IT-Security

ISO 27001 - Stempel mit Aussagekraft?

Datum: 19.03.2014
Autor(en): Stanislav Wittmann

Ob unternehmerisches Eigeninteresse oder Kundenforderung - die Gründe für eine Zertifizierung nach ISO 27001 können vielfältig sein. Sicher ist: Der Weg dorthin ist oftmals zeitintensiv und verschlingt viel Geld. Bleiben die Fragen: Wo liegen die Vorteile und wo die Hürden?

Um ins Thema ISO-27001-Zertifizierung einzusteigen, lohnt sich zunächst ein Blick auf das dahinter stehende Regelwerk. Die Grundlage der Zertifizierung bildet die Norm **DIN ISO/IEC 27001**[1]. Ob alte oder neue Norm – beide lassen sich zunächst in drei Teile gliedern. Die neue Norm soll neben vier einleitenden Kapiteln einen Hauptteil mit insgesamt sieben Normforderungen enthalten, die zwecks Zertifizierung zu berücksichtigen sind. Den dritten Teil bildet der Anhang. Dieser besteht aus einer normativen Anlage.

Der normative Teil (Anhang A) ist für die Zertifizierung wegweisend. In diesem sind Maßnahmenziele und Maßnahmen dargestellt - die so genannten "ISO Controls". Sie geben letztlich vor, welche Informationssicherheitsziele umzusetzen sind. Immer vor dem Hintergrund der drei Grundwerte Vertraulichkeit, Verfügbarkeit und Integrität. Wohlgemerkt sind die Vorgaben der Norm keine Bauanleitung, vielmehr Ratschläge zur Umsetzung. Beim **Bundesamt für Sicherheit und Informationstechnik (BSI)**[2] finden sich weitere Tipps - auch die ISO-Norm 27002 bietet Unterstützung, indem sie die Controls der 27001 detaillierter beschreibt. Das Ziel der Norm ist ein ganzheitliches, aber vor allem individuell abgestimmtes Schutzkonzept, das kontinuierlich verbessert und weiterentwickelt wird. Jedes Unternehmen soll für sich selbst entscheiden, welchen Sicherheitsgrad es für angemessen hält.

Die ISO 27001 ist zwar als solche eine neue internationale Norm, gleichwohl übernimmt sie Prinzipien anderer Standards. So ist der Demming-Zyklus ("Plan-Do-Check-Act", kurz PDCA - siehe Grafik unten) auch ein obligatorischer Bestandteil im **Qualitätsmanagement der ISO 9001**[3]. Solche Parallelen helfen bei der Implementierung und macht den Firmen Mut, selbst eine ISO 27001 einzuführen. Wichtige Erkenntnis: Der Weg zur Zertifizierung ist nicht unendlich. Um ihn beschreiten zu können, bedarf es zweier wesentlicher Voraussetzungen. Zum einen einer Führungsebene, die voll und ganz hinter dem Projekt steht (das "Management Commitment"). Zum anderen ausreichender personeller, finanzieller und zeitlicher Ressourcen - diese ergeben sich quasi automatisch, wenn erstgenannte Bedingung erfüllt ist.

Möglichkeiten der Zertifizierung

Die ISO 27001 - Zertifizierung ist an einen Prozess gekoppelt. Zunächst muss das Unternehmen entscheiden, welche Zertifizierung es sich wünscht. Möglich ist diejenige nach ISO 27001, aber auch die so genannte "ISO 27001-Zertifizierung auf Basis IT-Grundschutz". Letztere wird seit dem Jahre 2006 angeboten, ist zwar aufwändiger, aber wegen des höheren Umfangs aussagekräftiger als die "einfache" ISO 27001.

Beide Wege erfordern einen **unabhängigen und zertifizierten Auditor**[4]. Bei den Zertifizierungen gibt es dennoch Unterschiede. **Die ISO 27001-Zertifizierung auf Basis IT-Grundschutz**[5] fordert beispielsweise neben den Controls auch, dass entsprechende Maßnahmen des BSI-Grundschutzkataloges erfüllt sind. Als Richtwert für das Zertifikat dienen 82 Prozent Erfüllungsquote. Dazu das Beispiel "Serverraum" - dieser ist im BSI-Grundschutzkatalog in den Bausteinen der zweiten Schicht **(B. 2.4)**[6] zu finden. Von den dort aufgeführten 16 Maßnahmen müssen mindestens 13 umgesetzt werden, um eine Zertifizierung für den Serverraum zu erlangen. Bestimmte Maßnahmen wie ein Rauchverbot sind dabei obligatorisch.

Jedes Zertifikat ist drei Jahre lang gültig, muss jedoch jährlich durch ein Überwachungsaudit bestätigt werden. Wer sich für eine Zertifizierung entscheidet, sollte zudem mit drei bis fünf Jahren Vorarbeit rechnen, bis der Stempel erfolgen kann.

Anforderungen

Zunächst ist ein Informationssicherheits-Management-System, **kurz ISMS**[7], einzuführen. Es dient als Zentrum für alles, was im Bereich IT-Sicherheit angestellt wird, und ist fortlaufend zu überwachen, zu warten und zu verbessern - am besten durch Fachpersonal in ausreichendem Maß. So benötigt ein mittelständisches Unternehmen mit 500 Mitarbeitern erfahrungsgemäß eine ISMS-Vollzeitstelle.

Ist ein ISMS errichtet, gilt es so genannte Klassifizierungen für Unternehmenswerte festzulegen - erneut vor dem Hintergrund der drei Grundwerte Vertraulichkeit, Integrität und Verfügbarkeit. Die nachstehende Grafik veranschaulicht das anhand eines Drei-Stufen-Modells:

- Stufe 1 umfasst öffentliche Dokumente (Vertraulichkeit), die durch Verfälschung eher unbedeutende Schäden bis 500 Euro verursachen (Integrität) und bei einem Ausfall von einer Woche für das Unternehmen keinen "Beinbruch" darstellen (Verfügbarkeit).
- Stufe 2 umfasst unternehmensinterne Dokumente die bei Verfälschung geringe monetäre Schäden bis 5000 Euro verursachen und nicht länger als 24 Stunden ausfallen dürfen.
- Stufe 3 umfasst vertrauliche Dokumente (Gehälter, personenbezogene. Daten nur für ausgewählte Personen), die bei Verfälschung hohe Schäden über 5.000 Euro verursachen und nicht über drei Stunden ausfallen dürfen.

Das Beispiel ist konstruiert und sicherlich kann es vorkommen, dass Unternehmen auch mehr als drei Stunden Ausfallzeit für

vertrauliche Dokumente tolerieren können. Klar wird jedoch, dass eine Klassifizierung von Unternehmenswerten anspruchsvoll und zeitaufwändig ist. Deshalb braucht es fachkundiges Personal, das idealerweise nicht auch noch Verwaltungsaufgaben in der IT oder ähnliches übernimmt. Es dauert Zeit, eine Risikomatrix aufzustellen, die Risiken der einzelnen Abteilungen zu bewerten und zahlreiche Interviews zu führen. Auch muss die Geschäftsführung regelmäßig über die offen gelegten Risiken unterrichtet werden - dieses "Management Review" steht mindestens einmal pro Jahr an.

Eventuell lohnt es sich, mit Externen zusammenzuarbeiten, die bestimmte Prozesse schneller einführen und dem internen ISMS-Team die Arbeit erleichtern können. Gerade im Bereich "Security Awareness", um die Mitarbeiter für das Thema IT-Security zu sensibilisieren, ist Unterstützung von außen ratsam.

Die Fakten

Nun zu den harten Fakten: Um im KMU-Bereich ein Projekt zur Zertifizierung nach ISO 27001 überhaupt auf die Beine zu stellen, braucht es etwa 30 bis 50 Tage und eine Vollzeitstelle. Eine Zertifizierung kann nach drei Jahren erfolgen. Nach etwa einem Jahr ist der Break Even erreicht - heißt: ein umfangreiches Sicherheitskonzept, welches bei gewissenhafter Umsetzung wenige Schwachstellen besitzt. Ein ISMS erwirtschaftet natürlich keinen direkten Gewinn - kann sich als Investition aber durchaus rentieren.

Hierzu wieder ein Beispiel: In einem Unternehmen verschwinden jährlich etwa fünf Datenträger wie CDs und USB-Sticks und/oder mobile Geräte wie Notebooks, Tablets oder Smartphones - weil sie verloren oder gestohlen wurden. Im Rahmen eines ISMS verfügt das Unternehmen über einen - auch von der ISO-Norm geforderten - Prozess, der derartige Sicherheitsvorfälle abdeckt ("Incident Management"). Er protokolliert ausführlich den Verlust von mobilen Datenträgern und Geräten.

Das Unternehmen stellt fest, dass die Verluste in erster Linie auf Messen und Geschäftsreisen auftreten. Zwei Motive liegen damit auf der Hand: Unachtsamkeit der Mitarbeiter und Spionage. Eine Awareness-Kampagne "Spionageprävention auf Geschäftsreisen" kann Abhilfe schaffen. Eine weitere Möglichkeit ist, alle mobilen Geräte nur mit dem absoluten Minimum an benötigten Daten auszustatten, um mögliche Schäden zu begrenzen. Geht die Zahl der "Incidents" durch die indirekt per ISMS umgesetzten Sicherheitsmaßnahmen zurück, hat sich das Ganze bereits rentiert. Gleichwohl sei gesagt: Ein solcher Prozess ist auch ohne ISMS möglich.

[Hinweis auf Bildergalerie: **Governance-, Risk- and Compliance-Tools, auch für Facebook und Cloud -**] [gal1]

In jedem Fall aber lassen sich durch ein gewissenhaft geführtes ISMS Schwächen aufdecken und potenzielle Risiken vermindern. "Ziel soll es sein, schrittweise das Sicherheitsniveau zu erhöhen, Risiken bewusst zu kontrollieren und das Zertifikat als Bestätigung der erfolgreichen Arbeit zu sehen. Der Lead Auditor sollte dabei als Sparringspartner dienen, der zusammen mit seinem Kunden das ISMS zielgerichtet auf den Scope und die Gegebenheiten ausrichtet", resümiert Andreas Teuscher, Vorstand der **ISACA Germany Chapter e.V.**[8] und ISO 27001 Lead Auditor.

Hürden bei der Einführung

Ein ISMS oder eine **Security Policy**[9] einzuführen, sollte keine großen Schwierigkeiten bereiten. Manch andere Maßnahmen können sich jedoch komplizierter gestalten als zunächst gedacht. So fordert die 27001-Norm unter dem Punkt "personelle Sicherheit" (Iso Control: A 7), Sicherheitsmaßnahmen vor, während und nach dem Anstellungsverhältnis eines Mitarbeiters ein. Maßnahmen vor dem Arbeitsverhältnis können eine Sicherheitsüberprüfung des Bewerbers oder Geheimhaltungsklauseln im Arbeitsvertrag sein. Nach dem Anstellungsverhältnis ist dafür Sorge zu tragen, dass bestimmte Berechtigungen wieder entzogen werden. Während des Arbeitsverhältnisses können Awareness-Kampagnen helfen, die Informationssicherheit aufrecht zu erhalten.

Zu beachten ist bei allen Vorgängen jedoch immer auch das **Bundesdatenschutzgesetz (BDSG)**[10]. "Durch das Ausmaß des heutigen Einsatzes von automatischen bzw. elektronischen Datenverarbeitungssystemen scheint es unvorstellbar, Informationssicherheit ohne Datenschutz umzusetzen", unterstreicht Datenschützer Michael Werner. Unternehmen müssten diverse Paragraphen berücksichtigen, um das Persönlichkeitsrecht zu wahren - hier seien laut Werner insbesondere §3a (Datenvermeidung und Datensparsamkeit) und §5 BDSG (Datengeheimnis) zu nennen. Der Betriebsrat spiele ebenso eine wichtige Rolle, wenn beispielsweise für Mitarbeiter eine Leitlinie für Informationssicherheit erstellt werde.

Die hohe Kunst eines hochwertigen ISMS ist es, den Spagat zwischen den Abteilungen zu schaffen. Gleichzeitig sind sämtliche Maßnahmen zu dokumentieren. "Wer schreibt, bleibt" - hier nicht nur ein Leitspruch, sondern eine klare Forderung der Norm. Die Dokumentationsanforderung (Punkt 7.5 der ISO 27001) dient nicht nur zur Exkulpierung, wenn Rechtsstreitigkeiten vorhanden sind. Je ausführlicher die Dokumentation, desto besser auch für das Audit.

Fazit

Der Gesetzgeber fordert sie nicht ein - gleichwohl erfüllt die ISO 27001 gesetzliche Auflagen und bietet Vorteile. So lässt sich mit ihr eindeutig nachweisen, dass beispielsweise Sicherheitsanforderungen nach **§11 BDSG**[11] erfüllt sind (Erhebung, Verarbeitung, Nutzung personenbezogener Daten im Auftrag). Das ist für Outsourcing-Dienstleister von Rechenzentren und Telekommunikationsanbieter von erheblichem Vorteil.

Jedoch ist die Zertifizierung nicht ausschließlich zur rechtlichen Absicherung gedacht. "Tatsächlich bietet ein zertifiziertes Sicherheitsunternehmen seinen Kunden auf den ersten Blick mehr Sicherheit fürs Geld… das sollte man zumindest denken", sagt der langjährige Unternehmer Thorsten Hoth.

Gerade in diesen Tagen, wo das Thema IT-Sicherheit eine große Aufmerksamkeit erfährt, wird sich der Zertifizierungstrend möglicherweise verstärken. Dennoch ist Vorsicht angebracht, denn eine Zertifizierung hat zunächst nur eine eingeschränkte Aussagekraft. Zumindest verschafft sie einem Unternehmen einen Wettbewerbsvorteil: "Klar ist, dass viele Ausschreibungen, an denen Sicherheitsunternehmen teilnehmen, eine Zertifizierung heutzutage schon selbst fordern oder zumindest wünschen", unterstreicht

Hoth.

Die ISO 27001 ist ein umfassendes Sicherheitskonzept, das unternehmerisches Eigeninteresse widerspiegeln soll - individuell und auf die jeweiligen Bedürfnisse abgestimmt. Wer dabei nicht ehrlich zu sich selbst ist, verliert. Hoth resümiert: "Wer das Qualitäts-Management nicht richtig lebt, hat zwar einen ISO-Stempel, aber keine Garantie für Qualität."

Nur mit eigener Abteilung und Rückendeckung des Vorstands ist eine Zertifizierung sinnvoll. Nur, um gesetzliche Anforderungen zu erfüllen, Wettbewerbsvorteile zu erzielen oder Medienpräsenz zu erhaschen, ist eine ISO 27001 zu "teuer". (sh)

Links im Artikel:

[1] **http://www.beuth.de/de/norm/din-iso-iec-27001/103960154**
[2] **https://www.bsi.bund.de/DE/Home/home_node.html**
[3] **http://www.beuth.de/en/standard/din-en-iso-9001/110767367**
[4] **https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzZertifikat/Veroeffentlichungen/ISO27001Auditoren/auditoren27001.html**
[5] **https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzSchulung/WebkursITGrundschutz/Zertifizierung/Zertifizierungsprozess/zertifizierun**
[6] **https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKataloge/Inhalt/_content/baust/b02/b02004.html**
[7] **http://www.computerwoche.de/a/zertifiziertes-isms%2C2538518**
[8] **http://www.isaca.de/**
[9] **http://www.computerwoche.de/a/richtlinien-sorgen-fuer-mehr-it-sicherheit%2C546399**
[10] **http://www.gesetze-im-internet.de/bdsg_1990/BJNR029550990.html**
[11] **http://www.gesetze-im-internet.de/bdsg_1990/__11.html**
