Die wichtigsten Fragen (und Antworten) rund um ISO 27001

Know-how Die Zertifizierung nach ISO 27001 ist nicht zu unterschätzen, bringt aber viel Mehrwert sowohl für den IT-Dienstleister wie auch den Endkunden. Nachfolgend die wichtigsten Fragen und Antworten, die man sich als Unternehmen stellen sollte.

Von Simon Maurer

ISO 27001, der Standard für Informationssicherheit, ist zweifelsohne die wichtigste Zertifizierung im Informatikumfeld. Aufgrund immer höherer Anforderungen an Datensicherheit sowie zunehmender Cybervorfälle interessieren sich entsprechend immer mehr Unternehmen für das Zertifikat respektive dafür, ob der eigene IT-Dienstleister die Vorgaben der Norm erfüllt. Doch um was geht es bei ISO 27001? Was bringt die Zertifizierung einem IT-Dienstleister, und was bringt es dem Endkunden, auf einen ISO-zertifizierten Dienstleister zu setzen. Antworten auf diese und weitere Fragen:

DER AUTOR

Simon Maurer ist Cybersecurity-Experte und selbständiger Berater. Eine grosse Zahl von Firmen wurden von ihm bei der erfolgreichen Einführung der Informationssicherheit begleitet und beraten. Er wird zudem als externer Lead Auditor für Informationssicherheit bei der Schweizerischen Vereinigung für Qualitäts- und Management-Systeme (SQS) eingesetzt. Er verfügt über Ausbildungen an den Universitäten in Zürich, Boston, Fudan und London. Maurer blickt auf eine über 30-jährige Führungskarriere in der Informatik zurück. simon@maurer.management, +41 79 459 63 91

Was ist Informationssicherheit?

Wenn ich KMU-Firmenchefs diese Frage stelle, dann höre ich oft: «Ja, wir haben Informatiksicherheit». Wenn ich etwas nachfrage, wie genau sie die Informatik in der Firma schützen, dann höre ich Begriffe wie Antivirus oder manchmal auch Firewall.

Ich stelle fest, dass das Bewusstsein für das Thema Schutz der Informationen steigt, nicht zuletzt aufgrund der vielen Vorfälle, die in den letzten Jahren publik geworden sind. Aber vielfach hat das Thema noch nicht die nötige Aufmerksamkeit im Verwaltungsrat und der Geschäftsführung und oft werden die Themen Informationssicherheit, Informatiksicherheit und Datenschutz verwechselt.

Was ist denn diese Informationssicherheit wirklich?

Es geht – wie der Name sagt – um den Schutz von Informationen, und zwar ungeachtet von ihrer Form. Was bedeutet «ungeachtet ihrer Form»? Informationen sind oft in digitalen Formaten vorhanden, aber auch in analoger Form, wie zum Beispiel auf Papier. Oder sie sind als Wissen in den Köpfen der Menschen vorhanden.

Wie kann eine Firma ihre Informationen schützen?

Bei digitalen Informationen sind eine Vielzahl von Schutzmassnahmen nötig. Nur eine Antivirus-Lösung und eine Firewall sind in den meisten Fällen nicht genug. Ein Beispiel: Haben Sie einmal Ihr Backup kontrolliert und geprüft, ob es wirklich funktioniert? Also nicht nur eine Datei wiederherstellen, sondern sämtliche gesicherten Daten? Funktioniert dann Ihr Buchhaltungssystem noch? Und sind Ihre Backup-Daten von Ihren produktiven Daten physisch getrennt – oder könnte ein Hacker auch die Datensicherungen verschlüsseln? Dies ist nur ein einzelnes Beispiel. Der Schutz digitaler Daten ergibt sich aus der Summe einer Vielzahl von untereinander vernetzten Massnahmen.

Der Schutz von analogen Informationen hat aufgrund der Digitalisierung und dem Covid-Lockdown in den letzten Jahren etwas an Bedeutung verloren. Und trotzdem gehen heute noch immer wichtige Original-Dokumente verloren. Sei es durch Unachtsamkeit, Diebstahl oder durch Feuer oder Wasser. Haben Sie alle Ihre gültigen Kunden- und Lieferantenverträge greifbar? Sind alle Personaldossiers während ihrer Aufbewahrungsfristen gesichert? Oder ein ganz einfaches Beispiel: Entfernen Ihre Mitarbeitenden nach den Sitzungen jeweils Informationen an Whiteboards oder auf den Flipcharts? Ist der Papierentsorgungsprozess geregelt und wird er konsequent angewendet? Sie glauben nicht, was ich bei Rundgängen in Firmen alles an vertraulichen Informationen finde, die «einfach so herumliegen», zum Beispiel auch bei den Druckern.

Und wie schützt man denn Informationen in den Köpfen der Menschen? Wenn Mitarbeitende Ihre Firma verlassen, dann nehmen sie ihr Wissen mit, das können Sie nicht verhindern. Aber Sie können sich mit Geheimhaltungsvereinbarungen

bis zu einem gewissen Grad absichern. Wichtig dabei ist, dass diese Vereinbarungen mit Mitarbeitenden und Lieferanten konsequent abgeschlossen werden. Sie sollten auch über die Periode der Beschäftigung hinaus gelten und haben idealerweise kein Verfallsdatum. Noch viel wichtiger ist, dass Sie die Menschen regelmässig schulen und ihnen aufzeigen, wie wichtig der Schutz der Informationen ist und was die Konsequenzen sind, wenn die Regeln der Firma nicht angewendet werden. Sie müssen die Einhaltung Ihrer Regeln auch kontrollieren.

Für den bestmöglichen Schutz der Informationen einer Firma existiert ein internationaler Standard, die Norm ISO 27001. Sie wird zurzeit überarbeitet und sollte noch im Jahr 2022 in der neuen Version erscheinen. Bei der Implementierung dieses Standards in Ihrer Firma profitieren Sie vom Expertenwissen von vielen weltweit tätigen Fachleuten und schützen Ihre wertvollen Informationen dadurch bestmöglich.

Was nützt die Informationssicherheit einem ICT-Dienstleister?

Mit einer ISO-27001-Zertifizierung kann ein ICT-Dienstleister seinen Endkunden nicht nur aufzeigen, dass er das Thema Informationssicherheit ernst nimmt. Vielmehr beugt er auch gegen Ausfälle durch Cybervorfälle vor.

Vorbeugen ist besser als heilen

Zuerst einmal das Thema «Kosten eines Vorfalls» und dazu ein Beispiel. Wieviel Umsatz macht Ihre Firma an einem Arbeitstag? Und wieviel kostet ein Arbeitstag an Löhnen, Dienstleistungen und so weiter? Gehen Sie einmal davon aus, dass Sie bei einem Cybervorfall in Ihrer Firma – zum Beispiel bei einer Verschlüsselung Ihrer Daten durch einen Hacker – während Tagen oder vielleicht sogar Wochen weniger oder sogar keinen Umsatz machen werden, je nachdem wie abhängig Sie von der Informatik sind. Zusätzlich zum Umsatzverlust erhöhen sich die Kosten in Ihrer Firma deutlich. Ich spreche von Kosten für die Schadensbehebung und den Wiederanlauf, aber auch für Löhne und Überzeiten, die zu einem späteren Zeitpunkt geleistet werden müssen, um die aufgestauten Arbeiten nachzuholen. In Einzelfällen kann ein solcher Vorfall für eine Firma lebensbedrohlich werden. Laut einer Studie des deutschen Branchenverbandes Bitkom beliefen sich die Schäden durch Cyberangriffe in den Jahren 2020/21 allein in Deutschland auf 220 Milliarden Euro. Wir sprechen also nicht von Bagatellen.

Prüfen Sie folgendes Szenario: Berechnen Sie eine Woche Umsatzverlust und die doppelten Kosten, welche normalerweise in einer Woche anfallen würden. Nun stellen Sie die einmaligen Projektkosten für den Aufbau und die regelmässigen Kosten für den Betrieb der Informationssicherheit in eine Relation zu den Kosten eines solchen Vorfalls. Vergessen Sie nicht: Wenn Sie nichts tun, kann Sie ein Vorfall jederzeit und wiederholt treffen, im schlimmsten Fall mehrmals pro Jahr. Indem Sie Ihre Firma vor Informationssicherheitsvorfällen schützen, vermeiden Sie bestmöglich die hohen Folgekosten. Sie dürfen davon ausgehen, dass der Aufbau und der Betrieb der Informationssicherheit in Ihrer Firma deutlich weniger kosten als die Behebung der Folgeschäden von Vorfällen.

Was bringt die Einführung der Informationssicherheit sonst noch?

Hier zehn mögliche Beispiele:

1. Das Know-how und die Kompetenzen der Mitarbeitenden steigen in Bezug auf Schutz der wertvollen Informationen.
2. Arbeit wird generell transparenter, verbindlicher und nachweislicher erledigt.
3. Projekte und der Betrieb der Informatik werden noch professioneller.
4. Die Verfügbarkeit der Informatik steigt.
5. Personalprozesse sind strukturierter dokumentiert und nachweislicher durchgeführt.
6. Der Umgang mit Lieferanten wird basierend auf den vorhandenen Risiken professionalisiert.
7. Der Umgang mit Veränderungen wird besser gesteuert.
8. Vorhandene Verbindlichkeiten werden besser erkannt.
9. Die Firma ist auf Vorfälle vorbereitet und kann schneller und besser handeln.
10. Das Risikomanagement wird professionalisiert.

Was nützt die Informationssicherheit den Kunden des ICT-Dienstleisters?

Sofern sich der ICT-Dienstleister durch eine unabhängige und akkreditierte Zertifizierungsstelle auditieren und zertifizieren lässt, können die Kunden des ICT-Dienstleisters darauf vertrauen, dass der internationale Standard ISO 27001 gemäss Vorgaben umgesetzt ist und weiterentwickelt wird. Die Kunden können sich deshalb darauf verlassen, dass die ihrem Dienstleister anvertrauten Informationen bestmöglich informationssicher behandelt werden.

Wichtig ist, dass auch die Zertifizierungsstelle von Bundesstellen regelmässig überprüft und für ihre Zertifizierungstätigkeit offiziell akkreditiert wird. Damit ist sichergestellt, dass sie den höchsten Anforderungen an ihr Personal und ihre Prozesse gerecht wird und somit ihre Audits seriös und professionell durchführt. In der Schweiz sind drei Zertifizierungsstellen von der schweizerischen Akkreditierungsstelle zugelassen. Die Details dazu finden sich auf der Webseite der Bundesverwaltung: sas.admin.ch

Was ist der Aufwand für die Informationssicherheit?

Es lässt sich nicht von der Hand weisen, dass eine ISO-Zertifizierung ein erhebliches Investment von Zeit und Geld bedeutet. Diesen Aufwand an einer Zahl festzumachen, ist unmöglich – zu individuell sind die Voraussetzungen in jedem Unternehmen.

Was ist der Zeitaufwand?

Die meisten Projekte, die ich begleite, dauern zwischen einem halben und einem Jahr. Länger sollte ein Projekt nicht Zeit erhalten, sonst verliert es unterwegs an Momentum. Es ist klar – das Tagesgeschäft hat jeweils Priorität. Aber Change-Projekte, wie die Einführung der Informationssicherheit, brauchen vom zuständigen Team ein dranbleiben, sonst steigt der Aufwand überdurchschnittlich an, weil man sich immer wieder neu ins Thema einarbeiten muss und sich das Know-how nicht zielgerichtet und vernetzt aufbaut.

Wie hoch sind die Kosten?

Unterschätzen Sie diese nicht. Zusätzlich zum Aufwand der internen Mitarbeitenden während des Aufbaus und für den Betrieb der Informationssicherheit kommen oft noch Beratungskosten plus Kosten für die Zertifizierung dazu. In vielen Projekten überlegen sich die Firmen, ihre Be-

triebsplattform in der Cloud neu aufzubauen. Auch hier addieren sich die Projekt- und Betriebskosten. Gesamthaft entstehen substanzielle Investitionen in die sichere Zukunft einer Firma.

Im Idealfall starten Sie mit einer GAP-Analyse durch einen spezialisierten Berater. Während dieser Phase und im Rahmen einer dafür nötigen überschaubaren Investition erkennen Sie den Zustand Ihrer Firma im Kontext der Informationssicherheit und können die Kosten für die Folgephase der Projektumsetzung genauer kalkulieren. Dadurch sind Sie in der Lage, einen fundierten Entscheid zu treffen.

Wieviel Manpower wird benötigt?
Diese ist abhängig von der Firmengrösse und der Ausgangslage, welche im Rahmen einer GAP-Analyse festgestellt werden kann. Erfahrungen zeigen: Während der Projektphase wird gesamthaft zirka eine Vollzeitstelle benötigt. Diese Aufwände verteilen sich jedoch auf verschiedene Rollen in einer Firma, wie zum Beispiel das Management, die Projektleitung, die Informatik, das Personalwesen oder die Beschaffung. Der interne Aufwand ist ebenfalls abhängig von Vorkenntnissen, welche in der Firma vorhanden sind und einem möglichen Einsatz von spezialisierten Beratern.

Was sind Stolpersteine bei der Einführung der Informationssicherheit in einer Firma?

Ich erlebe immer wieder die gleichen Themen. Hier ein paar Beispiele aus meinem Fundus:

Eine Firma will das Zertifikat, weil einer ihrer Kunden es fordert oder weil sie es aus Marketingzwecken haben will. Aber eigentlich möchte man den ganzen Aufwand nicht leisten, und das Management ist auch nicht bereit, sich mit dem Thema zu befassen. Mein Rat an solche Firmen: Macht es richtig oder nicht. Informationssicherheit fängt beim Management an, wenn dieses nicht überzeugt ist, glauben die Mitarbeitenden auch nicht daran.

Der «Das schaffen wir mit links und alleine»-Ansatz: Projekte erhalten zu wenig Zeit und Ressourcen und fehlende Kompetenzen werden ignoriert. Dann macht sich Frust breit, zuerst im Projekt-Team und am Schluss auch im Management, weil die Ergebnisse nicht kommen. Mein Rat an solche Firmen: Holt euch Hilfe in Bezug auf Know-how und ein realistisches Projektvorgehen.

Der Copy/Paste-Ansatz: Man sucht sich im Internet irgendwelche Vorlagen zusammen und dokumentiert wild darauf los, ohne den Kontext der Firma zu kennen und zu beachten. Daraus entsteht ein dokumentierter Soll-Zustand, der mit der Realität innerhalb der Firma nichts zu tun hat. Die Umsetzung eines solchen Idealbildes wird dann zu teuer oder ist überhaupt nicht möglich. Mein Rat an solche Firmen: Bleibt pragmatisch und passt euer Managementsystem der Firmengrösse und der vorhandenen Komplexität an. Holt euch Hilfe, wenn ihr es nicht allein schafft. Die Investition in Beratung ist am Schluss wesentlich kosteneffizienter als ein Übungsabbruch.

Die ISO-27001-Norm wird nicht gelesen und/oder nicht verstanden. Ja, die Sprache eines Normdokumentes taugt nicht als Bettlektüre. Die Aussagen im Dokument lassen viel Interpretationsspielraum zu. Das ist durchaus gewollt, denn diese Norm soll international und in jeder Branche umsetzbar sein. Mein Rat an solche Firmen: Investieren Sie in die Kompetenzen Ihres Personals und lassen Sie Schlüsselpersonen entsprechende Weiterbildungen absolvieren.

Wie also starten mit dem Thema Informationssicherheit?

Diskutieren Sie das Thema im Verwaltungsrat und in der Geschäftsleitung. Wenn Unsicherheiten bestehen, holen Sie sich Hilfe. Lassen Sie von einem qualifizierten Berater eine GAP-Analyse erstellen. Dabei wird geprüft, welche Themen des internationalen Standards ISO 27001 in der Firma bereits gut umgesetzt und dokumentiert sind und welche noch nicht. Mit diesem Ergebnis werden Sie in der Lage sein, einen qualifizierten Entscheid zu treffen, basierend auf einer seriösen Aufwandschätzung. Investieren Sie in die Kompetenzen Ihres Personals. Stellen Sie eine Projektorganisation auf und geben Sie eine ambitiöse, aber realistische Projektplanung vor. Kontrollieren Sie den Projektfortschritt. Und lassen Sie das Managementsystem zertifizieren, ein Audit-Termin treibt die Arbeiten im Projekt an, ähnlich wie eine Prüfung nach einer Ausbildung. Und seien Sie bereit, die nötigen Entscheide zu treffen. ■