Cyber-Security-Standards für den Mittelstand

Innovative VdS-Systemlösungen für Informationssicherheit und Datenschutz

VdS Cyber Security

Informationssicherheit und Datenschutz in KMU realisieren

VdS gehört zu den weltweit renommiertesten Institutionen für die Unternehmenssicherheit mit den Schwerpunkten Brandschutz, Security, Naturgefahrenprävention und Cyber-Security. Die Dienstleistungen umfassen Risikobeurteilungen, Prüfungen von Anlagen, Zertifizierungen von Produkten, Firmen und Fachkräften sowie ein breites Bildungsangebot.

Das VdS-Gütesiegel genießt einen ausgezeichneten Ruf in Fachkreisen und bei Entscheidern. Zu den Kunden zählen Industrie- und Gewerbebetriebe aller Branchen, international führende Hersteller und Systemhäuser, kompetente Fachfirmen sowie risikobewusste Banken und Versicherer.

Inhalt

Sehr geehrte Damen und Herren,

die Implementierung eines angemessen IT-Sicherheitsniveaus in Unternehmen hat verschiedene Facetten: Neben der nach wie vor steigenden Bedrohung durch Cyber-Kriminalität sind es vor allem die gestiegenen gesetzlichen Anforderungen für Datenschutz, die viele Unternehmen vor große Herausforderungen stellen. Im Fokus steht insbesondere die Datenschutz-Grundverordnung – kurz DSGVO –, mit der europaweit einheitliche Regelungen für die Verarbeitung von personenbezogenen Daten geschaffen wurden.
Die DSGVO ist noch längst nicht in allen Unternehmen umgesetzt – vor allem dem Mittelstand fehlen häufig die personellen, finanziellen und organisatorischen Kapazitäten, um die geforderten Regelungen angemessen abzubilden.

Genauso gravierend ist die IT-Sicherheitslage, die viel zu oft durch einen unzureichenden Schutz gekennzeichnet ist und Cyber-Kriminellen einfache Wege zum Datendiebstahl bzw. -missbrauch offen lässt. Dabei ließen sich diese Lücken in den meisten Fällen durch unkomplizierte Maßnahmen schließen, die neben der eigenen IT-Sicherheit noch weitere Vorteile bieten. So bildet ein nachgewiesener IT-Schutzgrad die sinnvolle Basis, um IT-Restrisiken beispielsweise mit Cyber-Policen zu versichern und das Risikomanagement im Unternehmen zu stärken. Die Voraussetzung dafür muss nicht zwangsläufig der international anerkannte ISO-27000er-Standard sein, der in kleineren und mittelständischen Unternehmen ohnehin zu hohe Ressourcen bindet. Vielmehr geht es darum, ein individuell abgestimmtes IT-Schutzniveau zu erreichen, das von Versicherern als valides Risikoprofil akzeptiert wird.

Eine ausgezeichnete Grundlage für den Mittelstand sind die prämierten Richtlinien der VdS-10000er-Reihe, die wir Ihnen in dieser Broschüre detailliert vorstellen möchten. Die Richtlinien sind auf die Möglichkeiten und Bedürfnisse von mittelständischen Unternehmen zugeschnitten und beschreiben Anforderungen sowohl zur Implementierung von Informationssicherheit von KMU als auch zur Umsetzung der DSGVO. Darüber hinaus stehen mehrere Verfahrensrichtlinien zur Verfügung, die praxisnah bei der Realisierung eines angemessenen IT-Sicherheitsniveaus unterstützen. Eine wichtige Stellschraube für IT-Sicherheit bzw. Datenschutz bilden die Managementsysteme, die in den Richtlinien der VdS-10000er-Reihe deshalb einen hohen Stellenwert haben.

Wir freuen uns über Ihr Interesse und stehen Ihnen als kompetenter Partner für IT-Sicherheit und Datenschutz gerne zur Seite.

Ihr
Thomas Adenauer
VdS-Abteilungsleiter Cyber Security

Richtlinien VdS 10000

Informations-
sicherheit
für KMU

Die Richtlinien VdS 10000 decken systematisch alle relevanten Handlungsfelder für ein angemessenes IT-Sicherheitsniveau ab.

Im Zeitalter der Digitalisierung ist die Informationssicherheit ein wesentlicher Eckpfeiler für ein verantwortungsvolles Risikomanagement. Eine gut organisierte Informationssicherheit muss jedoch bei den individuellen Voraussetzungen der Unternehmen ansetzen – sonst wird sie zu teuer oder ist nicht umsetzbar. Die Basis dafür schaffen die Richtlinien VdS 10000.

IT-Sicherheit für den Mittelstand.
In den Richtlinien VdS 10000 sind die Anforderungen für ein angemessenes IT-Sicherheitsniveau beschrieben. Die Richtlinien richten sich speziell an kleinere und mittelständische Unternehmen (KMU), umfassen einen praktikablen Maßnahmenkatalog für ein Managementsystem und verfolgen systematisch das Ziel, den Informationssicherheitsstatus eines Unternehmens zu verbessern. Mit gut verständlichen Formulierungen, kategorisiert in MUSS-, KANN- und SOLLTE-Anforderungen in den Handlungsfeldern Organisation, Technik, Prävention und Management, lassen sich schnell Maßnahmen umsetzen, die das Schutzniveau in kürzester Zeit erhöhen. Zusätzlich kann eine Zertifizierung nach VdS 10000 auch jederzeit der Einstieg in die ISO-27000er-Reihe sein, die VdS ebenfalls durch sein Zertifizierungsportfolio abdeckt.

Richtlinien VdS 10000 setzen an der unternehmerischen Praxis an.
Die Richtlinien unterscheiden nach einer entsprechenden Risikoanalyse im Wesentlichen zwischen kritischen und unkritischen Ressourcen (Systeme, Prozesse, Dienste und Netzwerke). Für die unkritischen Ressourcen gilt, dass ein Basisschutz ausreicht. Beispielsweise genügen hier u. a. regelmäßige Updates, Netzwerkprotokollierung, Schutz vor Schadsoftware und Zugriffsbeschränkungen. Bei den kritischen Ressourcen müssen zusätzliche Maßnahmen getroffen werden, wie die Bestimmung von tolerierbaren Ausfallzeiten und die Schaffung von Redundanzen, um die Anforderungen der Richtlinien zu erfüllen. Alle Maßnahmen sind eingebettet in eine belastbare Struktur, die es u. a. ermöglicht, geänderte Rahmenbedingungen zu identifizieren und ggf. im Sinne des PDCA-Zyklus Veränderungen zu initiieren. Um das VdS-10000-Zertifikat zu erlangen, prüfen Auditoren die erforderliche Dokumentation und überzeugen sich vor Ort von der angemessenen Umsetzung der Maßnahmen.

Branchenneutral und von vielen Versicherungsunternehmen akzeptiert.
Durch den generischen Aufbau sind die Richtlinien branchenunabhängig anwendbar. In der Konsequenz bieten die Richtlinien VdS 10000 damit auch eine ausgezeichnete Grundlage, um beispielsweise in öffentlichen Verwaltungen, institutionellen Einrichtungen und Organisationen sowie in Verbänden und Vereinen den IT-Sicherheitsstandard auf ein passendes Schutzniveau zu heben. Weiterer Vorteil einer Zertifizierung nach VdS 10000 ist die Akzeptanz durch viele Versicherer. Denn Versicherungsunternehmen haben ein hohes Vertrauen in VdS-Bewertungen – ein System, das sich nicht zuletzt im Brandschutz seit mehr als 100 Jahren bewährt. Deshalb kann ein VdS-Zertifikat ggf. eine Einzelfallbetrachtung beim Kunden ersetzen und die Auslagerung von Restrisiken z. B. über eine Cyber-Police erleichtern.

100
JAHRE

Versicherungsunternehmen haben ein hohes Vertrauen in VdS-Bewertungen – ein System, das sich nicht zuletzt im Brandschutz seit mehr als 100 Jahren bewährt.

Richtlinien VdS 10010

Wegweiser zur Umsetzung der DSGVO

Mit der Veröffentlichung der Richtlinien VdS 10010 hat VdS ein weiteres wichtiges Handlungsfeld im Bereich Cyber-Security erschlossen, das eine hohe gesetzliche Relevanz hat: den Datenschutz. Diese Richtlinien beschreiben einen praktikablen Weg zur Umsetzung der Anforderungen, die sich aus der europäischen Datenschutz-Grundverordnung (DSGVO) ergeben.

Gesetzliche Anforderungen für Datenschutz verschärft.
Seit 25. Mai 2018 gilt EU-weit die Datenschutz-Grundverordnung – kurz DSGVO –, mit der einheitliche Regelungen für die Verarbeitung und Speicherung von personenbezogenen Daten geschaffen wurden. Eine wesentliche Veränderung zur bisherigen Rechtslage ist die sogenannte Rechenschaftspflicht der verantwortlichen Stelle. Jede Behörde und jedes Unternehmen, die personenbezogene Daten verarbeiten, müssen jederzeit und vollständig nachweisen können, dass sie sämtliche Vorgaben der DSGVO einhalten. Dazu wird ein Datenschutzmanagement notwendig, das als Führungssystem klar definierte Leit- und Richtlinien, Prozesse, Rollen und Verantwortlichkeiten sowie Kontrollen offenlegt. Hinzu kommen die bereits bestehenden Anforderungen an prüffähige Dokumentationen und klare Kommunikationsregeln.

VdS-Richtlinien rücken Datenschutzmanagement in den Fokus.
Vor diesem Hintergrund hat VdS mit den Richtlinien VdS 10010 einen Standard geschaffen, der auch kleineren und mittleren Unternehmen einen praktikablen Weg zur Umsetzung der DSGVO aufzeigt. Damit können die rechtlichen, organisatorischen und technischen Anforderungen der DSGVO strukturiert und mit möglichst geringem Aufwand realisiert werden. Im Kern beschreiben die Richtlinien VdS 10010 ein auditierungs- und zertifizierungsfähiges Datenschutzmanagementsystem, von dem neben den KMU auch größere, mittelständisch geprägte Unternehmen mit flachen Hierarchiestrukturen profitieren können. Vom Aufbau sind die Richtlinien VdS 10010 den Cyber-Security-Standards VdS 10000 sehr ähnlich. Beide Richtlinien erleichtern den Aufbau eines Datenschutzmanagementsystems, das idealerweise als Ansatz für ein integriertes Managementsystem genutzt wird.

Maßgebliche Inhalte der Richtlinien VdS 10010.
Neben Regelungsinhalten zum Datenschutzbeauftragten, Datenschutzmanager und Datenschutzteam spielt die Leitlinie zum Datenschutz eine herausragende Rolle. Darin bekennt und verpflichtet sich das Topmanagement zum Datenschutz. Zudem werden die Ziele und der Stellwert des Datenschutzes im Unternehmen definiert sowie die Konsequenzen einer Nichtbeachtung festgelegt. Unterstützende Richtlinien zum Datenschutz werden individuell auf das

Unternehmen zugeschnitten. Diese müssen jedoch die Grundsätze der DSGVO adressieren: Rechtmäßigkeit, Zweckbindung, Treu und Glauben, Verhältnismäßigkeit, Transparenz, Datenminimierung, Richtigkeit, Speicherbegrenzung, Vertraulichkeit, Verfügbarkeit und Integrität sowie Nachweisbarkeit. Daneben muss ein Informationssicherheitsmanagement mit dem Scope „personenbezogene Daten“ bestehen. Des Weiteren fordern die Richtlinien VdS 10010 Verfahren, um die von der DSGVO geforderten Prozesse u.a. für die Wahrung von Betroffenenrechten, die Sensibilisierung von Mitarbeitern, das Erstellen und Pflegen des Verarbeitungsverzeichnisses, das Vertragsmanagement insbesondere bei Auftragsverarbeitung, die Durchführung der Risikoanalyse und Datenschutzfolgeschätzung sicherzustellen.

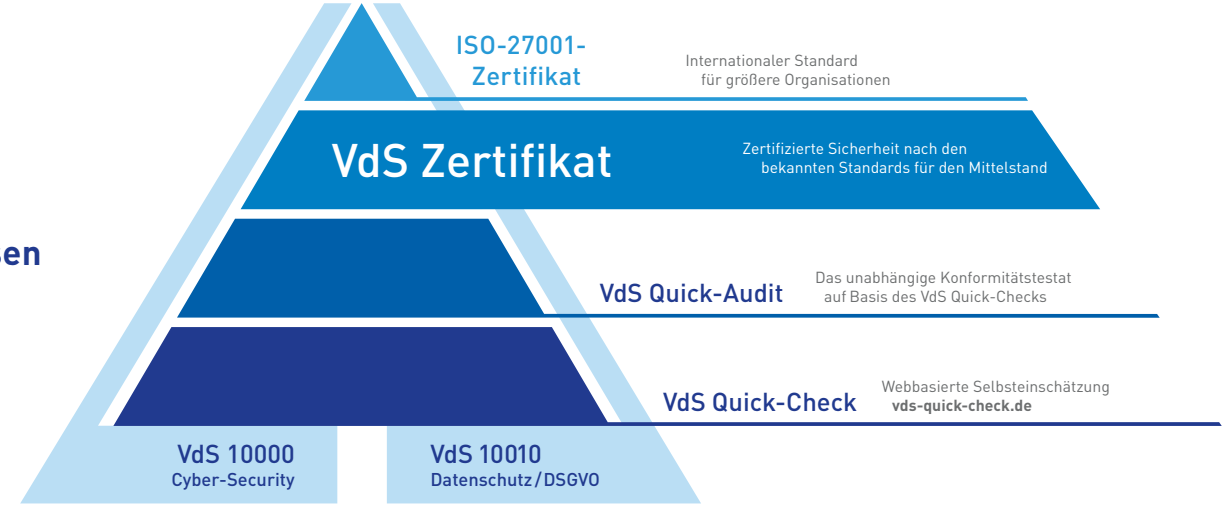
Die Richtlinien VdS 10010 setzen die Anforderungen der Datenschutz-Grundverordnung (DSGVO) um.

Management-systeme für KMU

VdS-zertifizierte Sicherheit

〉 Ein konsequentes Informations-managementsystem nach VdS-Richtlinien setzt erhebliche Synergien frei.

Informationssicherheit und Datenschutz haben einen gemeinsamen Nenner: In beiden Aufgaben spielen die Organisation und das Informations-managementsystem eine Schlüsselrolle.
Bei einer Zertifizierung nach VdS-Richtlinien lassen sich deshalb erhebliche Synergien realisieren.



Der VdS-Rundum-Schutz für den Mittelstand.
Eine Zertifizierung nach VdS 10000 bestätigt, dass Ihre Informationssicherheit vollumfänglich den Anforderungen der zugrunde liegenden Richtlinien entspricht und Ihr Unternehmen angemessen vor den wichtigsten Gefahren geschützt ist. Die Anforderungen sind speziell auf den Mittelstand zugeschnitten und sind so konzipiert, dass organisatorische und finanzielle Handlungsspielräume erhalten bleiben. Eine gleichzeitige Implementierung von Managementsystemen in den Bereichen der Informationssicherheit und des Datenschutzes verspricht darüber hinaus hohe Synergieeffekte, da einige personelle und organisatorische Maßgaben für beide Handlungsfelder gleichzeitig bedient werden können. Deshalb lohnt es sich, die ohnehin notwendigen Instrumente für IT-Sicherheit und Datenschutz parallel zu implementieren. In der Konsequenz werden in den Richtlinien VdS 10002 Verfahren beschrieben, die zu einer Zertifizierung von Managementsystemen für KMU (Informationssicherheit und Datenschutz) führen.

Kompetente Unterstützung bei der Umsetzung.
Nicht alle Unternehmen verfügen über die Kapazitäten und das Fachpersonal (z. B. IT-Abteilung, Informationssicherheitsverantwortliche), um die empfohlenen Maßnahmen in einer angemessenen Zeit umzusetzen. Denn selbstverständlich kann die Vorbereitung auf eine VdS-Zertifizierung auch inhouse geplant und modelliert werden. Dazu wurden die VdS-Richtlinien in einer verständlichen Sprache formuliert, die eine systematische Abarbeitung der erforderlichen Maßnahmen ermöglicht.

Falls jedoch keine entsprechenden Ressourcen zur Verfügung stehen, können Unternehmen auch die Hilfe von VdS-anerkannten Beratern in Anspruch nehmen. Nach Abschluss aller Vorbereitungen prüfen unsere Auditoren die notwendige Dokumentation und überzeugen sich vor Ort von der richtigen Umsetzung aller Maßnahmen. Der zeitliche Aufwand hängt dabei von der Unternehmensgröße ab. Die Gültigkeitsdauer des VdS-Zertifikats beträgt drei Jahre, wobei jährliche (im Umfang reduzierte) Re-Audits vorgesehen sind.

VdS Quick-Audit

Neutrale und unabhängige Expertise

Das Testat des VdS-Quick-Audits ist ein wertvoller Baustein bei der Vorsorge zur Erfüllung der Anforderungen an die Informationssicherheit.

Basierend auf dem Ergebnis eines Quick-Checks untersuchen unsere Auditoren die getroffenen Maßnahmen zur Cyber-Security in Ihrem Unternehmen vor Ort. Das Quick-Audit ist insbesondere für kleine Unternehmen geeignet und wird in der Regel einen Tag dauern.

Testat für Informationssicherheit und Datenschutz.

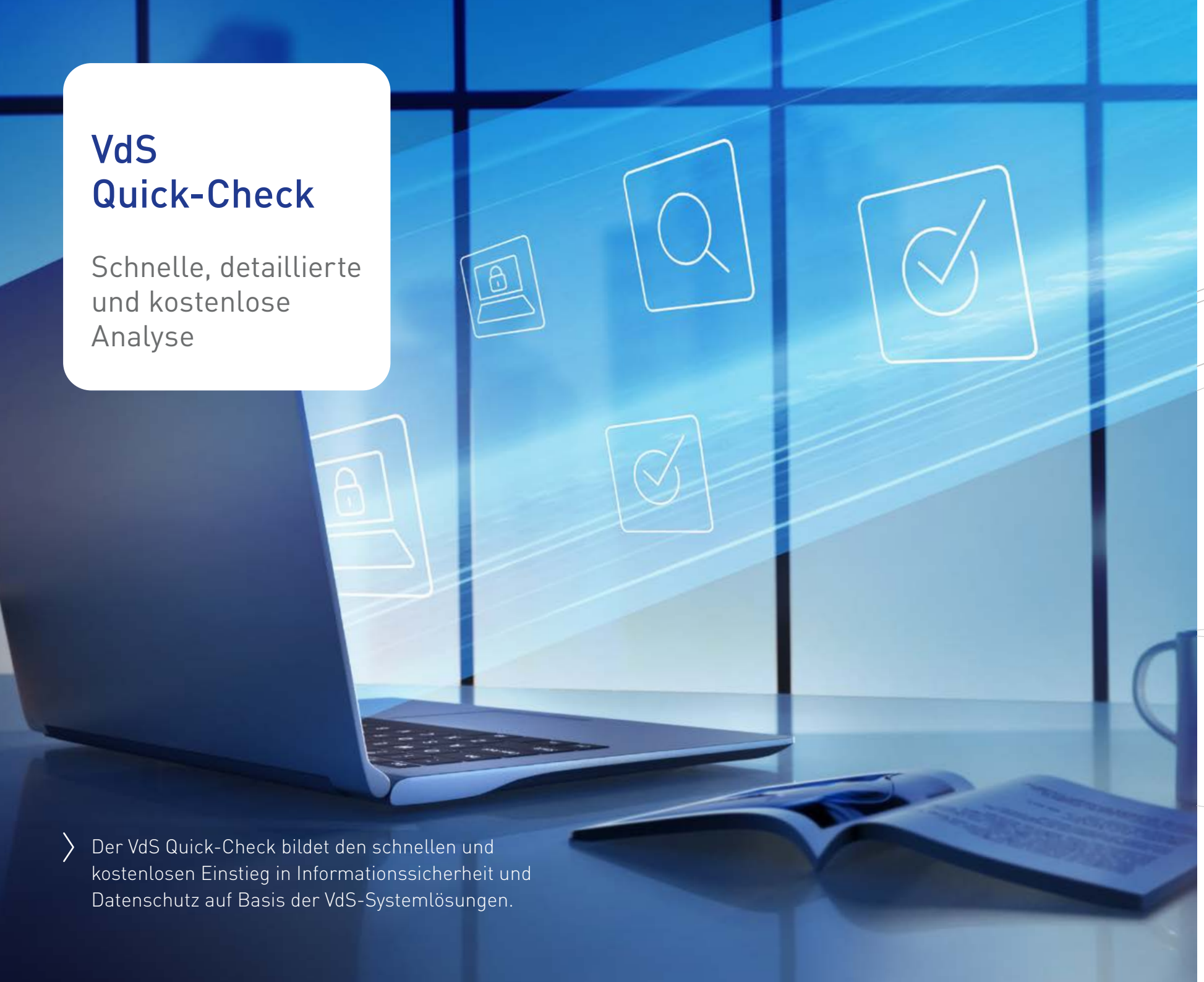
VdS führt das Quick-Audit sowohl für die IT-Sicherheit als auch für den Datenschutz durch. Gerne informieren wir Sie vorab ausführlich, wie das jeweilige Verfahren abläuft, und vereinbaren einen Termin mit Ihnen. Grundlage sind die Verfahrensrichtlinien VdS 10001 „VdS Quick-Audit", die auf die Ermittlung eines systematischen, unabhängigen, dokumentierten Prozesses zur Erlangung von Aufzeichnungen, Darlegungen von Fakten oder anderen relevanten Informationen und deren objektive Begutachtung abzielen. Eine ideale Grundlage für ein Erstgespräch – aber auch für das Verfahren selbst – stellen beispielsweise die Ergebnisse eines kostenlosen Quick-Checks dar, die wir ebenfalls für Informationssicherheit und Datenschutz – hier insbesondere im Hinblick auf die DSGVO – anbieten. Der Audit-Bericht nach Abschluss der Untersuchung zeigt Punkt für Punkt, welche Maßnahmen bereits wirken, und deckt bestehende Lücken auf. Selbstverständlich erhalten Sie auch Vorschläge zur Verbesserung Ihrer Cyber-Security.

Ihr Vorteil: die unabhängige Expertise.

Der Quick-Audit-Bericht wird im Gegensatz zu den Selbstauskünften des Quick-Checks von unabhängiger Seite erstellt. Deshalb stellt er in Verbindung mit dem VdS-Konformitätstestat einen wertvollen Baustein bei Ihrer Vorsorge zur Erfüllung der Anforderungen an die Informationssicherheit dar.
Da das VdS Quick-Audit eine Momentaufnahme ist, empfehlen wir, das Quick-Audit in angemessenen Zeitabständen zu wiederholen. Dann wissen Sie, ob die getroffenen Maßnahmen mit der Entwicklung Ihres Unternehmens und geänderten Bedrohungslagen Schritt halten. Und Sie können sich wieder vollständig auf Ihr Kerngeschäft konzentrieren.

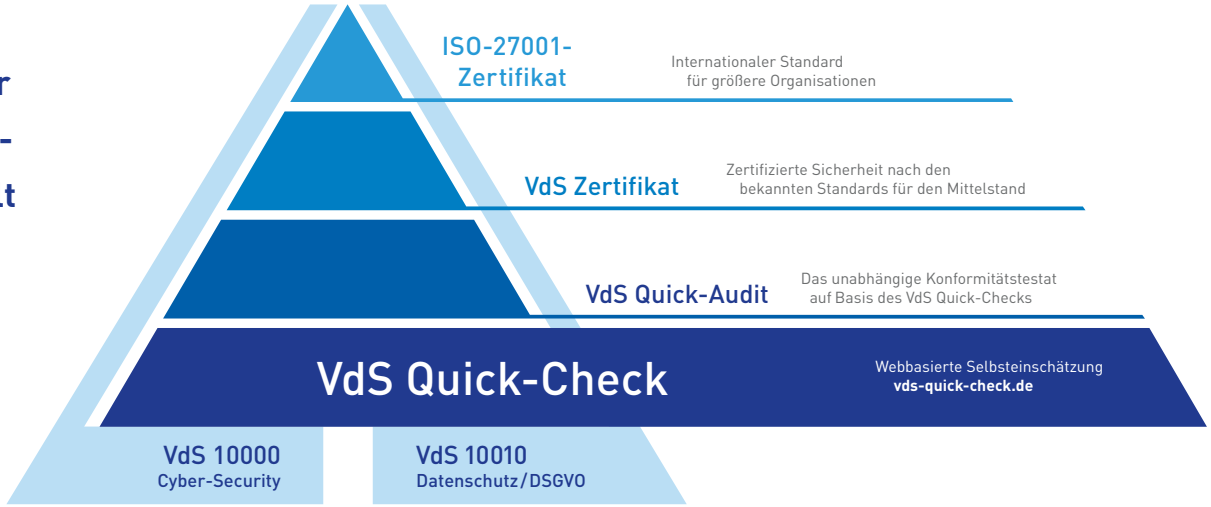
VdS Quick-Check

Schnelle, detaillierte und kostenlose Analyse



Der VdS Quick-Check bildet den schnellen und kostenlosen Einstieg in Informationssicherheit und Datenschutz auf Basis der VdS-Systemlösungen.

Mit dem webbasierten Tool „VdS-Quick-Check“ können Sie sich selbst einen ersten Überblick über den Status der Informationssicherheit Ihres Unternehmens verschaffen. Der Fragenkatalog ermittelt in den unterschiedlichen Handlungsfeldern den individuellen Schutzgrad des Unternehmens.



Geeignet für alle Unternehmensgrößen.
Schnell, detailliert und kostenlos.
Der VdS-Quick-Check ist ein kostenloses Online-Tool, das kleineren und mittelständischen Unternehmen eine methodische Analyse des aktuellen Status quo im Bereich Cyber-Security ermöglicht. Mit dem Fragenkatalogen wird in verschiedenen Handlungsfeldern, wie beispielsweise der Organisation, Technik, Prävention und dem Management oder auch den Verarbeitungsgrundsätzen, der individuelle Schutzgrad des Unternehmens ermittelt. Am Ende entsteht ein ausführlicher PDF-Bericht, der konkrete Handlungsempfehlungen enthält. Darin sind Maßnahmen enthalten, die sofort umsetzbar sind und unmittelbar das Schutzniveau verbessern. Für eine schnelle Orientierung sorgt ein Ampelsystem, das insbesondere die sofort verbesserungsbedürftigen Handlungsfelder auf den ersten Blick sichtbar macht.

Die VdS-Quick-Checks decken verschiedene Handlungsfelder ab.
Je nach Bedarf können Sie zwischen den Quick-Checks für Office-IT, Produktions-IT und Datenschutz wählen. Im Rahmen des Quick-Checks für Office-IT bitten wir Sie um die Beantwortung von 39 Fragen zu sicherheitsrelevanten Themen im Unternehmen. Der ergänzende Quick-Check für Produktions-IT unterstützt bei der Bestandsaufnahme des IT-Sicherheitsstatus von Produktionsanlagen in kleinen und mittleren Unternehmen (KMU) und umfasst insgesamt 42 Fragen. Im Fokus des Datenschutz-Quick-Checks stehen die Anforderungen eines Datenschutzmanagementsystems. Die Auswertung dieses Quick-Checks ermöglicht einen guten Einstieg in die Umsetzung der DSGVO nach VdS 10010. Die Beantwortung der Fragen dauert jeweils etwa 20 bis 30 Minuten. Die Ergebnisse werden abschließend in einer Matrix abgebildet, welche die aktuelle Risikosituation im Unternehmen übersichtlich darstellt.

VdS-anerkannte Cyber-Berater

Qualifizierte Unterstützung nach Maß

Kleineren und mittelgroßen Unternehmen fehlen oft die Ressourcen, um eine adäquate Informationssicherheit bzw. einen adäquaten Datenschutz zu realisieren. Professionelle Hilfe bieten VdS-anerkannte Berater, die mit den Cyber-Richtlinien VdS 10000 und anderen relevanten VdS-Schutzstandards vertraut sind und bei ihren Kunden implementieren können.

VdS-anerkannte Expertise.
VdS-anerkannte Berater haben nachgewiesen, dass sie KMU punktgenau technisch und organisatorisch auf eine VdS-zertifizierte Informationssicherheit vorbereiten können und stets über aktuelles Expertenwissen verfügen, um bei der Aktualisierung und Härtung der Cyber-Security in Unternehmen ein verlässlicher Partner zu sein. Bei IT-Sicherheitslösungen unterstützen sie dabei, Effizienz und Risikotransparenz in Unternehmen zu steigern, so dass sich Kunden wieder auf ihre Kernprozesse konzentrieren können. Ein von VdS-anerkannten Beratern implementiertes IT-Sicherheitssystem erzeugt bei Lieferanten, Kunden und Versicherern ein hohes Vertrauen in die Fähigkeit, Daten sicher zu schützen und Einschränkungen der Lieferfähigkeit zu minimieren. Daraus ergeben sich erhebliche Wettbewerbsvorteile.

Ihr Weg zur Anerkennung als VdS-Berater.
VdS bietet selbstverständlich auch ein Berater-Anerkennungsverfahren für die Gebiete IT-Sicherheit und Datenschutz an: Den VdS-anerkannten Berater für Cyber Security und für Datenschutzmanagementsysteme. Wichtig hierbei ist, dass Gegenstand der Anerkennung nicht die informationstechnische oder datenschutzrechtliche, sondern die Managementsystem-bezogene Beratung ist. Die Anerkennungsverfahren sind in den Richtlinien VdS 10003/ VdS 10004 beschrieben. Zur Erlangung der Anerkennung muss eine Prüfung bestanden werden, die im Anschluss an die Lehrgänge und ggf. einen zusätzlichen Workshop-Tag durchgeführt wird. Die VdS-Anerkennung als ISMS-/DSMS-Berater gilt vier Jahre und wird auf Wunsch verlängert.

VdS-Lehrgänge für Cyber Security

Kompetentes Wissen für die Praxis

Konzepte zur Unternehmenssicherheit greifen nur dann, wenn die handelnden Personen über das notwendige Wissen verfügen. Dies gilt für die eigenen Mitarbeiter in gleichem Maß wie für beauftragte Dienstleister rund um das Thema Sicherheit. Wissen zu bündeln und weiterzugeben und damit nachhaltig Standards zu setzen, ist eines der Hauptziele von VdS. Hinter diesem Anspruch steht insbesondere auch ein fokussiertes Informations- und Schulungsangebot im Bereich Cyber-Security.

Informationssicherheitsbeauftragte/-r

Der Lehrgang zielt auf das Management der Informationssicherheit ab. Teilnehmerinnen und Teilnehmer erhalten das notwendige Wissen und die unverzichtbaren Werkzeuge, um angemessene Informationssicherheit im Unternehmen zu etablieren und die notwendigen Sicherheitsmaßnahmen miteinander zu verzahnen. Der Lehrgang beinhaltet die Vermittlung von theoretischem Wissen sowie praktischen Übungen und schließt mit einer Prüfung ab.

Die Richtlinien 10000 und 10010

Die Lehrgänge erläutern die Inhalte der VdS-Richtlinien 10000 bzw. 10010 und stellen allen Teilnehmenden konkrete Vorgehensweisen zur Verfügung, Informationssicherheit effektiv zu implementieren, zu überprüfen und zu auditieren. Die Lehrgänge sind allerdings nicht vergleichbar mit der Prüfung zum VdS-anerkannten Berater für Cyber Security.

Erste Hilfe im IT-Schadenfall

In diesem Lehrgang werden die Teilnehmehrinnen und Teilnehmer für IT-Schadenfälle sensibilisiert und lernen, wie sie mit Ruhe und Sachverstand einem Schadenfall begegnen, wer die richtigen Ansprechpartner sind und wie die Ermittler bei ihrer Arbeit bestmöglich unterstützt werden können.

E-Learning

VdS bietet Ihnen maßgeschneiderte, browsergeführte und auf Wunsch für Ihr Unternehmen gebrandete E-Learning-Module zu den Themenkreisen IT-Sicherheit und Datenschutz an. Das Angebot beinhaltet Maßnahmen wie Erfolgskontrolle und aktive Elemente, z. B. Übungen zu den Problemfeldern Spam und Phishing.

Richtlinien VdS 10000 und VdS 10010 zum Download

Die Richtlinien VdS 10000 und VdS 10010 stehen Ihnen im Internet unter vds.de/cyber zum Download bereit. Hier finden Sie auch weiterführende Informationen rund um den Cyber-Security-Standard von VdS.

Kontakt

E-Mail: cyber@vds.de

Impressum

VdS Schadenverhütung GmbH
Amsterdamer Straße 174
D-50735 Köln

vds.de/cyber

VdS 5569 : 2018-10 (01)