Schlussbericht

„mIT Standard sicher - Entwicklung und Verbreitung eines Standards für KMU-geeignete IT-Sicherheitsberatung (KMU SEC)“

Zuwendungsempfänger:

Partner	Förderkennzeichen
Der Mittelstand. BVMW e.V.	01MS21003A

Autor/en: Marc Dönges

Laufzeit des Vorhabens: 01.03.2022 – 31.08.2024

Erstellungsdatum: 20.12.2024

Inhalt

1. Darstellung des Projektes 3
   1.1. Aufgabe und Ziel des Projektes 3
   1.2. Ausgangslage zu Beginn des Projektes bei Klein- und Kleinstunternehmen in Deutschland 3
   1.3. Struktur des Projektes 4
      1.3.1. Partner 4
      1.3.2. Arbeitsplanung 5
   1.4. Zusammenarbeit mit 5
      1.4.1. Unterauftragnehmern 5
      1.4.2. Assoziierten Partnern 6
      1.4.3. Netzwerk Mittelstand-Digital 7
2. Ergebnisse / Zielerreichung 8
   2.1. Ist-Soll Abgleich quantifizierbarer Ergebnisse 8
   2.2. Darstellung inhaltlicher Ergebnisse 10
      2.2.1. Zentraler Projektleistungen 10
      2.2.2. Gewonnene Erkenntnisse 12
      2.2.3. Beitrag zu den förderpolitischen Zielen 12
3. Nutzen und Verwertung 14
   3.1. Nutzen 14
      3.1.1. Für die Partner 14
   3.2. Verwertung / Nachhaltigkeit 14
      3.2.1. Weiterführungsmöglichkeiten 14
      3.2.2. Wirtschaftliche Verwertung durch die Projektpartner 15
      3.2.3. Wissenschaftliche Verwertung durch die Projektpartner 15
      3.2.4. Anschlussfähigkeit 15
4. Anlagen: 16
   4.1. Veröffentlichungen (Liste) 16

1. Darstellung des Projektes

1.1. Aufgabe und Ziel des Projektes

Das Projekt *mIT Standard sicher* verfolgte das Ziel, kleine und mittlere Unternehmen (KMU) in Deutschland bei der Sicherung ihrer IT-Infrastrukturen zu unterstützen, indem ein praxisnaher Beratungsstandard entwickelt und etabliert wurde. Dieser Standard sollte es IT-Dienstleistern ermöglichen, KMUs systematisch und nachvollziehbar bei der Umsetzung grundlegender IT-Sicherheitsmaßnahmen zu beraten. Ein zentrales messbares Ziel war die Veröffentlichung einer DIN SPEC, die als Richtlinie für IT-Berater dient. Darüber hinaus sollten durch gezielte Öffentlichkeitsarbeit der Einsatz des Standards bei IT-Dienstleistern gefördert und die Nachfrage bei Klein- und Kleinstunternehmen geschaffen werden. Unter anderen sollten mindestens 300 Teilnehmende in Schulungen und Veranstaltungen erreicht und mindestens 20 externe Veranstaltungen zur Verbreitung des Standards durchgeführt werden.

Im Verlauf des Projekts zeigte sich, dass die Resonanz auf den Beratungsstandard die ursprünglichen Erwartungen übertraf. Der Fokus wurde daher erweitert, um die Verbreitung und Akzeptanz des Standards durch intensivere Kommunikationsmaßnahmen zu fördern, wie beispielsweise durch eine verstärkte Präsenz in sozialen Medien und zusätzliche Veranstaltungen. Dadurch konnte die Reichweite des Standards erhöht und eine breitere Zielgruppe angesprochen werden. Diese Anpassungen unterstreichen die dynamische Ausrichtung des Projekts auf die tatsächlichen Bedürfnisse der Zielgruppen und die Relevanz eines einheitlichen IT-Sicherheitsstandards in einer zunehmend digitalisierten Wirtschaft.

1.2. Ausgangslage zu Beginn des Projektes bei Klein- und Kleinstunternehmen in Deutschland

Zu Beginn des Projekts *mIT Standard sicher* standen viele kleine und kleinste Unternehmen (KMU) in Deutschland vor erheblichen Herausforderungen im Bereich der IT-Sicherheit. Trotz der zunehmenden Digitalisierung ihrer Geschäftsprozesse und der damit verbundenen Abhängigkeit von IT-Systemen verfügten zahlreiche Unternehmen nicht über ausreichende Schutzmaßnahmen gegen Cyberangriffe. Insbesondere fehlte es häufig an systematischem Wissen über die Anforderungen an IT-Sicherheit, an den notwendigen personellen und finanziellen Ressourcen sowie an konkreten, leicht umsetzbaren Handlungsempfehlungen. Diese Problematik wurde durch die immer komplexer werdende Bedrohungslage verschärft: Phishing, Ransomware-Angriffe und Datenlecks nahmen in Häufigkeit und Schwere zu, während das Risikobewusstsein in vielen Unternehmen nur unzureichend entwickelt war.

Eine zentrale Herausforderung bestand darin, dass viele KMU keinen Zugang zu spezialisierter IT-Sicherheitsberatung hatten oder deren Nutzen nicht erkannten. IT-Dienstleister, die potenziell als Multiplikatoren fungieren könnten, verfügten oftmals selbst nicht über standardisierte Ansätze, um ihren Kunden effektive und bedarfsgerechte Lösungen anzubieten. Dies führte zu einem erheblichen Sicherheitsgefälle, das KMUs gegenüber größeren Unternehmen benachteiligte und sie anfälliger für Cyberbedrohungen machte.

Das Projekt setzte sich daher zum Ziel, eine Lösung zu entwickeln, die die Brücke zwischen KMUs und IT-Dienstleistern schlägt. Zentral war die Entwicklung eines Beratungsstandards, der nicht nur die Grundlagen der IT-Sicherheit adressiert, sondern auch praxisnah und an die spezifischen Bedürfnisse von KMUs angepasst ist. Ein besonderer Fokus lag dabei darauf, die Hemmschwelle für KMUs zu senken, sich mit IT-Sicherheitsmaßnahmen auseinanderzusetzen, und gleichzeitig IT-Dienstleister in die Lage zu versetzen, diese Maßnahmen zielgerichtet zu vermitteln.

Im Verlauf des Projekts wurde deutlich, dass die ursprünglichen Herausforderungen durch die Dynamik der Digitalisierung weiter an Dringlichkeit gewannen. Die rasante Zunahme digitaler Technologien in nahezu allen Branchen führte zu neuen Risiken, insbesondere im Kontext der Cloud-Nutzung, der mobilen Arbeit und der wachsenden Abhängigkeit von digitalen Plattformen. Diese Entwicklungen flossen in den Beratungsstandard mit ein, um sowohl den aktuellen Bedrohungen als auch den fortschreitenden Anforderungen an IT-Sicherheit gerecht zu werden.

Die Verlängerung des Projekts bis August 2024 bot zudem die Möglichkeit, auf diese dynamischen Entwicklungen einzugehen und die Reichweite sowie die Wirksamkeit der Maßnahmen zu erhöhen. So konnte der Beratungsstandard weiter verfeinert und seine Verbreitung durch zusätzliche Kommunikations- und Schulungsmaßnahmen gezielt intensiviert werden. Insgesamt verdeutlicht die Ausgangslage die Notwendigkeit eines strukturierten Ansatzes zur Verbesserung der IT-Sicherheit in KMUs und unterstreicht die zentrale Rolle eines einheitlichen Standards, wie ihn *mIT Standard sicher* entwickelt hat.

1.3. Struktur des Projektes

1.3.1. Partner

Der Mittelstand, BVMW e.V., übernahm als alleiniger Fördermittelnehmer eine zentrale Rolle bei der Umsetzung des Projekts *mIT Standard sicher*. Als größte freiwillige Interessenvereinigung für kleine und mittelständische Unternehmen in Deutschland brachte der BVMW seine weitreichende Expertise sowie sein etabliertes Netzwerk von Unternehmen und IT-Dienstleistern in das Projekt ein. Der Verband fungierte als Schnittstelle zwischen den beteiligten Akteuren, koordinierte die verschiedenen Projektaktivitäten und war maßgeblich für die inhaltliche Entwicklung und Verbreitung des Beratungsstandards verantwortlich. Neben der Organisation von Veranstaltungen und Webinaren setzte der BVMW umfassende Kommunikationsmaßnahmen um, um die Zielgruppe zu sensibilisieren und über die Relevanz von IT-Sicherheit aufzuklären.

Darüber hinaus gewährleistete der Verband durch seine Vernetzung den direkten Zugang zu KMUs und IT-Dienstleistern, wodurch die Bedürfnisse und Herausforderungen dieser Zielgruppen frühzeitig in die Standardentwicklung einfließen konnten. Als Stimme des Mittelstands trug der BVMW dazu bei, den Beratungsstandard praxisnah und umsetzungsorientiert zu gestalten. Die Rolle als Fördermittelnehmer umfasste auch die strategische Steuerung des Projekts, die Überwachung der Zielerreichung sowie die Berichterstattung gegenüber den Fördergebern. Damit war der BVMW nicht nur Initiator, sondern auch Treiber und Garant für den Erfolg des Projekts.

1.3.2. Arbeitsplanung

Die Arbeitsplanung des Projekts *mIT Standard sicher* war von einer klaren Strukturierung in vier zentrale Arbeitspakete geprägt, die aufeinander aufbauten und eine effiziente Umsetzung der Projektziele sicherstellten. Zunächst wurden im AP 1 *Projektmanagement* die organisatorischen Grundlagen geschaffen, darunter regelmäßige Austausche mit dem Unterauftragnehmer. Im zweiten Arbeitspaket erfolgte die *Identifikation und Ausformulierung des Standardisierungsvorhabens*. Hierzu wurden die Anforderungen von KMUs und IT-Dienstleistern erfasst, Stakeholder eingebunden und ein Konzept für die Erstellung der DIN SPEC entwickelt.

Das dritte Arbeitspaket konzentrierte sich auf die *Erstellung und Veröffentlichung der DIN SPEC*. Neben der inhaltlichen Ausarbeitung umfasste dies auch die Entwicklung eines Geschäftsplans zur Etablierung des Standards über die Projektlaufzeit hinaus. Insbesondere die inhaltliche Ausarbeitung des Standards umfasste sehr viel Zeit und zahlreiche gemeinsame Sitzungsstunden mit dem DIN SPEC-Konsortium bis April 2023.

Parallel dazu wurde in einem vierten Arbeitspaket der Fokus auf *Transfer und Öffentlichkeitsarbeit* gelegt, um den Standard in die Breite zu tragen. Dies beinhaltete Webinare, Tutorials, Social-Media-Kampagnen und die Erstellung von Materialien wie Broschüren und Leitfäden. Auch war das Arbeitspaket auf den Aufbau eines *Transfernetzwerks* ausgerichtet, um die langfristige Anwendung des Standards durch Veranstaltungen, Kooperationen und Netzwerkarbeit sicherzustellen.

Im Verlauf des Projekts wurde die Arbeitsplanung durch eine kostenneutrale Verlängerung bis August 2024 angepasst, um auf dynamische Entwicklungen in der IT-Sicherheitslandschaft reagieren zu können. Diese zusätzliche Zeit ermöglichte es, weitere Veranstaltungen durchzuführen und weiter in die Verbreitung des Standards zu investieren. Die strukturierte Arbeitsplanung gewährleistete somit nicht nur eine zielgerichtete Umsetzung der Projektinhalte, sondern auch eine nachhaltige Verankerung der Projektergebnisse.

1.4. Zusammenarbeit mit

1.4.1. Unterauftragnehmern

Der Unterauftragnehmer **DIN e.V.** übernahm eine entscheidende Rolle bei der Entwicklung der DIN SPEC 27076. Als zentrale Institution für Normung und Standardisierung in Deutschland war der DIN e.V. maßgeblich für die methodische und prozessuale Begleitung der Erstellung der DIN SPEC verantwortlich. Er stellte sicher, dass die Entwicklung den hohen Anforderungen an Transparenz, Konsens und Qualität entsprach, die für normbasierte Dokumente notwendig sind.

In enger Zusammenarbeit mit dem Mittelstand, BVMW e.V., unterstützte der DIN e.V. die Einbindung relevanter Stakeholder und begleitete die strukturierten Workshops zur Erarbeitung der Inhalte. Dabei sorgte er für eine ausgewogene Berücksichtigung der Interessen von KMUs, IT-Dienstleistern und weiteren Experten. Neben der fachlichen Begleitung trug der DIN e.V. auch durch die Veröffentlichung der DIN SPEC zum kostenfreien Download im Online-Shop des Beuth-Verlags zur langfristigen Sichtbarkeit und Anwendbarkeit des Standards bei.

Diese Partnerschaft vereinte die praxisnahe Expertise des BVMW mit den Kompetenzen des DIN e.V. und bildete eine solide Basis für die erfolgreiche Standardisierung und Einführung der DIN SPEC 27076, die speziell auf die Bedürfnisse kleiner und mittlerer Unternehmen zugeschnitten ist.

1.4.2. Assoziierten Partnern

Assoziierte Partner im klassischen Sinne von durch LOI an das Projekt gebundene Institutionen hatte mIT Standard sicher nicht. Bereits zu Beginn war jedoch wichtig, dass die Einbindung von Fachpartnern, Expert:innen und IT-Sicherheitsdienstleistern entscheidend für den Erfolg des Projekts sein würde. Dementsprechend galt es zu Beginn das DIN SPEC-Konsortium zur Ausarbeitung des CyberRisiko-Checks zu gründen. Mittels eines Kickoff-Workshops konnten erste Interessent:innen eingebunden werden. Schnell war klar, dass ein Großteil der Teilnehmenden des Kickoff-Workshops auch an der konstituierenden Sitzung des DIN SPERC Konsortiums teilnehmen würde.

Elementar war die Beteiligung des BSI insbesondere durch Manuel Bach, welcher gemeinsam mit dem Projektleiter Marc Dönges die Konsortialleitung übernahm. Das BSI steuerte entscheidendes Fachwissen bei, unter anderem traf es eine Vorauswahl der BSI-Grundschutzbausteine, die in die DIN SPEC übernommen werden sollten. Die Zusammensetzung des restlichen Konsortiums stellte sich als sehr förderlich für das Gesamtergebnis heraus: Zahlreiche IT-Dienstleister, die die Ansprüche und Situation ihrer mittelständischen Kundschaft und Kleinstbetrieben gut kannten, beteiligten sich intensiv an der Erarbeitung. Außerdem flossen die Erfahrungen verschiedener Organisationen wie dem Mittelstand-Digital Zentrum Lingen Münster Osnabrück, dem Mittelstand-Digital Zentrum Chemnitz und der Digitalagentur Berlin ein. Durch diese Zusammensetzung und nicht zuletzt die Leitung von Der Mittelstand, BVMW e.V. konnte eine sehr hohe Zielgruppenorientierung des Endprodukts festgehalten werden.

An der Entwicklung beteiligt waren:

B2 Berlin Beratungsgesellschaft mbH
Thomas Balzer
—
Basec GmbH
Jannik Schumann
—
Bundesamt für Sicherheit in der Informationstechnik
Manuel Bach, Angela Steiner
—
2Consulting UG (haftungsbeschränkt)
René Eck
—
Datenbeschützerin Regina Stoiber GmbH
Regina Stoiber
—
Der Mittelstand, BVMW e.V.
Marc Dönges, Julian Rupp
—
Deudat GmbH
Mario Arndt
—
Digitalagentur Berlin GmbH

Paul Sonnenberg
—
DResearch Digital Media Systems GmbH
Ines Peters
—
FINOBIT GmbH
Antje Kühn, Stefan Reichel
—
IFIS-FR Ingenieurbüro für Informationssicherheit
Bernd Frenz
—
Institut für betriebliche Integration und Digitalisierung (IBID), THB
Felix Eifert, Prof. Dr. Andreas Johannsen, Daniel Kant
—
InTo-Consulting GmbH
Ines Tóth-Strichirsch
—
IT-Dienstleistungsgesellschaft mbH Emsland
Alexander Bose
—
LWsystems GmbH & Co. KG
Ansgar Licher
—
mindt.systems UG (haftungsbeschränkt)
Heiko Mindt
—
OFFICESCHOCH GmbH
Melanie Schoch
—
Scio GmbH
Markus Wolff
—
Securepoint GmbH
Mathias Millahn
—
tti Technologietransfer und Innovationsförderung Magdeburg GmbH
Andreas Neuenfels
—
Vidano GmbH
Bianca Bach

1.4.3. Netzwerk Mittelstand-Digital

Das Mittelstand-Digital Netzwerk von Beginn an mitgedacht und bereits zum Kickoff-Workshop eingeladen. Das tti Technologietransfer und Innovationsförderung Magdeburg GmbH (MDZ Chemnitz) und die IT-Dienstleistungsgesellschaft mbH Emsland (MDZ Lingen.Münster.Osnabrück) nahmen daraufhin als stetiges Mitglied unter großem Zeitaufwand an der DIN SPEC-Entwicklung teil. Die Arbeitsstände wurden auch vermehrt in der Arbeitsgruppe IT-Sicherheit vorgestellt. Sowohl in der Entwicklung der DIN SPEC als auch in der späteren Verbreitung war das Mittelstand-Digital Netzwerk von entscheidender Bedeutung.

2. Ergebnisse / Zielerreichung

2.1. Ist-Soll Abgleich quantifizierbarer Ergebnisse

Die Projektziele können als erreicht und in Teilen als übererfüllt bewertet werden. Zusammenfassend betrachtet ging es in dem Projekt in einem ersten Schritt um die Entwicklung eines neuen Standards für die IT-Sicherheitsberatung von Klein- und Kleinstunternehmen. In einem zweiten Schritt ging es schließlich um die dazugehörige Öffentlichkeitsarbeit um diesen in die Anwendung bei IT-Dienstleistern zu bringen sowie die Nachfrage bei Klein- und Kleinstunternehmen zu schaffen bzw. zu erhöhen.

In der folgenden Tabelle lässt sich im Detail ablesen, welche Deliverables konkret gesetzt wurden und welche davon erfüllt (grün) oder nicht erfüllt (rot) wurden. Der Abschnitt „Sonstiges“ listet (On-Top-)Errungenschaften bzw. ÖA-Ziele des Projekts auf, die nicht in der Vorhabensbeschreibung festgehalten waren.

Die nicht erfüllten Deliverables lassen sich wie folgt erklären:

- Presseinformationen: Es wurde nur eine statt zwei Pressemitteilungen versandt. Der Grund dafür liegt im fehlenden Neuigkeitswert, der eine zweite PM gerechtfertigt hätte. Die erste wurde zur Veröffentlichung der DIN SPEC über die Kanäle des BVMW versandt. Danach bestand das Projekt hauptsächlich aus ÖA-Maßnahmen. Hier hatte jedoch kein Deliverable mehr ausreichend Neuigkeitswert um eine PM zu rechtfertigen.
- Erreichte TN über beide Veranstaltungen: Insbesondere bei der Kickoff-Veranstaltung im August 2022 konnten die angestrebten Teilnehmerzahlen nicht erreicht werden. Insgesamt sind dabei bei den beiden großen Veranstaltungen nur 200 von 300 angestrebten Teilnehmern erreicht. Dies wird jedoch mehr als kompensiert durch die Teilnehmer in den 10 durchgeführten Webinaren. Hier wurden 838 von 300 angestrebten Teilnehmern erreicht.
- Verteilte Broschüren als Beileger DER Mittelstand: Aufgrund einer Reduktion der Auflage des Magazins von 33.000 auf 32.000 wurden auch entsprechend weniger Broschüren als Beilage verteilt.
- Erneutes Nachdrucken der Broschüren: Wurde ausgesetzt, da zu Projektende noch sehr viele Exemplare übrig waren und Interessenten oft die digitale Version bevorzugen.

Arbeitspakete	Deadline laut VB	Soll laut VB	Ist
1_Administration			
Konsortialtreffen haben stattgefunden	PM 24 (Februar 2024)	7	**Wöchentlich**
Statusmeetings haben stattgefunden	PM 24 (Februar 2024)	2	**2**
Zwischenbericht		2	**2**
Abschlussbericht		1	**1**
2_Identifikation und Ausformulierung des Standardisierungsvorhabens			
Konzept Workshop	PM 2 (April 2022)	1	**1**
Liste relevanter Stakeholder	PM 2 (April 2022)	1	**1**
Workshop mit mind. 5 Teilnehmenden hat stattgefunden	PM 2 (April 2022)	1	**1**
Überblick über Bedarfe der Stakeholder	PM 2 (April 2022)	1	**1**
3_Erstellung und Veröffentlichung der DIN SPEC			
Erstellung und Veröffentlichung des Geschäftsplans	PM 4 (Juni 2022)	1	**1**
Überblick relevanter Inhalte für die DIN SPEC	PM 6 (August 2022)	1	**1**
DIN SPEC veröffentlicht	PM 11 (Januar 2023)	1	**1**
4_Transfer und Öffentlichkeitsarbeit			
Konzept Öffentlichkeitsarbeit ist fertiggestellt	PM 2 (April 2022)	1	**1**
Kommunikationskonzept zur Beteiligung an der Erarbeitung des Standards ist entwickelt	PM 2 (April 2022)	1	**1**
Konzept Öffentlichkeitsarbeit wurde auf Aktualität geprüft und ggfs. Angepasst	PM 12 (Februar 2023)	1	**1**
Übersicht zu Vorteilen des Standards in der Beratung ist erarbeitet	PM 12 (Februar 2023)	1	**1**
Kommunikationskampagne: „hohe Sicherheit braucht einen Standard“ ist erarbeitet	PM 12 (Februar 2023)	1	**1**
Presseinformationen versandt	PM 24 (Februar 2024)	2	**1**
Social-Media-Ads Kampagne	PM 24 (Februar 2024)	1	**1**
Veröffentlichungen erzielt	PM 24 (Februar 2024)	20	**28**
4a_Veranstaltungen			
Auftaktveranstaltung	PM 6 (August 2022)	1	**1**
Webinare 1-2	PM 1 bis PM 4 (Juni 2022)	2	**2**
Webinare 3-8	PM 5 bis PM 18 (August 2023)	6	**8**
Webinare 9-10	PM 19 bis PM 24 (Februar 2024)	2	**2**
Erreichte TN über alle 10 Webinare	PM 24 (Februar 2024)	300	**838**
Transferveranstaltung	PM 24 (Februar 2024)	1	**1**
Erreichte TN über beide Veranstaltungen	PM 24 (Februar 2024)	300	**200**
4b_Tutorials			
Videotutorials für den Beratungsstandard wurden entwickelt	PM 18 (August 2023)	2	**2**
4c_Materialien			
Checkliste I	PM 12 (Februar 2023)	1	**1**
Checkliste II	PM 24 (Februar 2024)	1	**1**
Broschüre	PM 18 (August 2023)	1	**1**
Verteilte Broschüren als Beileger DER Mittelstand		33.000	**32.000**
Verteilte Broschüren		2.000	**2.000**
Leitfaden	PM 24 (Februar 2024)	1	**1**
4d_Transfernetzwerk			
Die Entwicklung des Standards wurde in mindestens. 10 Transfergesprächen/ Veranstaltungen/ Runden Tischen /Sitzungen /Kommissionen vorgestellt	PM 6 (August 2022)	10	**27**
Der Beratungsstandard wurde auf mindestens 20 externen Veranstaltungen vorgestellt	PM 24 (Februar 2024)	20	**36**
Sonstiges (nicht als Deliverable gesetzt)			
Auf externen VA erreichte Personen		kein Deliverable	**4652**
Über Publikationen erzielte Reichweite		kein Deliverable	**472000**
Stunden DIN SPEC Entwicklung		kein Deliverable	**102,5**
Impressions LinkedIn		kein Deliverable	**338.622**
Follower LinkedIn		kein Deliverable	**689**
Aufrufe Webseite		kein Deliverable	**115.823**
Besucher:innen Webseite		kein Deliverable	**45.555**
Downloads der DIN SPEC bei beuth.de (Stand: Dezember 2024)		kein Deliverable	**6.832**
Gelistete IT-Dienstleister im Verzeichnis (vor Offline-Nehmen im August 2024)		kein Deliverable	**240**
Kostenneutrale Verlängerung März-August			
Weitere externe Veröffentlichungen wurden erzielt	PM 30 (August 2024)	4	**4**
An Klein- und Kleinstunternehmen gerichtete Werbekampagne (Print-anzeige oder Radiospot) hat stattgefunden	PM 30 (August 2024)	1	**1**
Wöchentliche Bespielung der Social-Media-Kanäle (mIT Standard sicher/Transferstelle Cybersicherheit/Der Mittelstand. BVMW) hat statt-gefunden	PM 30 (August 2024)	Wöchentlich	**Wöchentlich**
Erneutes Nachdrucken der Broschüre bzw. der Checklisten hat stattgefunden (2.000 zusätzlich verteilte Exemplare)	PM 30 (August 2024)	1	**0**
Der Beratungsstandard wurde auf 4 weiteren externen digitalen oder Präsenzveranstaltungen oder Fach-messen (bspw. Hannover Messe) vorgestellt	PM 30 (August 2024)	4	**11**
240 zusätzlich erreichte Personen durch externe digitale oder Präsenz-VA/Fachmessen	PM 30 (August 2024)	240	**652**
Der Beratungsstandard wurde in mind. 4 weiteren WebImpulsen von Netzwerkpartnern (z.B. der Transferstelle Cybersicherheit) eingebun-den	PM 30 (August 2024)	4	**siehe ext. VA**
120 zusätzliche erreichte Personen über Einbindung in WebImpulsen	PM 30 (August 2024)	120	**siehe ext. VA**
Das BSI wurde bei der Entwicklung ihrer eigenen Schulungsformate zum Einsatz des Standards unterstützt	PM 30 (August 2024)	1	**1**
Das Netzwerk von aktuell über 150 den Standard anwendenden IT-Dienstleistern wurde weiterhin gepflegt und über die Verfügbarkeit des neuen Online-Tools des BSI unterrichtet	PM 30 (August 2024)	1	**1**

Abbildung 1: Deliverables und Zielerreichung

2.2. Darstellung inhaltlicher Ergebnisse

2.2.1. Zentraler Projektleistungen

Als zentrale Projektleistung ist in erster Linie die Entwicklung des Beratungsstandards für IT-Sicherheit in Klein- und Kleinstunternehmen zu nennen. Der **CyberRisiko-Check**, basierend auf der DIN SPEC 27076, ist ein Meilenstein in der IT-Sicherheitsberatung für kleine Unternehmen. Sein Erfolg liegt in seiner einzigartigen Kombination aus Praxisnähe, Nutzerfreundlichkeit und gezielter Förderung. Der Check wurde speziell für kleine Betriebe mit bis zu 50 Mitarbeitenden entwickelt und berücksichtigt deren spezifische Ressourcen- und Wissenssituation. Durch seine klar strukturierten Schritte ermöglicht er Unternehmen eine schnelle und kostengünstige Einschätzung ihres Cybersicherheitsniveaus sowie konkrete Handlungsempfehlungen zur Verbesserung.

Ein zentraler Aspekt, der den CyberRisiko-Check besonders macht, ist die enge Verbindung zwischen Theorie und Praxis. Er orientiert sich an den tatsächlichen Bedürfnissen kleiner Unternehmen und bietet eine niedrigschwellige Einstiegsmöglichkeit in das Thema Cybersicherheit. Er fragt nicht danach, wie kleine Unternehmen ein möglichst hohes Cybersicherheitsniveau mit einem möglichst vollständigen Maßnahmenkatalog erreichen können, sondern danach wie Unternehmen mit möglichst geringem Ressourcenaufwand die wichtigsten Bedrohungen managen können. Dies hebt ihn von anderen Standards ab, die oft komplex und ressourcenintensiv sind. Unternehmen erhalten nicht nur eine umfassende Analyse ihrer aktuellen IT-Sicherheitslage, sondern auch priorisierte Maßnahmen und Hinweise zu Förderprogrammen, die die Umsetzung erleichtern. Dies schafft eine sofortige und nachhaltige Wirkung, indem es Unternehmen befähigt, eigenständig und effizient ihre Sicherheitsmaßnahmen zu verbessern.

Darüber hinaus unterstützt der CyberRisiko-Check die Auswahl qualifizierter IT-Dienstleister, die auf Basis des Standards arbeiten. Dies sorgt für Transparenz und Vertrauen zwischen Unternehmen und Beratern. Indem er ein gleichbleibend hohes Beratungsniveau sicherstellt, trägt der Check maßgeblich dazu bei, das allgemeine Cybersicherheitsniveau im Mittelstand zu erhöhen. Unternehmen werden durch den Check nicht nur resilienter gegenüber Cyberangriffen, sondern auch wettbewerbsfähiger in einer zunehmend digitalisierten Wirtschaft.

Insgesamt zeichnet sich der CyberRisiko-Check durch seine Skalierbarkeit und Flexibilität aus. Seine einfache Implementierung und die Möglichkeit, ihn individuell an die Gegebenheiten einzelner Betriebe anzupassen, machen ihn zu einem unverzichtbaren Werkzeug für kleine Unternehmen, die ihre digitale Sicherheit stärken und zugleich ihre Marktposition verbessern möchten.

Wie der CyberRisiko-Check nach DIN SPEC 27076 funktioniert

Der CyberRisiko-Check, entwickelt auf Basis der DIN SPEC 27076, ist ein praxisorientiertes Werkzeug, das kleinen und kleinsten Unternehmen (KKU) dabei hilft, ihr IT-Sicherheitsniveau systematisch zu bewerten und zu verbessern. Der Check ist klar strukturiert und einfach in der Anwendung, wodurch er speziell auf die Anforderungen von Betrieben mit begrenzten personellen und finanziellen Ressourcen zugeschnitten ist.

Ablauf und Prozess
Der Check beginnt mit einer Vorbereitung durch das Unternehmen. Dieses nutzt kostenfreie Informationsmaterialien, darunter Checklisten und Broschüren, um sich mit dem Ablauf und den Anforderungen vertraut zu machen. Der eigentliche Prozess umfasst drei wesentliche Schritte:

1. Ist-Analyse: Gemeinsam mit einem qualifizierten IT-Dienstleister wird eine Bestandsaufnahme der bestehenden IT-Sicherheitsmaßnahmen durchgeführt. Dabei wird geprüft, welche Schutzmaßnahmen bereits implementiert sind und welche Schwachstellen bestehen.

2. Erarbeitung von Handlungsempfehlungen: Basierend auf der Analyse erstellt der Dienstleister priorisierte Empfehlungen. Diese sind praxisnah und auf die spezifischen Bedürfnisse des Unternehmens zugeschnitten, sodass die Umsetzung möglichst effizient erfolgen kann.

3. Umsetzung und Nachbereitung: Die Empfehlungen können entweder direkt vom Unternehmen oder mit Unterstützung des Dienstleisters umgesetzt werden. Zudem erhalten Betriebe eine Übersicht über mögliche Förderprogramme, die finanzielle Unterstützung für die Maßnahmen bieten

Zeitaufwand und Ergebnis
Der gesamte Prozess des CyberRisiko-Checks ist so gestaltet, dass er mit einem überschaubaren Zeitaufwand verbunden ist. Die Durchführung der Ist-Analyse und die Erstellung der Empfehlungen nehmen in der Regel nur wenige Stunden in Anspruch. Der Vorteil liegt in der klaren Strukturierung und der effizienten Prozessführung, wodurch kleine Betriebe den Check problemlos in ihren Arbeitsalltag integrieren können.

Am Ende des Checks erhält das Unternehmen:

- Einen detaillierten Bericht: Dieser umfasst die Ergebnisse der Ist-Analyse, identifizierte Schwachstellen und priorisierte Handlungsempfehlungen.
- Handlungskatalog: Konkrete, leicht umsetzbare Maßnahmen zur Verbesserung der IT-Sicherheit.
- Übersicht über Förderprogramme: Hinweise auf finanzielle Unterstützungen, die die Umsetzung erleichtern.
- Qualifizierte Beratung: Durch die Zusammenarbeit mit einem zertifizierten IT-Dienstleister wird sichergestellt, dass die Lösungen auf die individuellen Bedürfnisse des Unternehmens abgestimmt sind

Besonderheit für Unternehmen
Betriebe, die den CyberRisiko-Check durchführen lassen, profitieren von der strukturierten Herangehensweise, die Transparenz und Vergleichbarkeit bietet. Der Check ermöglicht es den Unternehmen, ihr IT-Sicherheitsniveau zu einem Bruchteil der üblichen Kosten zu steigern und sich gezielt gegen Cyberangriffe zu schützen. Gleichzeitig erhalten sie durch die standardisierte Beratung eine höhere Entscheidungs- und Handlungskompetenz im Bereich der Cybersicherheit. Dies trägt nicht nur zur Verbesserung ihrer Resilienz bei, sondern stärkt auch ihre Wettbewerbsfähigkeit in der digitalen Wirtschaft.

Die zweite große Projektleistung ist das umfassende **Paket an Öffentlichkeitsarbeitsmaßnahmen**, das der Veröffentlichung der DIN SPEC 27076 folgte. Es hatte zum Ziel, das Angebot des CyberRisiko-Checks bei IT-Dienstleistern zu erhöhen und die Nachfrage bei kleinen Unternehmen zu fördern.

In diesem Rahmen wurden zwei größere Informationsveranstaltungen mit 200 Teilnehmeden abgehalten, zehn Webimpulse mit 838 Teilnehmenden durchgeführt, eine knapp 35.000 mal verteilte Broschüre für Klein- und Kleinstunternehmen entwickelt, ein Leitfaden für Dienstleister geschrieben, zwei Erklärvideos mit knapp 16.000 Views auf Youtube produziert, eine LinkedIn-Community mit knapp 700 Followern aufgebaut, Social-Media- und Google-Ad-Kampagnen geschaltet, zahlreiche externe Veröffentlichungen publiziert und das Projekt auf einer Vielzahl an Events und Messen mit über 4.600 erreichten Personen platziert.

Ein großer Indikator des Erfolgs im Sinne der Durchdringung der Zielgruppe IT-Dienstleister sind die Downloadzahlen der DIN SPEC auf beuth.de. Im Dezember 2024 meldete DIN e.V., dass die DIN SPEC 6.832-mal kostenfrei heruntergeladen wurde. Im Dienstleisterverzeichnis von mit-standard-sicher.de hatten sich bis August 2024 240 Dienstleister gelistet, die den CyberRisiko-Check für kleine Unternehmen anbieten. Das Verzeichnis wurde kurz vor Projektende abgeschaltet. Das BSI bespielt das Thema jedoch mehrfach weiter: Es hat ein Online-Tool entwickeln lassen, mit dem IT-Dienstleister den CyberRisiko-Check deutlich einfacher umsetzen können und einen automatisierten DIN SPEC-konformen Ergebnisbericht ausgeben können. Das Tool können nur Dienstleister nutzen, die sich haben schulen lassen. Daraufhin können diese sich auch im BSI-Dienstleisterverzeichnis listen lassen. Das BSI meldete im Dezember 2024 über 700 geschulte IT-Dienstleister bundesweit, die den CyberRisiko-Check anbieten und bereits über 250 durchgeführte CyberRisiko-Checks im Tool. Wie viele CyberRisiko-Checks insgesamt durchgeführt wurden, lässt sich jedoch nicht beziffern, da dies dezentral durch die IT-Dienstleister passiert.

2.2.2. Gewonnene Erkenntnisse

Folgende Learnings können nach Durchführung des Projekts festgehalten werden:

- **Die Zielgruppe muss im Fokus der Entwicklung eines jeden Angebots stehen**. Der BSI-Grundschutz ist zwar ein umfangreiches und annähernd vollständiges Kompendium an Cybersicherheitsmaßnahmen, es erreicht die Zielgruppe von kleinen und Kleinstunternehmen jedoch kaum. Diese fühlen sich durch den utopisch-großen Zeit- und Ressorcenaufwand von dem Standard und auch den Anforderungen an Dokumentation überfordert. Besser ist ein Ansatz, der die begrenzte Zeit, das begrenzte Personal und die begrenzten finanziellen Mittel kleiner Unternehmen mitdenkt. Dadurch animiert der CyberRisiko-Check kleine Unternehmen das Thema anzupacken.
- **Die Perspektive der Zielgruppe muss bei einer Standardentwicklung einfließen**. Natürlich ist es schwierig Kleinstunternehmen selbst zum Mitarbeiten in einem DIN SPEC Konsortium zu bewegen. Die IT-Dienstleister, die ihre Kundschaft sehr gut kennen, die Mittelstand-Digital-Zentren und nicht zuletzt der BVMW haben die Zielgruppenperspektive bei der Standardentwicklung sehr gut vertreten und eingebracht. Solche Konsortien müssen divers aufgebaut sein und sollten nicht ausschließlich auf Fachexpert:innen bauen.
- **Breite Kooperationen sind elementar, um einen neuen Standard zu etablieren**. Die großen Downloadzahlen der DIN SPEC und das damit starke Durchdringend der Zielgruppe der IT-Dienstleister war nur durch die breite Zusammenarbeit mit dem bereits durch andere Projekte etablierten Netzwerk des BVMW möglich. Die Einbindung des BSI hat dem Projekt von Anfang an fachlichen Rückenwind gegeben.

2.2.3. Beitrag zu den förderpolitischen Zielen

Die Ziele der Initiative „IT-Sicherheit in der Wirtschaft“ nach Bekanntmachung vom 21.12.2018 wurden wie folgt adressiert:

1. **Sensibilisierung und Unterstützung von KMU und Handwerk beim Thema IT-Sicherheit im Zuge ihrer digitalen Transformation.**

Einen Standard für die Cybersicherheitsberatung von Klein- und Kleinstunternehmen gab es bisher nicht. Sich an einem solchen orientieren zu können ist eine große Unterstützung für kleine Unternehmen. Der Ergebnisbericht, der nach Durchführung des CyberRisiko-Checks ausgehändigt wird, sensibilisert Betriebe ganz konkret zu nötigen Maßnahmen und erläutert auch, warum diese Maßnahmen umgesetzt werden sollten.

2. **Stärkung von Wettbewerbs- und Innovationsfähigkeit von KMU durch den sicheren Einsatz digitalisierter Prozesse und Geschäftsmodelle.**

Der CyberRisiko-Check schließt Einfallstore für Angreifer:innen und macht Unternehmen somit resilienter. Diese Resilienz und die Prävention langer Ausfallzeiten und hohen Schadenssummen führen in letztlicher Konsequenz natürlich auch zu einer Stärkung der Wettbewerbs- und Innovationsfähigkeit der Betriebe.

3. **Förderung technologischer, organisatorischer und arbeitsgestaltender IT-Sicherheitskompetenzen sowie Stärkung von Sicherheit und Vertrauen (Anbieter/Anwender) von IKT-Systemen inkl. Hard- und Software.**

Der CyberRisiko-Check beinhaltet Maßnahmen aus den Bereichen Technik, Organisation und Mensch und weist daraufhin hin, an welchen Stellen Schulungen und Sensibilisierung von Führungskräften nötig sind.

4. **Erhöhung des IT-Sicherheitsniveaus in KMU**

Der CyberRisiko-Check misst ganz genau das Cybersicherheitsniveau in Unternehmen unter 50 Beschäftigten durch das Ausgeben eines Risikoscores und gibt konkrete Handlungsempfehlungen aus, um diesen zu verbessern. Defizite werden verdeutlicht und mit einfach verständlichen Begründungen versehen. Die besondere Niedrigschwelligkeit des Angebots mit Blick auf geringen Zeit-, Personal- und Ressourcenaufwand ist ebenfalls ein Novum in der Angebotslandschaft für kleine Unternehmen.

5. **KMU befähigen selbstständig kompetente IT-sicherheitsrelevante Entscheidungen zu treffen.**

Viele kleine Unternehmen haben den Wunsch, sich einen IT-Dienstleister ins Haus zu holen, der das Thema Cybersicherheit bei ihnen anpackt. Mit dem standardisierten Vorgehen des CyberRisiko-Checks erhalten Betriebe einen Ergebnisbericht, der Defizite aufzeigt und erklärt, visualisiert und entsprechende Maßnahmen empfiehlt und begründet. Auf dieser Basis können Geschäftsführungen kleiner Unternehmen informierte Entscheidungen zum weiteren Vorgehen treffen.

3. Nutzen und Verwertung

3.1. Nutzen

3.1.1. Für die Partner

Das Thema Cybersicherheit ist für die Mitglieder des BVMW grundsätzlich von großer Relevanz. Diese konnten direkt davon profitieren, dass ihr Verband federführend in der Entwicklung und Verbreitung eines neuen Cybersicherheitsstandards war. Sie haben von den zahlreichen kostenfreien Informationsangeboten direkt über die Kanäle des Verbands erfahren und konnten diese nutzen. Mitglieder, die verbandsintern in den Arbeitsgemeinschaften Digitales und IT-Sicherheit aktiv waren, konnten zur DIN SPEC-Entwicklung eingeladen werden. Der Verband hat damit auch thematisch sein Profil geschärft. Die gewonnenen Erkenntnisse und Kontakte helfen bei der Durchführung aktueller (bspw. Transferstelle Cybersicherheit im Mittelstand) und zukünftiger Projekte.

3.2. Verwertung / Nachhaltigkeit

3.2.1. Weiterführungsmöglichkeiten

Angebotsteile bzw. neue Angebote, die weit über das Scope von mIT Standard sicher hinausgehen, werden im Prinzip über zwei Arten weitergeführt:

1. **Durch das Engagement des BSI**

Das BSI bespielt den CyberRisiko-Check mit weiterführenden Angeboten, die mit den finanziellen Mitteln des Projekts nicht abzudecken gewesen wären und die Vorhabensbeschreibung weit überschreiten. Dazu zählen:

a) Entwicklung eines **Online-Tools**, das es IT-Dienstleistern einfacher macht, den CyberRisiko-Check durchzuführen. Diese müssen nun nicht mehr manuell Ergebnisse dokumentieren und Berichte erstellen, sondern können dies automatisiert geschehen lassen. Die Berichte sind dabei garantiert DIN SPEC-konform. Die Daten aus dieser Plattform können außerdem anonymisiert genutzt werden, um ein mögliches Lagebild kleiner Unternehmen anzufüttern.
b) Angebot von **regelmäßigen Schulungen**, die IT-Dienstleister qualifizieren den CyberRisiko-Check richtig zu verstehen und anzuwenden. Erst wenn die Schulung durchlaufen wurde, erhalten Dienstleister Zugang zum Online-Tool.
c) Erstellung eines bundesweiten **IT-Dienstleisterverzeichnisses**, damit Betriebe ihren Dienstleister für den CyberRisiko-Check finden können. Hierzu erhalten nur Dienstleister Zugang, die die Schulung abgeschlossen haben.
d) Weiterführende **Öffentlichkeitsarbeit** zum CyberRisiko-Check, weit über die Laufzeit des Projekts mIT Standard sicher hinaus.

Durch diese Maßnahmen findet eine Verstetigung des Angebots außerhalb der Fördertöpfe von Mittelstand-Digital statt.

2. **Durch das direkt im zeitlichen Anschluss gestartete Projekt Transferstelle Cybersicherheit im Mittelstand**

Die Projektleitung bzw. Projektmitarbeiter von mIT Standard sicher stiegen im Juli 2024 in das Projekt Transferstelle Cybersicherheit im Mittelstand ein. Der CyberRisiko-Check wurde dementsprechend eingehend bei der Planung zukünftiger Maßnahmen mitgedacht. Dazu zählt:

a) Regelmäßige Webimpulse für IT-Dienstleister, um diese über den richtigen Einsatz des CyberRisiko-Checks zu informieren.

b) Regelmäßige Webimpulse für KMU, die die Vorteile des CyberRisiko-Checks erläutern und animieren, diesen zu nutzen
c) Nutzen des Fragenkatalogs des CyberRisiko-Checks als Basis für den Leitfaden der CYBERDialoge (einstündige Orientierungsgespräche für KMU)
d) Regelmäßige Öffentlichkeitsarbeit und Veranstaltungspräsenz und Einbau des CyberRisiko-Checks in Vorträge der Transferstelle Cybersicherheit.

3.2.2. Wirtschaftliche Verwertung durch die Projektpartner

Eine wirtschaftliche Verwertung durch den BVMW ist aktuell nicht vorgesehen.

3.2.3. Wissenschaftliche Verwertung durch die Projektpartner

Eine wissenschaftliche Verwertung durch den BVMW ist aktuell nicht vorgesehen.

3.2.4. Anschlussfähigkeit

Anschlussfähig bzw. eingeschränkt anschlussfähig sind folgende Möglichkeiten:

- Der CyberRisiko-Check bzw. die DIN SPEC 27076 kann bis 2029 noch einmal überarbeitet werden. Hierzu müsste das DIN SPEC-Konsortium nochmal zusammenkommen. Es könnte dann Anpassungen am Standard vornehmen, die dem Feedback aus der Zielgruppe entsprechen. Eine weitere Möglichkeit sind Anpassungen mit Blick auf die NIS-2-Richtlinie. Hierzu wäre ein Delta-Papier nötig, das die Differenz der aktuellen DIN SPEC zur NIS-2-Konformität aufzeigt.
- Der CyberRisiko-Check bzw. die DIN SPEC 27076 muss nach spätestens sechs Jahren in eine Norm überführt werden. Hierzu müssen zahlreiche Prozesse zur Abstimmung mit Standardisierungsgremien durchlaufen werden. Die Teilnahme am Konsortium ist jedoch nicht kostenfrei und auch die Norm wird dann nicht mehr kostenfrei herunterladbar sein.
- Mit einer Studie könnten IT-Dienstleister im Cybersicherheitsbereich wie auch Klein- und Kleinstunternehmen vorab befragt werden, um eine zielgruppengerechte Weiterentwicklung des Standards sicherzustellen.
- Es wird weiterhin den Bedarf geben, den CyberRisiko-Check niedrigschwellig bei IT-Dienstleistern zu bewerben und zu erklären, um diese dazu zu animieren, ihn bei ihrer mittelständischen Kundschaft anzubieten. Dies übernimmt aktuell mit regelmäßigen Terminen das BSI, um neue Dienstleister auf das Verzeichnis zu bringen und zur Nutzung des Online-Tools zu bewegen.
- Es wird weiterhin den Bedarf geben, den kleinen und Kleinstunternehmen die Vorteile des CyberRisiko-Checks zu erläutern, um die Nachfrage in der Zielgruppe zu erhöhen. Diese Aufgabe übernimm aktuell die Transferstelle Cybersicherheit im Mittelstand, die den CyberRisiko-Check an vielfachen Punkten ihrer Customer Journey an den Mittelstand trägt.

4. Anlagen:

4.1. Veröffentlichungen (Liste)

Externe Veröffentlichungen

Nr.	Datum	Titel	Ort der Veröffentlichung	Verlinkung
1	24.03.2022	IT-Sicherheit für kleine Unternehmen- aber mit Standard!	Blog des MDZ Berlin	https://digitalzentrum-berlin.de/kmu-sec
2	01.06.2022	Der Mittelstand	DER Mittelstand Ausgabe 03/2022, Juni/Juli, S. 84	https://www.bvmw.de/fileadmin/01-Presse_und_News/Publikationen/DER_Mittelstand/2022/03-2022/DER-Mittelstand-3-2022.pdf
3	09.06.2022	Digitalisierung im Mittelstand: Die drei großen Hürden	Gothaer Maklerblog. 06/2022	https://gothaer-maklerblog.de/mittelstand-digitalisierung-huerden/
4	17.06.2022	Die Bedrohungslage wächst dramatisch	Wirtschafts News	https://www.yumpu.com/de/document/read/67003889/1cyber-sicherheitskongress-des-bvmw-mainz-bingen
5	15.08.2022	Cybersicherheit im Mittelstand praxisnah angehen	Tagesspiegel Background Cybersicherheit	https://background.tagesspiegel.de/cybersecurity/cybersicherheit-im-mittelstand-praxisnah-angehen
6	10.01.2023	Cybersicherheit anpacken: So hilft der Beratungsstandard von "mIT Standard sicher" kleinen Betrieben	TISIM Blog	https://www.tisim.de/cybersicherheit-anpacken-so-hilft-der-beratungsstandard-von-mit-standard-sicher-kleinen-betrieben/
7	20.01.2023	Kopf aus dem Sand: Cybersicherheit für kleine Betriebe	DER Mittelstand	
8	04.04.2023	Effizient das Cybersicherheitsniveau steigern	DER Mittelstand	
9	05.04.2023	IT-Sicherheit einfach anpacken: Mit der neuen DIN SPEC 27076	MDZ Berlin Blog	
10	01.05.2023	BSI Paper	BSI Tagungsband des 19. IT-Sicherheitskongresses	
11	02.05.2023	Wie kleine und Kleinstunternehmen im Rahmen der SPEC 27076 Security-Awareness umsetzen können	Netzpalaver	https://netzpalaver.de/2023/05/02/wie-kleine-und-kleinstunternehmen-im-rahmen-der-spec-27076-security-awareness-umsetzen-koennen/

12	04.05.2023	CyberRisiko-Check - Wirkungsvoller Schutz für kleine und Kleinstunternehmen	BSI Webseite	https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Informationen-und-Empfehlungen/KMU/CyberRisikoCheck/CyberRisikoCheck_node.html
13	05.06.2023	Security: Wie der Cyberrisiko-Check kleine Unternehmen schützen soll	Heise.de	https://www.heise.de/hintergrund/Security-Wie-der-Cyberrisiko-Check-kleine-Unternehmen-schuetzen-soll-9162982.html
14	04.06.2023	IT-Sicherheit einfach anpacken mit dem CyberRisiko-Check	Wirtschafts-News_CyberSicherheitskongress 2023	https://www.yumpu.com/de/document/view/68225266/wirtschafts-news-cyber-sicherheitskongress-2023
15		Tagesspiegel Background		
16	30.06.2023	Initiative für den Mittelstand: Cybersicherheit für alle!	Pressnetwork.de	https://pressnetwork.de/initiative-fuer-den-mittelstand-cybersicherheit-fuer-alle/
17	17.07.2023	mSs präsentiert neuen Cybersecurity Standard	Mittelstand-Digital	https://newsletter.mittelstand-digital.de/MDN/Redaktion/DE/Newsletter/2023/43/Meldungen/43_Aktuelles_mIT_Standard_sicher.html
18	31.07.2023	Wirkungsvoller Schutz für kleine und Kleinstunternehmen	BSI	chrome-extension://efaidnbmnnnibpcajpcglclefindmkaj/https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Magazin/BSI-Magazin_2023_01.pdf?__blob=publicationFile&v=5
19		Der neue CyberRisiko-Check nach DIN SPEC 27076	Zeitschrift IT-Sicherheit	Artikel am 21.7. abgesendet
20	23.08.2023	Resilienz Paper M-D	M-D Magazin	https://www.mittelstand-digital.de/MD/Redaktion/DE/Publikationen/Wissenschaft-trifft-Praxis/magazin-wissenschaft-trifft-praxis-ausgabe-20.pdf?__blob=publicationFile&v=3
21	23.08.2023	IT-Sicherheit für KMU: Jetzt einsteigen - mit CyberRisiko-Check nach DIN SPEC 27076	Beuth Webseite	https://www.beuth.de/de/themenseiten/managementsysteme/informationssicherheitsmanagement/cyberrisikocheck-nach-din-spec-27076

22	30.08.2023	So können sich KMU vor Cyber-Bedrohungen schützen	Security Insider	https://www.security-insider.de/so-koennen-sich-kmu-mit-beratung-vor-cyber-bedrohungen-schuetzen-a-71948709c6f23a234586f08032c4c5a1/
23	06.09.2023	Mehr Schutz für kleine Betriebe	Agrar Technik	
24	25.09.2023	Der CyberRisiko-Check	IT-Sicherheit Management und Technik	https://www.datakontext.com/EPaper/index/active/1/epaper/20490
25	26.10.2023	ISMS ist doch nix für KMU? Doch ist es!	BVMW Webseite	https://www.bvmw.de/de/muenchen/unternehmertum/news/isms-ist-doch-nix-fuer-kmu-doch-ist-es
26	15.10.2023	Durchführung des CRC	BSI Lagebericht	https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Lageberichte/Lagebericht2023.pdf?__blob=publicationFile&v=6
27	13.11.2023	Cybersicherheit für KMU	BR 2	
28	17.01.2024	CyberRisiko-Check: Mit DIN SPEC 27076 setzen sich kleine Unternehmen mit IT-Sicherheit auseinander	Webseite one4IT	https://one4-it.de/cyber-risiko-check-mit-din-spec-27076-setzen-sich-kleine-unternehmen-mit-it-sicherheit-auseinander/
29	23.03.2024	CyberRisikoCheck: IT-Sicherheit für kleine und mittlere Unternehmen	Webseite BSI	https://www.bsi.bund.de/DE/Service-Navi/Presse/Pressemitteilungen/Presse2024/240323_CyberRisikoCheck.html
30	25.03.2024	CyberRisikoCheck: BSI will IT-Sicherheit in kleinen Unternehmen stärken	Heise.de	https://www.heise.de/news/CyberRisikoCheck-BSI-will-IT-Sicherheit-in-kleinen-Unternehmen-staerken-9664791.html
31	05.05.2024	Der Mittelstand	Das Seepferdchen in IT-Sicherheit für Unternehmen	
32	15.05.2024	Cbyerkriminalität - das unterschätzte Problem	Tagesspiegel Background Cybersicherheit	

Eigene Veröffentlichungen

Nr.	Titel	Art der Veröffentlichung	Verlinkung
1	Der CyberRisiko-Check: IT-Sicherheit einfach anpacken	Broschüre	https://mit-standard-sicher.de/download/33691/?tmstv=1680263947
2	Die Anwendung des CyberRisiko-Checks	Leitfaden	https://mit-standard-sicher.de/download/34230/?tmstv=1694174890
3	Vor dem CyberRisiko-Check	Checkliste	https://mit-standard-sicher.de/download/34152/?tmstv=1689845362
4	Nach dem CyberRisiko-Check	Checkliste	https://mit-standard-sicher.de/download/34167/?tmstv=1689849340
5	Die Vorteile des CyberRisiko-Checks für KMU	Erklärvideo	https://www.youtube.com/watch?v=YtH-jnPXTl4
6	So wenden IT-Dienstleister den CyberRisko-Check richtig an	Erklärvideo	https://www.youtube.com/watch?v=NCd3dDF6ez0