructure – TSI
- TÜV SÜD Zertifiziertes Rechenzentrum

Empirische Analyse: Fokus Herausgeber

Abbildung 9: Verteilung der Zertifizierungen und Siegel nach Herausgeber-Kategorie



Quelle: WIK Recherche

Siegel und Zertifikate werden an Unternehmen vergeben, wenn bestimmte Prüfkriterien erfüllt sind. Die Prüfkriterien legt die Zertifizierungsstelle fest.* Die Normen und Standards, die ihnen zugrunde liegen, werden vom Herausgeber des Siegels bzw. Zertifikats definiert. Die Herausgeber lassen sich drei Kategorien zuordnen (Abb. 9):

- Öffentliche Institutionen (z. B. BSI)
- Private, gemeinnützige Organisationen (z. B. Internationale Organisation für Normung – ISO, eco – Verband der Internetwirtschaft e. V.)
- Private, gewinnorientierte Organisationen (z. B. VdS Schadenverhütung GmbH, technische Prüforganisationen wie TÜV)

Private, gemeinnützige Stellen legen oft nur die Standards fest und führen keine eigene Zertifizierung durch. Bei 21 Siegeln / Zertifizierungen dieser Kategorie ist das bei 11 der Fall. In 10 Fällen wird das Siegel / Zertifikat von derselben Stelle auch verliehen.

Wenn Standards für Siegel / Zertifikate von privaten, gewinnorientierten Stellen festgelegt werden, führen sie in der Regel die Zertifizierung auch selbst durch (18 von 19 Fällen).

Öffentliche Stellen legen zum Teil nur die Standards fest (vier von neun Fällen), zum Teil überlassen sie die Zertifizierung anderen Prüfstellen.

* Bei einem Standard wird nur festgelegt, was und nicht wie er erfüllt werden muss. Die Ausgestaltung der Anforderungen eines Standards ist Teil unternehmerischen Wettbewerbs. Das gleiche gilt für den Prüfprozess.

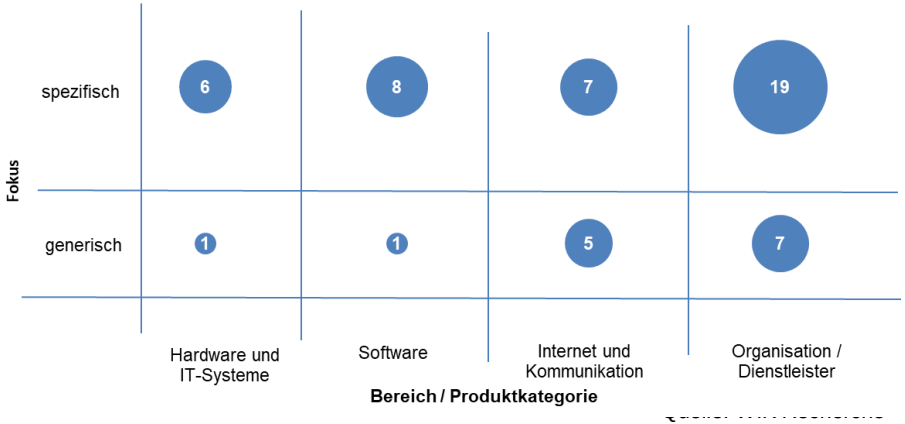
Empirische Analyse: Fokus Prüfgegenstand

Siegel und Zertifizierungen werden nicht pauschal in allen Bereichen und für alle Produkte eingesetzt.

Wir haben sie in vier Bereiche bzw. Produktkategorien (Hardware und IT-Systeme, Software, Internet und Kommunikationsdienste sowie Organisation/ Dienstleister) aufgeteilt und unterschieden, ob sie generisch für Informationssicherheit insgesamt gelten oder spezifisch (für die Teilbereiche IT-Sicherheit, Datensicherheit und Datenschutz) (Abb. 10).

Die Untersuchung zeigt, dass nur wenige Zertifizierungen (13) einen generischen Ansatz haben und Informationssicherheit allgemein abdecken. Der Großteil der Zertifizierungen (32) deckt nur Teilbereiche ab oder bezieht sich auf die Sicherheit von Dienstleistern (4).

Abbildung 10: Fokus der Siegel / Zertifikate nach Bereich bzw. Produktkategorie*



* Die Summe in dieser Auswertung ist etwas höher, als die Gesamtzahl der identifizierten Siegel / Zertifikate, da manche Siegel / Zertifikate für mehrere Bereiche bzw- Produktkategorien angewendet werden können.

Empirische Analyse: Fokus Prüfgegenstand

> *„Ein Siegel für einzelne Geräte dokumentiert eine Momentaufnahme und die Absicht eines Herstellers, IT-Sicherheit ernst zu nehmen. Es können durch ein Update oder Release bzw. durch die Integration in das Unternehmen neue Schwachstellen entstehen.“*
>
> Stephan Schwichtenberg, Bundesverband IT-Mittelstand e. V.

Im **Bereich Hardware und IT-Systeme** wurden sieben Siegel / Zertifikate identifiziert. Es handelt sich um IT-Sicherheits-Zertifizierungen für bestimmte Produkte oder Datenschutz-Zertifikate. Nur ein Zertifikat deckt die Informations-sicherheit eines IT-Produkts insgesamt ab. Drei Zertifizierungen sind ausschließlich für Hardware und IT-Systeme anwendbar, vier weitere auch in anderen Bereichen.

Im Bereich **Software** wurden neun Siegel / Zertifikate identifiziert. Eine generische Zertifizierung belegt die Informationssicherheit mit der Abdeckung von Sicherheitslücken. Acht spezifische Zertifizierungen beziehen sich auf Datenschutz/-sicherheit von Software allgemein oder auf Apps bzw. die IT-Sicherheit von Software in Kraftfahrzeugen oder Ausweisfunktionen. Sechs Zertifizierungen sind ausschließlich für Software anwendbar, drei weitere auch in anderen Bereichen.

Im Bereich **Internet und Kommunikation** wurden 12 Siegel / Zertifikate identifiziert. Fünf gelten generisch für die Informationssicherheit bei Cloud-Diensten. Drei decken Datenschutz/-sicherheit bei Cloud-Diensten ab, eine die IT-Sicherheit bei Cloud-Diensten und drei die IT-Sicherheit bei Kommunikationswegen und -produkten sowie in Autos. 10 Zertifizierungen sind ausschließlich für Internet und Kommunikation anwendbar.

Am verbreitetsten sind Siegel / Zertifikate im Bereich **Organisation / Dienstleister** (26). Sieben dienen generisch dem Nachweis von Informationssicherheit in Organisationsstrukturen, wobei drei davon nur in einzelnen Branchen gelten. 15 Zertifizierungen beziehen sich auf Datenschutz/-sicherheit in den Organisationen und vier stehen für eine sichere Organisation bzw. Dienstleister.

Empirische Analyse: Fokus Kosten

> *„Die Kosten eines qualitativ hochwertigen Zertifikates sind schnell im 5-stelligen Bereich. Dazu kommen noch die internen Aufwände. Das ist für KMU oft eine Herausforderung.“*
>
> Sebastian Meissner, EuroPriSe GmbH

Öffentlich zugängliche Informationen zu Kosten sind die Ausnahme. Es konnten nur in sieben von 49 Fällen Preise für Zertifizierungen ermittelt werden.

Die Preisgestaltung kann untergliedert werden in

- Festpreise (je Produkt / Laufzeit / Unternehmensgröße),
  - die pauschal dem Aufwand des Prüfumfangs entsprechen,
  - einer monatlichen oder jährlichen Mitgliedsgebühr über die Laufzeit des Siegels / Zertifikates entsprechen.
- Aufwandsabhängige Preise, die entsprechend der Kosten für individuelle Prüfumfänge anfallen.

Der größte Kostentreiber sind nach Expertenangaben indirekte Kosten, d. h. Kosten, die in den geprüften Unternehmen entstehen, um die Prüfkriterien erfolgreich zu erfüllen und zu erhalten.

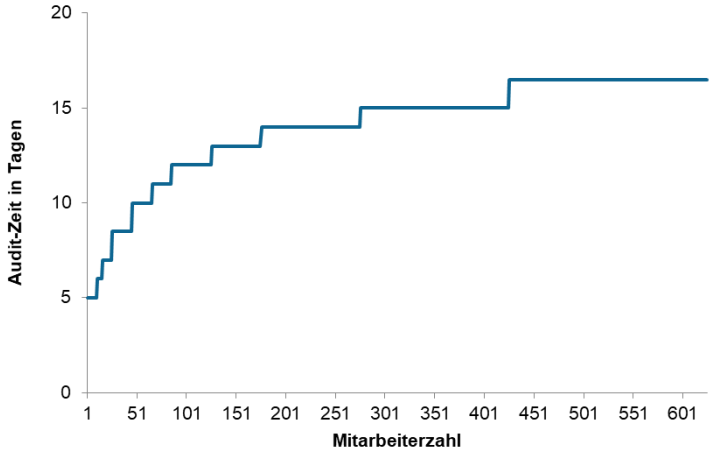
Die kostengünstigsten Siegel und Zertifikate in der Untersuchung basieren auf einem geringen Prüfumfang. Eine Selbstauskunft des Unternehmens ist dann ausreichend. Dafür werden Gebühren von ca. 300 bis 400 €/Jahr fällig. In einem Fall wird die Selbstauskunft von unabhängigen Auditoren überprüft. In diesem Fall werden Gebühren von ca. 4.000 €/Jahr fällig. Für KMU reduziert sich der Preis auf ca. 2.000 €/Jahr.

Bei einer umfangreicheren Prüfung mit externen Auditoren gibt es zwei Festpreis-Varianten:

- Variante 1: Insgesamt wird eine Summe zwischen 10.000 und 30.000 € aufgerufen, je nachdem wie viele Sterne mit dem Siegel vergeben werden. Die Sterne sind gleichbedeutend mit der Prüfintensität.
- Variante 2: Der Preis für Testat und Zertifikat richtet sich nach der Mitarbeiterzahl und liegt zwischen 1.250 € für Kleinstunternehmen und 25.000 € für Unternehmen mit mehr als 1.500 Mitarbeitenden.

Empirische Analyse: Fokus Kosten

Abbildung 11: Berechnung der erforderlichen Audittage im Rahmen einer Zertifizierung nach den Vorgaben der ISO 27006, Anhang B



Quelle: WIK Recherche, Daten aus ConformityZert GmbH (2021): Zertifizierung Auditdauer und Preise, S. 4

Wenn aufwandsabhängige Preise verlangt werden, können sich diese je nach Siegel / Zertifikat und Zertifizierungsstelle deutlich unterscheiden.

Teilweise gibt es standardisierte Rechnungen und Tabellen, die den Prüfumfang festlegen. Der Aufwand einer Zertifizierung nach ISO 27006 ist beispielsweise abhängig von der Anzahl der Mitarbeitenden (Abb. 11). Kleine und mittlere KMU haben hier einen vergleichsweise höheren Aufwand.

Außerdem hängt der Aufwand von der Anzahl der zu prüfenden Standorte, der Komplexität des Gesamtsystems bzw. des zu zertifizierenden Produkts, Systems oder Geschäftsbereiches sowie Synergieeffekten durch bereits vorhandene Zertifizierungen ab.[40] Die Zahl der verpflichtenden Prüftage kann um max. 30 % reduziert werden. Beim Überwachungsaudit und der Re-Zertifizierung gelten zudem kürzere Audit-Zeiten (1/3 bzw. 2/3 der veranschlagten Tage). Im ersten Jahr muss, so Expertenschätzungen, je nach Umfang, mit 4.000 bis 20.000 € gerechnet werden. Hinzu kommen Beratungskosten zwischen 3.000 und 15.000 €. Je nach Aufwand muss für den Vorgang von der Beratung bis zur Zertifizierung mit zwei bis 12 Monaten gerechnet werden.[41] [42] [43]

Andere Zertifizierungen können noch kostenintensiver sein. Für die Zertifizierung von Smart Meter Gateway wurden in Deutschland bspw. deutlich mehr als eine Millionen Euro, in den Niederlanden nur 40.000 € veranschlagt.[44]

Aus Sicht des geprüften Unternehmens sind die Kosten in Bezug zu setzen zu dem Markterfolg des zertifizierten Produkt bzw. der Dienstleistung. Ob sich eine Zertifizierung finanziell lohnt, ist auch eine Frage der Mengeneffekte und Zahlungsbereitschaft der Kunden.

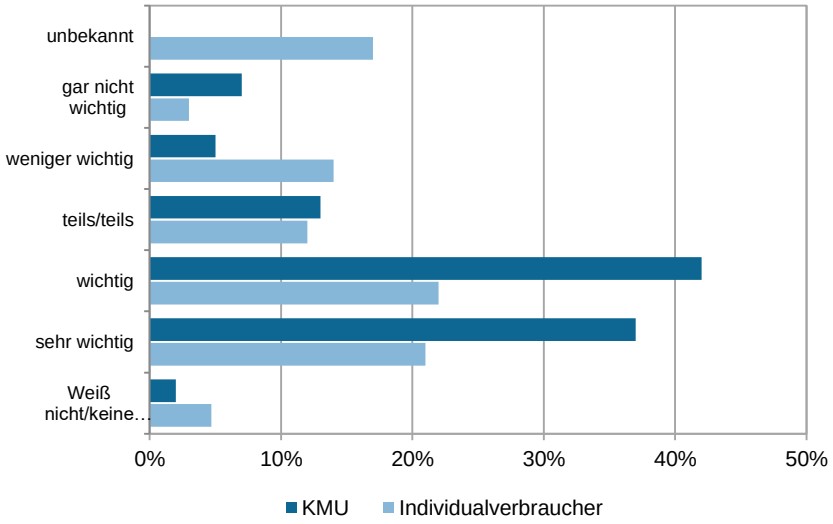
Empirische Analyse: Fokus Akzeptanz

Es gibt kaum Erhebungen, die das Ausmaß der Akzeptanz einzelner Siegel und Zertifikate in Unternehmen belegen. Wir haben daher aus Studien und Expertengesprächen Faktoren identifiziert, die für die Akzeptanz entscheidend sind.

Siegel und Zertifikate werden von KMU überwiegend als (sehr) wichtig angesehen (Abb. 12). KMU legen beim Einkauf mehr Wert darauf, als es Individualverbraucher tun.

Dennoch haben KMU oft Probleme, die Siegel und Zertifikate zu bewerten.[45] Eine wichtige Rolle für den Bekanntheitsgrad spielen herausgebende Institutionen. Etwa 60 % der KMU kennen Siegel und Zertifikate. Größtenteils handelt es sich dabei um Zertifizierungen nach ISO-Normen oder um von bekannten technischen Prüforganisationen herausgegebene Zertifikate.[46]

Abbildung 12: Wichtigkeit von Zertifikaten oder Gütesiegeln beim Einkauf von Produkten oder Dienstleistungen



Quelle: BMWi (2018): Gütesiegel und Zertifikate für IT-Sicherheit S. 35 f. (unveröffentlicht)

Empirische Analyse: Fokus Akzeptanz

Es existieren zahlreiche Hemmnisse für die Anwendung von Gütezeichen in KMU (Abb. 13).

Bekanntheit ist kein zuverlässiger Indikator für Vertrauen.

Bekanntheit erzeugt nicht pauschal auch Vertrauen in die inhaltliche Botschaft eines Gütezeichens.

Die Glaubwürdigkeit wird vielmehr durch verschiedene Faktoren positiv beeinflusst, die dem Konzept „Vertrauen“ entsprechen.

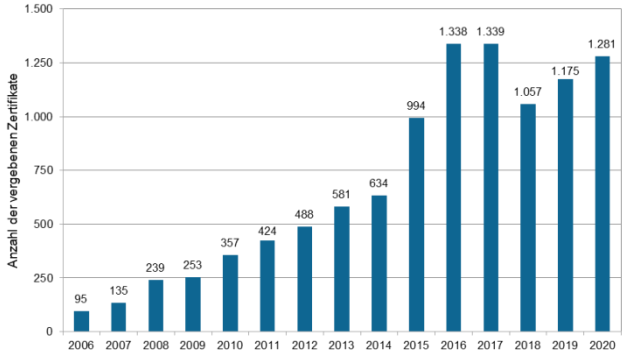
Zwischen der Kenntnis des Bewertungsinhalts und dem Vertrauen in Gütezeichen besteht ein positiver Zusammenhang. Die Unabhängigkeit des Auditors und der Zertifizierungsstelle sowie die Offenlegung der Prüfkriterien fördern die Glaubwürdigkeit in besonderem Maße.[47]

Abbildung 13: Hemmnisse bei der Berücksichtigung von Gütesiegeln oder Zertifikaten

Quelle: BMWi (2018): ebd. S. 35 f. (unveröffentlicht)

Empirische Analyse: Fokus Akzeptanz

Abbildung 14: Das bekannteste Zertifikat im Bereich Informationssicherheit ist im Vergleich zur Gesamtzahl an Unternehmen in Deutschland kaum verbreitet



Quelle: ISO (2021): Bestand an gültigen ISO-27001-Zertifikaten in Deutschland in den Jahren 2006 bis 2020, zitiert nach de.statista.com, URL https://de.statista.com/statistik/daten/studie/829353/umfrage/bestand-an-vergebenen-iso-27001-zertifikaten-in-deutschland/ abgerufen am 24.11.2021

Insgesamt ist die Verbereitung selbst von bekannten Zertifikaten im Bereich der Informationssicherheit in Deutschland sehr gering (Abb. 14).

Wir haben die Siegel und Zertifikate daraufhin untersucht, ob die Grundlagen der Prüfkriterien sowie die Prüfkriterien offengelegt werden, die Gültigkeitsdauer des Zertifikats angegeben und Informationen zur Unabhängigkeit des Auditors bzw. der Akkreditierung der Zertifizierungsstelle publiziert werden.

Grundlage der Prüfkriterien: Von den untersuchten Siegeln und Zertifikaten werden 16 (rund ein Drittel) auf Basis (inter-)nationaler Normen und Standards verliehen. Dabei können die einzelnen Zertifizierungsstellen (bzw. deren Auditoren) unterschiedliche Prüfkriterien nutzen. Bei den übrigen Zertifizierungen werden eigene Prüfkriterien zu den Normen und Standards hinzugefügt oder auch eigene Prüfkriterien definiert. Dies ist z. B. der Fall, wenn sich noch keine Normen und Standards etabliert haben (z. B. DSGVO).

Offenlegung der Prüfkriterien: Beim Großteil (38 von 49) der Siegel und Zertifikate ist ersichtlich, ob und nach welchen Normen und Standards diese vergeben werden. Die Prüfkriterien sind der Zertifizierungsstelle, dem Auditor und den zertifizierten Unternehmen bekannt. Die zugrundeliegenden Normen und Standards sind nicht immer kostenlos öffentlich einsehbar. Wenn Siegel und Zertifikate auf selbst entwickelten Prüfkriterien basieren, werden diese kaum offengelegt. Für 19 Zertifikate sind alle Prüfkriterien veröffentlicht.

Empirische Analyse: Fokus Akzeptanz

Akkreditierungspflicht: Eine generelle Akkreditierungspflicht der Zertifizierungsstellen von unabhängiger dritter Stelle (z. B. DAkkS) besteht in Deutschland nicht. Bei sieben der untersuchten Gütezeichen auf Basis von (inter-)nationalen Normen und Standards wird dies vom Herausgeber empfohlen. In drei Fällen gilt eine Akkreditierungspflicht der Auditoren. Beim BSI-Grundschutz muss eine Akkreditierung über das BSI erfolgen.

Unabhängigkeit des Auditors: Bei 46 Zertifizierungen finden sich offen zugängliche Informationen zu den Auditprozessen. In 38 Fällen ist ein Vor-Ort-Audit notwendig, in acht Fällen ist eine Selbstauskunft ausreichend. Das Vor-Ort-Audit wird in 30 Fällen von unabhängigen Auditoren durchgeführt und in acht Fällen von der Zertifizierungsstelle. Die Selbstauskunft wird bei drei Zertifizierungen überprüft; in einem Fall von unabhängigen Auditoren.

Gültigkeitsdauer des Zertifikats: In der Regel sind Siegel und Zertifikate nur eine begrenzte Zeit gültig. Die Gültigkeitsdauer ist nicht immer angegeben. Bei fünf der untersuchten Zertifizierungen ist das Zertifikat an Mitgliedschaften und Selbstauskünfte gebunden und läuft somit nicht aus. Eine Re-Zertifizierung ist hier nicht notwendig.

35 Zertifizierungen besitzen eine Gültigkeit zwischen 12 und 36 Monaten. Bei 16 der mehrjährig gültigen Zertifizierungen ist alle 12 Monaten (in einem Fall alle sechs) eine Re-Zertifizierung notwendig. Vier Zertifikate sind rückwirkend für die geprüfte Version des Produkts gültig.

Im Bereich Informationssicherheit sind verschiedene Normen für die **Akkreditierung von Zertifizierungsstellen** relevant. Es sind 24 Zertifizierungsstellen für Produkte, Prozesse und Dienstleistungen im Bereich Informationstechnik / Informationssicherheit / Cybersecurity und 54 Zertifizierungsstellen für Managementsysteme im Bereich Informationssicherheitsmanagementsysteme (ISMS) / Datenschutz akkreditiert.[48]

Schlussfolgerungen

Herausgeber	Der Markt bietet zahlreiche Normen und Standards auf denen Zertifizierungen aufbauen. Dritte können die Zertifizierung durchführen. Dadurch ist das Niveau der Zertifizierung immer im Zusammenhang mit dem Zertifizierungsprozess zu sehen und nicht nur im Zusammenhang mit dem Herausgeber.
Produktkategorie	Die meisten Siegel und Zertifizierungen beziehen sich nur auf spezifische Teilbereiche der Informationssicherheit. Dadurch ist ersichtlich, welche Produktkategorie genau zertifiziert wurde. Ein einfacher Vergleich in Hinblick auf „sichere“ bzw. „unsichere“ Produkte, Dienstleistungen oder Unternehmen ist nicht sinnvoll.
Kosten	Die Kosten für KMU sind nur schwer zu bewerten. Es fallen hohe direkte und indirekte Kosten an, die zum Teil übertragen werden auf die Kunden. KMU sind oftmals nicht bereit die Kosten zu tragen. Es werden eher die kurzfristigen Kosten, als der langfristige Nutzen für eigene interne Prozesse, Marketing oder Kundenakquise gesehen.
Akzeptanz	Die untersuchten Siegel und Zertifikate finden kaum breite Akzeptanz bei KMU. (Grundlagen der) Prüfkriterien sind zum Großteil für die Nachfrager intransparent. Inwieweit die Validierung der Kriterien durch unabhängige Dritte erfolgt, ist im Einzelfall zu betrachten.

Inhalt

- Ausgangslage
- Elemente einer Qualitätsinfrastruktur
- Empirische Analyse
- **Fallbeispiele**
- Schlussfolgerungen
- Handlungsempfehlungen

Fallbeispiel: DSGVO-Zertifikat

„Die Akkreditierung für das DSGVO-Zertifikat ist komplex. Es sind schon einige aus dem Akkreditierungsprozess ausgestiegen.“

Dr. Irene Karper, datenschutz cert GmbH

„Der größte Nutzen der DSGVO-Zertifikate dürfte bei Angeboten der Auftragsdatenverarbeitung liegen.“

Henry Krasemann, Unabhängiges Landeszentrum Datenschutz Schleswig-Holstein

Die 2018 in Kraft getretene Datenschutzgrundverordnung (DSGVO) schafft ein europaweit einheitliches Datenschutzniveau. In der DSGVO ist auch deren Zertifizierung geregelt. Die Zertifizierung dient dem Nachweis, dass die Verordnung von den zertifizierten Unternehmen bzw. Auftragsdatenverarbeitern eingehalten wird. Die besonderen Bedürfnisse von Kleinstunternehmern sowie kleinen und mittleren Unternehmen sollen dabei berücksichtigt werden (Art. 42 Abs.1 DSGVO). Aufgrund der technischen Komplexität ist derzeit noch keine Zertifizierungsstelle für den Bereich der DSGVO in Europa akkreditiert. Kurzfristig rechnen Experten mit circa 15 bis 20 akkreditierten Konformitätsbewertungsprogrammen in Deutschland und entsprechend mehr akkreditierten Zertifizierungsstellen.

Grundsätzlich ist das DSGVO-Zertifikat freiwillig, hat jedoch neben Marketingzwecken noch weitere Vorteile. Beispielsweise erfordert die Übermittlung personenbezogener Daten an ein Drittland oder eine internationale Organisation die Gewährleistung des Schutzniveaus. Dieses kann u. a. durch die Zertifizierung nachgewiesen werden (Art. 44 DSGVO). Gemäß Art. 83 Abs. 2 lit. j). DSGVO reduziert durch eine erfolgreiche DSGVO-Zertifizierung das Risiko eines Bußgeldes in der Praxis fast auf null, denn die Kriterien und das konkrete Zertifikat werden durch die Aufsichtsbehörde in jedem Einzelfall genehmigt. Da Cloud Computing nach Artikel 28 der DSGVO als Auftragsverarbeitung eingestuft wird, können Datenschutz-Zertifikate dabei helfen, den rechtlichen Rahmen für die Cloud-Nutzung zu setzen. In der Studie Cloud Security 2021 gaben bereits 87,9 % der befragten Unternehmen die Datenschutz-Zertifizierung nach DSGVO als wichtiges Kriterium im Bezug auf Cloud Services an[55]. Außerdem können gesetzliche Vorgaben die Zertifizierung nach der DSGVO verlangen, z. B. bei der ärztlichen Videosprechstunde (Anlage 31b BMV-Ä).

Fallbeispiel: DSGVO-Akkreditierung

Artikel 42 und 43 der Datenschutzgrundverordnung bestimmen Zertifizierung und Zuständigkeiten. In Deutschland übernimmt die Deutsche Akkreditierungsstelle (DAkkS) die Systemprüfung und die jeweilige bundesländerspezifische Datenschutzaufsichtsbehörde die Fachprüfung von Programm und Zertifizierungsstelle.

Die Systemprüfung des DAkkS erfolgt nach der DIN EN ISO/IEC Norm 17065 für Produkt-, Prozess- oder Dienstleistungs-zertifizierungsstellen und beinhaltet beispielsweise die Personalkompetenz und Einspruchsmöglichkeiten. Die Fachprüfung durch die zuständige Datenschutzaufsichtsbehörde bewertet die in dem Programm festgelegten Zertifizierungskriterien. Danach folgt die Akkreditierung der Zertifizierungsstelle für das akkreditierte Programm.

Bisher wurde noch kein Programm und keine Zertifizierungsstelle akkreditiert. Die Ausgabe und die Werbung mit Siegeln, Gütezeichen oder Zertifikaten, die eine Konformität mit der DSGVO bestätigen, ohne dass eine staatliche Akkreditierung besteht, ist verboten und kann nach § 3 Abs. 2 AkkStelleG untersagt werden. Damit ist die Werbung mit Konformitätsaussagen zur DSGVO unzulässig.

Antragsphase Programmprüfung

Programmprüfung

Die System-Programmprüfung wird von der DAkkS durchgeführt und die Fach-Programmprüfung von der zuständigen Datenschutzaufsichtsbehörde.

Antragsphase Akkreditierung

Akkreditierungsphase

Dokumentenprüfung und Begehung der Zertifizierungsstelle durch Fachbegutachter der Datenschutzbehörde und Systembegutachter der DAkkS + sog. Witnessbegutachtung beim Kunden der Zertifizierungsstelle müssen erfolgreich durchlaufen werden.

Akkreditierung

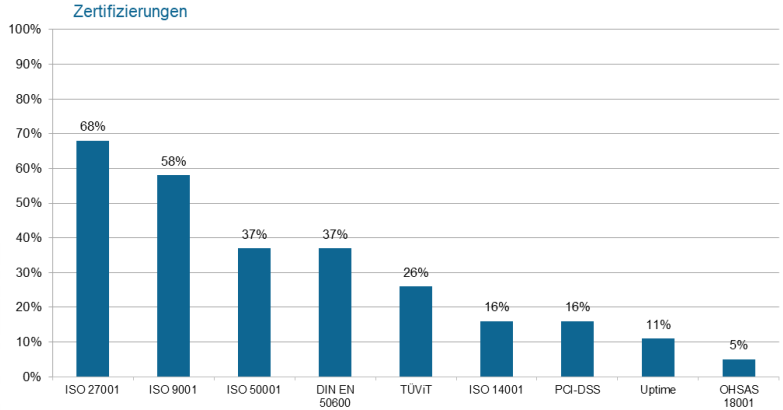
Überwachungsphase

Die Anzahl der Wiederholungsbegutachtungen wird nach einem risikobasierten Ansatz der DAkkS festgelegt, in der Regeln alle 12 Monate. Die Akkreditierung ist auf längstens fünf Jahre befristet.

Quelle: WIK Recherche. Eigene, vereinfachte Darstellung des Akkreditierungsprozesses nach der Datenschutzkonferenz (DSK): https://www.datenschutzkonferenz-online.de/media/oh/20190315_oh_akk_c.pdf

Fallbeispiel: Rechenzentren

Abbildung 16: Genutzte Zertifikate von Rechenzentrum-Betreibern



Quelle: GDA & PwC (2020): Data Center Outlook 2021

Der Begriff Rechenzentrum wird im Sicherheitskontext an der Funktionalität und nicht an der Ausführungsform oder Größe ausgerichtet. Es wird im Bereich der Informationssicherheit und Zertifizierung nicht zwischen Rechenzentrum und Serverraum unterschieden.[56] Die Informationssicherheit in Rechenzentren erfordert neben der IT-Sicherheit und dem Datenschutz auch physische Sicherheitsmaßnahmen, die z. B. vor unbefugtem Zutritt und Datendiebstahl oder Ausfälle durch Hochwasser schützen. RZ-Betreiber nutzen hauptsächlich neun verschiedene Zertifikate (Abb. 16).

Die Verfügbarkeit von Rechenzentren ist aufgrund der darauf aufbauenden Geschäftsmodelle der Kunden besonders relevant. Es hat sich eine Klassifizierung von Rechenzentren in verschiedene Verfügbarkeitsklassen etabliert. In Deutschland unterscheidet der Trusted Site Infrastructure (TSI) seit 2001 vier Verfügbarkeitsklassen und das Data Center Star Audit vergibt bis zu fünf Sterne.

Die 2014 in Kraft getretene Norm DIN EN 50600 beschreibt Anforderungen an die physische Sicherheit von Rechenzentrum und unterscheidet dabei vier Verfügbarkeitsklassen. Die Zertifizierungsstellen erstellen eigene Prüfkataloge. Diese unterscheiden sich, sodass auch die Einteilung in die Verfügbarkeitsklassen nach DIN EN 50600 zwischen verschiedenen Zertifizierungsstellen nicht zwangsläufig übertragbar ist. Die Klasseneinteilung der Zertifikate ist dadurch ohne genaue Kenntnisse der Prüfkataloge nicht eindeutig.

Fallbeispiel: Doctolib

TÜV geprüfter Datenschutz
TÜV Saarland
Bereich: Datenschutz

internet privacy standards (ips)
datenschutz cert GmbH
Bereich: Datenschutz

HDS-Zertifizierung (Health Data Hosting)
„Agence du Numérique en Santé“ (ANS)
Bereich: Datenschutz

Cybersecurity Rating Certificate
CYRATING
Bereich: IT-Sicherheit

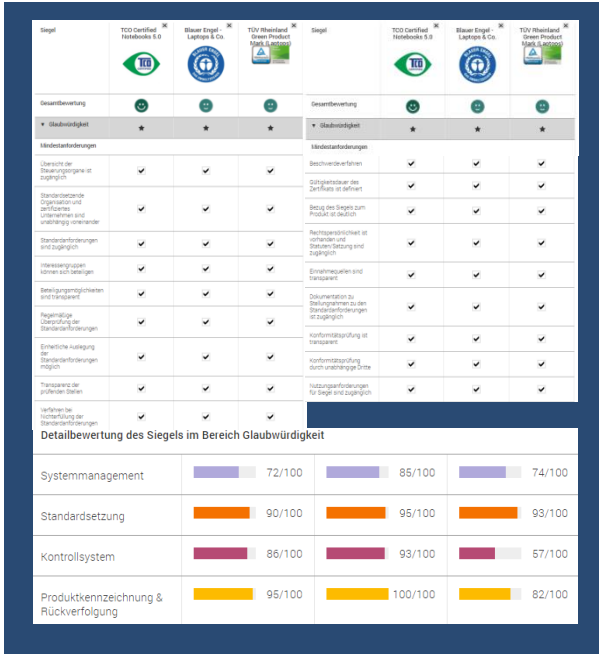
Die 2013 gegründete französische Doctolib GmbH bietet eine Software für das Termin- und Patientenmanagement von Arztpraxen und Kliniken an. Seit 2016 ist das Angebot in Deutschland verfügbar und wird nach Unternehmensangaben von circa 12.000 Ärzten und Ärztinnen in Deutschland genutzt. Unter anderem organisierte Doctolib die Vergabe der Corona-Impftermine des Landes Berlin.

Die Terminvereinbarung einer Person bei einem Arzt gehört zu den personenbezogenen Gesundheitsdaten (Art. 4 Abs. 14 DSGVO) für deren Verarbeitung es konkrete Vorgaben gibt. Für Videosprechstunden besteht darüber hinaus eine gesetzliche Pflicht zur Zertifizierung. Anbieter müssen nachweisen, dass ihre Dienste die Anforderungen an Vertraulichkeit, Integrität und Verfügbarkeit der personenbezogenen Daten erfüllt (§ 365 Abs. 1 SGB V). Doctolib benutzt mehrere Zertifikate, um einen hohen Datenschutz und IT-Sicherheit nachzuweisen.

Doctolib stand mehrmals wegen seines Umgangs mit dem Datenschutz in der Kritik. Unter anderem gab Doctolib Daten (u. a. Suchbegriffe von Nutzenden) an Facebook und Outbrain weiter, hat dies aber nach der Kritik gestoppt. Das Terminvermittlungsportal von Doctolib wurde im Juni 2021 mit dem BigBrotherAward in der Kategorie „Gesundheit“ ausgezeichnet. Sie kritisierten u. a., dass es den Zertifikaten wegen fehlender Transparenz und Vergleichbarkeit an Glaub- und Vertrauenswürdigkeit fehle.[57]

Fallbeispiel: Vergleichsportale

Abbildung 17: Möglichkeit zum Vergleich von Siegeln einer Produktgruppe auf www.siegelklarheit.de



Quelle: Siegelklarheit.de: Screenshot

Es gibt verschiedene unabhängige Vergleichsportale, um Siegel und Zertifikate mit ihren Produkteigenschaften und Zertifizierungssystemen sichtbar zu machen. Beispiele für vergleichende Portale für Zertifikate und Siegel gibt es von:

- Deutsche Gesellschaft für Internationale Zusammenarbeit (GIZ), um die Umsetzung hoher Umwelt- und Sozialstandards voranzutreiben[58]
- Die VERBRAUCHER INITIATIVE e. V., um über ökologische, soziale, Gesundheits-, Regional- und Seniorenlabels zu informieren[59]
- Bundesministerium für Wirtschaft und Energie (BMWi), um über Erfahrungen und Anforderungen von Cloud-Anbietern und Cloud-Anwendern zu informieren[60]
- ENISA, um über die Sicherheit und Zuverlässigkeit von Cloud-Diensten zu informieren (bis 2019)[61]

Verbrauchersiegel vergleicht zum Beispiel das Portal Siegelklarheit (Abb. 17). Ein entsprechendes Portal für KMU zum Thema Informationssicherheit könnte Suchkosten für KMU vermindern, dem Prinzipal-Agent-Problem entgegenwirken sowie die Glaubwürdigkeit von (geeigneten) Siegeln und Zertifikaten erhöhen.

Alternativen zu Zertifikaten und Siegeln

> *„Akkreditierung und Siegel sind zu weich. Das bringt kein Vertrauen. Stärkere gesetzliche Vorgaben und Mindeststandards sind erforderlich.“*
>
> Martin Schaletzky, Softline Group AG

Neben Siegeln und Zertifikaten gibt es weitere Möglichkeiten, Vertrauen in IT-Sicherheit aufzubauen:

Sicherheitsvorschriften und Regulierungen: Hoheitliche Stellen können IT-Schutzmaßnahmen gesetzlich vorschreiben und dabei auf bereits bestehende Sicherheitslücken eingehen.

Produkthaftung und indirekte Vermittlerhaftung: Haftung zwingt Hersteller und Dienstleister, notwendige IT-Sicherheitsvorkehrungen zu treffen. Kritiker der Produkthaftung weisen auf Hemmnisse in Hinblick auf die Innovationsgeschwindigkeit hin. Zudem ist abzuwägen, wann die Haftung eintritt.[49]

Transparente Daten-Ökosysteme: GAIA-X oder ähnliche offene Dateninfrastrukturen können durch ihre Struktur Vertrauen schaffen.

(Freiwillige) Offenlegung von Informationen: Das freiwillige Aufdecken von Vorfällen und Schwachstellen (z. B. als Vorbildfunktion) oder Druck von außen (z. B. zivilgesellschaftliche Gruppen) kann Unternehmen dazu motivieren, frühzeitig transparent zu handeln.[50]

Cyberversicherung: Durch Versicherungen gegen Schäden durch Cyber-Sicherheitsvorfälle werden mit günstigen Prämien Anreize für Organisationen geschaffen, angemessene Vorsichtsmaßnahmen zu treffen. Versicherungsgesellschaften belohnen dabei Investitionen in die Sicherheit.[51]

Reputationssysteme: Veröffentlichte Bewertungen durch Kunden bestätigen, dass Normen und Standards implementiert wurden. Unternehmen können selbst öffentlich erklären, dass sie Normen und Standards einhalten. Zertifizierung ist keine Pflicht.[52]

Fallbeispiel: GAIA-X

Das europäische Projekt GAIA-X hat das Ziel, eine leistungs- und wettbewerbsfähige, sichere und vertrauenswürdige Dateninfrastruktur für Europa aufzubauen. Eine Dateninfrastruktur ermöglicht den Zugang, die Speicherung, den Austausch und Nutzung von Daten gemäß vordefinierter Regeln.[53] GAIA-X kann als weitere Alternative zu vorhandenen Gütezeichen gelten, um Vertrauen zu schaffen.

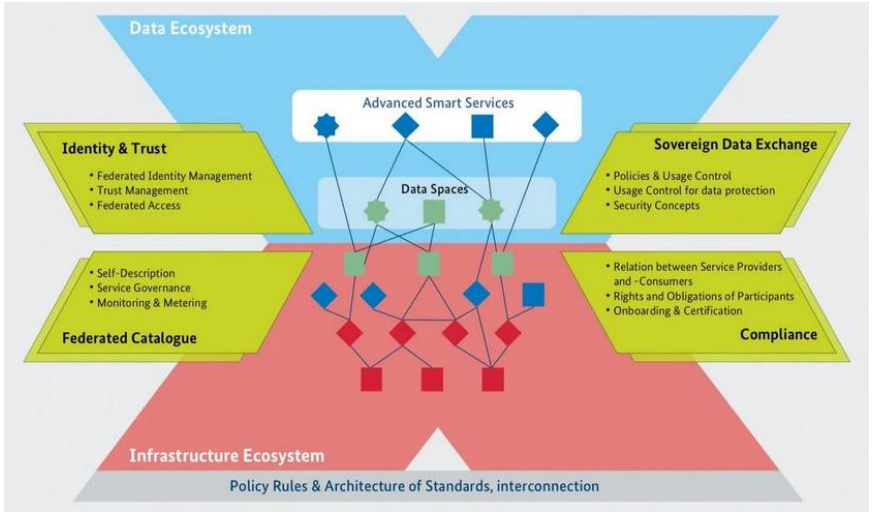
Die Architektur folgt dem Prinzip der Dezentralisierung. GAIA-X ist ein Ökosystem aus einer Vielzahl von Plattformen, die dem gemeinsamen GAIA-X-Standard folgen (Abb. 15). Jeder Akteur, der den Kompatibilitätsnachweis erbringt, wird Teil von GAIA-X. Dadurch soll Vertrauen geschaffen werden und besonders KMUs ermöglicht werden, Daten zu speichern und zur (Weiter-) Verwendung zur Verfügung zu stellen, ohne ihre Datensouveränität zu verlieren.

Laut Experten werden die ersten über GAIA-X angebotenen Services voraussichtlich 2022 starten. Der Mobilitätssektor ist Vorreiter.

„Wenn KMU in Produktionsketten mit Großunternehmen eingebunden sind, müssen sie zwangsläufig ihre Daten teilen. Viele KMU haben damit aber schlechte Erfahrungen gemacht, da diese Kenntnisse von den Konzernen oft auch z. B. für Preisverhandlungen genutzt werden. Daher ist ein wesentlicher Aspekt für eine offene Kooperation das Vertrauen zwischen den Partnern. Dieses entsteht aber nur, wenn es Transparenz über die Datennutzung gibt und Sanktionsmöglichkeiten bestehen.“

Matthias Brucke, Gründer und Gesellschafter der embeteco GmbH & Co. KG

Abbildung 15: Überblick über die verschiedenen Rollen und das Zusammenspiel mit den GAIA-X-Komponenten und den föderierten Diensten



Bildquelle: BMWi (2020): GAIA-X: Das europäische Projekt startet in die nächste Phase

Fallbeispiel: GAIA-X

„GAIA-X ist ein Kompatibilitätsnachweis. Das ist kein Zertifikat, sondern mehr als das. Jeder im Federated Service Catalogue angebotene Service erfüllt die Kriterien von GAIA-X. Das trägt zu mehr Wettbewerb bei.“

Keran Sivalingam, Deutsches Forschungszentrum für Künstliche Intelligenz

Die Rahmenbedingungen von GAIA-X wurden nach den Prinzipien Offenheit, Transparenz und Vertrauen gestaltet. Folgende Faktoren sollen eine vertrauensvolle Dateninfrastruktur schaffen:

Staatliche Akteure und Marktakteure
Der kooperative Ansatz mit der Beteiligung staatlicher Akteure stärkt Vertrauen. Die Federated Services werden von der Gaia-X Association for Data and Cloud (AISBL) beauftragt.

Offene Standards
Die Federated Services sind offene Standards und als Open-Source-Code für alle einsehbar.

Registrierung
Jede rechtliche Einheit muss sich für die Nutzung bei der Gaia-X Association for Data and Cloud (AISBL) registrieren. Dadurch entsteht Transparenz in Bezug auf die Nutzenden bei GAIA-X.

Vertragliche Absicherung: Dienstgütevertrag
Ein durchsetzbarer rechtlicher Rahmen reduziert das Ungleichgewicht zwischen KMU und großen Unternehmen.

Datensouveränität
Die Datenhoheit behält der Bereitsteller. Es ist jederzeit bekannt, wer wie auf Daten zugreift.

Quelle: WIK Recherche, Experteninterviews

GAIA-X Label

GAIA-X[54] nutzt Labels („Siegel“), um ein gemeinsames Level an Datenschutz, Transparenz, Sicherheit, Portabilität und Flexibilität sowie europäischer Kontrolle zu gewährleisten. Die GAIA-X Compliance und Label Rahmenbedingungen definieren standardmäßig drei Gruppen von Konformitätskriterien, die als GAIA-X Basic Label bezeichnet werden können. Darüber hinaus können externe Akteure (z. B. Regierungen, Unternehmen, Normungsorganisationen) eigene bereichsspezifische Labels definieren. Dabei soll GAIA-X sicherstellen, dass jedes Label Mindestanforderungen an Kompatibilität für jeden Service erfüllt. Für die Entwicklung und Umsetzung von GAIA-X Labels sind zwei wesentliche Rollen definiert:

- **Label-Eigentümer**: Diese Akteure initiieren bereichsspezifische Label. Sie bestimmen den Namen des Labels sowie einen Anforderungskatalog. Der Label-Eigentümer beauftragt die GAIA-X Association mit der Entwicklung und Vergabe des Labels und benötigt deren formale Zustimmung.
- **Label-Aussteller**: Diese Einrichtungen werden von der GAIA-X Association mit der Implementierung und Vergabe eines Labels beauftragt. Dafür wird der Anforderungskatalog in jeweils überprüfbare Voraussetzungen unterteilt. Diese werden dann in den GAIA-X Label und Compliance Rahmenbedingungen zur Verifizierung kodiert.

Prinzipen der GAIA-X Labels:

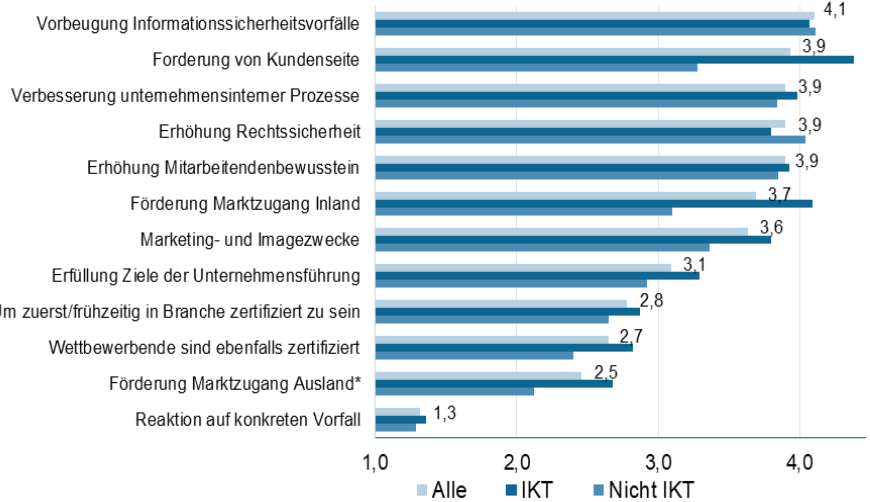
- Kein pauschales, anbieterweites Label
- Keine Kontrolle von Anbietern
- Föderation der Verifizierung
- Gemeinsame Rahmenbedingungen für die Konformität
- Kompatibilität
- Skalierbarkeit

Inhalt

- Ausgangslage
- Elemente einer Qualitätsinfrastruktur
- Empirische Analyse
- Fallbeispiele
- Schlussfolgerungen
- Handlungsempfehlungen

Warum werden Gütezeichen genutzt?

Abbildung 18: Motive zur Anwendung von ISO/IEC 27001



Quelle: Mirtsch, M. et al (2020): Die Nutzung und Wirkung der Norm ISO/IEC 27001 für Informationssicherheit in Unternehmen in Deutschland, S. 16 (IKT: Unternehmen, die zur Informations- und Kommunikationstechnik-Branche gehören)

Differenzierung im Wettbewerb

Mit einem Gütezeichen sind Unternehmen in der Lage, das Vertrauen von Kunden zu gewinnen. Es bestätigt, dass die Organisation ein angemessenes Sicherheitsniveau erreicht hat und aufrecht erhält und somit Zuverlässigkeit beweist. Ein Unternehmen hebt sich dadurch von Wettbewerbern ab. Zertifikate bilden ein Mittel zur Reduktion von Komplexität sowie Informationsasymmetrien und damit Entscheidungsunsicherheiten potenzieller Kunden.

Interne Beweggründe im Unternehmen

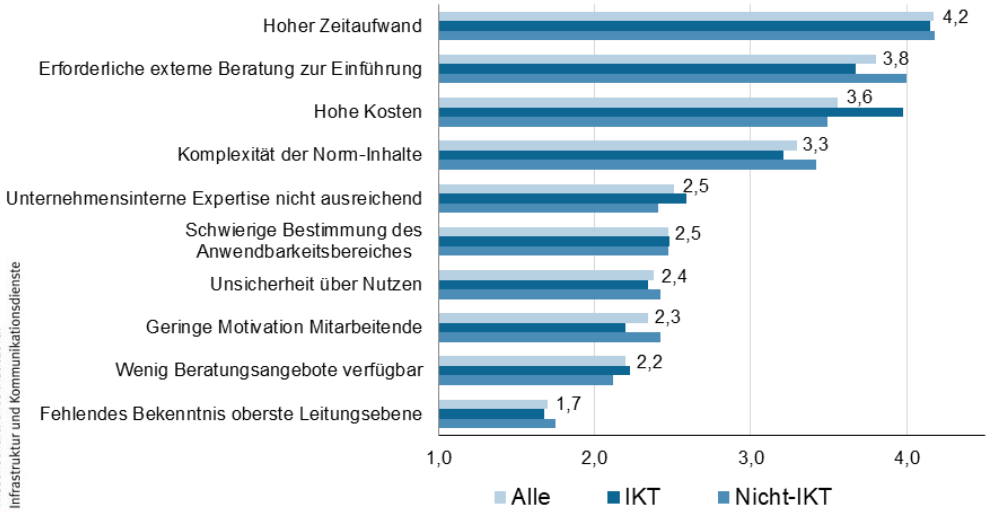
Dazu gehört die präventive Erkennung von Schwachstellen, um mögliche Kosten durch IT-Sicherheitsvorfälle zu reduzieren (Abb. 18). Der Aufbau eines Qualitätsmanagements mit Zertifizierung erleichtert zudem den Nachweis der Erfüllung entsprechender Sorgfaltspflichten bei eventuell anfallenden Routineprüfungen oder nach Vorfällen (z. B. Schadensersatzhaftung wegen Sorgfaltspflichtverstoß nach DSGVO).

Externe Vorschriften

Externe Vorschriften, die Treiber für Zertifizierungen sind, können entweder gesetzliche Anforderungen sein (bspw. DSGVO, KRITIS-Unternehmen) oder von Kunden und Auftraggebern bzw. innerhalb einer Lieferkette gestellt werden. Zum Beispiel in der Automobilindustrie sorgen Hersteller so für ein gleichbleibendes Qualitätsniveau.[62]

Warum werden Gütezeichen nicht häufiger genutzt?

Abbildung 19: Schwierigkeiten bei der Implementierung und Zertifizierung der ISO/IEC 27001



Quelle: Mirtsch, M. et al (2020) ebd., S. 21

Die größte Hürden (Abb. 19) stellen oftmals der

- Zeitaufwand,
- Beratungen,
- Kosten und
- Komplexität für KMU dar.[63]

Ob ein Dienstleister oder Produktanbieter bereit ist, die Kosten für eine Zertifizierung zu zahlen, hängt letztendlich davon ab, ob seine Kunden bereit sind, die auf sie umgelegten Kosten zu zahlen. KMU nennen die Erhöhung von Kosten als eines der zentralen Hemmnisse.[64] Viele IT-Dienstleister sind überzeugt, dass KMU ohnehin zu wenig Budget für Sicherheit einplanen. Investitionen in Zertifizierungen erscheinen erst recht nicht rentabel,[65] wie in Studien belegt ist.[66] [67] Der hohe Aufwand können außerdem dazu führen, dass Entwickler keine Software-Updates durchführen, für die eine neue Zertifizierung notwendig wäre.[68]

Es ist oftmals kaum ersichtlich, welche Qualitätsversprechen hinter einzelnen Siegeln und Zertifikaten stehen. Über die Hälfte der KMU gibt in einer Umfrage an, dass der unverständliche Umfang oder die unklare Bedeutung ein Hemmnis sind. KMU werden durch neue Gütezeichen auch mit neuen Informationsasymmetrien konfrontiert.[69]

Schlussfolgerungen

Zertifikat / Zertifizierung

„Zertifizierung […] ist die Feststellung durch eine Zertifizierungsstelle, dass ein Produkt, ein Prozess, ein System, ein Schutzprofil […], eine Person […] oder ein IT-Sicherheitsdienstleister bestimmte Anforderungen erfüllt.“[70]

Gütezeichen / -siegel

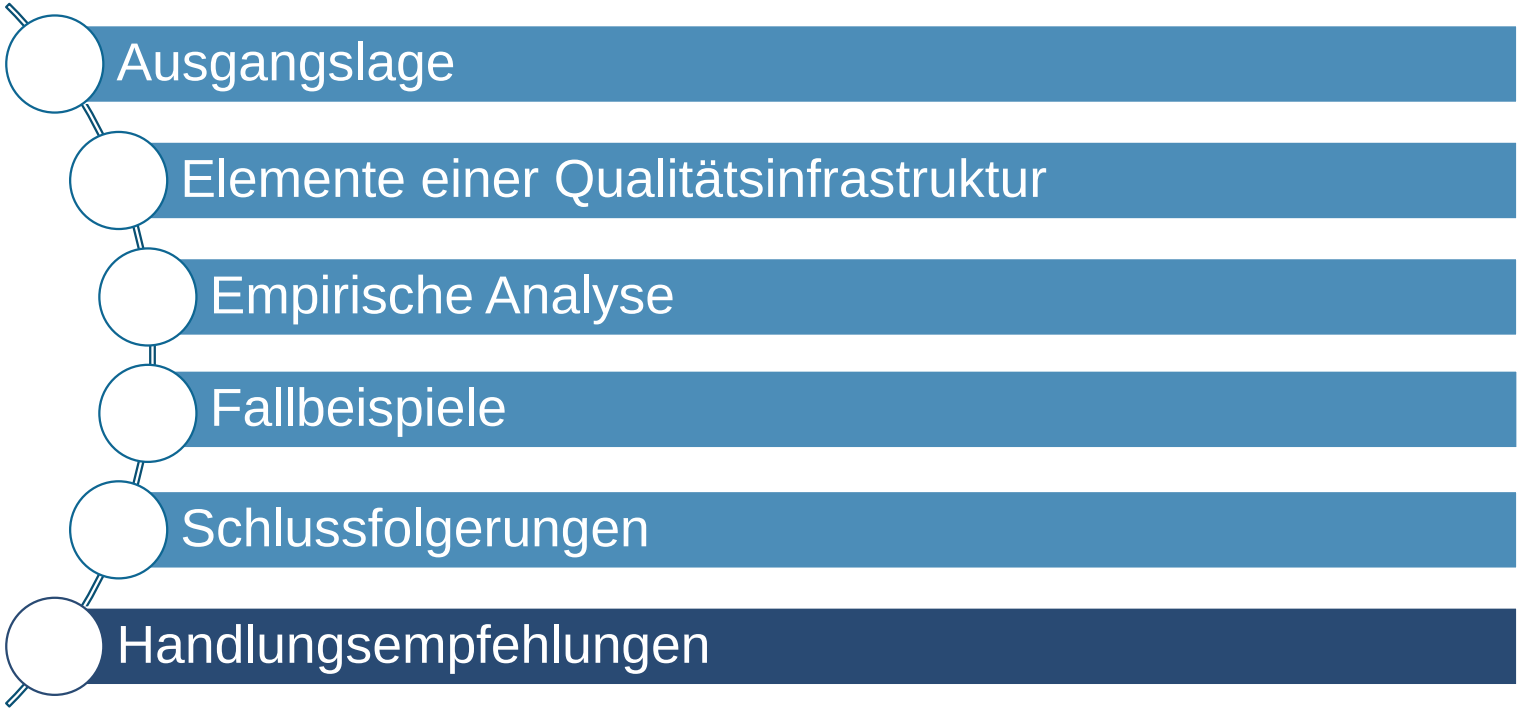
„Grafische oder schriftliche Kennzeichnung von Angeboten, die dem Verbraucher eine bestimmte Güte und Qualität signalisieren“.[71]

Siegel und Zertifikate beschreiben Kennzeichnungen, die die Einhaltung festgelegter Kriterien beglaubigen. Die Kriterien sollten aus anerkannten Standards oder Normen abgeleitet werden. Sie sollen von anerkannten (= akkreditierten) Institutionen nur an die Hersteller und Dienstleister vergeben werden, die die Einhaltung von Prüfbestimmungen zu den Kriterien erfüllen. Siegel und Zertifikate bieten keine Gewährleistung dafür, dass die Schutzziele der Informationssicherheit gegenwärtig und künftig auch gewährleistet sind. Sie garantieren nur, dass zum Prüfungszeitpunkt Konformität zu den Prüfkriterien besteht, die den Siegeln und Zertifikaten zugrunde liegen.

Weder Eigenschaften noch Vergabemechanismen sind für Gütezeichen im Bereich Informationssicherheit gesetzlich geregelt. Siegel, die mit aufwendigen, vertrauensvollen Zertifizierungen erlangt werden, stehen neben Siegeln mit geringer oder wenig relevanter Aussagekraft. In der Regel zahlt das antragstellende Unternehmen die Zertifizierung, so dass Interessenskonflikte entstehen können (Principal-Agent-Theory). Konkurrenzdruck unter Zertifizierungsstellen könnte einen Anreiz schaffen, niederschwellige Kriterien mit weniger Prüfungsumfang anzubieten und mit niedrigeren Preisen mehr Kunden zu gewinnen.

So kann für unsichere Anbieter und Dienstleister die Versuchung entstehen, Siegel und Zertifikate mit geringer Aussagekraft und weniger strengen Prüfkriterien zu erwerben, da ihre Kunden wiederum ohnehin kaum zwischen diesen und hochwertigen Siegel und Zertifikaten unterscheiden können und diese nicht durch das Zahlen höherer Preise honorieren.[72]

Inhalt


Ausgangslage
Elemente einer Qualitätsinfrastruktur
Empirische Analyse
Fallbeispiele
Schlussfolgerungen
Handlungsempfehlungen

Handlungsempfehlungen

Um den gezeigten Hürden für KMU entgegenzuwirken, sind Maßnahmen notwendig, die Siegel und Zertifikate bekannter machen, über Inhalte informieren und dabei unterstützen, rationale Entscheidungen treffen zu können. Mögliche Handlungsoptionen umfassen die folgenden Punkte:

- Bereitstellung von Informationsmaterial durch geeignete, unabhängige Stellen zum Thema Siegel und Zertifizierung:
  - Informationen für Unternehmen, die sich zertifizieren lassen möchten
  - Informationen für Unternehmen, die verwendete Siegel und Zertifikate einordnen möchten
- Vorhandene Strukturen verwenden (z. B. Mittelstand-Digital), um Entscheidungshilfen zur Verfügung zu stellen.
- Teilnahme an Förderprogrammen mit dem Einsatz von zertifizierten Dienstleistungen und Produkten verbinden. Verwendung von Siegeln und Zertifikaten bei Förderprogrammen wie go-digital. Verwendung von Vouchern prüfen.
- Informations- und Vergleichsportal (vgl. Trusted Cloud) speziell für IT- und IT-Sicherheits-Gütezeichen.
- Gütezeichen untersuchen in Hinblick auf ihre Eignung für KMU. Gegebenenfalls KMU-Gütezeichen etablieren.

Zusammenfassung im WIK-Schlaglicht

Wir haben unsere Studienergebnissen in praktische Hilfestellungen zusammengefasst, mit denen sich kleine und mittlere Unternehmen selbstständig oder mit Unterstützung weiter auseinandersetzen können. Dafür wurden Handlungsempfehlungen aus den wichtigsten Ergebnissen abgeleitet. Das WIK-Schlaglicht kann hier abgerufen werden:
WIK-Studie_Schlaglicht_Vertrauen_in_Datenverarbeitung_2021.pdf

Vielen Dank an die Expertinnen und Experten der Interviews

- Jörg Asma, PwC PricewaterhouseCoopers GmbH Wirtschaftsprüfungsgesellschaft
- Sandra Balz, Transferstelle IT-Sicherheit im MIttelstand (TiSIM), Deutschland sicher im Netz e.V. (DsiN)
- Matthias Brucke, embeteco GmbH & Co. KG
- Alexandra Horn, DIN Deutsches Institut für Normung e. V.
- Richard Huber, Fraunhofer-Institut für Offene Kommunikationssysteme FOKUS
- Dr. Irene Karper, datenschutz cert GmbH und stellv. Vorsitzende des Gütesiegelboards der Initiative D21
- Dr. Silvia Knittl, PwC PricewaterhouseCoopers GmbH Wirtschaftsprüfungsgesellschaft
- Henry Krasemann, Unabhängiges Landeszentrum Datenschutz Schleswig-Holstein
- Sebastian Meissner, EuroPriSe GmbH
- Nadja Menz, Fraunhofer-Institut für Offene Kommunikationssysteme FOKUS
- Georg Molinari, Deutsche Akkreditierungsstelle GmbH (DAkkS)
- Martin Schaletzky, Softline Group AG
- Stephan Schwichtenberg, Bundesverband IT-Mittelstand e. V. (BITMi)
- Keran Sivalingam, Deutsches Forschungszentrum für Künstliche Intelligenz (DFKI)
- Rolf Walter, TÜV Rheinland Consulting GmbH

Die Verantwortung für alle Inhalte liegt bei den Autoren.

Quellen:

[1] Gabler Wirtschaftslexikon: Revision von Vertrauen, unter: https://wirtschaftslexikon.gabler.de/definition/vertrauen-50461/version-384763 abgerufen am 10.11.2021
[2] Coester, U.; Pohlmann, N. (2021): Vertrauen – ein elementarer Aspekt der digitalen Zukunft, in: DuD – Datenschutz und Datensicherheit, Ausgabe 2/2021
[3] DAkkS (2016): Besondere Anforderungen und Festlegungen für die Akkreditierung von Zertifizierungsstellen für Produkte nach DIN EN ISO/IEC 17065:2012 für den Bereich der Schiffsausrüstungsrichtlinie, S. 3, gemäß DIN EN ISO/IEC 17000: Konformitätsbewertung – Begriffe und allgemeine Grundlagen
[4] Luhmann, N. (1968): Vertrauen
[5] Clases, C.; Wehner, T. (2020): Vertrauen, in: Lexikon der Psychologie, unter: https://www.spektrum.de/lexikon/psychologie/vertrauen/16374 abgerufen am 16.11.2021
[6] Akerlof, G. A. (1970): The Market for „Lemons“: Quality Uncertainty and the Market Mechanism, in: The Quarterly Journal of Economics, 84. Jg. (1970), Nr. 3, S. 488-500
[7] Hillebrand, A., Niederprüm, A., Thiele, S., Schäfer, S. (2017): Aktuelle Lage der IT-Sicherheit in KMU, WIK-Studie im Auftrag des BMWi, S. 44
[8] DsiN (2021): DsiN-Praxisreport 2020 Mittelstand@IT-Sicherheit
[9] Hillebrand, A., et al (2017): ebd.
[10] Köhler, C. et. al. (2021): IT-Dienstleister als Akteure zur Stärkung der IT-Sicherheit bei KMU in Deutschland – Abschlussbericht, S. 95 - 99
[11] Bahr, I. (2019): Datenschutz und Datensicherheit in kleinen und mittelständischen Unternehmen, Studie für Capterra
[12] KfW-Research (2021): KfW-Digitalisierungsbericht Mittelstand 2020 sowie KfW-Research (2019): Unternehmensbefragung - Digitalisierung, S. 9 – 14
[13] Kleinhans, J.-P. (2018): Standardisierung und Zertifizierung zur Stärkung der internationalen IT-Sicherheit, S. 8 f., Studie für Stiftung Neue Verantwortung e. V.
[14] Moore, T. (2010): The economics of cybersecurity: Principles and policy options, S. 106, in: International Journal of Critical Infrastructure Protection, Volume 3, Issues 3–4, December 2010, Pages 103-117
[15] Moore, T. (2010): ebd. S. 106 f.
[16] Bauer, J. M.; van Eeten, M. J. G. (2009): Cybersecurity:Stakeholderincentives,externalities, and policyoptions, S. 707-710 in: Telecommunications Policy, Volume 33, Issues 10–11, November–December 2009, Pages 706-719
[17] Moore, T. (2010): ebd. S. 105 f.
[18] Akerlof, G. A. (1970): ebd., S 488 – 500
[19] PwC (2021): Bio im Aufwind, PwC-Konsumentenbefragung zu Bio-Lebensmitteln und deren Kennzeichnung, Januar 2021
[20] Köhler, C. et. al. (2021): ebd. S. 122 f.
[21] Köhler, C. et. al. (2021): ebd. S. 54, 77, 86 f., 99
[22] Köhler, C. et. al. (2021): ebd. S. 56
[23] Klemeschov, A. et. al. (2014): IT-Dienstleister und IT-Sicherheit in KMU, S. 4, 15
[24] BMWi (2018): Gütesiegel und Zertifikate für IT-Sicherheit, S. 35 (unveröffentlicht)
[25] Köhler, C. et. al. (2021): ebd. S. 96, 118
[26] Köhler, C. et. al. (2021): ebd. S. 87, 99
[27] BMWi: Konformitätsbewertung und Akkreditierung, unter: https://www.bmwi.de/Redaktion/DE/Textsammlungen/Technologie/konformitaetsbewertung-und-akkreditierung.html abgerufen am 1.12.2021
[28] Gabler Wirtschaftslexikon: Norm, unter: https://wirtschaftslexikon.gabler.de/definition/norm-39791 abgerufen am 10.12.2021
[29] DIN: Finanzierung der Normungsarbeit, unter https://www.din.de/de/din-und-seine-partner/din-e-v/finanzierung abgerufen am 10.12.2021
[30] Europäische Union (2012): Verordnung (EU) Nr. 1025/2012 des Europäischen Parlaments und des Rates, in Amtsblatt der Europäischen Union
[31] Buhl, T, Schönhof, R. (2021): Wer sie gestaltet beherrscht den Markt: Normen und Standards, in „Fraunhofer-Positionspapier zu Normen und Standards“
[32] DIN: DIN in Europa, unter: https://www.din.de/de/din-und-seine-partner/din-in-der-welt/din-in-europa abgerufen am 10.12.2021
[33] DIN: Normenausschuss Informationstechnik und Anwendungen, unter https://www.din.de/de/mitwirken/normenausschuesse/nia abgerufen am 10.12.2021
[34] BSI (2021): Verfahrensbeschreibung zur Anerkennung von Prüfstellen und Zertifizierung von IT-Sicherheitsdienstleistern Version 3.9 vom 30.09.2021

Quellen:

[35] § 1 Abs.2 AkkStelleG
[36] § 9 Abs. 1 BSI-Gesetz
[37] Europäische Union (2008): VERORDNUNG (EG) Nr. 765/2008 des Europäischen Parlaments und des Rates, in Amtsblatt der Europäischen Union
[38] Deutscher Verband Unabhängiger Prüflaboratorien e. V. (2021): „Sonderstudie: Kosten der Akkreditierung“, unter https://vup.de/officeForm/mrkt/index.php abgerufen am 9.12.2021
[39] Deutscher Verband Unabhängiger Prüflaboratorien e. V. (2021) „Meldung: Akkreditierungskosten beeinflussen den Markt und schwächen KMU“, unter https://vup.de/artikel.html?typ=i&id=3523 abgerufen am 9.12.2021
[40] DQS: ISO 27001 ZERTIFIZIERUNG; unter https://www.dqs.de/de/audits/iso-27001/?gclid=EAIaIQobChMI-rqoxPqw9AIVTKqWCh0PEwFxEAAYASAAEgJEOfD_BwE, abgerufen am 24.11.2021
[41] ISO-Portal: ISO/IEC 27001 Informationssicherheit für Unternehmen, unter https://iso-portal.de/iso-27001/ abgerufen am 24.11.2021
[42] Rumpel, R. et. al. (2011): Zertifizierung von Informationssicherheit in Unternehmen – ein Überblick, Studie für BITKOM
[43] ConformityZert GmbH (2021): Zertifizierung Auditdauer und Preise, S. 5
[44] European Commision (2017): Proposal for a Regulation of the Eurpean Parliament and of the Council on ENISA, the "EU Cybersecurity Agency", and repealing Regulation (EU) 526/2013, and on Information and Communication Technology cybersecurity certification ("Cybersecurity Act"), S. 125 f.
[45] BMWi (2018): ebd. S. 34 f., 36 (unveröffentlicht)
[46] BMWi (2018): ebd. S. 34 f., 35 (unveröffentlicht)
[47] Grieger (2013) - Gütesiegel in Deutschland, S. 16 ff.
[48] DAkkS: Datenbank akkreditierter Stellen, unter https://www.dakks.de/de/akkreditierte-stellen-suche.html abgerufen am 04.11.2021
[49] Moore, T. (2010): ebd. S. 107 f., 110
[50] Moore, T. (2010): ebd. S. 108 f.
[51] Moore, T. (2010): ebd. S. 109
[52] ISO: MANAGEMENT SYSTEM STANDARDS, unter https://www.iso.org/management-system-standards.html abgerufen am 24.11.2021
[53] BMWi und BMBF (2019): Das Projekt GAIA-X – Eine vernetzte Dateninfrastruktur als Wiege eines vitalen, europäischen Ökosystems
[54] GAIA-X AISBL (2021): GAIA-X Labelling Framework
[55] Schonschek, O. (2021): Cloud Security 2021, S. 14
[56] BSI: Rechenzentrums-Definition, unter https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Informationen-und-Empfehlungen/Empfehlungen-nach-Angriffszielen/Hochverfuegbarkeit/Rechenzentren/Rechenzentren.html abgerufen am 1.12.2021
[57] Weichert, T. (2021): Arztterminvermittlung über Doctolib Datenschutz - Anspruch und Wirklichkeit, Studie für Netzwerk Datenschutzexpertise
[58] Deutsche Gesellschaft für Internationale Zusammenarbeit (GIZ): Siegelklarheit.de, unter www.siegelklarheit.de abgerufen am 10.12.2021
[59] VERBRAUCHER INITIATIVE e. V.: Label-Online, unter https://label-online.de/ abgerufen am 10.12.2021
[60] BMWi: Trusted Cloud, unter www.trusted-cloud.de abgerufen am 10.12.2021
[61] European Union Agency for Cybersecurity (ENISA): Cloud Computing Certification - CCSL and CCSM unter https://resilience.enisa.europa.eu/cloud-computing-certification abgerufen am 10.12.2021

Quellen:

[62] Rumpel, R. et. al. (2011): ebd., S. 5 ff.
[63] Mirtsch, M.; et al (2020): Die Nutzung und Wirkung der Norm ISO/IEC 27001 für Informationssicherheit in Unternehmen in Deutschland, S. 20 f.
[64] BMWi (2018): ebd. S. 36 (unveröffentlicht)
[65] Köhler, C. et. al. (2021): ebd. S. 82
[66] Mirtsch, M. et al (2020): ebd., S. 19
[67] Hsu et. al. (2016): The Impact of ISO 27001 Certification on Firm Performance
[68] Kleinhans, J.-P. (2018): ebd., S. 23 f.
[69] BMWi (2018): ebd. S. 36 (unveröffentlicht)
[70] § 2 Artikel 7 BSI-Gesetz
[71] Gabler Wirtschaftslexikon: Gütezeichen, unter https://wirtschaftslexikon.gabler.de/definition/guetezeichen-36775/version-260222 abgerufen am 17.11.2021
[72] Edelman, B. (2009): Adverse Selection in Online “Trust” Certifications and Search Results, in: Electronic Commerce Research and Applications Volume 10, Issue 1, January–February 2011, Pages 17-25

wik Wissenschaftliches Institut für Infrastruktur und Kommunikationsdienste

KONTAKT

Annette Hillebrand
Senior Consultant
stv. Abteilungsleiterin Smart City/Smart Region

WIK Wissenschaftliches Institut für Infrastruktur und Kommunikationsdienste GmbH
Postfach 2000
53588 Bad Honnef
Tel.: +49 2224-9225-0 /-53
Fax: +49 2224-9225-68
eMail: a.hillebrand@wik.org
www.wik.org