mIT Standard sicher

IT-Sicherheit IN DER WIRTSCHAFT

Die Anwendung des CyberRisiko-Checks auf Basis der DIN SPEC 27076

Leitfaden für IT-Dienstleistungsunternehmen

Mittelstand-Digital

Gefördert durch:

Bundesministerium für Wirtschaft und Klimaschutz

aufgrund eines Beschlusses des Deutschen Bundestages

Leitfaden für die standardisierte Informationssicherheitsberatung nach DIN SPEC 27076

Dieser Leitfaden dient IT-Dienstleistungsunternehmen als Anleitung zur Anwendung des CyberRisiko-Checks auf Basis der DIN SPEC 27076. Dieser Standard wurde speziell für Klein- und Kleinstunternehmen mit bis zu 50 Beschäftigten entwickelt und legt großen Wert auf Einfachheit, Verständlichkeit und Praxistauglichkeit. Im Folgenden soll erläutert werden, welchen Mehrwert die Anwendung des CyberRisiko-Checks bringt, wie ein Beratungsprozess aus Sicht des umsetzenden Dienstleisters abläuft und auf welche Aspekte Anwender:innen ein besonderes Augenmerk richten sollten.

Die Idee hinter dem CyberRisiko-Check

Der CyberRisiko-Check auf Basis der DIN SPEC 27076 richtet sich explizit an die Zielgruppe von Klein- und Kleinstunternehmen. Dabei handelt es sich um Unternehmen mit bis zu 50 Mitarbeitenden. In Deutschland gibt es ca. 2,6 Millionen kleine und mittlere Unternehmen. Der Anteil der Klein- und Kleinstunternehmen daran beträgt ca. 96%. Die DIN SPEC 27076 adressiert somit eine sehr große Zielgruppe und blickt dabei vor allem auf diejenigen Unternehmer:innen, welche bisher noch kein großes Augenmerk auf das Thema Informationssicherheit gelegt haben.

Da die bisherigen Informationssicherheitsstandards auf dem Markt zu umfangreich für die Zielgruppe gewesen sind, hat das durch das Bundesministerium für Wirtschaft und Klimaschutz (BMWK) aus der Initiative IT-Sicherheit in der Wirtschaft geförderte Projekt **mIT Standard sicher** einen neuen bedarfsgerechten, wirtschaftsnahen und vor allem praxistauglichen Standard erarbeitet. Berücksichtigt wurden dabei Faktoren wie Zeit, Kosten und mangelnde personelle Ressourcen.

Somit wurde die DIN SPEC 27076 so konzipiert, dass die Durchführung des CyberRisiko-Checks so zeit- und kosteneffizient wie möglich ist. Ob der Prozess in Präsenz oder via Online-Meetings durchgeführt wird, ist dabei offen gestellt. Auf Basis mehrerer Testdurchläufe und Feedback aus der Praxis konnte ein Beratertag für die vier Schritte nach DIN SPEC 27076 als realistisch durchführbarer Zeitraum deklariert werden.

Der CyberRisiko-Check in Kürze

Der CyberRisiko-Check nach DIN SPEC 27076 ist ein effektives Instrument zur raschen Verbesserung der IT- und Informationssicherheit in kleinen Unternehmen. In kompakter Form bietet dieser Beratungsstandard eine klare Struktur und hilft, konkrete Handlungsempfehlungen an Betriebe auszugeben. Hier die wichtigsten Vorteile in Kürze:

Schneller Einstieg: Der CyberRisiko-Check ermöglicht kleinen Unternehmen einen unkomplizierten Einstieg in das Thema Informationssicherheit. In nur vier einfachen Schritten erhalten sie einen umfassenden Überblick über ihren IST-Zustand und die damit verbundenen Risiken.

Klare Anforderungen: Der Check definiert 27 Anforderungen, die in reguläre und Top-Anforderungen unterteilt sind. Dadurch wird Unternehmen aufgezeigt, welche Maßnahmen vorrangig umgesetzt werden sollten, um die größten Risiken zu minimieren.

Verständliche Abfrage: Die Abfrage der Anforderungen erfolgt durch vorgegebene Leitfragen, die leicht verständlich sind und zum Austausch anregen. Die Aufnahme des IST-Zustandes geschieht in Form eines Gesprächs, bei dem auch Raum für Rückfragen bleibt.

Transparente Auswertung: Der durchführende IT-Dienstleister bewertet die erfassten Daten und erstellt einen individuellen Ergebnisbericht. Dieser zeigt den Statuswert des Unternehmens und die relevanten Handlungsempfehlungen übersichtlich auf.

Praxisorientierte Empfehlungen: Die Handlungsempfehlungen sind klar formuliert und enthalten konkrete Maßnahmen, um Schwachstellen zu beheben und Risiken zu minimieren. Dadurch können Unternehmen gezielt an ihrer Informationssicherheit arbeiten.

Weiterführende Schritte: Der Ergebnisbericht soll als Grundlage für weitere Schritte dienen. Unternehmen können beauftragen, die empfohlenen Maßnahmen umzusetzen oder weitere Beratungen zur vertiefenden Sicherheitsverbesserung in Anspruch nehmen.

Entwickelt wurde die DIN SPEC 27076 in einem Konsortium von 21 Mitgliedern, das vom Bundesamt für Sicherheit in der Informationstechnik (BSI) und Der Mittelstand, BVMW e.V. geleitet wurde. Es bestand neben Transferstellen und Förderinitiativen aus zahlreichen IT-Dienstleistern mit Cybersicherheitsfokus, die ihre Praxiserfahrung mit einbrachten. Weitere Informationen zur Entwicklung des Standards erhalten Sie auf www.mit-standard-sicher.de.

Welche Dienstleister dürfen den CyberRisiko-Check einsetzen?

Es ist von entscheidender Bedeutung, dass der beratende IT-Dienstleister über eine umfassende fachliche Qualifikation verfügt, die sowohl akademisches als auch praxisbezogenes Wissen umfasst. Die Kompetenz zur Beratung sollte durch nachweisbare Qualifikationen bei der Kundschaft belegt werden können. Eine Überprüfung dieser Qualifikationen oder gar Zertifizierung durch eine unabhängige Stelle ist jedoch nicht vorgesehen.

Für eine qualifizierte Beratung sollten Berater folgende Eigenschaften erfüllen:

- Mindestens ein Jahr Erfahrung in der Durchführung von IT-Sicherheitsberatungen und Audits.
- Nachweis von mindestens drei Referenzprojekten zur Durchführung von IT-Sicherheitsberatungen und Audits mit Klein- oder Kleinstunternehmen.
- Nachweis des für die Beratung notwendigen methodischen Wissens zur Gesprächsmethode des semistrukturierten Leitfadeninterviews, beispielsweise durch eine erfolgreiche Teilnahme an einer Schulung zum Einsatz der DIN SPEC 27076 in der Beratung von KKU.

So soll sichergestellt werden, dass Unternehmen eine fundierte und kompetente IT-Sicherheitsberatung erhalten, die auf ihre spezifischen Bedürfnisse zugeschnitten ist.

Wie läuft der Beratungsprozess nach DIN SPEC 27076 ab?

Den CyberRisiko-Check führen Dienstleister in den folgenden vier Schritten durch.


JDBB4747
Forgot password?
LOGIN

1. Das Erstgespräch

Im ersten Schritt führen Sie als Dienstleistungsunternehmen ein Erstgespräch mit dem zu beratenden Unternehmen durch, um Informationen zum Beratungsprozess zu vermitteln. Dieses Gespräch kann entweder als Online-Meeting, Telefongespräch oder persönlich vor Ort stattfinden. Während des Erstgesprächs erheben Sie bereits erste Unternehmensdaten, die später in die Berichterstattung einfließen werden. Zudem geben Sie dem beratenen Unternehmen Hinweise, welche Dokumente (Notfallpläne, Back-up-Konzepte, Zugangskonzepte, etc.) vorbereitet werden sollten, um den Prozess zeitlich effizient zu gestalten. Die Details hierzu entnehmen Sie dem DIN SPEC-Dokument.

Des Weiteren wird festgelegt, welche Personen aus dem Betrieb am Beratungsprozess teilnehmen sollten. Das muss zumindest die Geschäftsführung sowie – falls vorhanden – die internen oder externen Informationssicherheitsbeauftragten sein. Ein dreistündiger Termin für die Aufnahme des IST-Zustandes wird vereinbart.

2. Die Erfassung des IST-Zustandes

Im zweiten Schritt führen Sie als IT-Dienstleistungsunternehmen den CyberRisiko-Check gemäß DIN SPEC 27076 durch. Die Durchführung kann in Präsenz, als Online-Meeting oder in einem hybriden Format stattfinden. Es ist wichtig sicherzustellen, dass die Geschäftsführung sowie die mit dem Schwerpunkt Informationssicherheit betrauten Personen oder externe Dienstleister:innen an dem Gespräch teilnehmen.

Sie erfragen nun Schritt für Schritt die 27 Anforderungen des CyberRisiko-Checks. Hierzu können die vorgegebenen Fragen verwendet werden. Sie sind so formuliert, dass sie auch für Betriebe ohne eigene IT-Expertise leicht verständlich sind und zum Austausch anregen. Die Erfassung des IST-Zustandes soll in Form eines Gesprächs erfolgen.

Bei Erfüllung einer Anforderung vergeben Sie die entsprechenden Punkte, die später den Statuswert des Unternehmens ergeben. Darüber hinaus dokumentieren Sie transparent stichpunktartig den Grund für das Erfüllen oder Nicht-Erfüllen einer Anforderung. Der Prozess zielt darauf ab, ein umfassendes Bild der aktuellen Sicherheitssituation des Unternehmens zu ermitteln und mögliche Schwachstellen zu identifizieren.

3. Die Auswertung und Erstellung des Ergebnisberichts

Als durchführender Dienstleister werten Sie nun die erhobenen Daten aus und erstellen einen individuellen Bericht gemäß den Vorgaben der DIN SPEC 27076. Auf der ersten Seite des Berichts werden die Ergebnisse des CyberRisiko-Checks für das Klein- oder Kleinstunternehmen (KKU) übersichtlich dargestellt.

Die Auswertung erfolgt anhand eines Spinnennetzdiagramms, das den Statuswert visualisiert und somit einen schnellen Überblick über die Sicherheitssituation des Unternehmens ermöglicht. Zudem werden die wichtigsten Handlungsempfehlungen klar und übersichtlich aufbereitet. Diese dienen als gezielte Leitlinien, um die relevantesten Sicherheitsrisiken zu minimieren und die IT-Sicherheit des KKU zu verbessern.

Als nächster Schritt wird ein erneuter Termin zur Präsentation der Ergebnisse vereinbart. In diesem Termin erläutern Sie dem KKU den Bericht, besprechen die gefundenen Ergebnisse und beantworten etwaige Fragen. Die Präsentation bietet dem KKU eine wertvolle Gelegenheit, die ermittelten Ergebnisse besser zu verstehen und sich mit Ihnen über die nächsten Schritte auszutauschen, um die Sicherheitsmaßnahmen gezielt umzusetzen.

4. Präsentation des Ergebnisberichts

Im abschließenden Schritt präsentieren Sie dem beratenen Unternehmen die Ergebnisse des CyberRisiko-Checks. Auch hier sollten wieder alle relevanten Personen – wie die Geschäftsführung – anwesend sein. Dabei erläutern Sie ausführlich den erstellten Ergebnisbericht und stehen für alle ausstehenden Rückfragen zur Verfügung. Der Bericht umfasst eine detaillierte Aufschlüsselung der erfüllten und nicht-erfüllten Anforderungen. Zudem werden die priorisierten Handlungsempfehlungen sowie sämtliche weiteren Empfehlungen zur Stärkung der IT- und Informationssicherheit präsentiert.

In den Anhängen des Berichts finden sich die ausführlichen Ergebnisse des Checks. Diese beinhalten sämtliche Handlungsempfehlungen und zusätzlich Informationen zu möglichen Fördermöglichkeiten, die dem Unternehmen bei der weiteren Umsetzung von IT- und Informationssicherheitsmaßnahmen helfen können.

Diese umfassende Präsentation ermöglicht dem beratenen Unternehmen eine fundierte Analyse der Cybersicherheitssituation und erleichtert die gezielte Planung und Umsetzung von Maßnahmen zur Risikominimierung. Die klaren Empfehlungen und transparenten Ergebnisse stellen sicher, dass das Unternehmen gut informierte Entscheidungen treffen kann, um seine IT-Infrastruktur zu schützen und sich vor Cyberbedrohungen zu wappnen.

Was ist der Anforderungskatalog und wie ist er anzuwenden?

Die 27 Anforderungen des CyberRisiko-Checks auf Basis der DIN SPEC 27076 basieren auf dem IT-Grundschutz des Bundesamtes für Sicherheit in der Informationstechnik (BSI) und verzichten bewusst auf akademische Vollständigkeit. Für kleine Unternehmen, die sich bisher noch kaum mit dem Thema Cybersicherheit auseinandergesetzt haben sind die Anforderungen als die grundlegendsten Maßnahmen zu verstehen, die nötig sind, um die gröbsten Einfallstore für Cyberangriffe in Betrieben zu schließen.

Um so verständlich und niedrigschwellig wie möglich vorzugehen, wurden offen gestellte Leitfragen für jede einzelne Anforderung entwickelt und getestet. Unternehmer:innen sollen dadurch nachdenken und ins Erzählen kommen. Dieses Vorgehen gewährt eine hohe Güte bei den gegebenen Antworten. Die Methode orientiert sich an einem semi-strukturierten Leidfadeninterview. Als Dienstleister, welcher die DIN SPEC 27076 anwendet, sollten Sie die Erhebung des IST-Zustandes unbedingt anhand der Leitfragen innerhalb des Anforderungskataloges vornehmen.

Die 27 Anforderungen bilden die Basis einer jeden Cybersicherheitsstrategie und sollten je nach Bedarf vollumfänglich im Unternehmen etabliert werden. Dabei werden folgende Themengebiete betrachtet:

In diesen Themengebieten findet sich eine unterschiedliche Anzahl an Anforderungen wieder. Neben den 22 **Basis-Anforderungen** verfügt der Katalog über fünf **Top-Anforderungen**. Diese sind essenziell, um ein höheres Niveau an Cybersicherheit zu erreichen und finden dadurch in der Wertung und dem zu erreichenden Statuswert eine besondere Gewichtung. Dazu zählen folgende Punkte:

Die Geschäftsführung muss die Gesamtverantwortung für die Informationssicherheit im Unternehmen tragen.

Organisation & Sensibilisierung

Alle Unternehmensangehörigen die die Unternehmens-IT nutzen, müssen mit der IT und dem Netzwerk sicher umgehen und verdächtige Vorkommnisse und Nachrichten (Phishing-Mails) identifizieren können. Hierfür bedarf es Einweisungen, Schulungen und Sensibilisierungsmaßnahmen.

Organisation & Sensibilisierung

Datensicherungen müssen in bestimmten Intervallen (branchenabhängig) durchgeführt werden.

Datensicherung

Updates für IT-Systeme und Software müssen installiert werden.

Patch- und Änderungsmanagement

Das Ausführen von aktiven Inhalten oder Makros (zum Beispiel in Tabellenkalkulationsprogrammen) muss standardmäßig deaktiviert sein.

Schutz vor Schadprogrammen

Wie funktioniert das Scoring-System?

Am Ende des CyberRisiko-Checks erhalten Unternehmen unter anderem auch einen **Statuswert**, der sich aus den Punktwerten der erfüllten und nicht-erfüllten Anforderungen zusammensetzt und wiedergibt, wie gut sie aufgestellt sind. Dieser Statuswert wird wie folgt errechnet:

Während Basis-Anforderungen entweder mit null Punkten (nicht erfüllt) oder einem Punkt (erfüllt) bewertet werden, gibt es für die Top-Anforderungen entweder minus 3 Punkte (nicht erfüllt) oder 3 Punkte (erfüllt). Eine Anforderung gilt insgesamt als erfüllt oder nicht erfüllt. Eine Abstufung von Punkten („teilweise erfüllt") ist nicht möglich. Falls eine teilweise Erfüllung besteht oder keine Aussage getroffen wurde, ist die Anforderung als „nicht erfüllt" zu werten. Rein rechnerisch kann somit ein negatives Ergebnis am Ende des CyberRisiko-Checks auftreten. Dies gilt es jedoch zu vermeiden. Der niedrigste auszuweisende Gesamtpunktewert für Unternehmen ist 0.

Falls bestimmte Anforderungen für ein Unternehmen als irrelevant angesehen werden, beispielsweise Anforderungen zum Arbeiten im Homeoffice, wenn keine Mitarbeiter im Unternehmen aus dem Homeoffice tätig sind, dürfen nachgelagerte Fragen zu diesem Aspekt nicht gestellt werden. Die für diese nicht relevanten Fragen theoretisch zu erreichenden Punkte müssen aus den maximal möglichen Punkten herausgerechnet werden. Der Maximalwert der erreichbaren Punkte wird somit dynamisch, abhängig davon, welche Anforderungen für das Unternehmen relevant sind. Im Ergebnisbericht wird kenntlich gemacht, welche Punkte aufgrund ihrer Irrelevanz nicht bewertet wurden.

Falls alle Anforderungen für das Unternehmen relevant sind und erfüllt werden, sind maximal 37 Punkte zu erreichen.

Wie sind die Handlungsempfehlungen zu verstehen?

Wird eine Anforderung nicht erfüllt so ist dem Unternehmen die passende Handlungsempfehlung mit dem Ergebnisbericht auszuhändigen. Handlungsempfehlungen verweisen auf Lösungsansätze. Bei der Entwicklung der Handlungsempfehlungen wurde vor allem darauf geachtet, auf verständliche Weise wiederzugeben **was** und **warum** etwas getan werden muss. Das „wie" wurde hierbei bewusst ausgeklammert. Dies gewährt eine branchenübergreifende Funktionalität des CyberRisiko-Checks.

Was gilt es beim Ergebnisbericht zu beachten?

Die umzusetzenden Handlungsempfehlungen erhält das Unternehmen mit der Aushändigung des Ergebnisberichts. Diesen müssen Sie dem beratenen Unternehmen vollumfänglich präsentieren. Hier soll das Unternehmen die Möglichkeit erhalten, Rückfragen gänzlich zu klären. Eine detaillierte Anleitung zur Erstellung des Ergebnisberichts findet sich in der DIN SPEC 27076 wieder.

Alternativ kann ab Herbst 2023 das vom Bundesamt für Sicherheit in der Informationstechnik eigens hierfür entwickelte Tool zur Anwendung gebracht werden. Achten Sie darauf, dass alle Merkmale des Ergebnisberichts tatsächlich angewandt werden. Essenziell ist die Unterschrift der Geschäftsleitung und Ihnen als durchführender Dienstleister.

Wie ist mit den Empfehlungen von Förderprogrammen umzugehen?

Sie als Dienstleistungsunternehmen sind dazu angehalten, Ihrer Kundschaft passende Fördertöpfe für die Durchführung des CyberRisiko-Checks einerseits und für die Umsetzung der daraus resultierenden Handlungsempfehlungen andererseits an die Hand zu geben. Diese Förderprogramme können sich aus Landes-, Bundesmitteln oder europäischen Fördertöpfen speisen. Eine Übersicht finden Sie beispielsweise auf der Webseite von mIT Standard sicher oder in der Förderdatenbank des Bundes.

Wie geht es nach der Präsentation des Ergebnisberichtes weiter?

Die ausgegebenen Handlungsempfehlungen können die Basis einer Folgeberatung bilden. Hierbei tritt die Expertise des Dienstleistungsunternehmens für das „wie" der Handlungsempfehlungen in Kraft. Klein- und Kleinstunternehmen erhalten somit einen transparenten Überblick über Produkte und Leistungen, welche durch den CyberRisiko-Check ausgegeben werden können. Als Dienstleistungsunternehmen kennen Sie Ihre

Kundschaft und können so mit Hilfe passgenauer Lösungsansätze eine sinnvolle Verbesserung der Cybersicherheit begleiten.

Welche Informationsmaterialien unterstützen den Beratungsprozess nach DIN SPEC 27076?

Für eine optimale Durchführung des CyberRisiko-Checks auf Basis der DIN SPEC 27076 können Sie auf verschiedene Begleitmaterialien des Projekts mIT Standard sicher zurückgreifen. Kleine Unternehmen werden durch **Checklisten** bei der Vorbereitung auf den CyberRisiko-Check wie auch bei der Nachbereitung unterstützt. Es ist zu empfehlen, diese vor bzw. nach der Durchführung an das Unternehmen auszugeben.

Außerdem steht eine **Broschüre** zur Verfügung, welche Unternehmen einen schnellen Überblick über die Vorteile und die Funktionsweise des CyberRisiko-Checks bietet.

Darüber hinaus werden ebenfalls zwei kurze Erklärvideos entwickelt. Eines richtet sich an kleine Unternehmen und soll den CyberRisko-Check kurz und knapp erläutern. Ein weiteres richtet sich an IT-Dienstleistungsunternehmen und erklärt im Stil eines Tutorials nochmals die Anwendung des CyberRisiko-Checks. Die Videos werden voraussichtlich im Herbst 2023 erscheinen.

Des Weiteren entwickelt das Bundesamt für Sicherheit in der Informationstechnik ein online nutzbares Tool, welches den Ergebnisbericht automatisiert und DIN SPEC 27076-konform ausgibt. Die Nutzung des Tools ist allerdings an bestimmte Anforderungen geknüpft. Hierbei wird vor allem die Expertise der Dienstleistungsunternehmen betrachtet. Das Tool soll im Herbst 2023 erscheinen.

Alle Begleitmaterialien finden sich zum kostenfreien Download auf www.mit-standard-sicher.de/informationsmaterialien

Wo finde ich weiterführende Informationen zur Umsetzung des CyberRisiko-Checks?

Die Grundlage zur Umsetzung des CyberRisiko-Checks ist das DIN SPEC-Dokument. Sie finden es unter diesem Link: www.mit-standard-sicher.de/informationsmaterialien

Was ist mIT Standard sicher?

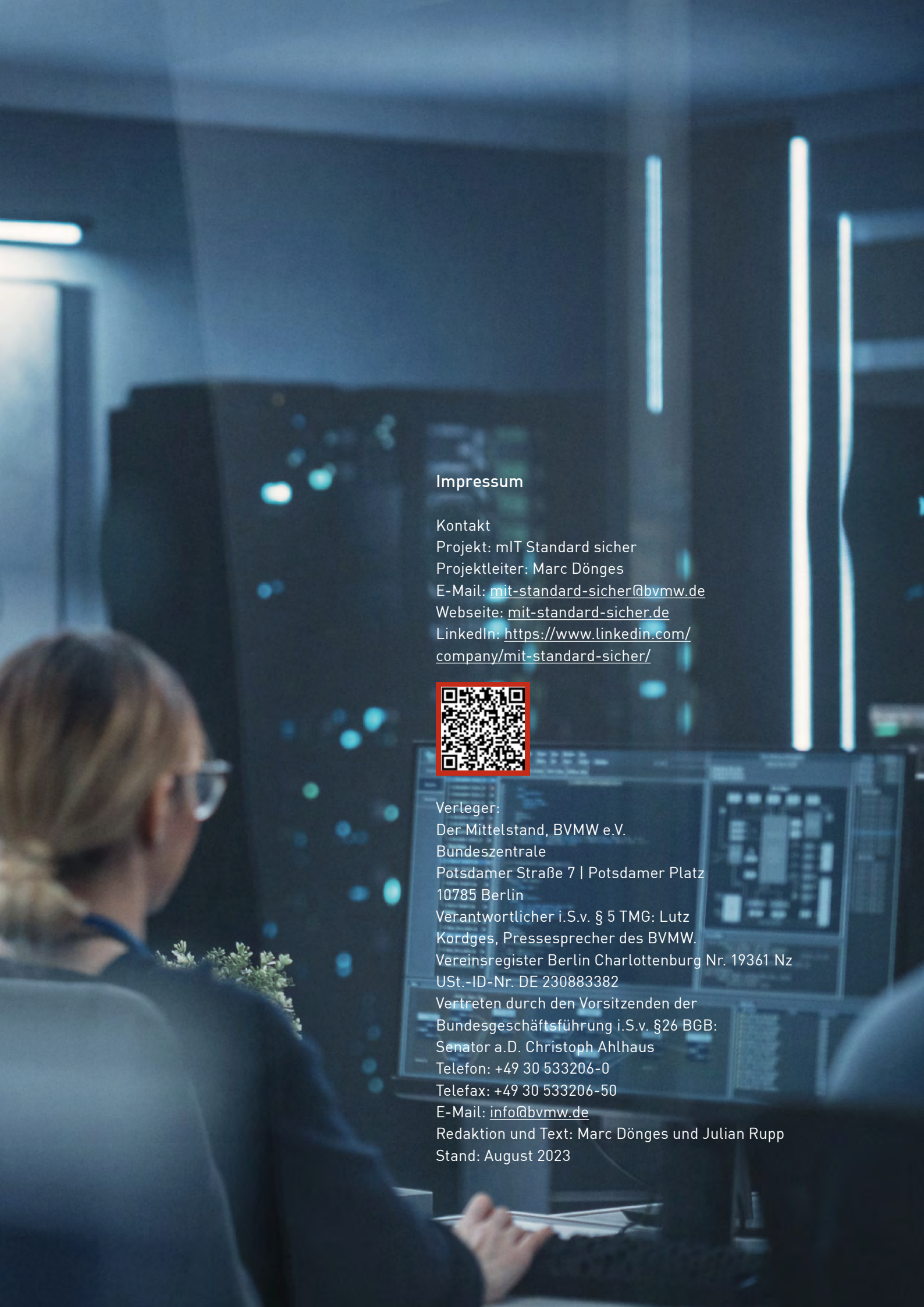
Das Projekt **mIT Standard sicher** dient der Entwicklung und Verbreitung eines neuen Beratungsstandards zur IT- und Informationssicherheit von Klein- und Kleinstunternehmen – der DIN SPEC 27076. Das Vorhaben wird von Der Mittelstand. BVMW e.V. geleitet und in Kooperation mit DIN e.V. umgesetzt.

mIT Standard sicher wird durch das Bundesministerium für Wirtschaft und Klimaschutz in der Initiative IT-Sicherheit in der Wirtschaft gefördert.

Was ist die Initiative IT-Sicherheit in der Wirtschaft?

Das Mittelstand-Digital Netzwerk bietet mit den Mittelstand-Digital Zentren, der Initiative IT-Sicherheit in der Wirtschaft und Digital Jetzt umfassende Unterstützung bei der Digitalisierung. Kleine und mittlere Unternehmen profitieren von konkreten Praxisbeispielen und passgenauen, anbieterneutralen Angeboten zur Qualifikation und IT-Sicherheit. Das Bundesministerium für Wirtschaft und Klimaschutz (BMWK) ermöglicht die kostenfreie Nutzung und stellt finanzielle Zuschüsse bereit.

Weitere Informationen finden Sie unter www.it-sicherheit-in-der-wirtschaft.de



Impressum

Kontakt
Projekt: mIT Standard sicher
Projektleiter: Marc Dönges
E-Mail: mit-standard-sicher@bvmw.de
Webseite: mit-standard-sicher.de
LinkedIn: https://www.linkedin.com/company/mit-standard-sicher/

Verleger:
Der Mittelstand, BVMW e.V.
Bundeszentrale
Potsdamer Straße 7 | Potsdamer Platz
10785 Berlin
Verantwortlicher i.S.v. § 5 TMG: Lutz Kordges, Pressesprecher des BVMW.
Vereinsregister Berlin Charlottenburg Nr. 19361 Nz
USt.-ID-Nr. DE 230883382
Vertreten durch den Vorsitzenden der Bundesgeschäftsführung i.S.v. §26 BGB:
Senator a.D. Christoph Ahlhaus
Telefon: +49 30 533206-0
Telefax: +49 30 533206-50
E-Mail: info@bvmw.de
Redaktion und Text: Marc Dönges und Julian Rupp
Stand: August 2023