Zertifizierung nach VdS 3473 – Eine „kleine ISO-27001“ für KMU?

Ulrich Greveler[1] · Robert Reinermann[2] · Mark Semmler[3]

[1]Hochschule Rhein-Waal
mail@ulrich-greveler.de

[2]VdS Schadenverhütung GmbH
rreinermann@vds.de

[3]Mark Semmler GmbH
sicherheit@mark-semmler.de

Zusammenfassung

Die vom VdS veröffentlichte Richtlinie VdS 3473 legt Mindestanforderungen an die Informationssicherheit fest und ist insbesondere auf KMU ausgerichtet. Die Anforderungen sind unterhalb der Kriterien des BSI-Grundschutzkatalogs und den Normen ISO 2700n angesiedelt, erlauben aber eine Kompatibilität der VdS 3473 zu diesen Normen. Die Richtlinie liegt zum Zeitpunkt der Erstellung dieses Beitrages als Entwurf vor; der Projektplan sieht vor, dass im Juli 2015 der Entwicklungsprozess mit der Veröffentlichung der Version 1.0 vorläufig abgeschlossen sein wird. Ein VdS-3473-Zertifikat gibt Versicherungsunternehmen eine belastbare Grundlage zur Tarifierung der Indeckungnahme von IT-Sicherheitsrisiken.

1 Einführung

Für den Erfolg eines Unternehmens ist die Sicherheit der Daten, die gespeichert und verarbeitet werden, und die Aufrechterhaltung kritischer, IT-gestützter Geschäftsprozesse von essentieller Notwendigkeit. Die Nutzung IT-gestützter betriebswirtschaftlicher und logistischer Geschäftsprozesse sowie der Anschluss an das Internet sind unverzichtbare Erfordernisse, um im Wettbewerb bestehen zu können.

Zunehmende Vernetzung und die Auslagerung von Diensten in den Betriebsbereich externer Dienstleister bergen jedoch mittlerweile als *Cyberrisiken* bezeichnete Gefahren, die auch kleine und mittelständische Unternehmen (KMU) in ihrem Risikomanagement berücksichtigen müssen. Diese Risiken können zwar analog zu potentiellen Schäden aufgrund von Bränden, Diebstahl oder Haftungen versichert und damit transferiert werden; jedoch wird vor einer Indeckungnahme von Cyberrisiken durch einen Versicherer regelmäßig eine Eigenerklärung zum Status der unternehmensweiten IT-Sicherheit oder der Nachweis über ein Zertifikat eingefordert, was für KMU nicht selten eine Herausforderung oder gar ein mittelfristig unüberwindliches Hindernis darstellt [Chou15].

P. Schartner · K. Lemke-Rust · M. Ullmann (Hrsg.) · D•A•CH Security 2015 · syssec (2015) 159-167.

Die im März 2015 vom VdS als Entwurf veröffentlichte Richtlinie VdS 3473 legt Mindestanforderungen an die Informationssicherheit fest und ist insbesondere auf KMU ausgerichtet. Die Anforderungen sind nach Art und Umfang unterhalb der Kriterien des BSI-Grundschutzkatalogs und den Normen ISO 27001 und 27002 angesiedelt. Die VdS 3473 kann als Grundlage für eine Zertifizierung durch den VdS herangezogen werden.

1.1 Einordnung

Der Begriff *IT-Sicherheitsmanagement* wird erstmals im *Green Book* des *Commercial Computer Security Center* im *Department of Trade and Industry* (DTI, 1989) eingeführt, welches einen britischen Entwurf von Evaluationskriterien für IT-Sicherheit umfasste und ein Schema für die Zertifizierung gemäß dieser Kriterien umriss. Nach einer Analyse von verbreiteten Best Practices britischer Großunternehmen wurde vom DTI ein *Code of Practice* (1993) veröffentlicht, der schließlich zum Kriterienwerk BS 7799:1995 weiterentwickelt wurde.

Im Jahre 2000 veröffentlichte die ISO einen auf der BS 7799 aufbauenden internationalen Standard 17799:2000, der später in der ISO/IEC 27002:2005 mündete. Aus der verwandten Norm BS 7799-2:2002 (zertifizierungsfähige Spezifikation zur BS 7799, inkl. neu entwickeltem *Plan-Do-Check-Act*-Konzept) wurde die ISO/IEC 27001 entwickelt, die eine international verbreitete Zertifizierungsgrundlage konstituiert. Seit 2005 wurden ca. 25 neue Standards innerhalb der ISO-2700x-Familie etabliert, die teilweise branchenspezifische Normen und spezielle Themenbereiche (z.B. Gesundheitsinformatik oder Anforderungen an Auditoren) abdecken. Der Fokus der ISO-2700x-Familie liegt dabei auf Großunternehmen bzw. Konzernen und Behörden, die sich ihr *Information Security Management System* (ISMS) zertifizieren lassen können.

Das Bundesamt für Sicherheit in der Informationstechnik veröffentlichte 1994 eine erste Version des IT-Grundschutzhandbuchs, das empfohlene Sicherheitsmaßnahmen für den mittleren Schutzbedarf aufführte. Umsetzungsempfehlungen für ISMS wurden 2006 über den Standard BSI-100-2 in Verbindung mit IT-Grundschutz (über die aus dem Handbuch weiterentwickelten IT-Grundschutz-Kataloge) beschrieben. Im Zuge der Konvergenz nationaler und internationaler Standards zur Messung der Konformität zu IT-Sicherheitskriterienwerken kann seit 2006 ein *ISO/IEC 27001-Zertifikat auf Basis von IT-Grundschutz* [BSIZ14] erteilt werden.

Die Anzahl der ausgestellten Zertifikate nach ISO/IEC 27001 auf Basis von IT-Grundschutz beschränkt sich jedoch seit der Etablierung der Norm auf eine niedrige zweistellige Zahl per anno[1]. Im Vergleich dazu stellt eine ISO-Studie [ISO-11] im Erhebungszeitraum 2006-2011 eine mittlere dreistellige Zahl vergebener ISO/IEC 27001-Zertifikate per anno für Europa fest, wobei ein Unternehmen mehrere Zertifikate erhalten kann, da unternehmenseigene Informationsverbünde voneinander abgegrenzt und für sich zertifiziert werden können. Soweit Zertifikatsnehmer veröffentlicht sind, lässt sich sowohl bei in Deutschland vergebenen ISO/IEC 27001-Zertifikaten allgemein als auch beim Anteil der auf Basis von IT-Grundschutz erteilten Zertifikate eine starke Dominanz von Großunternehmen (z.B. Telekom Deutschland GmbH, Deutsche Post E-POST Solutions GmbH, Vodafone GmbH) und Behörden (z.B. Stadt Köln, Bundespolizeipräsidium, Kommunale Rechenzentren) feststellen, KMU-Zertifikatsnehmer stellen eher eine Randerscheinung dar und betreffen beispielsweise Dienstleister aus dem IT-Sicherheitsumfeld und spezialisierte Systemhäuser. Wichtige Treiber und Hinderungsgründe

[1] Vgl. aktuelle Liste auf der Webseite https://www.bsi.bund.de/DE/Themen/ZertifizierungundAnerkennung/Zertifizierung27001/ErteilteZertifikate/iso27001zertifikate_node.html (Zugriff 26. März 2015).

für die Entscheidung über die Beauftragung einer ISO-27001-Zertifizierung von KMUs [BaFo08, FDB08] lassen sich ausmachen.

Treiber:

- Bedrohungslage spitzt sich zu; erste Erfahrungen mit Incidents
- Compliance (gesetzlich, vertraglich)
- Nachweis gegenüber Versicherungen und Investoren

Hinderungsgründe:

- Hohe Kosten beim Aufbau der Organisation und des Zertifizierungsprozesses
- Kollision der Maßnahmen mit der Unternehmenskultur
- Geringe Wirkung auf die Position im Markt, unwesentlicher Werbeeffekt

2 Richtlinie VdS 3473

Die in der Entwicklung befindliche und für diesen Beitrag als Version 0.9.0 vom Juni 2015 vorliegende VdS-Richtlinie 3473 (im Folgenden kurz als VdS 3473 bezeichnet) umfasst Anforderungen zur Beurteilung der Risiken in Bezug auf Cyber-Security von Unternehmen und ist als „Richtlinie für den Mittelstand“ konzipiert. Die Richtlinie stellt ein Bindeglied zwischen VdS-Quick-Check/Quick-Audit (Zielgruppe: Kleinunternehmen) und Anforderungen zur Erlangung eines ISO-27001-Zertifikat dar. Ein VdS-3473-Zertifikat gibt dabei insbesondere einem Versicherer eine belastbare Grundlage zur Tarifierung der Indeckungnahme von IT-Sicherheitsrisiken eines Unternehmens. Das Fehlen dieser Grundlage führte teilweise zum Overpricing bei entsprechenden Produkten [BMR09]. Die Autoren der Richtlinie streben dabei an, eine Teilmenge der Anforderungen bestehender Normen wie ISO 2700n und BSI 100-1 bis 100-4 zu definieren, um eine Kompatibilität der VdS-3473 zu den genannten ISO-Normen zu ermöglichen [Rein15]. In diesem Beitrag wird nun untersucht, ob diese Kompatibilität gegeben ist und ob damit tatsächlich KMU eine zertifizierbare Option offensteht, bereits einen definierten Teil der Aufwände einer ISO-27001-Zertifizierung realisiert zu haben.

Die VdS-3473 sieht im vorliegenden Entwurf für die Systemlandschaft des Unternehmens eine Unterteilung in „kritische“ und „unkritische“ Systeme vor. Kriterien für das Label „kritisches System“ sind dabei u. a. die erhebliche Auswirkung auf die Geschäftsprozesse, Gefahr für Leib und Leben, Missbrauch personenbezogener Daten oder eine sich ruinös auswirkende Haftung nach einem Verstoß gegen Gesetze oder Verträge. Diese Unterteilung ist teilweise vereinbar mit den Schutzbedarfsfeststellungen gemäß IT-Grundschutz, die Schutzbedarfskategorien "normal", "hoch" (*Die Schadensauswirkungen können beträchtlich sein.*) und "sehr hoch" (*Die Schadensauswirkungen können ein existentiell bedrohliches, katastrophales Ausmaß erreichen.*) vorsehen und die eine Aktivität der Ableitung des Schutzbedarfs der IT-Systeme aus dem Schutzbedarf der Anwendungen beschreiben.

Die Unterteilung in „kritische“ und „unkritische“ Systeme ohne Zuordnung zu Sachgruppen oder Geschäftsprozessen ist begrenzt vereinbar mit dem Begriff des *Informationsverbundes* aus dem IT-Grundschutz, der die Gesamtheit von organisatorischen und technischen Objekten umfasst, die der Aufgabenerfüllung in einem klar bestimmten Bereich dienen. Ein ISMS gemäß ISO 27001-Zertifizierung muss keineswegs für ein gesamtes Unternehmen eingeführt werden. Bei positivem Zertifizierungsverlauf wird vielmehr für einen definierten Informationsverbund ein ISO-27001-Zertifikat erteilt. Die VdS 3473 zielt daher insbesondere auf Unternehmen, die

nur *einen* Informationsverbund umfassen, also nicht die Komplexität der IT-Landschaft eines Konzerns oder eines verteilten Unternehmens mit örtlich getrennten Geschäftsbereichen aufweisen. KMU werden damit verstärkt adressiert.

2.1 Fachliche Bereiche, Einzelmaßnahmen

Bei den in der VdS 3473 enthaltenen Einzelmaßnahmen handelt es sich konzeptionell um eine Auswahl möglicher Implementierungsoptionen der eher generischen ISO-2700x-Anforderungen und inhaltlich um ausgewählte technische Maßnahmen, die einen *Best Practice* der Betriebssicherheit typischer IT-Systeme darstellen und die jeweils einigen in den IT-Grundschutz-Katalogen enthaltenen Maßnahmen eine Entsprechung finden bzw. damit übereinstimmen, d. h. es werden etablierte Sicherheitsmaßnahmen für Anwendungen und IT-Systeme eingefordert oder empfohlen. Zur Feststellung der Aufwärts-Kompatibilität der VdS-3473 zur ISO 27001 und zur Überprüfung der thematischen Abdeckung erfolgt eine Gegenüberstellung nach Abschnitten der jeweiligen Kriterienwerke (siehe Tabelle 1).

Tab. 1: Gegenüberstellung: ISO/IEC 27001:2013 vs. VdS 3473 (V. 0.4)

Abschnitte der ISO/IEC 27001:2013	Abschnitte der VdS-3473
0 Introduction	Allgemeines
1 Scope	Geltungsbereich
2 Normative references	Normative Verweisungen
3 Terms and definitions	Anhang: Glossar
4.1 Understanding the organization and its context	Ziele und Stellenwert der Informationssicherheit Rollen und Verantwortlichkeiten.
4.2 Understanding the needs and expectations of interested parties, (…) obligations	Nicht oder nur teilweise erfasst unter: Leitlinie zur Informationssicherheit
4.3 Determining the scope of the information security	Nicht oder nur teilweise erfasst unter: Leitlinie zur Informationssicherheit
4.4 Information security management system	Angerissen in: Anweisungen und Richtlinien Vision + Strategie
5.1 Leadership and commitment	Organisation, Topmanagement
5.2 Policy	Leitlinie zur Informationssicherheit
5.3 Organizational roles, responsibilities (…)	Verantwortlichkeiten
6.1.1 Actions to address risks and opportunities – general	Nur teilweise angerissen in: Anweisungen und Richtlinien
6.1.2 Information security risk assessment	Systeme, Umsetzung
6.1.3 Information security risk treatment	Systeme, Umsetzung
6.2 Information security objectives and planning to achieve them	(nicht abgedeckt, out of scope)
7.1 Resources, 7.2 Competence 7.3 Awareness, 7.4 Communication 7.5 Documented information	Personal & Schulungen (nicht im Detail, aber angerissen)
8.1 Operational planning and control 8.2 Information security risk assessment 8.3 Information security risk treatment	Aktualität der Informationen Umgang mit Sicherheitsvorfällen (nicht im Detail, aber angerissen)

Die Einzelmaßnahmen legen im Detail eine Menge von MUSS-Anforderungen fest (Bsp.: „*Das Unternehmen MUSS alle Lieferanten und sonstige Auftragnehmer verpflichten, die sie oder ihre Tätigkeit betreffenden Maßnahmen und Regelungen zur Informationssicherheit einzuhalten bzw. umzusetzen.*“ aus Kap. 4 der Richtlinie) und ergänzen diese um weitere SOLL-Anforderungen, die für die Erteilung eines Zertifikates nicht notwendigerweise nachzuweisen

sind (Bsp.: „*Schulungs- und Sensibilisierungsmaßnahmen SOLLTEN mit einem Wissenstest abschließen, um das Verständnis des Personals zu ermitteln.*“ Aus Kap. 8 der Richtlinie), deren Umsetzung aber empfohlen wird.

3 Kompatibilität zur ISO 27001

Die Gegenüberstellung aus Tabelle 1 zeigt, dass die aufgeführten fachlichen Abschnitte adressiert oder zumindest teilweise angerissen werden. Eine „Aufwärtskompatibilität“ der VdS 3473 zur ISO-27001 bzw. zum Zertifizierungsschema für die ISO-27001-Zertifizierung auf der Basis von IT-Grundschutz ist grundsätzlich gegeben, dabei ist jedoch die Einschränkung auf nur einen Informationsverbund zu berücksichtigen. Auffällig ist die Nichtberücksichtigung der thematischen Aspekte Mobilgeräte, Telearbeit und physische Sicherheit in den früheren Versionen der Richtlinie; diese wurde im Zuge eines Konsultationsprozesses in der zum Zeitpunkt der Erstellung dieses Beitrages vorliegenden Version 0.9.0 bereits berücksichtigt.

Da die VdS 3473 eine Unterteilung nur in kritische und unkritische Systeme vorsieht, fallen einige höchst sinnvolle Maßnahmen für Systeme weg, deren langfristiger Ausfall oder deren Kompromittierung sich nicht unmittelbar ruinös auswirken, jedoch trotzdem nicht unerhebliche Schäden verursachen können. Diese Abschwächung der Anforderungen ist im Zusammenspiel mit dem Verzicht der Betrachtung von physischer Sicherheit intendiert, um den Weg hin zu einer ersten ISMS-Zertifzierung für KMU zu ebnen.

3.1 Entwicklungsprozess der Richtlinie

Die ersten Entwürfe bis Version 0.1 wurden im Januar 2015 von einer kleinen Arbeitsgruppe erstellt. Hierzu wurden die Kernaussagen anerkannter Normen und Leitfäden gesammelt, die jeweiligen Anforderungen gegenübergestellt und jene Maßnahmen ausgewählt, die für KMU umsetzbar erschienen.

Version 0.1 wurde elektronisch über die VdS-Webseite veröffentlicht und in verschiedenen Business-Netzwerken mit der Bitte um Kommentierung bereitgestellt. Da die VdS 3473 auf ein recht breites Interesse stieß und eine Vielzahl von Kommentaren eingingen, entschloss sich das Normierungsgremium, den Entwicklungsprozess offen zu gestalten. Im Laufe des Entwicklungsprozesses konnte jeder Interessierte Ergänzungen, Kritik und Verbesserungsvorschläge einreichen, die im Normierungsgremium diskutiert, fachlich kommentiert und häufig auch umgesetzt wurden. Offensichtliche Verbesserungen wurden ohne fachliche Diskussion implementiert und umgehend veröffentlicht. Dadurch erschienen in kurzen Abständen neue Entwurfs-Versionen der Richtlinie, was die Einsender der Verbesserungen motivierte, sich weiter am Entwicklungsprozess zu beteiligen.

Kurz nach der Veröffentlichung der Version 0.4 zur CeBIT 2015 wurde die VdS 3473 auf zwei Workshops insgesamt 25 IT-Verantwortlichen sowie Administratoren vorgestellt und intensiv diskutiert. Die dadurch gewonnenen Erkenntnisse konnten in den weiteren Entwicklungsprozess einfließen.

Die Version 0.9 stellt einen Meilenstein dar und ist um verschiedene Mängel bereinigt, unter anderem:

- Berücksichtigung mobiler Geräte
- Vereinfachung der Kapitel 12 (IT-Outsourcing und Nutzung von Cloud-Diensten), 13 (Zugänge und Zugriffsrechte) und 14 (Datensicherung)

- Konzentrieren von Maßnahmen mit gleichem thematischen Gebiet in eigene Kapitel (wie z.B. „Umgebung“)
- Vereinheitlichung des Kapitelaufbaus
- Umstellen der Kapitel, um organisatorische und technische Maßnahmen zu bündeln

Der Projektplan sieht vor, dass am 01.07.2015 der Entwicklungsprozess mit der Veröffentlichung der Version 1.0 vorläufig abgeschlossen sein wird.

3.2 Designentscheidungen

Eine Vielzahl von Maßnahmen der ISO 27001 findet sich nicht in der 3473, weil der Umsetzungsaufwand als zu hoch angesehen wurde. So wurden viele Maßnahmen, die eine umfassende Analyse und Dokumentation erfordern, nicht in die 3473 aufgenommen. Die Anforderungen zur Erstellung einer Dokumentation sind nur in wenigen Maßnahmen der VdS 3473 enthalten. Darunter leiden naturgemäß die Nachvollziehbarkeit und die Möglichkeit, Arbeitsabläufe und deren Ergebnisse zu prüfen.

Weitere Anforderungen der Richtlinie sind konkreter als in der ISO 27001 formuliert. Hierzu zählen z.B. die Anforderungen an unternehmenseigene Richtlinien für Nutzer und Dienstleister. Die konkreteren Vorgaben sollen wieder den Implementierungsaufwand verringern, da sie schneller umgesetzt werden können.

Die Anforderungen an die Analyse der IT-Infrastruktur sind in der VdS 3473 im Gegensatz zu ISO 27001 stark reduziert und beschränkt sich auf das Identifizieren kritischer Prozesse und Ressourcen (Kapitel 7.2 der Version 0.9). Hierbei fordert die 3473 keine umfangreiche Analyse wie z.B. eine Business Impact Analyse gemäß BSI 100-4 oder ISO 22301, sondern empfiehlt diese Maßnahme lediglich. An ihrer Stelle kann ein generisches Vorgehen gewählt werden, was nur wenige, konkret vorgegebene Anforderungen erfüllen muss.

Gleiches gilt für die Vorbereitung auf Ausfälle. Auch hier wird ein Business Continuity Management gemäß BSI 100-4 oder ISO 22301 nur empfohlen, jedoch nicht vorgeschrieben. Das Unternehmen kann ein eigenes Vorgehen implementieren, muss allerdings zur Erfüllung der Norm für jedes kritische System einen Wiederanlaufplan erstellen und die Abhängigkeiten zwischen den kritischen Systemen erfassen.

Mit der Identifizierung der kritischen Ressourcen verzichtet die VdS 3473 auf ein umfassendes Wertemanagement, wie es in ISO 27001 vorgeschrieben ist. Eine Klassifizierung der Informationen ist ebenfalls nicht vorgesehen, weil die Einführung eines Ressourcenmanagements und einer Informationsklassifizierung in den meisten kleinen und mittelständischen Unternehmen einen tiefgreifenden Einschnitt in die bisherige Arbeitsweise darstellen würde.

Das Konzept der Sicherheitsbereiche in der ISO 27001 ist in der VdS 3473 nur rudimentär vorhanden und wird selbst in dieser Form nur für als *kritisch* eingestufte IT-Systeme und aktive Netzwerkkomponenten gefordert.

Mit diesen Vereinfachungen geht ein Verlust des erreichbaren Sicherheitsniveaus einher, zugleich wird aber der Implementierungsaufwand im Vergleich zur ISO 27001 stark verringert. Die verhältnismäßig einfache Implementierbarkeit ist ein wichtiger Aspekt für die Zielgruppe der Norm und soll dazu beitragen, KMU bewegen, den Aspekt der Informationssicherheit zu berücksichtigen und strukturiert auf die aktuellen Bedrohungen zu reagieren.

4 VdS-zertifzierte Informationssicherheit

Der VdS reagiert mit den Cyber-Richtlinien auf die wachsende Bedeutung der Informationssicherheit, welche die Unternehmenssicherheit mit ihren klassischen Handlungsfeldern Brandschutz, Security (Schutz gegen Einbruch, Diebstahl, Sabotage) und Naturgefahren (z.B. Überschwemmung, Starkregen) ergänzt. Die Erstellung der VdS 3473 fügt sich in die VdS-Systematik eines integrierten Sicherheitsansatzes – Erstellung von Normen und Richtlinien, Prüfung und Zertifizierung von Komponenten und Systemen, Prüfung und Zertifizierung von Unternehmen und Personen sowie Inspektionen und Revisionen (baubehördlich wie versicherungstechnisch) ein, die im Brandschutz und Einbruchsdiebstahlschutz seit Jahrzehnten etabliert ist (vgl. Abbildung 1).

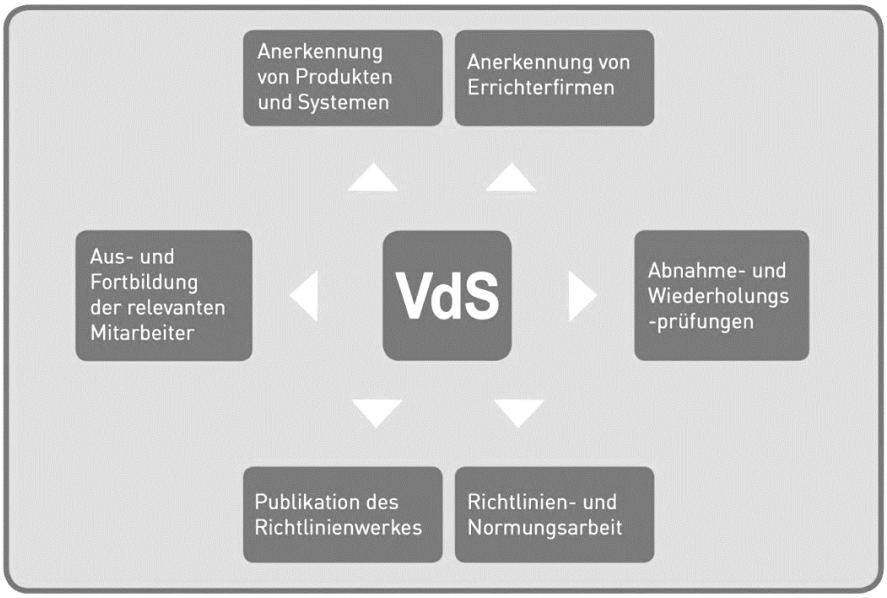

Abb. 1: Die VdS-Systematik des integrierten Sicherheitsansatzes

Mit der VdS 3473 stehen Anforderungen und Maßnahmen zur Beurteilung von IT-Risiken und das gewünschte Schutzniveau durch Normen und Richtlinien zur Verfügung. Sie sind explizit auf kleinere und mittlere Organisationen, wie z.B. KMU und Behörden, zugeschnitten und dienen als grundlegende Verfahrensrichtlinien zur Zertifizierung von Prozessen in Organisationen. Die Richtlinie VdS 3473 konzentriert die umzusetzenden Maßnahmen auf das technisch und organisatorisch Wesentliche für KMU und Behörden. Die Richtlinie kann auch als Grundlage genutzt werden, um sich zu einem späteren Zeitpunkt nach ISO 27001 und nach BSI-Grundschutz zertifizieren zu lassen. Die Richtlinie ist branchenneutral gehalten und daher für die meisten Organisationen direkt umsetzbar. Der modulare Aufbau ermöglicht zusätzlich die Entwicklung von branchenspezifischen Standards.

4.1 Einstieg in die Informationssicherheit für KMU

Mittels eines dreistufigen Verfahrens bietet VdS einen einfachen und umsetzbaren Einstieg in die zertifizierte Informationssicherheit. Der VdS-Quick-Check – ein kostenloses Webtool, das online[2] zur Verfügung steht – präsentiert Unternehmen einen ersten Überblick, wie der aktuelle

[2] Online verfügbar unter www.vds-quick-check.de

Status Ihrer Cyber-Security ist und wo Handlungsbedarf besteht. Der Quick-Check ist eine Selbstauskunft mit 39 Fragen aus den Handlungsfeldern Organisation, Technik, Prävention und Management und schließt mit einem ausführlichen Statusbericht zur Informationssicherheit ab (Abbildung 2).

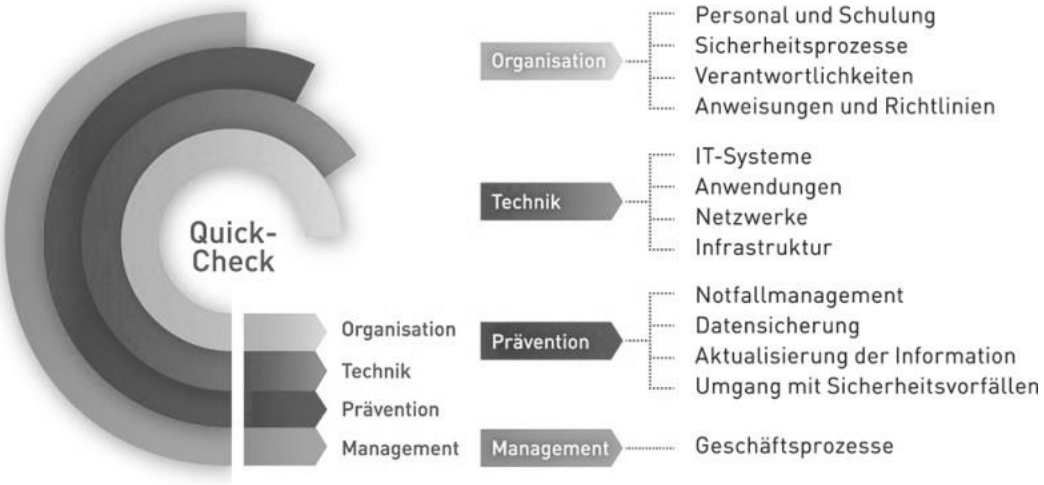

Abb. 2: Der VdS-Quick-Check ist in vier Teilbereiche unterteilt

Aufbauend auf den Ergebnissen des Quick-Checks können Unternehmen dann im zweiten Schritt mit dem sogenannten Quick-Audit [Rein15], das vor Ort von einem VdS-Auditor durchgeführt wird, den Status der Informationssicherheit testieren lassen und weitere Verbesserungsmaßnahmen ermitteln.

Mit der dritten Stufe, der VdS-Zertifizierung auf Basis der Cyber-Richtlinie VdS 3473, können Organisationen auch nach außen – gegenüber Kunden, Behörden, Eigentümern, Lieferanten und auch Versicherern – dokumentieren, dass Sie einen angemessenen Informationssicherheitsschutz implementiert haben. Der VdS-Quick-Check dient damit auch als Vorbereitung für eine Zertifizierung nach VdS 3473. In einem Zertifizierungsaudit und jährlichen Re-Audits vor Ort überprüfen VdS-Auditoren die Übereinstimmung mit den Richtlinien. Sind alle Anforderungen der Richtlinie VdS 3473 erfüllt, erhalten die Organisationen das VdS-Zertifikat.

4.2 Audits durch VdS-anerkannte Cyber-Berater

In Anlehnung an die etablierte VdS-Errichteranerkennung, z.B. für Einbruchmeldeanlagen oder Feuerlöschanlagen, bietet VdS auch IT-Dienstleistern, z.B. Systemhäusern und Securityberatern, ein Zertifizierungsverfahren an. Das Zertifikat für qualifizierte Dienstleister belegt, dass diese Firmen Unternehmen mittels qualifizierter Fachkräfte auf eine Zertifizierung vorbereiten können. Der VdS listet die zertifizierten Cyber-Security-Berater auf der VdS-Website. [Rein15]

5 Zusammenfassung und Ausblick

Mit einer zertifizierten Informationssicherheit nach VdS 3473 ergeben sich für KMU und Behörden folgende über den Zertifizierungsprozess nachweisbaren Sachverhalte:

- Das VdS-Zertifikat bestätigt, dass die Organisation technisch auf die wichtigsten Cyber-Angriffsszenarien vorbereitet ist und passende Schutzmaßnahmen generiert hat. Betriebsunterbrechungen durch Cyber-Attacken und Datendiebstahl werden unwahrscheinlich.

- Ein Zertifikat auf der Basis von VdS 3473 erzeugt bei Kunden, Lieferanten etc. Vertrauen, dass unter anderem die Datensicherheit und auch die Lieferfähigkeit gewährleistet sind und bietet somit Wettbewerbsvorteile.
- Unternehmen erweitern Ihr Risikomanagement um den Aspekt der Informationssicherheit. Unternehmen können sich wieder auf Ihre Kernprozesse konzentrieren.
- Das Restrisiko können Unternehmen auf einen Versicherer übertragen und damit die Strategie für die Existenzsicherung des Unternehmens erweitern.

Die Versicherungswirtschaft verfügte bisher über keinen umsetzbaren Standard, passende Produkte zum Schutz vor Cyberkriminalität anzubieten. Die VdS 3473 kann eine Basis für individuellen Versicherungsschutz sein.

Es ist zu erwarten, dass Branchenverbände wie der Gesamtverband der Deutschen Versicherungswirtschaft Musterbedingungen für die Cyber-Versicherung ausarbeiten, die unmittelbar auf zertifizierbare Informationssicherheit abheben. Die damit einhergehende Vereinheitlichung von Bedingungswerken beim Transfer von Cyberrisiken wird den Bedarf für umsetzbare Standards bei KMU weiter erhöhen.

Literatur

[BaFo08] Y.Barlette, V.V. Fomin: Exploring the Suitability of IS Security Management Standards for SMEs. Hawaii International Conference on System Sciences, Proceedings of the 41st Annual. IEEE 2008.

[BMR09] T. Bandyopadhyay, V. Mookerjee, R. Rao: Why IT managers don't go for cyber-insurance products. Communications of the ACM. Volume 52 Issue 11, November 2009. P. 68-73.

[FDB08] V.V. Fomin, J. H. De Vries, B. Yves: ISO/IEC 27001 information systems security management standard: exploring the reasons for low adoption. EuroMOT 2008 - The Third European Conference on Management of Technology. 2008.

[BSIZ14] BSI. Zertifizierung nach ISO 27001 auf der Basis von IT-Grundschutz. Zertifizierungsschema. Version 1.2. Bundesamt für Sicherheit in der Informationstechnik, 2014.

[Chou15] U. Choudhry: Der Cyber-Versicherungsmarkt in Deutschland – Eine Einführung. Springer Fachmedien Wiesbaden. Gabler 2014.

[ISO-11] ISO: The ISO Survey of Management System Standard Certifications. 2011. Online: http://www.iso.org/iso/home/standards/certification/iso-survey.htm (abgerufen: Dez. 2011)

[Rein15] R. Reinermann: Alternative zum IT-Grundschutz – Neue VdS-Richtlinien für die Cyber-Security. In: <kes> Special IT-Sicherheit in Kommunen und Behörden. SecuMedia Verlags-GmbH Ingelheim. Mai 2015.