ISO-Zertifizierung

Sichere Informationen

[21.10.2015] Vertrauen ist gut, Kontrolle ist besser – aus diesem Grund lässt der Zweckverband Kommunale Datenverarbeitung Oldenburg (KDO) die Informationssicherheit seiner Daten per Zertifizierung nachweisen.

Die Informationstechnik hat inzwischen fast alle gesellschaftlichen Bereiche erfasst und ist ein selbstverständlicher und teilweise unsichtbarer Bestandteil des Alltags geworden. Gerade Arbeits- und Geschäftsprozesse basieren zunehmend auf IT-Lösungen, sowohl in der Produktion als auch bei Einkauf, Vertrieb und Verwaltung. Aus diesem Grund wird auch der Schutz von IT-Systemen in Behörden und Unternehmen immer wichtiger. Denn die Liste potenzieller Gefährdungen und Schadensfälle ist lang: Mangelhafte Datensicherung und Befall durch Computer-Viren gehören ebenso dazu wie der kurzfristige Ausfall des Systemadministrators, Hackerangriffe oder Spionage. Unzureichend geschützte Informationen sind ein häufig unterschätztes Sicherheitsrisiko, das massive wirtschaftliche oder Imageschäden zur Folge haben kann. Dabei ist „ein vernünftiger Informationsschutz ebenso wie eine Grundsicherung der IT schon mit verhältnismäßig geringen Mitteln zu erreichen und der Weg zu mehr Sicherheit auch ohne große Budgets möglich“, wie Michael Hange, Präsident des Bundesamts für Sicherheit in der Informationstechnik (BSI) bereits im Jahr 2012 in einem Leitfaden zur Informationssicherheit sagte. Laut BSI ist die noch immer weit verbreitete Ansicht, dass Sicherheitsmaßnahmen zwangsläufig mit hohen Investitionen in Sicherheitstechnik und mit der Beschäftigung hoch qualifizierten Personals verknüpft sind, so nicht haltbar. Das Bundesamt fordert stattdessen einen „gesunden Menschenverstand, durchdachte organisatorische Regelungen sowie zuverlässige und gut informierte Mitarbeiter, die selbständig Sicherheitserfordernisse diszipliniert und routiniert beachten“.

Umfassende Lösung

Informationssicherheit darf allerdings keine Insellösung sein, da sie nicht nur die jeweiligen Einzelorganisationen, sondern auch Partner wie Lieferanten oder IT-Dienstleister betrifft. „Ein Zertifikat bestätigt, dass ein Unternehmen ein angemessenes Sicherheitsniveau erreicht hat, dieses aufrecht erhält und somit ein zuverlässiger Partner ist“, erklärt Matthias Lohmann von der Beratungsfirma Jester Secure IT aus Bergisch-Gladbach. Allerdings koste mehr Sicherheit zunächst einmal Geld – in der Regel ohne erkennbar mehr Umsatz zu generieren. An dieser Stelle sind aber die internen Nutzen nicht zu unterschätzen. Beispielsweise wird laut Lohmann die Qualität der Geschäftsprozesse oder die Kundenbindung verbessert oder die möglichen Verluste infolge von Sicherheitsschwachstellen reduziert. Nicht zuletzt kann sich eine Zertifizierung aber auch durch geringere Versicherungsprämien auszahlen. „Beim Thema Informationssicherheit müssen wir das, was unsere Kunden bisher auf vertraulicher Basis geglaubt haben, jetzt objektiv in Form von Zertifikaten nachweisen“, skizziert Rolf Beyer, Geschäftsführer des Zweckverbands Kommunale Datenverarbeitung Oldenburg (KDO), die jüngsten Entwicklungen. Grund sei ein wachsender Marktdruck durch andere Datenzentralen oder IT-Dienstleister bei öffentlichen Ausschreibungen. „Verfügbarkeit, Integrität und Vertraulichkeit sowie die Kontrolle von Daten sind heute das Gut, mit dem Unternehmen wettbewerbsfähig bleiben“, bestätigt Matthias Lohmann.

Native Implementierung nach ISO

Jester Secure IT implementiert bei der KDO derzeit ein Management-System nach der Norm ISO 27001 nativ, ein international anerkanntes und aus der Unternehmenspraxis stammendes Modell für Informationssicherheit. ISO 27001 auf Basis IT-Grundschutz nennt sich das zweite hierzulande übliche Verfahren. Es wurde Mitte der 1990er Jahre vom BSI entwickelt und gilt nur in Deutschland. Obwohl es sich bei beiden Verfahren um ISO-Zertifizierungen handelt, sind die Ansätze unterschiedlich. Die internationale Norm ISO 27001 nativ geht als Management-System prozesshaft der Frage nach, wie Informationssicherheit in einem Unternehmen gehandhabt wird. Wie werden Sicherheitslücken identifiziert und Sicherheitsmaßnahmen geplant und umgesetzt? Wie werden die Maßnahmen kontrolliert und gegebenenfalls verbessert? „Dabei steht der Schutz verschiedenster Informationen im Mittelpunkt, ob in geschriebener, elektronischer oder gesprochener Form“, erklärt Berater Matthias Lohmann. Der IT-Grundschutz betrifft mehr die Informationstechnik, zum Beispiel die Sicherheit der Server für einen konkret definierten Informationsverbund. Das Verfahren schafft zwar konkrete technische Sicherheit, ist aber unflexibel wenn es um Prozesse oder neue Technologien geht. Warum die KDO die Norm ISO 27001 native präferiert, erklärt Geschäftsführer Rolf Beyer: „Technische Innovationen sind in unserem Unternehmen sehr wichtig und entwickeln sich schneller als man den IT-Grundschutz anpassen könnte. Da würden wir ständig hinterher hängen.“

BSI-Zertifizierung

Allerdings wird in öffentlichen Ausschreibungen zunehmend die Zertifizierung nach BSI Grundschutz verlangt – aus Unwissenheit über die Qualität der nativen Zertifizierung, wie der KDO-Geschäftsführer vermutet. Das kann zur Folge haben, dass fachlich geeignete Anbieter nicht teilnehmen können – und damit die Auswahl für die ausschreibenden Stellen enorm eingeschränkt wird. Darüber hinaus ist bei einer BSI-Zertifizierung immer zu beachten, für welchen Informationsverbund sie vorliegt. Denn beim BSI-Grundschutz wird meist nicht das Unternehmen als Ganzes zertifiziert, sondern lediglich bestimmte Bereiche, etwa ein Fachverfahren, das Helpdesk oder eine Server-Landschaft. Sinnvoll kann auch eine Kombination der beiden Verfahren sein. Mit der ISO 27001 native lässt sich beispielsweise ein Management-System aufbauen und ein bestimmtes Fachverfahren, etwa für das Personenstandswesen, per Add-on-Sicherheitskonzept zusätzlich nach IT-Grundschutz zertifizieren. In einem Übersichtspapier des Branchenverbands Bitkom zur Zertifizierung von Informationssicherheit in Unternehmen kommen die Autoren zu dem Ergebnis, dass für mehr Sicherheit beim Einsatz von IT-Systemen beide Ansätze gleichermaßen geeignet sind. Trotzdem besagt das Papier, dass ISO 27001 native mehr Spielraum besitzt, die BSI-Norm starrer und insgesamt meist aufwendiger ist und aufgrund der speziellen Dokumentationsanforderungen nur als Insellösung betrieben werden kann. Auch bei der internationalen Ausrichtung eines Unternehmens führt laut Bitkom kein Weg am ISO-native-Verfahren vorbei.

()

Dieser Beitrag ist in der Oktober-Ausgabe von Kommune21 erschienen. Hier können Sie ein Exemplar bestellen oder die Zeitschrift abonnieren.

Stichwörter: IT-Sicherheit, Jester Secure IT, BSI, ISO, Bitkom