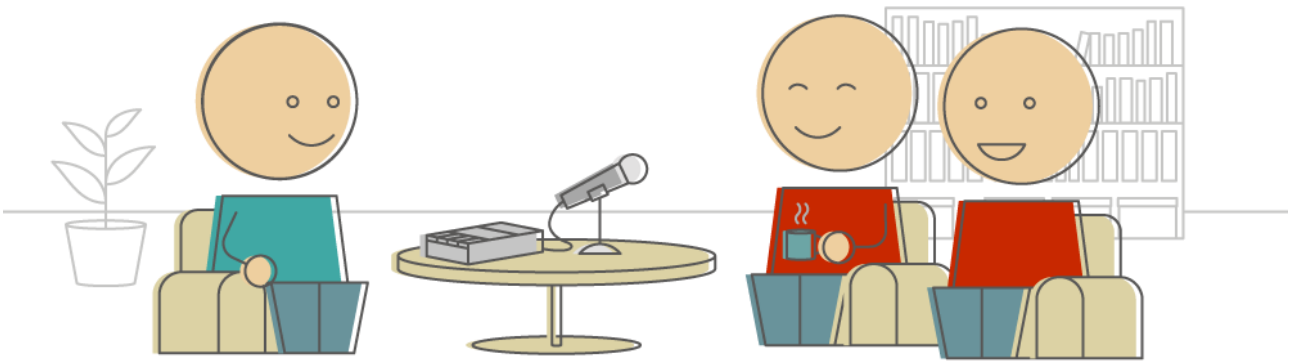
ISO 27001 – Die Implementierung in der Praxis

SECURITY EXPERTEN IM INTERVIEW

Wien, im Jänner 2020

In der ISO 27001 Norm sind die Anforderungen für Einrichtung, Umsetzung, Aufrechterhaltung und fortlaufende Verbesserung eines Informationssicherheits-Managementsystems (ISMS) festgelegt. Als professioneller IT-Dienstleister hat sich die d-con.net GmbH verpflichtet gefühlt, selbst ein ISMS aufzubauen und das Unternehmen nach ISO 27001 zertifizieren zu lassen. Dabei war das primäre Ziel, das Vertrauen der d-con.net Auftraggeber weiter zu stärken – durch angemessene technische und organisatorische Vorkehrungen rund um die Norm. Hier im Interview berichten die Hauptakteure der Implementierung, dass die Ergebnisse das ursprüngliche Ziel weit übertroffen haben.



David Rosenberg ist der Sicherheitsbeauftragte von d-con.net. Er hat die Einführung des ISMS federführend geleitet. David Rosenberg ist Project Manager bei d-con.net und verfügt über langjährige IT-Erfahrungen, die er unter anderem als Leiter von europaweiten Großprojekten sammeln konnte.

Roman Rathler ist der technische Leiter von d-con.net. Zuständig für das Business Development des Unternehmens hat er auf die Entwicklung des ISMS starken Einfluss genommen. Roman Rathler ist seit über 20 Jahren im Netzwerk- und Security-Bereich tätig und verfügt über tiefgehendes praktisches Know-how im Aufbau sicherer Infrastruktur.

Lesen Sie auf den folgenden Seiten den spannenden Bericht der beiden vom Weg zur Zertifizierung.

Seit März 2019 ist d-con.net offiziell nach ISO 27001 zertifiziert.
Warum habt ihr euch überhaupt darauf eingelassen?

Roman Rathler: Ganz ehrlich, unser ursprüngliches Motiv war schlichtweg ein Marketingmotiv. Als IT-Security Anbieter wollten wir unseren Auftraggebern nachweisen können, dass wir selbst modernen Sicherheitsstandards folgen und unsere Prozesse dementsprechend ausgerichtet sind. Dafür ist uns die ISO 27001 Plakette als passendes Mittel erschienen. Wir sind davon ausgegangen, dass uns die Zertifizierung vor allem bei Großkunden dabei hilft, leichter durch die obligatorischen Lieferantenchecks zu kommen. Kurz gesagt, wir wollten es potenziellen Auftraggebern leichter machen, unser Unternehmen zu beauftragen.

Ist diese Idee aufgegangen?
Hilft die ISO 27001 Zertifizierung euch heute wirklich dabei, Neukunden zu überzeugen?

David Rosenberg: Definitiv ja. Das Zertifikat ist ein Qualitätssiegel, das nicht in Frage gestellt wird. Neue Auftraggeber wissen nun, dass Informationssicherheit bei uns unternehmensweit verankert ist und systematisch gepflegt und weiterentwickelt wird. Uns selbst war allerdings vorab nicht klar, wie steinig der Weg bis zur Zertifizierung sein würde. Wir haben eineinhalb Jahre daran gearbeitet, ein wirklich umfassendes System zu entwickeln und zu etablieren.

„Die ISO 27001 Implementierung hat uns einen kontrollierten Umgang mit allen sicherheitsrelevanten Themen gebracht"
David Rosenberg, Sicherheitsbeauftragter

Warum war es so aufwändig, die praktische Umsetzung der Norm zu verwirklichen?

David Rosenberg: Naja, das fängt schon damit an, dass man erst einmal ein Verständnis dafür entwickeln muss, wie die Norm interpretiert werden muss. Um ein einfaches Beispiel zu nennen: In der ISO 27001 ist an vielen Stellen von „Werten" die Rede. Dass damit Assets zusammengefasst werden, also Computer, Softwarelizenzen, Immobilien, Mitarbeiter usw., ist nicht auf den ersten Blick erkennbar. Wie dieses simple Beispiel zeigt, hat man mit der ISO 27001 keine fertige Anleitung, sondern ein Regelwerk zur Selbstdefinition. Die notwendige Übersetzungs- und Interpretationsarbeit muss man also erst einmal leisten.

Ok, aber Normen sind ja immer abstrakt formuliert.
War das der einzige Grund für die lange Implementierungsdauer?

David Rosenberg: Nein. Der Hauptgrund war, dass wir es uns wirklich nicht leicht gemacht haben. Während der Auseinandersetzung mit der Materie haben wir erkannt, dass die Implementierung der Norm eine Riesenchance für unser Unternehmen bietet. Sie hat uns viele Stellen aufgezeigt, an denen wir Verbesserungen vornehmen konnten. Obwohl diese Optimierungen von der ISO 27001 gar nicht verlangt werden, haben wir sie gleich mit erledigt. Dadurch haben wir ein umfassendes, unternehmensweites System für unser IT-Change Management eingeführt.

Die Arbeit an der ISO 27001 Zertifizierung hat also mehr gebracht als die Plakette?

Roman Rathler: Auf alle Fälle, ja. Durch neu erarbeitete Vorgangsweisen konnten wir einen großen Mehrwert generieren. Mit der Implementierung der ISO 27001 haben wir neben dem IT-Change Management auch einige andere Prozesse standardisiert und in unseren zentralen Tools besser abgebildet. Das hilft uns nun nachhaltig in unglaublich vielen Bereichen. Ein einfaches Beispiel ist das Onboarding eines neuen Mitarbeiters. Alles ist definiert und durchdacht, ein neuer Mitarbeiter ist bei uns nun innerhalb kürzester Zeit produktiv. Bereits am ersten Morgen liegen seine Visitenkarten und sein Büroschlüssel auf seinem Schreibtisch, sein Notebook ist fertig aufgesetzt und seine Accounts sind bereits angelegt. Ein anderes Beispiel betrifft die Implementierung neuer Managed Services. Das „d-con.net Patch Management Service" wurde unter Einsatz unserer neuen Projekt-Standards etabliert. Innerhalb kürzester Zeit waren Ziele festgelegt, Risiken bewertet, Kosten ermittelt, Messkriterien eingeführt, Verantwortliche definiert und dann auf Basis unserer neuen Change-Management Richtlinien implementiert und dokumentiert. Das Service war sehr rasch im produktiven Betrieb und alles in allem kann man sagen, dass wir als Mehrwert eine drastische Qualitäts-Steigerung im IT-Servicemanagement erzielt haben.

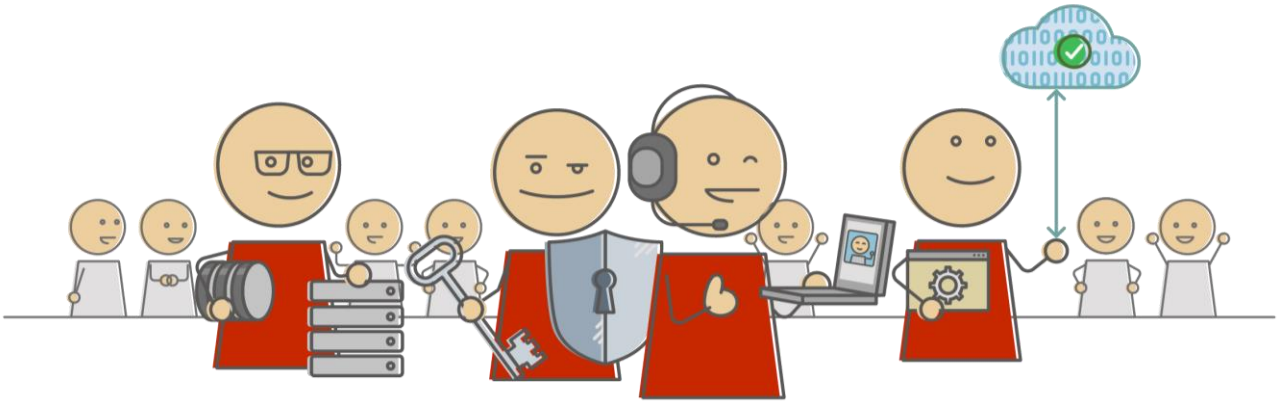
„Ein großer Mehrwert der Implementierung war, dass wir auch die Qualität der Services für unsere Kunden steigern konnten.
Roman Rathler, technischer Leiter

Was kann man Unternehmen empfehlen, die ebenfalls nach ISO 27001 zertifizieren wollen?

David Rosenberg: Als wichtigsten Tipp möchte ich nennen, man soll nicht am falschen Platz sparen. Es zahlt sich hier wirklich aus, externe Kompetenz ins Haus zu holen. Wir hatten zum Glück einen sehr fähigen Berater, der uns vor allem beim Einarbeiten in die Materie geholfen hat. Darüber hinaus macht es Sinn, den Kontakt mit anderen zu suchen, die sich mit derselben Aufgabe beschäftigen oder vielleicht sogar schon zertifiziert sind. Der Erfahrungsaustausch kann viel bringen und helfen, Sackgassen zu vermeiden. Außerdem sollte man unbedingt realistisch bleiben, was den Aufwand betrifft. Die Implementierung braucht einfach Zeit, vor allem wenn man so gründlich vorgeht, wie wir das getan haben.

Roman Rathler: Alle Kollegen in technisch arbeitenden Unternehmen sollten sich bewusst sein, dass die technische Umsetzung bei der ISO 27001 Implementierung das geringste Problem darstellt. Mit dem Informationssicherheit-Managementsystem (ISMS) wird ein organisatorisches System eingeführt. Dem sollte man noch hinzufügen, dass man sich bei der Implementierung bloß nicht im Detail verlieren darf. Man sollte niemals vergessen, dass die Norm ein Regelwerk zur Selbstdefinition ist. Immer wieder sollte man sich Fragen stellen wie: Was passt in meine Organisation? Was ist relevant für mich? Muss ich das anwenden? Wenn man das beherzigt, dann hat man gute Chancen, aus der Implementierung wirklichen Nutzen zu ziehen.

d-con.net ist ein strategisches Asset



d-con.net ist ein strategischer Dienstleistungspartner. Wir arbeiten laufend daran, unseren Auftraggebern Hochtechnologie zu erschließen und in Best Practices IT-Lösungen verfügbar zu machen. Bei uns erhält man hochmoderne Systeme und leistungsfähige Managed Services, immer am Puls der Zeit. Da unsere Auftraggeber oft international agierende Unternehmen sind, werden unsere Kunden rund um den Globus in ihren Landesniederlassungen auf allen Kontinenten unterstützt.

d-con.net GmbH
Johannesstraße 48a
2371 Hinterbrühl, Österreich
+43 1 616 32 17 – 0
www.d-con.net
office@d-con.net