P R E S S E M I T T E I L U N G

Rhein S.Q.M. GmbH, Ebereschenweg 2a, 67067 Ludwigshafen

29. November 2016

ISO 27001 oder Eine IT-Norm, die alle etwas angeht!

Wer glaubt, ein Unternehmen müsse sich nur mit der Zertifizierung nach DIN ISO/IEC 27001 beschäftigen, wenn es zu den schätzungsweise rund 2.000 sogenannten KRITIS-Betreiber gehört, die bisher vom Gesetzgeber dazu verpflichtet wurden, irrt. Wolfgang Rhein, dessen Qualitätsmanagement-Beratung Rhein S.Q.M. GmbH Unternehmen unter anderem auch im Bereich IT-Sicherheitsgesetz und ISO 27001 berät, warnt alle Organisationen vor Schadenersatzansprüchen im Fall von Industriespionage und Cyberattacken.

„Wenn in einem Monat in Deutschland gut 10.000-mal nach ‚ISO 27001' und verwandten Begriffen gegoogelt wird, dann kann man davon ausgehen, dass das Thema gerade in den Unternehmen wieder brodelt", konstatiert denn auch Peter Miller, der als Experte für IT-Sicherheit Unternehmen im Auftrag von Rhein S.Q.M. berät. Diese Aufmerksamkeit kommt dabei nicht von ungefähr: Schlagzeilen zu Krypto-Trojanern, die – in Krankenhausrechner eingeschleust – die Gesundheitsversorgung lahmlegen oder Unternehmen, die Millionenbeträge in der virtuellen Bitcoin-Währung als Lösegeld berappen, um Datenlecks wieder zu stopfen, feuern die Debatte regelmäßig von Neuem an.

Nur noch etwas mehr als ein Jahr Übergangsfrist

Für einige Unternehmen drängt tatsächlich mittlerweile die Zeit. Der Gesetzgeber hat im Juli 2015 das „Gesetz zur Erhöhung der Sicherheit informations-

technischer Systeme“ verabschiedet, dessen sperriger Titel landläufig mit „IT-Sicherheitsgesetz“ verkürzt wird, und ergänzend am 3. Mai 2016 die sog. KRITIS-Verordnung in Kraft gesetzt. Danach werden Unternehmen, die die Grundversorgung der Bevölkerung mit Strom und Gas gewährleisten, gesetzlich verpflichtet, bestimmte Anforderungen zu erfüllen, zu denen unter anderem auch die Zertifizierung nach ISO 27001 gehört. Bis 31.1.2018 müssen also zahlreiche Strom- und Gasnetzbetreiber der Bundesnetzagentur ein ISO-27001-Zertifikat vorlegen, das die Umsetzung des IT-Sicherheitskataloges dokumentiert. „Wenn man bedenkt, dass man in nahezu allen Projekten von mindestens sechs, eher aber neun Monaten Vorbereitungszeit ausgehen muss, sollten sich die betroffenen Unternehmen zeitnah mit dem Thema befassen und im 1. Quartal 2017 zumindest schon mal erste Grundüberlegungen und Abschätzungen zu den benötigten Ressourcen durchführen“, rechnet Miller vor. Die verbleibende Frist, ergänzt der QM-Berater und Lead Auditor, sei vor allem dann knapp, wenn ein zertifizierungsfähiges Informations-Sicherheits-Management-System (ISMS) komplett neu eingeführt werden müsse. Die Erfahrung aus vergangenen Zertifizierungsvorbereitungen zeigt: Selbst wenn die IT relativ gut dasteht, das heißt beispielsweise eine Netzwerk- und Hardwareplanung vorliegt oder Rollen- und Berechtigungskonzepte definiert sind, gibt es oft noch Lücken zwischen dem, was da ist und dem, was die ISO 27001 fordert. Im Besonderen ist hier auf die Dokumentation und Nachvollziehbarkeit der Prozesse und Anforderungen hinzuweisen – die aus Erfahrung in der Regel unvollständig oder weitgehend nicht vorhanden sind.

Die drei Schritte zur Zertifizierung

Die Vorbereitung auf die ISO-27001-Zertifizierung startet daher auch stets mit einem Workshop, der der Bestandsaufnahme beim Kunden dient und für den

etwa drei Tage veranschlagt werden müssen. Mittels dieser GAP-Analyse wird aufgenommen, was schon da ist – schließlich ist das Ziel immer, auf einer bestehenden Systematik aufzubauen – und mit den Anforderungen der Norm abgeglichen.

In einem zweiten Step, der sechs bis neun Monate in Anspruch nimmt, werden die identifizierten Lücken nach und nach geschlossen. Möglich ist das Ganze nur, wenn das Management voll dahintersteht, daher muss die Zertifizierung auf oberster Ebene aufgehängt sein. Schließlich sind Aspekte wie Unternehmenspolitik, Unternehmensleitlinien oder Freigabe durch die Geschäftsführung nicht nur „nice to haves“, sondern inhaltliche Bestandteile der Zertifizierung nach der ISO 27001. „Die oberste Führungsebene trägt also ganz offiziell die Verantwortung für das Informations-Sicherheits-Management-System.“, stellt Miller klar und ergänzt: „Was natürlich nicht ausschließt, die Umsetzung zum Beispiel an den IT-Leiter zu delegieren.“ Die Frage hingegen, ob die Zertifizierungsvorbereitung komplett an einen externen Partner outgesourced werden kann, muss ganz klar verneint werden. Unternehmen können sich Anregungen und Ansätze von außen holen und auch die erforderlichen Dokumente extern schreiben lassen. Die Umsetzung muss aber zwingend intern erfolgen.

Denn beim dritten Schritt, dem Audit, reicht nur die Theorie nicht aus. Im Vergleich zu anderen Zertifizierungen kann die Norm nicht nur formal, also mit einer Dokumentenprüfung, abgebildet werden, sondern beim Audit wird explizit auch die Umsetzung, also die Praxis, geprüft. Bei guter Vorbereitung sei die Zertifizierung selbst aber eigentlich nur noch Formsache, beruhigt Miller.

Konkrete Controls sorgen für gute Umsetzbarkeit

Während die Revision der ISO 9001:2015 durch Unschärfen und wenig klare Forderungen in die Kritik geraten ist, enthält die ISO 27001 sehr konkrete Maßnahmenforderungen. Diese werden im Annex A der ISO 27001 (siehe auch ISO 27002) auf Basis einer Art Checkliste ins eigene Unternehmen und in die eigenen Prozesse eingebunden und umgesetzt. Ergänzt wird das Grundgerüst aus ISO 27001 und 27002 durch die Normen ISO 27017, ISO 27018 sowie der ISO 27019, die erweiterte Controls enthalten, und die als „Can dos" im Gegensatz zu den „Must dos" der Basisnorm freiwillig sind. Eine Ausnahme allerdings stellen hier wiederum die KRITIS-Unternehmen aus der Energieversorgungsindustrie dar: Um die Anforderungen aus dem IT-Sicherheitsgesetz erfüllen zu können, ***müssen*** sich diese ergänzend zur ISO 27001 mit dem Zusatz ISO 27019 zertifizieren lassen.

Vertragliche statt gesetzliche Verpflichtung

Freiwillig ist die gesamte ISO 27001 momentan noch für alle nicht in der KRITIS-Verordnung benannten Organisationen. Allerdings wird in einem zweiten Teil der KRITIS-Verordnung, die bereits für Anfang 2017 erwartet wird, die Definition, wer als Grundversorger eine Rechtspflicht zur Gewährleistung von IT-Sicherheit zu erfüllen hat, weiter ausgedehnt. So könnten Rechenzentrumsbetreiber, die Finanz- und Versicherungsbranche oder der gesamte Gesundheits- und Medizintechnikbereich bald unter die Verpflichtung fallen.

Manchmal ergibt sich eine Verpflichtung aber auch gar nicht über den Gesetzgeber, sondern durch kundenspezifische Forderungen, die beispielsweise Automobilhersteller mit ihren Zulieferern vertraglich vereinbaren. Damit begegnen Auftraggeber proaktiv dem oft noch fehlenden Sicherheitsverständnis und dem

mangelhaften Risikobewusstsein ihrer Dienstleister. Ganz überraschend kommen diese Anforderungen im Übrigen nicht: „Die erste Welle mit Forderungen nach Erfüllung der ISO-27001-Standards gab es von den Automobilherstellern bereits 2009“, erinnert sich Miller. Die folgende Wirtschaftskrise habe die Bemühungen etwas ausgebremst, aber die Forderung, dass man sich als Zulieferer um IT-Sicherheitsstandards kümmern sollte, stand im Prinzip seither im Raum. Doch erst seit die Hersteller wieder konkret auffordern, die Zertifizierung durchzuführen, und zeitgleich Negativschlagzeilen von organisierter Internetkriminalität die Runde machen, erhält das Thema wieder höhere Priorität und auch eine gewisse Dringlichkeit.

„Stand der Technik“ als Maxime für alle Unternehmen

Doch Ausfälle bei den IT-Systemen kann sich in einer modernen Gesellschaft heute auch außerhalb der KRITIS-Betreiber kaum jemand leisten. „Deshalb gehören zur ISO-27001-Zielgruppe nicht nur die Unternehmen, die von Gesetzeswegen müssen, sondern im Prinzip alle Unternehmen weltweit.“, bringt es Wolfgang Rhein, Gründer und Geschäftsführer der Rhein S.Q.M. GmbH auf den Punkt. Das, so Rhein weiter, ergebe sich schlichtweg daraus, dass die ISO 27001 den Stand der Technik widerspiegle, und man, sollte man diesen als Unternehmen nicht erfüllen, eine große Angriffsfläche biete. Tritt nämlich eine IT-Störung auf und hat ein Unternehmen nicht nachgewiesenermaßen im Vorfeld strukturiert potenzielle Risiken identifiziert, die auf die Informationssicherheit einwirken könnten, und keine Sicherungsmaßnahmen entwickelt, um diese Gefährdungen zu eliminieren bzw. zu minimieren, kann ihm schuldhaftes Handeln vorgeworfen werden. Im Zuge der Überarbeitung der Normen haben unter anderem der risikobasierte Ansatz in der ISO 9001:2015 und das Risikomanagement in der ISO 27001:2013 Einzug gehalten. Die Bewertung des

eigenen Unternehmens wird dadurch mehr in den Mittelpunkt gerückt, und somit können bekannte und erkannte Risiken als Chancen genutzt werden.

„Insbesondere“, da ist sich Rhein sicher, „gilt das für große Konzerne die sich die ISO 27001, deren Umsetzung in der Tat nicht ganz günstig ist, auch leisten könnten. Im Falle einer Klage – zum Beispiel aufgrund von Datenschutzproblemen – würde vermutlich jeder Richter befinden, dass von großen Unternehmen erwartet werden kann, die Anforderungen aus der Norm zu erfüllen. Urteile werden ‚nach Stand der Technik‘ gefällt und wenn man exakt dieses durch eine ISO-27001-Zertifzierung nachweisen kann, kann man sich gegen Klagen absichern und Schadenersatzansprüche abwehren. Im anderen Fall könnte der Richter entscheiden, dass das Unternehmen schuldhaft gehandelt hat.“ Und das wird dann unter Umständen viel teurer als die ISO-27001-Zertifizierung gewesen wäre.

(1.262 Wörter, 9.501 Zeichen inkl. Leerzeichen)

P R E S S E M I T T E I L U N G

Hintergrundinformationen zur Rhein S.Q.M. GmbH

Die Organisationsberatung Rhein S.Q.M. wurde 2004 in Ludwigshafen gegründet und 2013 in eine GmbH umgewandelt. Der Schwerpunkt liegt bis heute im Bereich des Qualitätsmanagements für die Automobilindustrie sowie die Luft- und Raumfahrtbranche, auch wenn das Team rund um Gründer und Geschäftsführer Wolfgang Rhein zwischenzeitlich international in über 40 Branchen mit einer Abdeckung von mehr als 50 Regelwerken und Standards tätig ist. Die Leistungen in der Qualitätsmanagement-Beratung sowie im integrierten Management erstrecken sich dabei auch auf angrenzende Bereiche wie Umweltmanagement, Energiemanagement, Arbeitsschutzmanagement, Hygienemanagement sowie die Integration branchenspezifischer Standards. Neben der Beratung und operativen Unterstützung beim Aufbau und der Zertifizierung von Managementsystemen werden über die eigene Qualitätsakademie Seminare, Trainings und Workshops angeboten. Die Rhein S.Q.M. GmbH begleitet Organisationen außerdem dabei, die Einhaltung von Kunden- und Branchenforderungen in der gesamten Lieferkette sicherzustellen. Mehr Informationen zum Unternehmen sowie seinen Dienstleistungen im Internet unter www.qm-projects.de.

Pressekontakt

Wolfgang Rhein

Rhein S.Q.M. GmbH, Ebereschenweg 2a, 67067 Ludwigshafen

Telefon: +49 6061-9674-15, E-Mail: presse@qm-projects.de

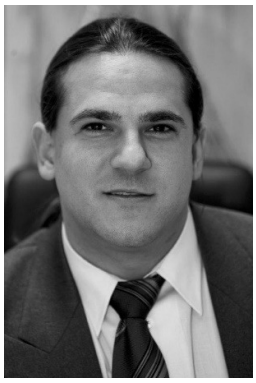
P R E S S E M I T T E I L U N G

Verfügbares Bildmaterial

Bildunterschrift

Peter Miller ist im Partnernetzwerk der Rhein S.Q.M. GmbH einer der Experten für IT-Sicherheit.

Dateiname: “20161129_Peter-Miller_Experte-ISO-27001-IT-Sicherheitsgesetz_Rhein-SQM.jpg”



Bildunterschrift

Wolfgang Rhein, Gründer und Geschäftsführer der Rhein S.Q.M. GmbH, sieht die ISO-27001-Zertifizierung für alle Unternehmen als relevant an.

Dateiname: “20161129_Wolfgang-Rhein_Qualitaetsmanagement-Experte-Rhein-SQM.jpg”