WIK – Schlaglicht

Dezember 2021

Vertrauen in Datenverarbeitung

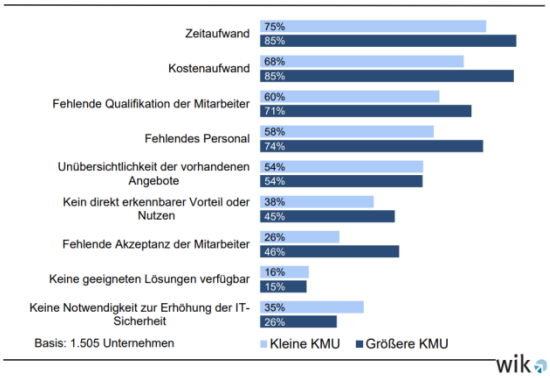
Dieses WIK-Schlaglicht basiert auf einer wissenschaftlichen Studie im Rahmen des Forschungsprogramms des Wissenschaftlichen Instituts für Infrastruktur und Kommunikationsdienste (WIK). Ziel der zugrundeliegenden Kurzstudie war die Identifikation von Faktoren, die Siegel und Zertifizierungen mit hohem Vertrauen ausmachen. Das Schlaglicht wendet sich speziell an kleine und mittelständische Unternehmen (KMU). Wir möchten unsere Studienergebnisse in praktische Hilfestellungen für KMU übertragen.

Autoren: Annette Hillebrand, Pirmin Puhl, Jana Stuck, Saskja Schäfer, WIK-Wissenschaftliches Institut für Infrastruktur und Kommunikationsdienste GmbH, Rhöndorfer Str. 68, 53604 Bad Honnef

Informationssicherheit in Deutschland

Kleinen und mittleren Unternehmen (KMU)* wird zunehmend bewusst, dass ihre Daten geschützt sein müssen. Viele KMU sind mit Entscheidungen darüber, welche Systeme für einen ausreichenden Schutz angeschafft werden, überfordert. Anforderungen an Datensicherheit und Datenschutz sowie Komplexität der Risikosituation in KMU und mangelnde Kenntnisse im Bereich IT-Sicherheit führen dazu, dass Entscheider bei Investitionen zurückhaltend sind (Abb. 1).[1] Sie achten bei der Auswahl darum eher auf Preis und Funktionalität.[2] Auf der anderen Seite fehlen durch die geringe Nachfrage Anreize für Hersteller und Anbieter, sichere Produkte und Dienstleistungen von sich aus anzubieten.[3]

Abbildung 1: Hemmnisse bei der Verbesserung der IT-Sicherheit aus Sicht der KMU



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)

Die Schwierigkeit besteht demnach für KMU darin, mit geringem Aufwand herauszufinden, welches der Angebote vertrauenswürdig ist und ihre IT-Risiken vermindert. Für Anbieter und Hersteller von Produkten und Dienstleistungen besteht die Herausforderung darin, sichtbar zu machen, dass ihre Produkte und Dienstleistungen dem gewünschten Sicherheitsniveau entsprechen (Abb. 2).

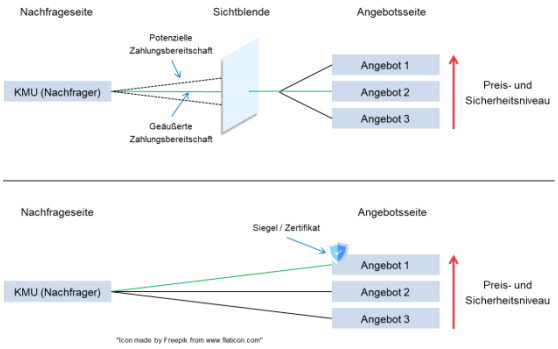
* Definition nach Institut für Mittelstandsforschung (IfM) Bonn, <500 MA, <50 Million Umsatzerlös/ Jahr

[1] KfW-Research (2021): KfW-Digitalisierungsbericht Mittelstand 2020 sowie KfW-Research (2019): Unternehmensbefragung - Digitalisierung, S. 9 – 14

[2] 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

[3] Kleinhans, J.-P. (2018): Standardisierung und Zertifizierung zur Stärkung der internationalen IT-Sicherheit, S. 8 f., Studie für Stiftung Neue Verantwortung e. V.

Abbildung 2: 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

Um Vertrauenswürdigkeit zu garantieren, haben sich in den vergangenen Jahrzehnten Siegel und Zertifikate etabliert. Unternehmen können den eigenen Betrieb zertifizieren, um dort sichere Datenverarbeitung zu gewährleisten und zusätzlich auch auf zertifizierte Anbieter oder Produkte vertrauen. Kunden sollen, ohne dass sie das Angebot im Detail kennen, mit Siegeln und Zertifikaten vermittelt bekommen, dass gewünschte (Sicherheits-)Anforderungen eingehalten werden.

Qualitätsinfrastruktur in Deutschland

Als Qualitätsinfrastruktur wird das Zusammenwirken aller Bestandteile bezeichnet, die für eine verlässliche Qualitätssicherung notwendig sind (Abb. 3). Dazu gehören die Normung und Standardisierung, die Akkreditierung, die Prüfdienstleistung (Audit) und die Zertifizierung. In diesem System werden von (inter-)nationalen Gremien mit Normen und Standards Sicherheitsanforderungen festlegt, deren Einhaltung durch unabhängige Prüfstellen (Auditoren) begutachtet und von Zertifizierungsstellen bescheinigt. Die Zertifizierungsstellen erbringen dabei zusätzlich einen Nachweis ihrer Kompetenz, wenn sie durch unabhängige Stellen akkreditiert wurden.

Abbildung 3: 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

Akkreditierte öffentliche sowie private gemeinnützige und gewinnorientierte Institutionen können Vertrauen durch Zertifizierungen generieren. Dabei sollten die Prüfbestimmungen auf anerkannten Normen und Standards beruhen und die Einhaltung durch unabhängige Auditoren geprüft werden. Es können auch Gütezeichen mit weniger strengen Standards und Vergaberegeln genutzt werden, wenn zum Bespiel gesetzliche Regelungen nichts anderes vorschreiben. Auf den ersten Blick ist oft nicht ersichtlich, welche Ansprüche an Gütezeichen bestehen und welche Qualitätsinfrastruktur dahintersteht.

Akkreditierung

Eine Akkreditierung „*ist die Bestätigung von unabhängiger dritter Seite, dass eine Konformitätsbewertungsstelle* [Anm. der Autoren: die Zertifizierungsstelle] *die (fachliche) Kompetenz zur Durchführung bestimmter Konformitätsbewertungstätigkeiten* [Anm. der Autoren: also zur Zertifizierung] *besitzt.*“[4] Es werden also die Prüfer darauf geprüft, ob sie selbst geeignet sind, eine Prüfung durchzuführen.

[4] BMWi: Akkreditierung, unter https://www.bmwi.de/Redaktion/DE/Artikel/Technologie/akkreditierung.html abgerufen am 14.12.2021

Prinzipiell ist eine Akkreditierung für das Ausstellen eines Siegels oder einer Zertifizierung nicht erforderlich. Sie erhöht allerdings das Vertrauen in die Zertifizierungsstelle und das Zertifikat. Ausnahmen gibt es, wenn eine Rechtsvorschrift die Akkreditierung der Bewertungsstelle anordnet, wie z. B. für die Datenschutzgrundverordnung (DSGVO).

Aktuell gibt es in Deutschland 24 akkreditierte Zertifizierungsstellen für Produkte, Prozesse und Dienstleistungen im Bereich Informationstechnik / Informationssicherheit / Cybersecurity und 54 akkreditierte Zertifizierungsstellen für Managementsysteme im Bereich Informationssicherheitsmanagementsysteme (ISMS) / Datenschutz.[5]

Zertifikate und Siegel

Im Rahmen unserer Studie wurden 49 Siegel und Zertifizierungen identifiziert, die sich dem Bereich Informationssicherheit widmen und für KMU potenziell relevant sind.

Die Ergebnisse zeigen, dass der Markt zahlreiche Normen und Standards bietet, auf denen Zertifizierungen aufbauen. Da nicht nur die Herausgeber der Siegel und Zertifikate, sondern auch Dritte Zertifizierung durchführen können, ist das Niveau der Zertifizierung immer im Zusammenhang mit dem Zertifizierungsprozess zu sehen und nicht nur im Zusammenhang mit dem Herausgeber.

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.

Es fallen hohe direkte und indirekte Kosten bei der Zertifizierung an, die auf die Kunden der zertifizierten Produkte und Dienstleistungen übertragen werden müssten. KMU als Nachfrager sind jedoch oftmals nicht bereit, diese Kosten für mehr IT-Sicherheit zu tragen. Es werden eher die kurzfristigen Kosten als der langfristige Nutzen für eigene interne Prozesse, Marketing oder Kundenakquise gesehen.

Die untersuchten Siegel und Zertifikate finden kaum breite Akzeptanz in KMU. (Grundlagen der) komplexen Prüfkriterien sind aus KMU-Sicht häufig intransparent. Inwieweit die Validierung der Kriterien durch unabhängige Dritte erfolgt, ist von Fall zu Fall unterschiedlich. Das BSI (Bundesamt für Sicherheit in der Informationstechnik) und der VdS GmbH (Tochter des Gesamtverbandes der Deutschen Versicherungswirtschaft (GDV) bieten zum Beispiel Lösungen für KMU an, die mit vergleichsweise geringerem Ressourceneinsatz helfen können, ein angemessenes Schutzniveau zu etablieren.

Warum werden Siegel und Zertifikate genutzt?

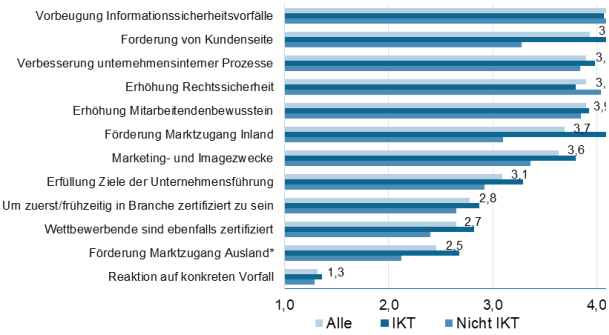
Mit einem Siegel bzw. Zertifikat können Unternehmen das Vertrauen von Kunden in ihre Produkte und Dienstleistungen stärken (Abb. 4). Es bestätigt, dass die Organisation ein angemessenes IT-Sicherheitsniveau erreicht hat und aufrecht erhält und somit Zuverlässigkeit beweist. Ein Unternehmen kann sich damit am Markt von Wettbewerbern abheben.

[5] DAkkS: Datenbank akkreditierter Stellen, unter https://www.dakks.de/de/akkreditierte-stellen-suche.html abgerufen am 04.11.2021

Auch interne Beweggründe können dazu führen, dass KMU Zertifizierungen durchlaufen. Schwachstellen werden frühzeitig erkannt und können Kosten durch IT-Sicherheitsvorfälle vorbeugen. Der Aufbau eines Qualitätsmanagements mit Zertifizierung erleichtert zudem den Nachweis der Erfüllung entsprechender Sorgfaltspflichten. Dies könnte nach Expertenmeinungen z. B. Schadensersatzhaftung wegen Sorgfaltspflichtverstoß nach DSGVO ausschließen.

Teilweise können auch externe Treiber für Zertifizierungen sorgen, indem gesetzliche Anforderungen (bspw. KRITIS) oder Anforderungen von Kunden und Auftraggebern z. B. innerhalb einer Lieferkette nach Zertifizierungen gestellt werden.

Abbildung 4: 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)

Warum werden Siegel und Zertifikate nicht häufiger genutzt?

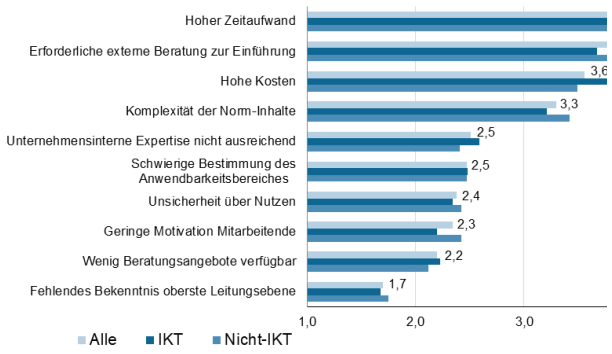
Zertifizierte Unternehmen nennen den Zeitaufwand, notwendige Beratungen, Kosten und Komplexität als größte Hürden, die sich ihnen während des Zertifizierungsprozesses stellten (Abb. 5).[6]

Ob Dienstleister oder Produktanbieter bereit sind, die Kosten für eine Zertifizierung auf sich zu nehmen, hängt letztendlich von der Bereitschaft der Kunden ab, höhere Preise zu bezahlen. Viele KMU verzichten darauf, entsprechende Qualitätsmerkmale zu erwerben, wenn sie die Kosten nicht überwälzen können.[7] Viele IT-Dienstleister sind überzeugt, dass KMU ohnehin zu wenig Budget für Sicherheit einplanen. Investitionen in Zertifizierungen erscheinen oft nicht rentabel.[8]

Für die Adressaten der Siegel und Zertifikate ist oftmals kaum ersichtlich, welche Qualitätsversprechen dahinter stehen. Über die Hälfte der KMU gibt in einer Umfrage an, dass der Umfang oder die unklare Bedeutung ein Hemmnis bei der Berücksichtigung sind. Verschiedene Siegel werden demnach gar nicht erst nachgefragt, da sie unverständlich wirken.[9]

[6] Mirtsch, M.; Blind, K. (2020): Die Nutzung und Wirkung der Norm ISO/IEC 27001 für Informationssicherheit in Unternehmen in Deutschland, S. 20 f.
[7] 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
[8] Köhler, C. et. al. (2021): IT-Dienstleister als Akteure zur Stärkung der IT-Sicherheit bei KMU in Deutschland – Abschlussbericht, S. 82
[9] BMWi (2018): Gütesiegel und Zertifikate für IT-Sicherheit, S. 36 (unveröffentlicht

Abbildung 5: Schwierigkeiten bei der Implementierung und Zertifizierung der ISO/IEC 27001



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

Definition

Siegel und Zertifikate beschreiben Gütezeichen, die die Einhaltung festgelegter Kriterien beglaubigen. Die Kriterien werden in der Regel aus Standards oder Normen abgeleitet. Sie sollten von anerkannten, also akkreditierten, Institutionen nur an diejenigen Hersteller und Dienstleister vergeben werden, die die Einhaltung von Prüfbestimmungen erfüllen.

Siegel und Zertifikate vermindern IT-Risiken und können im Haftungsfall hilfreich sein. Sie zeigen, dass zum Prüfungszeitpunkt die zugrunde liegenden Prüfkriterien erfüllt wurden.

Allerdings stehen Gütezeichen, die mit aufwändigen und kostenintensiven Zertifizierungen erlangt werden, neben Gütezeichen mit geringerer oder auf den ersten Blick nicht erkennbarer Aussagekraft. Ohne Recherche ist es oft nicht möglich zu erkennen, ob das Siegel oder Zertifikat den eigenen Ansprüchen eines KMU genügt.

Die Studie kann unter diesem Link kostenfrei eingesehen werden:

https://wik.org/fileadmin/Studien/2021/WIK-Studie_Vertrauen_in_Datenverarbeitung_2021.pdf

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

Impressum

WIK – Schlaglicht

Woran erkenne ich vertrauenswürdige Siegel und Zertifikate?

Weil für kleine und mittelständische Unternehmen viele Siegel und Zertifikate nicht verständlich hinsichtlich Umfang oder Bedeutung sind, möchten wir KMU abschließend Leitfragen mit an die Hand geben, die die Entscheidung für oder gegen Zertifikate und Siegel unterstützen können. So kann individuell überprüft werden, ob das Siegel bzw. Zertifikat für die eigenen Zwecke geeignet erscheint.

	Ja	Nein
Vermittelt das Siegel / Zertifikat das, was mir vom Anbieter oder Dienstleister signalisiert wird?	◯	◯

Informationen auf der Website der Zertifizierungsstelle zeigen, ob das Siegel / Zertifikat für die jeweiligen Kunden verständlich dargestellt wird. Dabei ist es auch wichtig zu prüfen, welchen Geltungsbereich das Siegel / Zertifikat abdeckt, also ob es tatsächlich für die Produkte und Dienstleistungen gilt, für die sich ein KMU interessiert. Bei Siegeln / Zertifikaten für Managementsysteme kann z. B. das ganze Unternehmen oder nur ein Teilbereich geprüft sein. Informationen darüber finden sich in der Regel auf der zugehörigen Urkunde oder in öffentlich zugänglichen Datenbanken der Zertifizierungsstellen.

Vermittelt das Siegel / Zertifikat das, was für mein KMU wichtig ist?	◯	◯

Siegel / Zertifikate belegen, dass zum Prüfungszeitpunkt die Prüfkriterien, die den Siegeln und Zertifikaten zugrunde liegen, erfüllt wurden. Darum sollte überlegt werden, welche Daten, Anwendungen und Bereiche unerlässlich sind und ob diese vom verwendeten Siegel / Zertifikat abdeckt wird.

Ist die Zertifizierungsstelle akkreditiert?	◯	◯

Mit einer Akkreditierung wird von einer unabhängigen, vertrauenswürdigen Stelle bestätigt, dass Zertifizierungsstellen ihre Tätigkeiten nach international gültigen Maßstäben kompetent erbringen.

Ist die Prüfstelle (Auditor) von der Zertifizierungsstelle unabhängig?	◯	◯

Die Einhaltung der Prüfkriterien unterliegt der Kontrolle unabhängiger Dritter, um Interes-

senskonflikte zwischen Zertifizierungsstelle und Antragsteller zu vermeiden.

Erfolgt die Zertifizierung auf Basis von anerkannten Normen und Standards?

(Inter-)Nationale Normen und Standards werden im Konsens verschiedenster Akteuren in den Gremien definiert. In der Regel besteht die Möglichkeit diese Normen und Standards einzusehen. Wenn Zertifizierungsstellen eigene Richtlinien definieren, ist zu überlegen, inwiefern sie sich von bestehenden Normen und Standards unterscheiden.

Sind die Prüfkriterien offen einsehbar?

Anhand der Prüfkriterien kann nachvollzogen werden, wie die Vergabe des Siegels / Zertifikats erfolgt. Einsehbare bzw. offen kommunizierte Prüfkriterien machen nachvollziehbar, auf was bei der Vergabe des Siegels / Zertifikats geachtet wurde.

Hat das Siegel / die Zertifizierung eine begrenzte Gültigkeit?

Über Jahre kann technologischer Wandel Normen und Standards - und damit Prüfkriterien - ihre Relevanz beeinflussen. Siegel und Zertifikate haben manchmal nur eine begrenzte Laufzeit, um dem stets Rechnung tragen zu können.

Sind bei einer längerfristigen Gültigkeitsdauer zwischenzeitliche Check-ups notwendig?

Durch regelmäßige Check-ups kann sichergestellt werden, dass die Prüfungskriterien dauerhaft eingehalten werden.

Finde ich öffentliche Informationen zum Siegel / Zertifikat?

Datenbanken der Zertifizierungsstelle mit Unternehmen oder Produkten, die mit dem Siegel / Zertifikat ausgezeichnet wurden geben Hinweise, inwiefern es am Markt etabliert ist. Informationen von unabhängigen Dritten bieten eine zusätzliche Vertrauensbasis.

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

wik Wissenschaftliches Institut für Infrastruktur und Kommunikationsdienste