Das aktuelle Interview

VdS-Richtlinien 3473 – Cyber-Security für kleine und mittlere Unternehmen

Mit den VdS-Richtlinien 3473 wurde auf der diesjährigen CeBIT ein neuer Standard für Informationssicherheit in kleinen und mittleren Unternehmen (KMU) vorgestellt. Hier stellt sich die Frage: Wofür brauchen wir noch ein Regelwerk? Und was unterscheidet es von den bisherigen? Um etwas Licht ins Dunkel zu bringen, haben wir darüber mit den IT-Experten Mark Semmler und Michael Wiesner gesprochen, die beide an den neuen Richtlinien mitgearbeitet haben.

Mark Semmler (oben, 41) arbeitet seit mehr als 20 Jahren europaweit für die Absicherung von Informationen und IT-Infrastrukturen. Er gilt als ausgewiesener Experte der Informationssicherheit und ist auf Highlevel-Consulting und organisatorische Sicherheit spezialisiert (ISO 27000-Familie). Er ist durch seine auch in Funk und Fernsehen übertragenen Livehacking-Präsentationen einem breiten Publikum bekannt.

Michael Wiesner (unten, 38) ist Geschäftsführer der CTNS Security GmbH und seit über 20 Jahren als IT-Sicherheitsberater mit dem Schwerpunkt Risiko- und Informationssicherheitsmanagement tätig. Er ist ständiges Mitglied im Projektteam für VdS 3473.

1 Wie sind Sie in das Projektteam gekommen und was ist Ihre Rolle darin?

Mark Semmler: Ich bin der Teamleiter für die Erstellung der Richtlinien VdS 3473. Meine Aufgabe besteht darin, die einzelnen Aufgaben zu koordinieren, Teilergebnisse und Feedback zu sichten und neue Versionen der Richtlinien zu erstellen, die dann im Team diskutiert und häufig auch direkt verbessert werden. Zu VdS besteht eine langjährige Verbindung, die irgendwann einmal mit einer Sicherheitsüberprüfung und einem Vortrag vor der Leitungsebene von VdS Schadenverhütung angefangen hat. Als Robert Reinermann und Simon Goeden-Eicken mir das Vorhaben von VdS vorgestellt haben – das war Mitte 2014 –, habe ich aus dem Stand heraus zugesagt. Das Konzept aus Quick-Check, Quick-Audit und VdS-Richtlinien hat einfach gepasst und hat Potenzial, die Informationssicherheit in Deutschland wirklich nachhaltig voranzubringen.

Michael Wiesner: Anfang des Jahres erfuhr ich durch Mark Semmler von den geplanten VdS-Richtlinien für Informationssicherheit in KMU und war von der Idee begeistert. Wir diskutierten meine Anmerkungen zur damaligen Version, und kurze Zeit später bot mir Mark die Mitarbeit im Team an. Zunächst war ich für das Qualitätsmanagement (QM) beim Abschluss der einzelnen Entwicklungszyklen zuständig. Recht schnell nahm ich jedoch auch am Gestaltungsprozess teil, wo ich meine langjährigen Erfahrungen mit Informationssicherheit in KMU einbringen konnte. Neben diesem fachlichen Input liegt mein Schwerpunkt weiterhin im Bereich QM.

2 Wie kann man sich den Gestaltungsprozess der neuen VdS-Richtlinien 3473 vorstellen?

Michael Wiesner: Die VdS-Richtlinien werden durch ein Projektteam entwickelt, das sich alle ein bis zwei Wochen trifft, um intensiv an den Richtlinien zu arbeiten. Dazwischen werden die Arbeitspakete entwickelt und bearbeitet, die am Ende der Meetings verteilt werden. Durch die zeitnahe Veröffentlichung der

einzelnen Versionen und dem öffentlichen Konsultationsverfahren erhalten wir zusätzliches Feedback, was entsprechend in unsere Arbeit einfließt.

Mark Semmler: Wir – VdS und das gesamte Projektteam – haben bei der Entwicklung der VdS 3473 von Anfang an auf die Open-Source-Prinzipien gesetzt: Arbeite öffentlich. Gib jedem die Möglichkeit, Verbesserungen beizutragen. Veröffentliche viele kleine Schritte. Dokumentiere, was sich geändert hat und wie.

Dadurch haben wir eine breite Öffentlichkeit erreicht und überraschend viel Feedback erhalten. Wir konnten immer wieder einen Praxisabgleich fahren. – Konnten? Nein, wir mussten! Wir sind nämlich immer wieder von unseren Zielgruppen freundlich getreten worden. (lacht) Nicht zuletzt besteht natürlich auch ein reger Austausch mit den Teams, die sich mit dem Quick-Check und dem Quick-Audit beschäftigen.

3 Wir haben mit dem IT-Grundschutz des BSI (Bundesamt für Sicherheit in der Informationstechnik) und den ISO-Normen bereits etablierte Standards für Unternehmen. Wozu also ein weiteres Regelwerk?

Mark Semmler: Um Missverständnissen vorzubeugen: ISO und BSI sind sehr gute Normen. Leider hat die Praxis gezeigt, dass sie für KMU nur bedingt umsetzbar sind.

Michael Wiesner: Genau. Der IT-Grundschutz des BSI und die Normenreihe der ISO sind ausgereifte und sinnvolle Ansätze, Informationssicherheit wirksam zu managen. Leider wurde bei der Entwicklung jedoch zu wenig auf die Anforderungen von kleinen und mittleren Unternehmen geachtet. Der IT-Grundschutz adressierte ursprünglich nur Behörden, später wurde dies auch auf privatwirtschaftliche Organisationen ausgeweitet. Der „Hauch der Vergangenheit" haftet dem IT-Grundschutz jedoch leider immer noch an. Dementsprechend werden bereits in der Grundabsicherung Dinge gefordert, die für KMU nicht oder nur sehr aufwendig umsetzbar sind. Die Anforderungen der Grundschutzkataloge versuchen dabei über das „Gießkannenprinzip" so viele Gefährdungen wie möglich zu behandeln und entsprechende Maßnahmen dagegenzustellen. Allein diese schiere Fülle an Informationen überfordert KMU meist, wie die Erfahrungen aus der Praxis zeigen.

Mark Semmler: Ich kann nur beipflichten. Nicht ohne Grund gibt es nur sehr, sehr wenige Unternehmen, die ein Zertifikat „ISO 27001 nach BSI Grundschutz" besitzen.

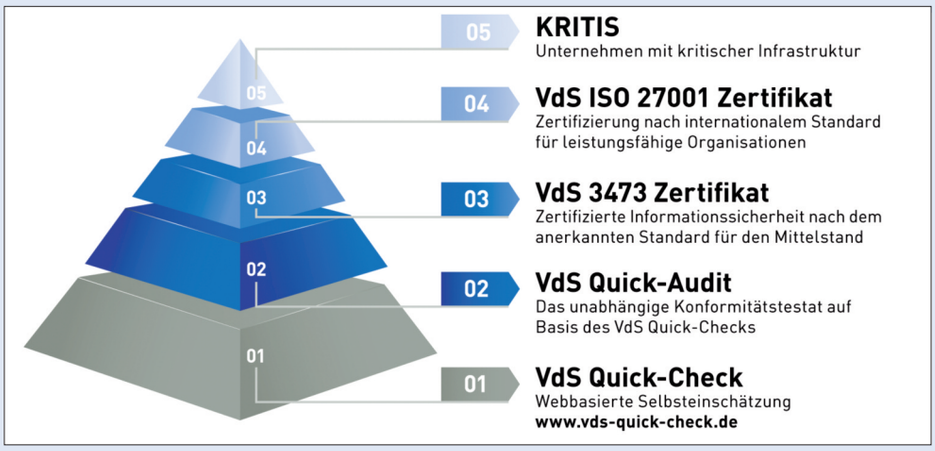
4 Und was ist mit der Norm ISO 27001? Diese definiert doch ihrem Geltungsbereich explizit, dass sie für Organisationen jeder Größenordnung geeignet ist.

Michael Wiesner: Grundsätzlich ist dies auch richtig. Die ISO-Normen sind sehr flexibel anwendbar, da sie auf sehr generische Art und Weise den Informationssicherheitsprozess und die Anforderungen an diesen beschreiben. Und genau hier liegt das Problem, da sie dadurch nicht wirklich greifbar sind. Es fehlt an konkreten Maßnahmenempfehlungen und einem Leitfaden, an dem sich die Sicherheitsverantwortlichen in KMU orientieren können. Mit der ISO 27002 wird zwar versucht, die Umsetzung etwas griffiger zu machen, trotzdem tun sich KMU schwer, diese Vorgaben in die Praxis umzusetzen.

Mark Semmler: Der Aufwand, die ISO 27001 umzusetzen, ist zwar weit geringer als beim BSI Grundschutz, überfordert aber noch immer die meisten KMU. ISO 27001 fordert z. B. eine sehr umfassende Analyse und eine ebensolche Dokumentation. Administratoren, IT-Verantwortliche und Geschäftsführer scheuen vor diesem Aufwand zurück und arbeiten lieber nach dem Motto „bisher ist doch alles gut gegangen". Um es mal bildlich auszudrücken: ISO und BSI verfolgen Ansätze, die sie in der Praxis zu Riesen werden lassen, und Riesen lädt man nur ungern zum Abendessen ein.

5 Was ist also bei den Richtlinien VdS 3473 anders?

Mark Semmler: Wir haben von Anfang an daran gearbeitet, die Richtlinien VdS 3473 umsetzbar zu gestalten. Viele Diskussionen im Team drehen sich um die Frage: „Können auch kleine Unternehmen diese Anforderung leisten?" Die drei Grundsätze der VdS 3473 lauten deshalb: Mache es so einfach wie möglich (aber nicht einfacher). Setze das Paretoprinzip um. (Anmerkung der Redaktion: Das Paretoprinzip, benannt nach Vilfredo Pareto, besagt,



Die drei Bausteine der VdS-Cyber-Security – Quick-Check, Quick-Audit und Zertifikat – richten sich vor allem an kleine und mittelständische Unternehmen (KMU)

dass 80 % der Ergebnisse in 20 % der Gesamtzeit eines Projekts erreicht werden.) Gib dem Unternehmen möglichst großen Gestaltungsspielraum. Damit heben wir uns sehr weit von ISO und BSI ab. Das bisherige Feedback aus den Unternehmen gibt uns offensichtlich Recht. Übrigens werden wir eine Umsetzungshilfe für die VdS 3473 entwickeln, um den Aufwand für KMU nochmals zu reduzieren. Wir möchten den Unternehmen sämtliche Vorlagen an die Hand geben, die nötig sind, die VdS 3473 umzusetzen. Die Unternehmen sollen nicht das Rad neu erfinden, sondern ihre Ressourcen sinnvoll einsetzen.

Michael Wiesner: Wir versuchen uns dabei auf das Wesentliche zu konzentrieren und einen direkten Praxisbezug für KMU herzustellen. Das war und ist natürlich nicht immer einfach, da ständig der Spagat zwischen Umsetzbarkeit und zwingender Notwendigkeit von einzelnen Vorgaben gemacht werden muss. Der wichtigste Punkt dabei ist, die komplette Vorgehensweise risikobasiert zu gestalten. Ganz ohne einen gewissen Grundschutz geht es natürlich nicht. Der heißt bei uns allerdings Basisschutz und beschränkt sich auf das unbedingt Notwendige.

Unter dem Kurzlink vds.de/cyber sind alle wichtigen Informationen von VdS rund ums Thema Cyber-Security gebündelt

6 Was kann man sich unter „risikobasierter Vorgehensweise“ vorstellen?

Mark Semmler: In der Praxis ist eine Risikoanalyse der Königsweg, wenn man sich effektiv und effizient um Gefährdungen kümmern will. Die VdS 3473 verpflichten ein Unternehmen, einen Basisschutz zu implementieren und sich dann den wirklich kritischen Teilen seiner IT-Infrastruktur zu widmen. Für diese muss eine Risikoanalyse und -behandlung durchgeführt werden.

Michael Wiesner: Exakt. Identifiziere deine „Kronjuwelen“ und schütze diese mit geeigneten Maßnahmen. Das ist natürlich leichter gesagt als getan. Für die Unternehmen bedeutet dies, dass sie sich zunächst einmal mit ihren Unternehmenswerten und Geschäftsprozessen auseinandersetzen müssen.

Im Grunde genommen müssen Unternehmen also zunächst eine Business-Impact-Analyse (BIA) durchführen. Allerdings fordern wir dies nicht in der Ausprägung wie andere Normen. Wir können hier keine 100 Prozent erreichen. Daher beschränken wir uns auf die allerwichtigsten Kernprozesse und risikobehaftete Prozesse, die wirklich katastrophale Schäden für das Unternehmen bedeuten, wenn diese nicht funktionieren, und schauen, welche Daten und IT-Systeme dafür notwendig sind. Je nach Anforderung an Vertraulichkeit, Integrität und Verfügbarkeit sind diese dann entsprechend zu schützen.

7 Und wenn diese Herangehensweise für größere Unternehmen nicht ausreicht? Insbesondere für den gehobenen Mittelstand könnte dies der Fall sein.

Michael Wiesner: Die VdS 3473 definieren ein gutes Schutzniveau, das klar eingegrenzt und versicherbar ist. Wenn ein Unternehmen in der Lage ist, eine komplette BIA auf Basis eines anerkannten Standards wie BSI 100-4 oder ISO 22301 durchzuführen, empfehlen wir dies ausdrücklich.

Für die meisten KMU ist dies jedoch nicht umsetzbar. Falls doch einmal die nötigen Ressourcen vorhanden sind, ist es jederzeit möglich, von VdS 3473 in Richtung ISO-Normen „upzugraden“, da Kompatibilität besteht.

8 Sind die VdS 3473 dann überhaupt auch für größere Unternehmen geeignet? Wo ziehen Sie hier die Grenze?

Michael Wiesner: Der Fokus richtet sich klar auf kleine und mittlere Unternehmen. Für KMU gibt es jedoch unterschiedliche Definitionen, z. B. über die Mitarbeiteranzahl oder den Jahresumsatz. Wir können diese Unterscheidung nicht treffen und überlassen es den Unternehmen selbst, ob sie die Richtlinien für sie passend halten oder nicht.

Bei größeren Unternehmen stellt sich diese Frage meist nicht, da entsprechende Rollen im Informationssicherheitsmanagementprozess ausreichend besetzt sind und längst ein Standard oder Framework ausgewählt oder entwickelt wurde.

Mark Semmler: Hier muss ich widersprechen. Viele größere Unternehmen beginnen erst jetzt, ihre Informationssicherheit strukturiert anzupacken. Wir haben bei der Vorstellung der VdS 3473 auf der CeBIT und danach zu unserer eigenen Überraschung erstaunlich viel Feedback von Unternehmen und Behörden erhalten, die aufgrund ihrer Nutzerzahlen ganz sicher nicht mehr zum klassischen Mittelstand zählen. Auch diese Organisationen scheinen sich in den VdS 3473 wiederzufinden und sie als Alternative zu ISO, BSI und eigenen Entwicklungen zu sehen. Es bleibt spannend!

9 Wie ist es denn überhaupt aktuell mit der Informationssicherheit bei KMU bestellt?

Mark Semmler: Aus dem Blickwinkel von fast fünfundzwanzig Jahren Praxis kann ich sagen, dass sich die Lage in den letzten Jahren nicht wesentlich verbessert hat. Diese Aussage mag resigniert erscheinen, aber sie spiegelt die Realität wider.

Informationssicherheit wird noch immer nicht als eine Aufgabe der Führungsebene verstanden und wird dementsprechend in den meisten Unternehmen auf Schultern abgeladen, die die damit verbundenen Aufgaben nicht stemmen können. Jeder Administrator, der einmal versucht hat, ohne Rückendeckung von ganz oben Informationssicherheit in „seiner" IT-Infrastruktur zu implementieren, kann davon ein Lied singen ...

10 Was versprechen oder erhoffen Sie sich persönlich von den neuen Richtlinien? Wo sehen Sie sie in einem Jahr?

Michael Wiesner: Ich erhoffe mir, dass die VdS 3473 von den Unternehmen angenommen werden. Als praxisnaher Leitfaden, auch wenn die Zertifizierung nach VdS 3473 nicht direkt angestrebt wird. Die Richtlinien sollen dabei helfen, das Informationssicherheitsniveau bei KMU zu erhöhen. Denn hier gibt es noch an vielen Stellen eine Menge Nachholbedarf. Wenn sich abzeichnet, dass wir mit unserer Arbeit einen Teil zu diesem Ziel beitragen konnten, bin ich persönlich sehr zufrieden. Ich denke, dass wir durch die Evaluierung in der Praxis noch einmal konstruktive Rückmeldungen erhalten werden, um die VdS 3473 weiter zu verbessern.

Mark Semmler: Der Slogan „VdS Cyber-Security – Der Brandschutz des 21. Jahrhunderts" trifft den Nagel auf den Kopf. In Sachen Informationssicherheit stehen wir heute dort, wo wir im Brandschutz vor 100 Jahren waren. Es ist aber dringend nötig, die Informationssicherheit in KMU auf ein Niveau zu heben, das den aktuellen Anforderungen entspricht. Heute ist der Brandschutz längst akzeptiert. Es ist eine Selbstverständlichkeit, dass bestimmte Unternehmen einen Brandschutzbeauftragten haben. Rauchmelder, Sprinkleranlagen und Brandschutzübungen sind heute Standard, weil sie Menschenleben und Unternehmenswerte schützen. VdS hat hier unendlich viel geleistet, und dieser Erfolg sollte auch der VdS Cyber-Security beschieden sein. Das Dreigestirn VdS Quick-Check, VdS Quick-Audit und VdS 3473 Zertifikat hat das Potenzial, die Informationssicherheit auf breiter Basis anzuheben, und ich wünsche mir, dass die VdS 3473 von möglichst vielen Unternehmen umgesetzt werden.

Obiger QR-Code leitet Ihr Smartphone direkt zum Download der VdS-Broschüre „Cyber-Security für kleine und mittlere Unternehmen (KMU)"