mIT Standard sicher

IT-Sicherheit IN DER WIRTSCHAFT

Der CyberRisiko-Check: IT-Sicherheit einfach anpacken

IT-Sicherheitsberatung nach der neuen DIN SPEC 27076

Mittelstand-Digital

www.mit-standard-sicher.de

Gefördert durch:

Bundesministerium für Wirtschaft und Klimaschutz

aufgrund eines Beschlusses des Deutschen Bundestages

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.

Der Mittelstand. BVMW e.V. Bundesverband

DIN

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

Vorwort

Die Digitalisierung bietet enorme wirtschaftliche Potenziale für den Mittelstand. Doch erfolgreiche Digitalisierung kann nur gelingen, wenn sie keine neuen Verwundbarkeiten schafft. Dafür muss IT- und Informationssicherheit von vornherein mitgedacht werden – keine leichte Aufgabe für kleine Unternehmen. Gerade Betriebe mit bis zu 50 Beschäftigten sind hier oft auf externe Beratungsdienstleistungen angewiesen. Dazu kommt, dass bestehende Zertifizierungen und Standards oft die personellen, zeitlichen und finanziellen Ressourcen dieser Betriebe übersteigen.

Das ändert sich mit dem neuen Beratungsstandard DIN SPEC 27076: Dieser soll durch IT-Sicherheitsdienstleister angeboten werden und den branchenübergreifend zu beratenden Unternehmen in kürzester Zeit die gefährlichsten Schwachstellen aufzeigen, den Sicherheitsstand messbar machen und Handlungsempfehlungen ausgeben. Der Standard wurde mit besonderem Fokus auf Zeit- und Kosteneffizienz für kleine Betriebe entwickelt.

Die DIN SPEC 27076 wurde von 27 Mitgliedern des DIN SPEC-Konsortiums erarbeitet. Das Bundesamt für Sicherheit in der Informationstechnik (BSI) und Der Mittelstand. BVMW e.V. leiteten das Konsortium, welches aus zahlreichen IT-Dienstleistern und Transferstellen bestand. Die vollständige Liste aller Mitglieder ist dem DIN SPEC-Dokument zu entnehmen.

_Inhalt

Der Standard in Kürze

Was ist die DIN SPEC 27076?

Die DIN SPEC 27076 ist ein neuer Beratungsstandard zur kosten- und zeiteffizienten Verbesserung der IT- und Informationssicherheit in kleinen Unternehmen. Dieser CyberRisiko-Check wird durch IT-Dienstleister eingesetzt und schafft ein Angebot für eine branchenunabhängige und bedarfsgerechte Beratung von Betrieben mit bis zu 50 Beschäftigten.

Der CyberRisiko-Check definiert 27 Anforderungen, die kleine Betriebe erfüllen müssen, um die relevantesten Risiken zu minimieren und offene Einfallstore für Angreifer:innen zu schließen. Diese werden in kurzen Sitzungen, die auch digital stattfinden können, durch IT-Dienstleister in verständlicher Weise abgefragt und anschließend ausgewertet. Auf dieser Basis erhält das Unternehmen Handlungsempfehlungen, mit denen es die Verbesserung der IT-Sicherheit initiieren kann.

Während bisherige Standards oft zu umfangreich und teuer in der Umsetzung waren, verfolgt die DIN SPEC 27076 einen besonders bedarfsgerechten und praxistauglichen Ansatz. Sie bietet Orientierung, Vergleichbarkeit und Transparenz gleichermaßen für Klein- und Kleinstunternehmen sowie für IT-Dienstleistungsunternehmen.

Welche Vorteile bietet eine Beratung nach DIN SPEC 27076?

Der auf dem Standard basierende CyberRisiko-Check bietet kleinen Betrieben in kürzester Zeit einen Überblick über die IST-Situation der Cybersicherheit des eigenen Unternehmens. Die hierzu entwickelten 27 Anforderungen sind in reguläre sowie die besonders wichtigen Top-Anforderungen aufgeteilt. Durch letztere erfahren Unternehmen, welche Handlungsempfehlungen sie zuerst umsetzen sollten. Diese sind leicht verständlich formuliert und enthalten konkrete Maßnahmen sowie Empfehlungen, wie mit aktuellen Schwachstellen umgegangen werden sollte. Die Handlungsempfehlungen werden in Form eines Ergebnisberichtes ausgegeben.

Der Ergebnisbericht für das beratene Unternehmen fasst alles kurz und knapp zusammen:

- Den eigenen Risiko-Statuswert inkl. Visualisierung der Schwachpunkte
- Die priorisiert umzusetzenden Handlungsempfehlungen und die weiteren umzusetzenden Maßnahmen
- Übersicht über relevante Förderprogramme, die bei weiteren IT-Sicherheitsmaßnahmen unterstützen können

Der Bericht kann die Basis einer Beauftragung zur Umsetzung der Maßnahmen oder einer Folgeberatung durch ein IT-Dienstleistungsunternehmen bilden.

Mit welchen Aufwänden muss ich bei einer Beratung nach DIN SPEC 27076 rechnen?

Der Beratungsstandard ist in der Form konzipiert, als dass der Prozess so schlank wie möglich bleibt und vollständig online durchgeführt werden kann. Ein kurzes Vorgespräch durch den IT-Dienstleister ist nötig, um die IST-Aufnahme vorzubereiten, erste Daten aufzunehmen und zu klären, wer am Prozess teilnehmen sollte. Die IST-Aufnahme selbst soll - wie auch die Präsentation des Ergebnisberichts - jeweils nicht mehr als drei Stunden Zeit in Anspruch nehmen.

Die Kosten der Beratung nach DIN SPEC 27076 können zudem gefördert werden. Eine Übersicht von Fördermöglichkeiten finden Sie auf www.mit-standard-sicher.de.

Wie geht es nach einer Beratung weiter?

Mit dem Ergebnisbericht inkl. Statuswert und aufgezeigten Schwachpunkten können Betriebe mit der richtigen Unterstützung ihre individuellen Handlungsempfehlungen anpacken. Nach der Umsetzung lohnt sich auch eine Wiederholung des CyberRisiko-Checks – hiermit kann geprüft werden, ob sich der eigene Statuswert verbessert hat.

Die DIN SPEC 27076 ist besonders zeit- und kosteneffizient gestaltet und bietet daher den idealen Einstiegspunkt zum Anpacken der IT-Sicherheit im Betrieb. Das bedeutet aber auch, dass nur das absolute Minimum an Anforderungen abgeprüft wird. IT-Sicherheit ist ein Prozess, den es langfristig zu verfolgen gilt. Das bedeutet, dass auch ein Erreichen des Maximalwertes keine vollumfängliche Sicherheit garantiert. Auch wenn alle Handlungsempfehlungen der DIN SPEC 27076 umgesetzt sind, gilt es die aktuellen Risiken weiterhin aufmerksam zu verfolgen und das Thema Informationssicherheit in alle Bereiche des Unternehmens hineinzutragen. In diesem Fall empfiehlt es sich, dranzubleiben und weiterführende Zertifizierungen anzugehen.

Der CyberRisiko-Status dient nicht nur dem eigenen Unternehmen, sondern kann auch an Kund:innen, Auftraggeber:innen, Investor:innen, sowie Banken, Versicherungen und Fördergeber:innen kommuniziert werden. Durch die Anwendung der DIN SPEC 27076 kann ein Qualitätsstandard nachgewiesen und so ein Vorteil am Markt erzielt werden.

Ablauf einer IT-Sicherheitsberatung

Eine IT-Sicherheitsberatung nach DIN SPEC 27076 geschieht in vier einfachen Schritten:

1. Das Gespräch zur Erstinformation

Das Dienstleistungsunternehmen informiert das zu zu beratende Unternehmen über den Ablauf. Dies kann via Online-Meeting, Telefongespräch oder in Präsenz erfolgen. Hierbei werden bereits erste Unternehmensdaten erhoben, welche später in die Berichterstattung miteinfließen. Weiterhin erhält das zu zu beratende Unternehmen Informationen darüber, welche Dokumente für einen effizienten Zeitablauf vorbereitet werden und welche Personen aus dem Betrieb am Prozess teilnehmen sollten. Es wird ein dreistündiger Termin für die Aufnahme des IST-Zustandes vereinbart.

2. Die Aufnahme des IST-Zustandes

Im zweiten Schritt führt das IT-Dienstleistungsunternehmen den CyberRisiko-Check nach DIN SPEC 27076 durch. Die Durchführung kann in Präsenz, via Online-Meeting oder als hybrides Format stattfinden. Es gilt sicherzustellen, dass die Geschäftsführung sowie die mit dem Themenschwerpunkt Informationssicherheit betrauten Personen oder externen Dienstleister:innen am Gespräch teilnehmen.

Der durchführende IT-Dienstleister fragt Schritt für Schritt die 27 Anforderungen des CyberRisiko-Checks ab. Das geschieht durch vorgegebene Fragen, die verständlich gehalten sind und zum Erzählen anregen. Die Aufnahme des IST-Zustands ist als Gespräch angelegt – es bleibt immer Zeit für die Klärung von Rückfragen. Bei Erfüllen der Anforderungen vergibt der IT-Dienstleister die jeweiligen Punkte, die sich später zum Statuswert des Unternehmens summieren. Er notiert außerdem transparent den Grund für ein Erfüllen oder Nicht-Erfüllen einer Anforderung.

3. Die Auswertung und Erstellung des Ergebnisberichts

Dieser Punkt wird vollständig vom durchführenden Dienstleister übernommen. Er wertet die erhobenen Daten aus und erstellt einen individuellen Bericht nach Vorgabe der DIN SPEC 27076. Auf der ersten Seite des Berichts erhält das Klein-, oder Kleinstunternehmen die Ergebnisse des CyberRisiko-Checks kompakt dargestellt. Dies geschieht über ein Spinnennetzdiagramm, sowie den ausgewiesenen Statuswert. Weiterhin werden die wichtigsten umzusetzenden Handlungsempfehlungen dort sichtbar aufbereitet. Ein erneuter Termin zur Präsentation der Ergebnisse wird vereinbart.

4. Die Präsentation der Ergebnisse

Im letzten Schritt präsentiert der Dienstleister dem beratenen Unternehmen die Ergebnisse, erläutert den Ergebnisbericht und beantwortet die ausstehenden Rückfragen. Er geht auf die einzelnen erfüllten und nicht-erfüllten Anforderungen ein und zeigt die priorisierten wie auch alle weiteren Handlungsempfehlungen auf. In den Anhängen des Berichts finden sich die detaillierten Ergebnisse inklusive aller Handlungsempfehlungen und Fördermöglichkeiten zur weiteren Umsetzung von IT- und Informationssicherheitsmaßnahmen.

mIT Standard sicher

Die sechs Themenbereiche

Organisation & Sensibilisierung

Betrachtet das managementseitige Engagement, sowie die Kompetenzverteilung und Sensibilisierung von Mitarbeitenden

Identitäts- und Berechtigungsmanagement

Regelt die Zugangs- und Zutrittsberechtigungen für physische und virtuelle Räumlichkeiten.

Datensicherung

Beschreibt Zuständigkeit, Umfang, Häufigkeit & Verfügbarkeit von Daten und deren BackUps.

Patch- und Änderungsmanagement

Prüft die Verfügbarkeit und Aktualität von eingesetzter Hard- und Software.

Schutz vor Schadprogrammen

Behandelt die Haupteinfallstore für Schadsoftware.

IT-Systeme und Netzwerke

Definiert die Sicherheitsmechanismen hinter der eingesetzten Informations- und Kommunikationstechnik.

Der richtige Einsatz des Standards für IT-Dienstleister

Der Beratungsprozess für IT-Dienstleister

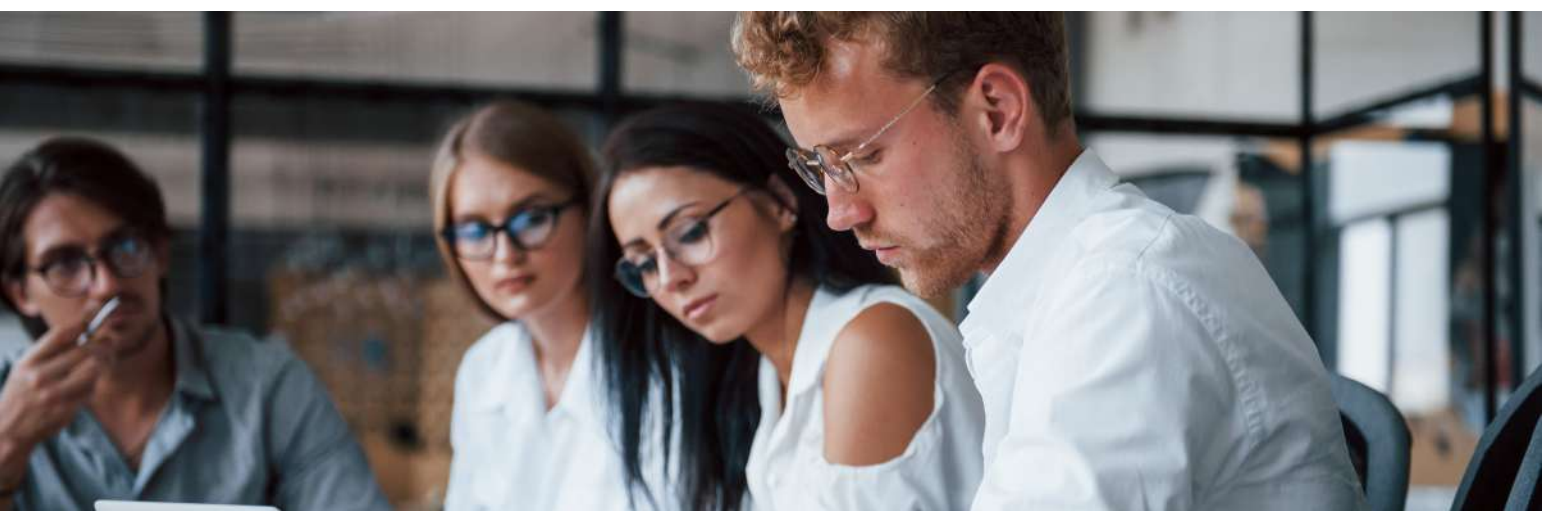
Eine korrekte Anwendung des Standards durch IT-Sicherheitsdienstleister wird durch die Beschreibung des Prozesses innerhalb der DIN SPEC 27076 gewährleistet. Neben den Anforderungen, welche ein IT-Dienstleistungsunternehmen erfüllen sollte, erfährt das beratende Unternehmen dort, wie der Gesamtprozess aufgebaut und eine korrekte Durchführung auf Basis der zur Verfügung stehenden Werkzeuge sichergestellt werden kann.

Der IT- und Informationssicherheitsberatung nach DIN SPEC 27076 liegt ein klarer Ablauf zu Grunde. Dieser beginnt mit der Geschäftsanbahnung und einem Gespräch, in welchem Erstinformationen zum Prozess der IST-Aufnahme, bzw. des CyberRisiko-Checks vermittelt werden. Hier muss der zeitliche Rahmen definiert und erste Daten aufgenommen werden. Welche Dokumente sollte das zu beratende Unternehmen vorbereiten und mitbringen? Wer aus dem Betrieb soll in den Prozess eingebunden werden? All das muss im Erstgespräch geklärt werden.

Nach der Erhebung des IST-Zustandes, für welche ein dreistündiger Termin geblockt wurde, erhält das beratene Unternehmen in einem vorher bestimmten Zeitraum den Ergebnisbericht mit dem ausgewiesenen CyberRisiko-Status. Zudem zeigt der kompakte Ergebnisbericht die nicht erfüllten Anforderungen in aller Deutlichkeit auf und weist das Unternehmen auf die Handlungsbedarfe hin. Der ausführliche Bericht enthält weitere, detaillierte Handlungsempfehlungen.

Die DIN SPEC 27076 verlangt zudem, dass die zu beratenden Unternehmen auf Fördermöglichkeiten hingewiesen werden. Dazu zählen sowohl Förderprogramme mit denen die Beratung selbst gefördert bzw. kofinanziert werden kann, als auch Fördermittel, die Unternehmen im Anschluss für die weitere Verbesserung ihres IT-Sicherheitsniveaus nutzen können. Es gilt, die kommunalen, Landes-, Bundes- und EU-Fördermittel zu prüfen.

Die Anwendung der DIN SPEC 27076 kann nach Umsetzung einiger – im besten Falle aller - Handlungsempfehlungen wiederholt werden, um Verbesserungen im Statuswert sichtbar zu machen. Erfüllt ein beratenes Unternehmen alle Anforderungen, ist es Notwendig, es für weiterführende bzw. anspruchsvollere Zertifizierungen zu sensibilisieren.



Die Bestandteile des Anforderungskatalogs

Anforderungen

Die Anforderungen bezeichnen einen Zustand, den ein Unternehmen erreichen muss, um das vertretbare Minimum an IT- und Informationssicherheit sicherzustellen. Das Dienstleistungsunternehmen muss stichpunktartig festhalten, weshalb eine Anforderung als erfüllt oder nicht erfüllt gewertet wurde. Eine erste Auskunft hierüber ist innerhalb der Ergebnispräsentation zu erteilen. Während der IST-Aufnahme muss das durchführende Dienstleistungsunternehmen keine Stellung zu den Anforderungen nehmen. Trifft eine Anforderung auf ein Unternehmen nicht zu, da es beispielsweise keine Mitarbeitenden im Homeoffice beschäftigt, so entfällt diese Anforderung für das zu prüfende Unternehmen. Damit verändert sich auch der maximal zu erreichende Status-Wert.

Leitfragen

Die IST-Erhebung ist explizit nicht als strikte Abfrage der Anforderungen, sondern als Gespräch angelegt. Jeder Anforderung ist eine Leitfrage zugeordnet, um IT-Dienstleistungsunternehmen dabei zu unterstützen verständliche und zielgerichtete Fragen zu stellen. Die Fragen sind meist offen formuliert und sollen das Gegenüber ins Erzählen bringen. Auf Basis dieser Erzählungen hat der Dienstleister einzuschätzen, ob die Anforderung erfüllt wurde oder nicht.

Handlungsempfehlungen

Die Handlungsempfehlungen bieten einfach und kompakt formulierte Anweisungen um einen bisher nicht erfüllten Zustand an Informationssicherheit zu erreichen. Die Handlungsempfehlungen beschränken sich auf das „Was muss geändert werden?“ und „Warum muss es geändert werden?“ und werden am Ende mit dem Bericht ausgegeben.

Statuswert

Jeder der 27 Anforderungen ist ein Punktwert zugeordnet. Diese teilen sich in 5 Top- und 22 reguläre Anforderungen auf. Die Top-Anforderungen tragen zu einer erheblichen Erhöhung des IT-Sicherheitsniveau bei und werden dementsprechend entweder mit +3 Punkten Erfüllung bzw. -3 Punkten bei Nichterfüllung gewertet. Reguläre Anforderungen werden mit +1 oder 0 Punkten bewertet. Eine Abstufung innerhalb der Punktevergabe bzw. Teilerfüllung einzelner Anforderungen ist nicht möglich.

Zudem sind einige Anforderungen in mehrere Komponenten aufgeteilt. So gilt eine Anforderung erst als erfüllt, wenn bspw. „02-1“, „02-2“ und „02-3“ positiv bewertet wurden. Der maximal zu erreichende Status-Wert ist 37. Rein rechnerisch ist ein negatives Ergebnis am Ende möglich. Das Dienstleistungsunternehmen muss in diesem Fall den Status-Wert 0 im Ergebnisbericht ausweisen.

Die detaillierten Informationen finden in der veröffentlichen DIN SPEC 27076 selbst:

Testimonials

„Da es bisher für ein auf IT-Dienstleistungen und Software spezialisiertes Unternehmen unserer Größe (10 Mitarbeiter), aus Aufwands- und Kostengründen in betriebswirtschaftlicher Hinsicht nicht sinnvoll war, eine ISO 27001 Zertifizierung anzustreben, hießen wir die Möglichkeit der DIN SPEC 27076 äußerst willkommen. Durch den erfolgreichen Abschluss der Befragung und Risikoanalyse haben wir jetzt die Möglichkeit, unseren Kunden zu zeigen, dass IT-Security und Datensicherheit in unserem Hause sichergestellt sind und höchsten Stellenwert haben."

Dietmar Franz
Geschäftsführer

HVBEST Event-Service GmbH

„Der Prozess zur Analyse unserer IT-Sicherheit war sehr aufschlussreich und hat einige Schwachstellen ans Licht gebracht- bei wirklich überschaubarem Aufwand."

Sebastian Bosse
Geschäftsführung

Biobote Emsland GmbH & Co. KG, Haren

mIT Standard sicher

Kontakt

Projekt: mIT Standard sicher

Projektleiter: Marc Dönges, Der Mittelstand, BVMW e.V.

E-Mail: mit-standard-sicher@bvmw.de

Webseite: mit-standard-sicher.de

LinkedIn:

https://www.linkedin.com/company/mit-standard-sicher/

Impressum

Herausgeber:

Der Mittelstand, BVMW e.V.
Bundeszentrale
Potsdamer Straße 7, 10785 Berlin

Verantwortlicher i.S.v. § 5 TMG: Harald Ehren,
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: Markus Jerger

Telefon: +49 30 533206-0
Telefax: +49 30 533206-50
E-Mail: info@bvmw.de

Redaktion und Text: Marc Dönges und Julian Rupp

**Druckerei: MÖLLER PRO MEDIA GmbH,
Zeppelinstr. 6, 16356 Ahrensfelde**

Stand: März 2023

mIT Standard sicher

BVMW-Bundeszentrale
Potsdamer Straße 7
10785 Berlin

+49 171 812 7417

mit-standard-sicher@bvmw.de
www.mit-standard-sicher.de