datenschutz-berater.de

45. Jahrgang DSB 02/2021

DATENSCHUTZ-BERATER

» Ihr zuverlässiger Partner für Datenschutz und Datensicherheit

Editorial

Stichwort des Monats

Datenschutz im Fokus

Aktuelles aus den Aufsichtsbehörden

Rechtsprechung

ISSN 0170-7256

dfv Mediengruppe

Anna Cardillo und Andreas Bethke

Zertifikat nach ISO/IEC 27001: Wie können Auftragsverarbeiter beim Verantwortlichen „punkten“?

Im letzten Beitrag wurde der „nichtverhandelbare“ Teil der ISO/IEC 27001, sprich die Kapitel 4-10, vor dem Hintergrund beleuchtet, inwieweit die Umsetzungsmaßnahmen bedeutsam für den Datenschutz sein können. Im Ergebnis wurde empfohlen, dass sich der Verantwortliche ein genaueres Bild von der Umsetzung einzelner Maßnahmen machen muss. In diesem Artikel soll der Fokus nun auf einzelnen Maßnahmen aus dem Anhang der Norm ISO/IEC 27001 liegen. Mit deren Darstellung kann ein Auftragsverarbeiter bei einer Prüfung durch den Verantwortlichen das nötige Vertrauen in eine datenschutzkonforme Auftragsverarbeitung aufbauen.

Der Anhang der ISO/IEC 27001

Der normative Anhang A der ISO/IEC 27001 enthält Referenzmaßnahmen und -Ziele, mit deren Umsetzung eine Risikominimierung der Informationssicherheit möglich ist. Diese Liste ist zwar umfangreich, aber nicht abschließend, so dass sich jede Organisation weitere individuelle Maßnahmen überlegen und umsetzen sollte. In der Praxis beschränken sich jedoch die umgesetzten Maßnahmen in einem ISMS oft nur auf den Anhang der ISO/IEC 27001. Die Abschnitte sind nummeriert mit A. 5 bis A. 18. Jeder Abschnitt beinhaltet dabei ein Maßnahmenziel und eine unterschiedliche Anzahl von Maßnahmen.

Der Anhang wird ergänzt durch die ISO/IEC 27002, die sich an dieser Struktur orientiert und zu jeder Maßnahme praktische Umsetzungsbeispiele gibt. Auditoren orientieren sich gern an diesen Beispielen, so dass jeder gut beraten ist, die Maßnahmen in Anlehnung an die ISO/IEC 27002 umzusetzen.

Ausgewählte Maßnahmen

Im Rahmen einer Zertifizierung muss der gesamte Anhang der ISO/IEC 27001 behandelt werden, sofern eine Maßnahme für den Geltungsbereich des ISMS in Frage kommt. Sofern das Unternehmen, das als Auftragsverarbeiter tätig ist und ein ISMS nach ISO/IEC 27001 betreibt, einen Nachweis erbringen möchte, dass es im Sinne des Art. 28 Abs. 3 S. 2 lit. c) DSGVO agiert, können einzelne Aspekte und Maßnahmen einem Verantwortlichen dargestellt werden. Der Absatz der DSGVO referenziert auf Art. 32 DSGVO, in dem es um die „Sicherheit der Verarbeitung“ geht und zielt damit im Kern auf die ISO/IEC 27001. Da nicht alle Maßnahmen aus dem Normanhang für einen Nachweis sinnvoll sind, sollen nun ausgewählte Maßnahmen beleuchtet werden.

A.6.2 Mobilgeräte und Telearbeit

Seit dem Frühjahr 2020 hat das Thema Telearbeit aka „Home-Office“ oder „remote Office“ Fahrt aufgenommen und fast jedes Unternehmen musste sich zwangsläufig der Herausforderung einer Umsetzung stellen. Doch bereits vor diesem Zeitpunkt war der Gebrauch von mobilen Endgeräten wie Smartphones, Tablets, Notebooks etc. in den Unternehmen weit verbreitet. Die Norm definiert das Maßnahmenziel, dass „die Informationssicherheit bei Telearbeit und der Nutzung von Mobilgeräten sichergestellt ist“. Das scheint zunächst leichter gesagt als getan. Die Norm fordert hier indes nur jeweils eine Richtlinie und die Umsetzung von unterstützenden Sicherheitsmaßnahmen, um die Risiken zu minimieren, die durch den Gebrauch von Mobilgeräten oder bei der Arbeit außerhalb des Unternehmens mit Zugriff auf interne Ressourcen entstehen. Die ISO/IEC 27002 schlägt vor, welche Inhalte die jeweilige Richtlinie für Mobilgeräte (Maßnahme A.6.2.1) und die Richtlinie für die Telearbeit (Maßnahme A.6.2.2) haben sollte und welche Themen bei der Erstellung berücksichtig werden sollten.

Für einen Verantwortlichen ist es von großem Interesse, wo seine personenbezogenen Daten verarbeitet werden, womit dies geschieht, von wo und wie der Zugriff auf die Daten erfolgt und wie die Zugänge hierbei abgesichert sind. Die Richtlinie selbst sollte hierbei keine geheimen Informationen wie z. B. Passwörter oder andere Authentifizierungs-Informationen enthalten und kann dem Verantwortlichen bei Bedarf ausgehändigt werden. Alternativ kann der Verantwortliche die Verarbeitung so einschränken lassen, dass Telearbeit nicht erlaubt ist, auch wenn dies in der Praxis wohl oft wenig hilfreich ist.

A.7 Personalsicherheit

Der Bereich Personalsicherheit deckt das gesamte Beschäftigungsverhältnis in den einzelnen Stufen von der Bewerbung über die Beschäftigung bis zum Ausscheiden ab. Ein genauer Blick auf die Maßnahmenziele zeigt, dass sich die Maßnahme nicht nur auf Beschäftigte beschränkt, sondern auch Auftragnehmer umfasst. Gefordert wird, dass sich jeder zum Zeitpunkt der Zusammenarbeit seiner Verantwortlichkeiten und Pflichten in Bezug auf die Informationssicherheit bewusst ist und dass diese auch nach Beendigung der vertraglichen Beziehung bestehen bleibt. Gemeint ist natürlich die Wahrung der Vertraulichkeit. Hierbei hilft die Erstellung eines Verhaltenskodex, der Vorgaben für Beschäftigte und Auftragnehmer in Bezug auf

Geheimhaltung, Datenschutz, ethische Grundsätze, angemessene Nutzung von Ressourcen sowie Geschäftspraktiken des Unternehmens enthält. Viele Unternehmen haben ihren Verhaltenscodex (auch „Code of Conduct") im Internet veröffentlicht (z. B. https://relined.eu/wp-content/uploads/2018/08/20180913-Verhaltenskodex-Relined-Fiber-Network.pdf).

Darüber hinaus spielt die Maßnahme A.7.2.2 der ISO/IEC 27001 eine wichtige Rolle. Diese Maßnahme umfasst ein regelmäßiges Aus-, Weiterbildungs- und Sensibilisierungsprogramm, bei dem nicht nur Aufgaben und Regeln vermittelt werden, sondern auch deren Gründe und Ziele. Gestützt werden sollten diese Maßnahmen durch Überprüfung des vermittelten Wissens. Ein Beispiel wäre eine Sensibilisierung zum Thema „Phishing-Mails" kombiniert mit dem tatsächlichen Versand von solchen E-Mails, bei dem der Mitarbeiter dazu verleitet werden soll, beispielsweise einen Link in der E-Mail anzuklicken.

A.8.1 Verantwortlichkeit für Werte

Das Thema Verantwortung spielt im gesamten Kontext des ISMS nach ISO/IEC 27001 eine große Rolle und findet sich an vielen Stellen wieder. In diesem Zusammenhang fordert die Norm, die „Werte" einer Organisation zu identifizieren und angemessene Verantwortlichkeiten festzulegen. Interessant wird es, wenn man diese Forderung mit dem Abschnitt A.6.2 kombiniert und es um die Mobilgeräte als Werte geht und wie deren Gebrauch und vor allem die Aus- und Rückgabe geregelt wird. Darüber hinaus fallen hierunter auch die Zugangsmöglichkeiten zum Firmennetz aus der Ferne wie z. B. dem Home-Office. Dies kann durch Hardware-Token und/oder VPN-Zugänge geschehen, um deren Verwaltung sich das Unternehmen kümmern muss. In der Regel bietet sich hier ein gut strukturierter und kontrollierbarer On- und Off-Boarding-Prozess an, den es zu etablieren lohnt und der alle Aspekte aus dem Abschnitt A.8.1 regelt.

A.8.3 Handhabung von Datenträgern

Zu Datenträgern gehören die klassischen Medien wie CDs, DVDs, Festplatten, USB-Sticks, aber auch Papier als nicht IT-spezifisches Medium. Jedes Unternehmen sollte sich Gedanken darüber machen, welche Arten von Datenträgern überhaupt (noch) zum Einsatz kommen und wie mit diesen Medien umgegangen wird. Ein besonderes Augenmerk wird für den Verantwortlichen im Kontext der Auftragsverarbeitung immer auf der Maßnahme A.8.3.2 Entsorgung liegen. Diese kann auf vielfältige Weise umgesetzt werden. Wichtig im Sinne des Datenschutzes ist es, dass der Nachweis über die Vernichtung erfolgt. Im eigenen Unternehmen lässt sich diese Forderung oft schwieriger umsetzen, so dass der Einsatz eines Entsorgungs-Dienstleisters sinnvoll ist. Ein Verzicht auf Datenträger scheint nicht praktikabel, solange IT-Client-Geräte wie z. B. Notebooks, PCs oder Server eingesetzt werden, die eine Festplatte beherbergen.

A.9 Zugangssteuerung

Die ISO/IEC 27001 fasst unter dem Begriff Zugang das zusammen, was Datenschützer mit Zutritt, Zugang und Zugriff differenzieren. Die Ursachen liegen in der Übersetzung des englischen Begriffes „access".

Der physische Zugangsschutz wird in Abschnitt A.11 ausgeführt, während sich Abschnitt A.9 sich auf Netzwerke und Dienste bezieht. Es werden vier Ziele definiert:

Erstens ist der Zugang zu Informationen und informations-verarbeitenden Einrichtungen eingeschränkt. Zweitens ist sichergestellt, dass befugte Nutzer Zugang zu Systemen und Diensten haben werden und unbefugter Zugang unterbunden wird. Drittens werden Benutzer für den Schutz ihrer Authentisierungsinformationen verantwortlich gemacht. Viertens ist unbefugter Zugang zu Systemen und Anwendungen unterbunden.

Diese Forderungen sollen über Zugangssteuerungsrichtlinien, Benutzerzugangsverwaltungen, -verantwortlichkeiten und einer Zugangssteuerung für Systeme und Anwendungen realisiert werden. Im Sinne einer praktischen Umsetzung des technischen Datenschutzes heißt das, dass man sich an jedem System authentifizieren (anmelden) muss, dass niemand seine Anmeldedaten mit anderen teilen darf, dass es formalistische Prozesse zur Zuteilung und zum Entzug von Zugangsdaten gibt und dass diese Prozesse auch überprüft werden. Über allem schwebt der Begriff des Berechtigungskonzeptes. Interessant ist die Maßnahme A.9.4.3, die regelt, wie ein System zur Verwaltung von Passwörtern ausgestaltet sein sollte. Mit einem solchen System fällt es Benutzern dann auch nicht mehr schwer, wenn der gleiche Benutzer für unterschiedliche Dienste unterschiedliche Passwörter nutzt. Oft finden sich in den Unternehmen jedoch Systeme mit „Einmalanmeldung", besser bekannt als Single sign-On (SSO). Dabei vertrauen sich die unterschiedlichen Systeme, so dass ein übergeordnetes System die Anmeldung bzw. das Weiterreichen von Authentifizierungsinformationen übernimmt.

Für starke Authentifizierung sollten laut ISO/IEC 27002 neben Kennwörtern auch kryptographische Verfahren, Smartcards, Token oder biometrische Verfahren eingesetzt werden.

A.11 Physische Sicherheit

Auch der physische Zutritt muss betrachtet werden. Das Ziel der Norm kommt auch dem Datenschützer bekannt vor: Unbefugter Zutritt, die Beschädigung und die Beeinträchtigung von Informationen und informationsverarbeitenden Einrichtungen der Organisation sind verhindert. Es

handelt sich hierbei um eine klassische Zutrittskontrolle, die bereits im Anhang des § 9 BDSG-a. F. verankert war. So sind dann auch die Maßnahmen A.11.1.2 Physische Zutrittssteuerung und A.11.1.3 Sichern von Büros, Räumen und Einrichtungen auszugestalten. Dabei gibt die Norm nur wenig Umsetzungsdetails vor, wie z. B. das Führen eines Besucherprotokolls, den Einsatz von elektronisch gestützten Zutrittssteuerungen, Ausweistragepflicht als Kennzeichnung von Mitarbeitern und Besuchern. Es fehlen klassische Maßnahmen wie z. B. der Einsatz von Wachpersonal oder eine technische Kameraüberwachung. Hier ist das Unternehmen jedoch immer frei mehr und treffendere Maßnahmen zu ergreifen.

A.12 Betriebssicherheit

Der Abschnitt A.12 beinhaltet den größten Maßnahmenblock mit insgesamt 7 Zielen. Hierbei geht es um den Schutz vor im Alltag auftretenden Gefahren, wie z. B. die bereits angesprochenen „Phishing-Mails". So beinhalten diese Ziele die Themen Betriebsabläufe und -verantwortlichkeiten, Schutz vor Schadsoftware, Datensicherung, Protokollierung und Überwachung, Steuerung von Software im Betrieb, Handhabung technischer Schwachstellen und Audits von Informationssystemen. Abgesehen vom ersten Thema, bei dem es um interne Abläufe und deren Optimierung geht, kann man die anderen Themen durchaus positiv nach außen darstellen. Dabei zielen die Themen Datensicherung, Schutz vor Schadsoftware und die Handhabung technischer Schwachstellen auf das Schutzziel Verfügbarkeit ab. Zudem kann aufgezeigt werden, wie technische Maßnahmen z. B. ein Anti-Viren- und Spam-Schutz mit organisatorischen Maßnahmen (z. B. Sensibilisierung), wie sie in der Maßnahme A.7.2.2 beschrieben sind, gekoppelt werden. Das Datensicherungskonzept muss dabei nicht komplett offengelegt werden. Auf der anderen Seite verrät der Auftragsverarbeiter kein Geheimnis, wenn er beschreibt, dass es einen Sicherungsserver gibt, der von allen virtuellen Servern stündlich einen sog. Snapshot sichert und zudem täglich in ein separates Rechenzentrum gespiegelt wird, wobei alle Daten stets verschlüsselt sind.

Ein komplexes Thema ist das Ziel A.12.4 Protokollierung und Überwachung. Zur Wahrung der Integrität der Daten ist dies unablässig und jedem ist bekannt, dass die Server- und Clientsysteme und fast jede Software protokollieren. Die Herausforderung besteht allerdings darin, diese Protokolle auch auszuwerten und für einen angemessenen Schutz der Protokolle vor Einsicht und Veränderung zu sorgen. Hierfür hat sich eine Lösung etabliert, die „Security Information and Event Management" (kurz SIEM) heißt. Dahinter verbirgt sich eine Art Protokollserver, der von allen angeschlossenen Systemen generierten Protokolle sammelt und sicher verwahrt. Mittels ausgeklügelter Filterfunktionen kann ein solches SIEM-System dann Warnungen erzeugen und auf protokollierte Ereignisse hinweisen. Wer bereits ein solches System erfolgreich im Einsatz hat, kann sich glücklich schätzen und darf dies auch gerne kundtun. Aber Achtung: Die „Lernphase" mit einem solchen System kann sich unter Umständen auch über ein paar Jahre erstrecken.

Zu guter Letzt wird im Abschnitt A.12 auf das Audit von Informationssystemen eingegangen. Hierbei geht es darum, die Systeme und Betriebsabläufe regelmäßig überprüfen zu lassen. Es bietet sich an, solche Audits durch externe und spezialisierte Unternehmen durchführen zu lassen. Auch dies kann für eine positive Außenwirkung sorgen. Oft verlangen Verantwortliche einen Einblick in Prüfprotokolle oder Auditberichte. Aus den Auditberichten gehen allerdings oft entsprechende Sicherheitslücken hervor, die nicht an Außenstehende kommuniziert werden dürfen und sollten. Hier besteht ein Spannungsverhältnis, was durch an sensiblen Stellen geschwärzte Auditberichte möglicherweise aufgelöst werden kann. Alternativ können Prüfzertifikate, Einhaltebestätigungen und Attestate unabhängiger Prüfer über regelmäßig stattfindende Audits der Systeme und Betriebsabläufe helfen. Eine Regelmäßigkeit in solchen Audits zeigt, dass ein Unternehmen auch an eventuellen Schwachstellen arbeitet. Dies wird durch die Maßnahme A.12.6.1 geregelt.

A.13.2 Informationsübertragung

Der Abschnitt A.13 der ISO/IEC 27001 beschäftigt sich mit der Kommunikationssicherheit im Unternehmen im Allgemeinen. Das Maßnahmenziel A.13.2 hat dabei sowohl die Informationsübertragung intern als auch mit externen Parteien im Fokus. Sofern an dieser Stelle bereits sauber gearbeitet wurde und Richtlinien erstellt wurden, wird die Ausgestaltung eines Auftragsverarbeitungsvertrags in puncto Daten- und Informationsaustausch zwischen Verantwortlichen und Auftragsverarbeiter relativ einfach. Technische Maßnahmen können dabei Austauschplattformen oder aber Verschlüsselungsmechanismen sein. Wie auch immer die Lösung aussieht, wichtig ist, dass Möglichkeiten für einen sicheren Informationsaustausch geschaffen werden.

A.15 Lieferantenbeziehungen

Neben der Kundenbeziehung steht natürlich auch die Lieferantenbeziehung im Fokus der Informationssicherheit. Zu den Lieferanten zählt die Norm auch Dienstleister. Ziel ist es, dass die Unternehmenswerte geschützt sind, zu denen Lieferanten Zugang haben. Hierzu muss zunächst eine Informationssicherheitsrichtlinie erstellt werden. In dieser sollte beispielsweise festgelegt werden, welche Maßnahmen (z. B. verpflichtende Security-Awareness-Schulungen) auch für das Personal von Dienstleistern gelten sollen. Darüber hinaus müssen mit jedem Lieferanten Sicherheitsvereinbarungen geschlossen werden, der Zugriff auf Informationen hat oder haben könnte. Solche Vereinbarungen können auch Vertragsbestandteil werden. Abschließend muss die Lieferkette im Kontext der Informationssicher-

heit betrachtet werden. So müssen sich die Regeln, die für einen Lieferanten gelten, auch auf seine Unterauftragnehmer erstrecken. Diese Maßnahme deckt sich mit der Forderung aus Art. 28 Abs. 4 DSGVO.

Maßnahme A.15.2.1 der ISO/IEC 27001 regelt die Überwachung und Überprüfung von Lieferantendienstleistungen. Die Norm spricht dabei drei Arten der Kontrolle an:

- Überwachen (monitor): Erfassung und ggf. Zusammenstellung von Kennzahlen, die in der Regel automatisiert und in Echtzeit gemessen werden.
- Überprüfen (review): Allgemeine Überprüfung, beispielsweise durch Auswertung von Service-Reports.
- Auditieren (audit): Durchführen oder in Auftrag geben von Audits (formalen Konformitätsbewertungen).

In der Praxis wird im Bereich der Lieferantenaudits nach einem einmaligen Vor-Ort-Audit in der Folge gerne mit Selbstauskünften gearbeitet.

A.16 Informationssicherheitsvorfälle

Ein effektiver Umgang mit Informationssicherheitsvorfällen gehört zu den wichtigsten Komponenten in der Ablauforganisation eines ISMS. Dem Datenschutzbeauftragten spielt das in die Karten, denn ein Datenschutzvorfall ist immer auch ein Informationssicherheitsvorfall. Für das Unternehmen bedeutet die Handhabung von Informationssicherheitsvorfällen, dass Verantwortlichkeiten und Verfahren festgelegt werden müssen, dass Informationssicherheitsereignisse so schnell wie möglich gemeldet und dass Beschäftigte und Auftragnehmer über mögliche Schwachstellen informiert werden. Im weiteren Verlauf müssen die Ereignisse beurteilt und Entscheidungen getroffen werden. Auch über die Reaktion auf Informationssicherheitsvorfälle muss sich das Unternehmen Gedanken machen. Typischerweise wird hier ein Workflow implementiert, der wie folgt aussehen kann:

- Feststellung, dass es sich um einen Informationssicherheitsvorfall handelt.
- Einleitung der erforderlichen Sofortmaßnahmen, um den Schaden zu begrenzen oder zu minimieren.
- Aufzeichnung des Vorfalls.
- Ausübung von Meldepflichten, falls erforderlich.
- Beweissicherung für eventuelle rechtliche Schritte, falls erforderlich.
- Analyse der Ursachen und möglicher Maßnahmen zur Vermeidung künftiger Sicherheitsvorfälle.

Abschließend sollte ein Review des Vorfalls erfolgen, um aus diesem Vorfall zu lernen.

A.18.1 Einhaltung gesetzlicher und vertraglicher Anforderungen

Sofern ein Unternehmen als Auftragsverarbeiter tätig ist und ein Informationssicherheitsvorfall auftritt, der als Datenschutzvorfall einen Verantwortlichen betreffend klassifiziert wird, ergibt sich hier die vertragliche Pflicht der Information an den Verantwortlichen. Um dieses Wissen auf eine breite Basis im Unternehmen zu stellen, welche externe Parteien zu informieren sind, gibt es das Maßnahmenziel A.18.1. In der Praxis bietet es sich an, tabellarische Übersichten zu erstellen, in denen Gesetze, Verordnungen und Verträge aufgelistet sind. Sofern die anhängigen Maßnahmen implementiert sind, ist das Unternehmen wieder einen Schritt weiter in Richtung „Compliance“.

Wo sind die Grenzen?

Aus der Aufstellung der Maßnahmen könnte nun der Eindruck entstehen, dass ein Auftraggeber einen tiefen und breiten Einblick in die Informationssicherheit bekommen soll. Das ist weder beabsichtigt noch zielführend. Wichtiger ist, dass der Auftraggeber als Verantwortlicher im Sinne des Datenschutzes ein gutes Gefühl für den Auftragsverarbeiter und seine Maßnahmen bekommt. Wie weit ein Auftragsverarbeiter dabei ins Detail geht, sollte er gut abwägen und selbst entscheiden.

Fazit:

Für einen Auftragsverarbeiter, der ein ISMS nach ISO/IEC 27001 betreibt, ist es nicht schwer, das Vertrauen eines Verantwortlichen zu gewinnen. Dazu muss er gar nicht alle Karten auf den Tisch legen und dem Verantwortlichen alle Richtlinien vorlegen. Vielmehr kann er einzelne Aspekte mit datenschutzrechtlicher Relevanz hervorheben und zum Beispiel in einer Art „Informationssicherheits-Feelgood-Dokument“ zusammenstellen. Frei nach dem Motto „tu Gutes und rede darüber!“. So gelingt es dem Verantwortlichen, sich ein umfassendes Bild über die Sicherheit der Informationsverarbeitung zu verschaffen. Damit werden weder Geschäftsgeheimnisse verraten noch wird gegen die eigenen Richtlinien verstoßen.

Autoren: **Anna Cardillo ist Rechtsanwältin bei Spirit Legal und spezialisiert auf Datenschutz – und Informationssicherheitsrecht. Sie berät Verantwortliche vor allem bei der Implementierung eines integrierten Informationssicherheits– und Datenschutzmanagements.**

Andreas Bethke ist Diplom Informatiker bei B3. Neben seiner Tätigkeit als externer Datenschutz- und Informationssicherheitsbeauftragter sowie als Datenschutzauditor berät er Unternehmen bei der Implementierung von ISMS nach ISO/IEC 27001.