Informationssicherheit in der Öffentlichen Verwaltung

Als Angestellte im Öffentlichen Dienst oder eines KRITIS-Unternehmens [1] werden Sie vermutlich gerade dabei sein, Ihr eigenes Informations-Sicherheits-Management-System (ISMS) einzuführen. Das neue IT-Sicherheitsgesetz, das der Bundestag am 12.6.2015 verabschiedet hat und das am 24.7.2015 veröffentlicht wurde, zielt darauf ab, die Informationssicherheit in Deutschland zu erhöhen, und stellt dabei die Anforderung an die sogenannten KRITIS, bis Anfang 2018 ein ISMS einzuführen und dieses ISMS nach der ISO 27001 [2] zertifizieren zu lassen.

KRITIS-Sektoren

In § 2 Abs. 10 des IT-Sicherheitsgesetzes werden die Sektoren Energie, Informationstechnik und Telekommunikation, Transport und Verkehr, Gesundheit, Wasser, Ernährung sowie Finanz- und Versicherungswesen als Kritische Infrastrukturen genannt. Weiterhin nennt das IT-Sicherheitsgesetz in § 8 Abs. 1 die Möglichkeit, Mindeststandards für die Sicherheit der Informationstechnik ganz oder teilweise als allgemeine Verwaltungsvorschriften für alle Stellen des Bundes zu erlassen. Bild 1 zeigt die Sektoren, die das Bundesamt für Sicherheit in der Informationstechnik (BSI) nennt.

Sektoren kritischer Infrastrukturen

Bild 1: KRITIS-Sektoren nach BSI

Treffen erster Vorkehrungen

Neu hinzugekommen sind im IT-Sicherheitsgesetz die §§ 8a bis 8d. § 8a nennt die Pflicht der KRITIS zur Umsetzung von angemessenen organisatorischen und technischen Vorkehrungen zur Vermeidung von Störungen der Verfügbarkeit, Integrität, Authentizität und Vertraulichkeit ihrer informationstechnischen Systeme, Komponenten und Prozesse. Die Frist für die Umsetzung beträgt zwei Jahre nach Inkrafttreten der Rechtsverordnung [3]. Der Nachweis für die Erfüllung der Anforderungen kann durch Sicherheitsaudits, Prüfungen oder Zertifizierungen erfolgen. Die Verordnung war beim Bundesministerium des Inneren (BMI) als Referentenentwurf ab 13.1.2016 einzusehen. Die Verordnung nennt eine 500.000er-Regel, nach der Unternehmen zu den KRITIS gehören, wenn jeweils 500.000 oder mehr Bürger von ihrer Leistung betroffen sind. Die Bewertungsskala der Verordnung kann beim BMI eingesehen werden. Aus ihr gehen die Schwellenwerte hervor, die für die jeweiligen Sektoren ausschlaggebend sind, ob eine Organisation zu den KRITIS gehört oder nicht. Man darf erwarten, dass die Schwellenwerte in den nächsten Jahren sukzessive herabgesetzt werden, um zukünftig die gesamte Infrastruktur in Deutschland sicherer zu machen.

Einrichten einer Meldestelle

Zurück zum IT-Sicherheitsgesetz: In § 8b wird gefordert, dass die Betreiber Kritischer Infrastrukturen dem BSI binnen sechs Monaten nach Inkrafttreten der Rechtsverordnung eine Kontaktstelle für die Kommunikationsstrukturen benennen müssen. Diese Stelle muss jederzeit erreichbar sein. Die KRITIS haben dabei erhebliche Störungen der Verfügbarkeit, Integrität, Authentizität und Vertraulichkeit ihrer IT-Systeme, Komponenten oder Prozesse, die zu einem Ausfall oder einer Beeinträchtigung der Funktionsfähigkeit der von ihnen betriebenen Kritischen Infrastrukturen führen können oder bereits geführt haben, zu melden. Die Meldung muss Angaben zu der Störung und den technischen Rahmenbedingungen enthalten, ebenso die vermutete oder tatsächliche Ursache, die Art der betroffenen Einrichtung oder Anlage sowie die Branche des Betreibers. Das Gesetz gibt aber auch die Möglichkeit, dass Organisationen, die dem gleichen Sektor angehören, eine gemeinsame übergeordnete Ansprechstelle benennen. § 8c gibt an, dass die § 8a und § 8b nicht auf Kleinstunternehmen sowie kleine und mittlere Unternehmen anzuwenden sind.

Bußgeldkatalog

§ 14 ist ein weiterer neuer Paragraph, der die Bußgelder definiert. In § 14 heißt es, ordnungswidrig handelt, wer vorsätzlich oder fahrlässig die genannten Vorkehrungen nicht, nicht richtig, nicht vollständig oder nicht rechtzeitig trifft oder eine Kontaktstelle nicht oder nicht rechtzeitig benennt oder eine Störungsmeldung nicht, nicht richtig, nicht vollständig oder nicht rechtzeitig macht. Diese Ordnungswidrigkeiten können mit Geldbußen zwischen fünfzigtausend und hunderttausend Euro geahndet werden.

Recht auf Erhebung von Nutzerdaten

Auch im Telekommunikationsgesetz gab es Änderungen. § 100 Abs. 1 gestattet nun dem Diensteanbieter, die Bestandsdaten und Verkehrsdaten der Teilnehmer und Nutzer zu erheben und zu verwenden, um Störungen oder Fehler an Telekommunikationsanlagen zu erkennen, einzugrenzen oder zu beseitigen. Einschränkungen der Verfügbarkeit von Informations- und Kommunikationsdiensten oder unerlaubter Zugriff auf Telekommunikations- und Datenverarbeitungssysteme werden als mögliche Störungen genannt.

Aufbau der ISO 27001:2013

Wenn Sie oder Ihre Kunden den KRITIS-Sektoren angehören, werden Sie nicht umhinkommen, ein ISMS in Ihrer Organisation einzuführen. Für Ihre ISMS-Einführung gibt es gute Nachrichten. Die ISO/IEC

27001:2013 basiert nämlich seit 2013 auf der neuen ISO High Level Structure [4]. Die Internal Organization for Standardization (ISO) hatte diese Struktur 2010 herausgegeben, um zukünftig eine leichtere Umsetzung unterschiedlicher Normen in einer Organisation zu ermöglichen. Bild 2 zeigt den Aufbau dieser High Level Structure. Alle ISONormen, die nach 2010 veröffentlicht werden, sind in dieses Schema eingepasst. Das bedeutet, die Normen haben gleiche Kapitel und nahezu identische Unterkapitel und Anforderungen. Unterschiede zeigen sich nur hinsichtlich der jeweiligen Ausprägungen einer bestimmten Norm. Siehe Bild 2.

Kommen wir nun zum Aufbau der ISO/IEC 27001:2013. Diese ISO-27001 ist in zehn Kapitel, wovon die ersten drei Kapitel der Einführung dienen, gegliedert. Nur die Kapitel 4 bis 10 haben normativen Charakter und werden bei einer ISO 27001-Zertifizierung geprüft. Weiterhin enthält die ISO 27001 einen Anhang A, der Maßnahmenziele und Maßnahmen enthält, die ebenfalls als Prüfungsgrundlage dienen. Diese Maßnahmenziele sind direkt aus der ISO 27002, Kap. 5-18 abgeleitet. Bild 3 zeigt Ihnen den Aufbau der ISO 27001, den Sie mit der ISO High Level Structure aus Bild 2 vergleichen können. Siehe Bild 3.

Die einzelnen Kapitel

Das Kapitel 4 KONTEXT DER ORGANISATION fordert, dass sich die Organisation Gedanken über ihren Sinn und Zweck macht. Sie muss sich bspw. die Fragen stellen: Welche Produkte oder Dienstleistungen bieten wir an? Womit positionieren wir uns auf dem Markt? Was unterscheidet uns von unseren Wettbewerbern? Was erwarten unsere Kunden von uns? In Kapitel 4.1 POSITIONIERUNG DER ORGANISATION muss die Organisation Themen auswählen, die ihr Kerngeschäft ausmachen. Also vor allem Prozesse, mit denen die Organisation ihr Geld verdient und die für die Informationssicherheit rele-

Bild 2: Aufbau der ISO High Level Structure

Bild 3: Aufbau der ISO 27001:2013

vant sind. Weiterhin soll die Organisation in Kapitel 4.2 INTERESSIERTE PARTEIEN alle Parteien, auch Stakeholder genannt, kennen und deren Anforderungen berücksichtigen. Diese interessierten Parteien sind in jedem Fall die Kunden, die Mitarbeiter und die Lieferanten. Darüber hinaus muss sie bei der Betrachtung der interessierten Parteien auch an eventuelle Kontakte zu Behörden denken. Anschließend muss die Organisation in Kapitel 4.3 ANWENDUNGSBEREICH klären, ob und wo sie das ISMS einführen möchte. Hat die Organisation nur einen oder mehrere Standorte? Soll das ISMS im ganzen Unternehmen, über alle Standorte oder nur in einem kleinen IT-Bereich eingeführt werden? Wenn alle diese Anfangsfragen beantwortet sind, kann die Organisation die Entscheidung fällen, ein ISMS einzuführen. Diese Entscheidung fällt in Kapitel 4.4 INFORMATIONSSICHERHEITSMANAGEMENT-SYSTEM.

Kapitel 5 FÜHRUNG nimmt die oberste Leitung in die Pflicht. Die oberste Leitung muss in Kapitel 5.1 FÜHRUNG UND VERPFLICHTUNG die Verantwortung für das ISMS übernehmen und sich dazu verpflichten, die Einführung zu unterstützen. In Kapitel 5.2 POLITIK muss die oberste Leitung eine Politik, auch Strategie bezeichnet, vorgeben. In dieser Politik muss sie ihre Verpflichtung für Informationssicherheit gegenüber ihren Kunden, Mitarbeitern und Lieferanten klar dokumentieren. Im Kapitel 5.3 ROLLEN, VERANTWORTLICHKEITEN UND BEFUGNISSE muss sie Verantwortliche für das ISMS bestimmen. Sie muss also mindestens eine Person benennen, die sich um die ISMS-Einführung kümmert, und diese Person den Mitarbeitern bekannt machen. Diese Person muss mit den notwendigen Befugnissen ausgestattet werden, um Änderungen durchsetzen zu können. Ein Informationssicherheitsbeauftragter wird von der Norm nicht konkret gefordert, aber es ist sinnvoll, diese Rolle in der Organisation zu besetzen. Der Informationssicherheitsbeauftragte wird sich dann ähnlich einem Projektleiter um die ISMS-Einführung kümmern und in Awareness-Schulungen [5] das Bewusstsein der Mitarbeiter für Informationssicherheit erhöhen. Weiterhin muss die oberste Leitung einen internen Auditor für die ISO 27001 benennen, der nach Einführung des ISMS regelmäßige interne Audits durchführen wird.

Bei der ISMS-Einführung ist das Kapitel 6 PLANUNG von allen Kapiteln das umfangreichste, trotz seiner wenigen Unterkapitel. Im Kapitel 6.1 MASSNAHMEN ZUM UMGANG MIT RISIKEN UND CHANCEN muss die Organisation ihre Themen aus Kapitel 4.1 und die Anforderungen der interessierten Parteien aus Kapitel 4.2 auf mögliche Risiken oder Chancen untersuchen. Diese Risikoanalysen sind in den meisten Fällen sehr umfangreich, zeitaufwendig und – vermutlich – nie erschöpfend. Außerdem muss die Organisation die möglichen Risiken im Zusammenhang mit den Maßnahmen aus Anhang A betrachten und analysieren. Ist die Organisation mit den Risikoanalysen und

Bild 4: Awareness-Veranstaltungen mit Dresdner IT-Unternehmen

der Bewertung der Maßnahmen aus Anhang A fertig, muss sie eine Erklärung der Anwendbarkeit (Statement of Applicability, SoA) erstellen, aus der hervorgeht, welche Maßnahmen aus Anhang A durch die Organisation nun tatsächlich umgesetzt werden. Erst durch die Ergebnisse der Risikoanalysen aus Kapitel 6.1 kann die Organisation in Kapitel 6.2 INFORMATIONSSICHERHEITSZIELE Ziele bestimmen, die für sie tatsächlich relevant und sinnvoll sind. Dabei ist zu beachten, dass Ziele klar formuliert und messbar sein müssen. Ein mögliches Ziel wäre bspw. Im Jahr 2016 wird ein Mitarbeiter durch ISO-27001-Weiterbildung zum Informationssicherheitsbeauftragten befähigt. Ein anderes Ziel wäre bspw.: Bis März 2017 sind alle Telearbeitsplätze nur noch mit einem Laptop-Gerätetyp ausgestattet, um die Wartung zu vereinheitlichen und zu vereinfachen.

In Kapitel 7 UNTERSTÜTZUNG beginnt die tatsächliche Umsetzung der zuvor geplanten Ziele. Zuerst werden in Kapitel 7.1 RESSOURCEN die erforderlichen Ressourcen bereitgestellt. Ressourcen umfassen bspw. Finanzen für neue Hardware, Software und Weiterbildung sowie Personal. In Kapitel 7.2 KOMPETENZ werden die bereits vorhandenen Kompetenzen überprüft und fehlende aufgebaut. Ziel von Weiterbildungsmaßnahmen ist ein tieferes Wissen der Mitarbeiter im Bereich Informationssicherheit. Das Kapitel 7.3 BEWUSSTSEIN fordert, dass das Bewusstsein der Mitarbeiter für die Informationssicherheit erhöht wird. In Awareness-Schulungen wird sich in den meisten Fällen der Informationssicherheitsbeauftragte vor die Belegschaft stellen und in Vorträgen erläutern, welche Aspekte der Informationssicherheit zukünftig mehr beachtet werden sollen. Siehe Bild 4.

In Kapitel 7.4 KOMMUNIKATION geht es um die Kommunikationsketten. Hier steht die Anforderung, zu klären, wer wann mit wem worüber und wie kommunizieren muss. Wichtig ist hier, dass alle Mitarbeiter ihre jeweiligen Ansprechpartner kennen, mit denen sie im Notfall kommunizieren müssen. Kapitel 7.5 DOKUMENTIERTE INFORMATION fordert die Dokumentation und deren Lenkung. Gelenkte Dokumente haben einen Titel, einen Autor, einen Prüfer, einen Freigeber, eine Versionsnummer, ein Erstellungsdatum, ein Prüfdatum und ein Freigabedatum. In diesem Kapitel werden die Richtlinien erstellt, die von der ISO 27001 gefordert werden.

Das Kapitel 8 BETRIEB fordert die Umsetzung von Prozessen für die Risikoerkennung, Risikobeurteilung und -behandlung. In Kapitel 8.1 BETRIEBLICHE PLANUNG UND STEUERUNG müssen also Prozesse umgesetzt werden, die es den Mitarbeitern ermöglichen, Risiken zu erkennen und zu melden. In Kapitel 8.2 INFORMATIONSSICHERHEITSRISIKOBEURTEILUNG müssen den Mitarbeitern Möglichkeiten gegeben werden, um Risiken beurteilen zu können. Das kann in Form von Checklisten mit Risiko-Schwellwerten geschehen, in denen man anhand von Themen die Kritikalität abschätzen kann. Kapitel 8.3 INFORMATIONSSICHERHEITSRISIKOBEHANDLUNG fordert Maßnahmen, um bekannte Risiken zu behandeln. Dabei muss auch die Dokumentation von Risiken oder Sicherheitsvorfällen für spätere Auswertungen angefertigt werden.

Das Kapitel 9 BEWERTUNG DER LEISTUNG hat das Ziel, die eingeführten Prozesse dahingehend zu überprüfen, ob sie wirksam sind und so umgesetzt wurden, wie sie geplant waren. In Kapitel 9.1 ÜBERWACHUNG, MESSUNG, ANALYSE UND BEWERTUNG wird gefordert, dass die Organisation geeignete Mittel zur Bewertung einsetzt. Kapitel 9.2 INTERNES AUDIT fordert regelmäßige interne Audits. Dabei werden auch Richtlinien und Arbeitsanweisungen auf ihre Wirksamkeit überprüft. Wichtig ist, dass die Audits von unabhängigen Prüfern durchgeführt werden. Zu beachten ist auch, dass der Informationssicherheitsbeauftragte, der das ISMS einführt, das ISMS nicht selbst auditieren kann, da er gegenüber seiner Arbeit nie vollständig objektiv ist und nicht unparteilich prüfen kann. Die MANAGEMENTBEWERTUNG findet in Kapitel 9.3 statt. Dieses Kapitel fordert von der Management-Ebene, die Bewertungen, Analysen und internen Auditberichte zu überprüfen. Diese Managementbewertung sollte mindestens einmal im Jahr stattfinden.

In Kapitel 10 VERBESSERUNG werden die Ergebnisse aus Kapitel 9 überprüft und Entscheidungen zur weiteren Umsetzung des ISMS getroffen. Kapitel 10.1 NICHTKONFORMITÄTEN UND KORREKTURMASSNAHMEN fordert Entscheidungen zum Umgang mit Abweichungen. Und Kapitel 10.2 FORTLAUFENDE VERBESSERUNG hat das Ziel, im Rückblick auf bereits Bestehendes Verbesserungspotenziale zu finden und das ISMS zu optimieren.

Die ISO 27002 ist ein Standardwerk aus der ISO-27000er-Reihe, das die Best Practice für die Implementierung eines ISMS mit Maßnahmenzielen und Maßnahmen untersetzt. Für die in ISO 27002 genannten Maßnahmen existieren keine Verpflichtungen. Sie sind auch keine Grundlage für die Zertifizierung. Dennoch sollten Sie sich die Maßnahmen ansehen und entscheiden, ob die eine oder andere Maßnahme Ihr ISMS sicherer macht.

Der Anhang A der ISO 27001 enthält 14 informationssicherheitsrelevante Themen, die in unterschiedliche Maßnahmenziele untergliedert sind. Die Themen aus Anhang A wurden direkt aus der ISO 27002 abgeleitet. Bild 5 stellt den Zusammenhang zwischen ISO 27001 und ISO 27002 graphisch dar. Siehe Bild 5.

Bei der Einführung Ihres ISMS müssen Sie den Anhang A in Ihren Risikoanalysen, die in Kapitel 6.1.3 INFORMATIONSSICHERHEITSRISIKOBEHANDLUNG der ISO 27001 gefordert sind, mitbetrachten und bewerten. Die

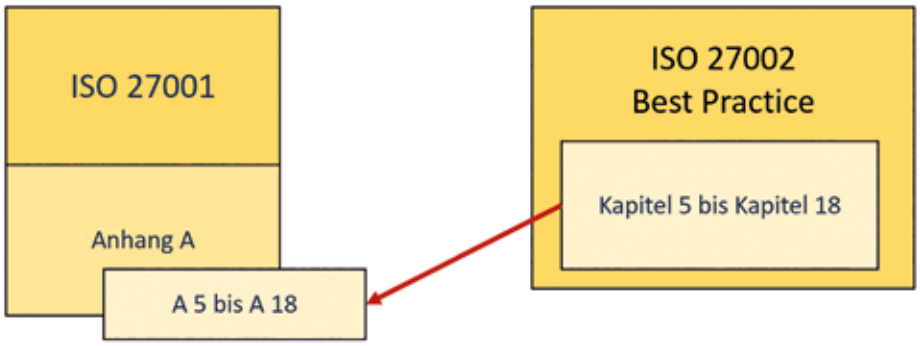

Bild 5: Zusammenhänge zwischen ISO 27001 und ISO 27002

Anforderungen, die der Anhang A dabei liefert, sind sehr allgemein. Wenn Sie kreativ genug sind, können Sie die geforderten Maßnahmen nach Ihrem Belieben umsetzen. In den meisten Fällen reichen die Formulierungen allerdings nicht aus, um eine Vorstellung zu gewinnen, welche Aspekte alle in einen Themenbereich fallen und ein ISMS sicherer machen.

Wer die ISO 27001 umsetzt, könnte sich natürlich in der Zertifizierung auf die allgemeinen Formulierungen berufen. Der Zertifizierung würde das nicht schaden. Allerdings ist Ihre Organisation dann mit so einem ISMS meist nicht wirklich sicherer als ohne dieses ISMS. Sie haben quasi Ihren aktuellen Stand dokumentiert und sind dabei eventuell nicht auf dem Stand der Technik.

Wenn Sie sichergehen möchten, dass Sie alle Aspekte der ISO-27000er-Reihe betrachtet haben, schauen Sie am besten in die ISO 27002 und prüfen sie die dort empfohlenen Implementierungsmaßnahmen.

Die nachfolgenden Informationssicherheitsthemen aus Anhang A sollen einen groben Überblick zu den jeweiligen Maßnahmen geben. Der Umfang der Darstellung ist keinesfalls erschöpfend.

In A5 der ISO 27001 wird ein Satz von INFORMATIONSSICHERHEITSRICHTLINIEN gefordert und deren regelmäßige Überprüfung und, wenn nötig, deren Aktualisierung.Unter dem Informationssicherheitsthema A6 befinden sich zwei Maßnahmenziele, zum einen die INTERNE ORGANISATION und zum anderen die Kombination aus MOBILGERÄTE UND TELEARBEIT.

Im Maßnahmenziel INTERNE ORGANISATION werden Maßnahmen aufgezählt, wie beispielsweise die Festlegung von Informationssicherheitsverantwortlichkeiten, die Aufgabentrennung und der Kontakt zu Behörden und speziellen Interessengruppen.

Das Maßnahmenziel MOBILGERÄTE UND TELEARBEIT fordert die Aufstellung von Richtlinien zum Umgang mit Mobilgeräten und zum Schutz von Informationen auf Mobilgeräten und am Telearbeitsplatz.

Das Informationssicherheitsthema A7 PERSONALSICHERHEIT gliedert sich in drei Bereiche. Hier geht es um Sicherheitsaspekte vor, während und nach der Beschäftigung.

Vor der Beschäftigung werden Sicherheitsüberprüfungen für neue Mitarbeiter empfohlen und vertragliche Vereinbarungen mit Beschäftigten, beispielsweise Vertraulichkeitsvereinbarungen in Arbeitsverträgen. Während der Beschäftigung werden alle Mitarbeiter auf die Umsetzung der gültigen Richtlinien verpflichtet. Außerdem werden Bewusstseinsschulungen durchgeführt, um den Mitarbeitern das relevante Informationssicherheitsbewusstsein verständlich zu machen. Weiterhin gilt ein Maßregelungsprozess, der den Mitarbeitern bekannt ist und der bei Informationssicherheitsverstößen zum Einsatz kommt. Für die Zeit nach der Beschäftigung sind ebenfalls Regelungen vorhanden. So müssen ausscheidende Mitarbeiter bspw. auf den Datenschutz und die Vertraulichkeit verpflichtet werden. Außerdem müssen dem ausscheidenden Mitarbeiter alle bisherigen Rechte im IT-System entzogen werden.

In A8 geht es um die VERWALTUNG DER WERTE der Organisation. Zuerst müssen die Werte inventarisiert und einem Mitarbeiter zugeordnet werden, der die Verantwortung für diese Werte übernimmt. Es müssen Regelungen zum ordnungsgemäßen Gebrauch von Werten und deren Rückgabe definiert werden. Für Werte wird außerdem eine Werteklassifizierung empfohlen. Anhand dieser Klassifizierung können Mitarbeiter Werte nach ihrer Kritikalität und Empfindlichkeit beurteilen und so sensibler mit kritischeren Werten umgehen. Weiterhin wird ein definierter Umgang mit Datenträgern empfohlen. Die Maßnahmen richten sich hierbei an Mitarbeiter zur Handhabung, Entsorgung und den Transport von Wechseldatenträgern.

A9 fordert, durch eine ZUGANGSSTEUERUNG den Zugang zu Informationen und informationsverarbeitenden Einrichtungen einzuschränken, und nennt als Maßnahmen die Erstellung einer Zugangssteuerungsrichtlinie und die Beschränkung des Netzzugangs für ausgewählte Mitarbeiter. Weiterhin soll es einen Prozess für die Benutzerregistrierung und Deregistrierung geben.

Die Mitarbeiter müssen sich außerdem der Verantwortung ihrer geheimen Authentisierungsinformationen bewusst sein und diese geheim halten. Der Zugang zu Systemen und Anwendungen muss darüber hinaus durch sichere Anmeldeverfahren abgesichert werden.

In A10 geht es um KRYPTOGRAPHIE. Dort, wo es sinnvoll ist, sollen kryptographische Maßnahmen zum Einsatz kommen. Auch hier wird eine Richtlinie erwartet. Diese soll den Gebrauch von kryptographischen Schlüsseln und deren Verwaltung regeln.

A11 Physische und umgebungsgebundene Sicherheit ist ein sehr umfangreiches Informationssicherheitsthema mit zwei Maßnahmenzielen. Zum einen sollen hier die SICHERHEITSBEREICHE und zum anderen die GERÄTE UND BETRIEBSMITTEL geschützt werden. Für die Sicherheitsbereiche gilt, dass sie vor unbefugtem Zutritt und vor externen oder umweltbedingten Bedrohungen geschützt werden. Die Geräte und Betriebsmittel sollen so geschützt werden, dass sie ohne Unterbrechung arbeiten können. Das bedeutet, sie müssen richtig platziert werden, ihre Versorgungseinrichtungen müssen bspw. vor Stromausfällen und die Verkabelungen müssen gegen Beschädigung geschützt sein. Das Entfernen von Werten muss unterbunden werden. Arbeitsumgebungen müssen vor unbefugtem Zugriff geschützt sein.

Bei der BETRIEBSSICHERHEIT in A12 geht es darum, einen ordnungsgemäßen Betrieb ohne Unterbrechungen zu gewährleisten. Das heißt, Nachfolger oder Vertreter können durch geeignete Dokumentation Arbeitsaufgaben zeitnah übernehmen, alle Änderungen werden gesteuert. Die benötigten Kapazitäten werden überwacht und sichergestellt. Und es besteht eine Trennung zwischen Entwicklungs-, Test- und Betriebsumgebungen. Weiterhin bestehen ein Schutz gegen Schadsoftware und ein Prozess zur Datensicherung. Ereignisse werden protokolliert und die Protokollinformationen vor Manipulationen geschützt. Zuletzt wird auch die Maßnahme genannt, die Geschäftsprozesse während der Audit-Tätigkeiten zu schützen.

A13 KOMMUNIKATIONSSICHERHEIT gibt Maßnahmen vor, die sich auf die Übermittlung von Informationen beziehen. Hier geht es vor allem um die Sicherheit bei der Übertragung in Netzwerken und die Einhaltung von Geheimhaltungsvereinbarungen.

A14 nennt Maßnahmen, die durchgeführt werden sollen, wenn Organisationen externe Leistungen beschaffen. Es geht hier um ANSCHAFFUNG, ENTWICKLUNG UND INSTANDHALTUNG. Zuerst sollen die Organisationen dabei ihre eigenen Anforderungen analysieren, um festzustellen, was eigentlich gebraucht wird, und erst danach soll nach Leistungen auf dem Markt gesucht werden. Leistungen, die durch die Organisation ausgelagert werden, müssen ebenfalls den eigenen Anforderungen genügen. Dabei sollen die Organisationen die Sicherheit in öffentlichen Netzen und den Schutz von Transaktionen betrachten.

Bei Entwicklungstätigkeiten soll das Thema Informationssicherheit im gesamten Produktlebenszyklus integriert sein. Dabei wird auch der Schutz der Testdaten gefordert.

Bei den LIEFERANTENBEZIEHUNGEN in A15 geht es in erster Linie um die vertraglichen Aspekte. In den Verträgen mit Lieferanten muss das Thema Informationssicherheit eingearbeitet sein. Diese Verträge müssen regelmäßig überprüft werden und bei Bedarf an das neue Informationssicherheitsniveau der Organisation angepasst werden. Für die Lieferkette gilt, dass die Lieferanten die Anforderungen der Organisation kennen müssen. Anschließend muss die Organisation die Lieferantendienstleistungen überwachen und Änderungen steuern.

Für die HANDHABUNG VON INFORMATIONSSICHERHEITSVORFÄLLEN muss es Verantwortliche geben, die von Mitarbeitern im Notfall informiert werden können. Weiterhin sind Prozesse zu etablieren, anhand derer man Risiken erkennen, beurteilen und behandeln kann. Alle Informationssicherheitsereignisse müssen geeignet gemeldet werden und die Beweismittel müssen aufbewahrt werden.

Ziel dieses Informationssicherheitsthemas ist die Notfallplanung für Krise oder Katastrophe. Die Maßnahmen nennen Umsetzungsmöglichkeiten, beispielsweise Dokumentationen, Prozesse und Verfahren, die vorhanden sein sollten, um im Notfall den Betrieb schnell wieder starten zu können. Hierzu zählt bspw. auch, dass es Kontaktlisten für Ansprechpartner diverser IT-Systeme gibt, die im Notfall zeitnah kontaktiert werden müssen. Als weitere Maßnahme in A17 wird der Aufbau von Redundanzen genannt.

Bei A18 COMPLIANCE geht es um die Einhaltung von gesetzlichen und vertraglichen Anforderungen. Hierzu zählt auch die Einhaltung der Anforderungen aus den Richtlinien der Organisation. A18 fordert außerdem die regelmäßige unparteiliche Überprüfung des ISMS auf dessen Wirksamkeit und Einhaltung der Gesetzlichkeiten.

Auch die empfohlenen Maßnahmen aus der ISO 27002 sind recht allgemein gehalten, aber sie geben einen breiten Überblick über mögliche Aspekte, die man eventuell vergessen würde. Nun werden Sie vermutlich feststellen, dass Sie durch die empfohlenen Maßnahmen aus der ISO 27002 Ihre Themen gut eingrenzen können, aber doch nicht vollständig technisch oder organisatorisch zum Leben erwecken können. An dieser Stelle empfehle ich einen gezielten Blick in den BSI IT-Grundschutz.

BSI IT-Grundschutz

Der BSI IT-Grundschutz ist mit Stand 2016 in 5 Bausteine (B) gegliedert, welche den Themen angehören: B1 Übergreifende Aspekte, B2 Infrastruktur, B3 IT-Systeme, B4 Netze und B5 Anwendungen. Desweiteren hat der IT-Grundschutz 6 Gefährdungskataloge (G) erstellt. Zu diesen gehören: G0 Elementare Gefährdungen, G1 Höhere Gewalt, G3 Organisatorische Mängel, G4 Menschliche Fehlhandlungen, G5 Technisches Versagen und G6 Vorsätzliche Handlungen.

Zuletzt sollen die Maßnahmenkataloge (M) genannt werden, welche in die Themen M1 Infrastruktur, M2 Organisation, M3 Personal, M4 Hardware und Software, M5 Kommunikation und M6 Notfallvorsorge unterteilt sind.

Bild 6 zeigt die BSI IT-Grundschutz-Kataloge mit Stand 2016. Die Abbildung soll zeigen, dass für jeden Baustein alle Gefährdungen möglich sind und diesen mit den Maßnahmen aus allen Maßnahmenkatalogen begegnet werden kann.

Bild 6: BSI IT-Grundschutz Stand 2016

Tabelle 1 zeigt Ihnen den Umfang der Kataloge mit Stand 2016. Es wird ersichtlich, dass es stellenweise mehrere hundert Elemente für ein Thema gibt. Die ältesten Elemente stammen aus dem Jahr 2009, die jüngsten aus 2014. Die Kataloge sind nicht mehr fortlaufend vorhanden, da regelmäßig Bausteine, Gefährdungen oder Maßnahmen aufgehoben werden.

Es macht bei der ISMS-Einführung keinen Sinn, alle Maßnahmen des BSI von oben nach unten in der Organisation zu implementieren. Vielmehr sollte man anhand der ermittelten Themen, die sich aus den Maßnahmen der ISO 27002 ergeben haben, gezielt nach IT-Grundschutz-Maßnahmen suchen und diese nach Überprüfung übernehmen.

Weiterhin würde eine komplette Übernahme aller IT-Grundschutz-Maßnahmen dazu führen, dass kein Prozess hinter den Maßnahmen steht. Ein fehlender Prozess führt in den meisten Fällen dazu, dass am Ende die Mitarbeiter stark überfordert sind und das ISMS nicht wirksam arbeitet. Die ISO empfiehlt deshalb ab 2010, Managementsysteme über die ISO High Level Structure mit dem PDCA-Zyklus einzuführen und am Leben zu halten.

Der PDCA-Zyklus

Die neue ISO High Level Structure beruht auf dem PDCA-Zyklus [6], was die Einführung eines ISMS-Managementsystems erleichtert. Eine kurze Erläuterung zum Aufbau und zur Wirkungsweise des PDCA-Zyklus:

Das ‚P' steht für PLAN und beinhaltet alle Tätigkeiten, die zur Planung eines ISMS, so bspw. Sicherheitsprozesse und -ziele, gehören. Die Kapitel 4 bis 6 der ISO 27001 gehören der PLAN-Phase an.

Das ‚D' steht für DO und konzentriert sich auf die Umsetzung der zuvor geplanten Prozesse, Ziele, Produkte oder Dienstleistungen. Die Kapitel 7 und 8 der ISO 27001 gehören der DO-Phase an.

Das ‚C' steht für CHECK und hat den Kerninhalt, zu prüfen, ob die eigentliche Umsetzung gemäß der Planung erfolgte. Hier spielen bspw. auch interne Audits eine Rolle. Das Kapitel 9 gehört der CHECK-Phase an.

Das ‚A' steht für ACT und verlangt Entscheidungen, ob und wie Verbesserungen durchgeführt werden sollen. Leistungsstarkes und Wirksames soll dabei erhalten oder verbessert und Fehlerhaftes korrigiert oder zukünftig verhindert werden. Bild 7 stellt die Normen-Kapitel je Umsetzungsphase graphisch dar. Das Kapitel 10 gehört der ACT-Phase an. Siehe Bild 7.

Der PDCA-Zyklus stellt einen rotierenden Kreislauf während der ISMS-Einführung und der anschließenden Aufrechterhaltung dar. Es wird somit von Ihnen nicht erwartet, dass Ihr ISMS nach seiner Einführung kein weiteres Verbesserungspotenzial mehr aufweist. Im Gegenteil, es ist im PDCA-Zyklus vorgesehen, dass Sie die Verbesserung Ihrer Prozesse und eingeleiteten Maßnahmen kontinuierlich aufrechterhalten und einen KVP, also einen kontinuierlichen Verbesserungsprozess, einführen.

Das bedeutet, Sie müssen nicht in Sorge geraten, wenn Sie zu Beginn der ISMS-Einführung noch nicht alle Anforderungen erfüllen können, denn nach jeder Iteration wird in der CHECK-Phase ein Review durchgeführt und in der ACT-Phase entschieden, was im nächsten Durchlauf verbessert werden soll.

Ihre ISMS-Einführung

Die ISMS-Einführung sollten Sie als internes Projekt auslegen. Projekte kosten meist viel Geld, sind auf einen beschränkten Zeitraum geplant, führen zu einem neuen Produkt oder einer neuen Dienstleistung und tragen ein gewisses Risiko des Scheiterns in sich.

Wenn Sie bereits sehr prozessorientiert arbeiten und dabei mit dem Thema Informationssicherheit bewusst umgehen, lohnt sich zu Beginn eine GAP-Analyse. In einer GAP-Analyse gehen Sie oder Ihr Berater einfach Anforderung für Anforderung durch die ISO 27001 und gleichen ab, ob Sie die eine oder andere Anforderung bereits erfüllen. Im Anschluss haben Sie einen Überblick über den Umfang an Ressourcen und Kompetenzen und auch über den zeitlichen Aufwand, den Sie einplanen müssen, um die noch fehlenden Anforderungen umzusetzen. Im nächsten Schritt bearbeiten Sie Kapitel für Kapitel die Norm-Anforderungen.

Zu Beginn Ihrer ISMS-Einführung müssen Sie in der PLAN-Phase festlegen, wohin die

Liste Bausteine		Liste Gefährdungen		Liste Maßnahmen	
B1	B1.0 – B1.17	G0	G0.1 – G0.46	M1	M1.1 – M1.80*
B2	B2.1 – B2.12	G1	G1.1 – G1.19	M2	M2.1 – M2.558*
B3	B3.101 – B3.406*	G2	G2.1 – G2.201*	M3	M3.1 – M3.96*
B4	B4.1 – B4.8	G3	G3.1 – G3.123*	M4	M4.1 – M4.469*
B5	B5.1 – B5.25*	G4	G4.1 – G4.99*	M5	M5.1 – M5.177*
		G5	G5.1 – G5.194*	M6	M6.1 – M6.159*

*Tabelle 1: Überblick BSI IT-Grundschutzkataloge (*einige Elemente der Reihe wurden aufgehoben)*

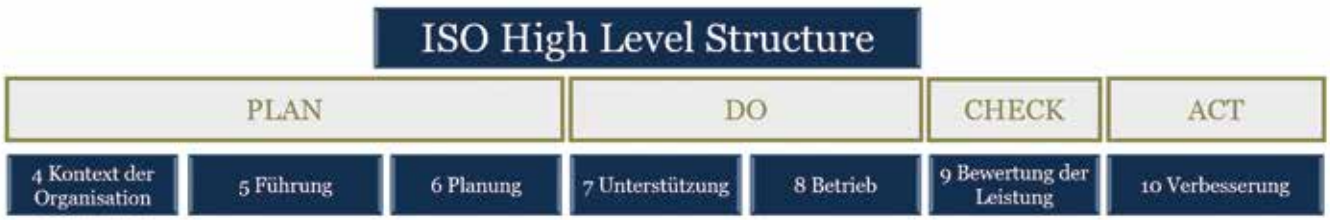

Bild 7: PDCA-Zyklus

Reise gehen soll. Wie wollen Sie Ihre Mitarbeiter zur Informationssicherheit erziehen? Welche Anforderungen kommen dabei von Ihren Kunden? Welche Anforderungen stellen Sie an Ihre Lieferanten? Diese Phase wird auch als GOVERNANCE bezeichnet.

Für Kapitel 4 und 5 sind in der Regel keine externen Berater nötig, da die Organisationen meist am besten wissen, welche Aufgaben sie nach außen hin vertreten und wer zur Gruppe der Stakeholder gehört. Auch die Politik und die Benennung von Verantwortlichen kann von der Organisation selbstständig durchgeführt werden.

Ab Kapitel 6 wird es für einen internen Mitarbeiter, der das ISMS neben seinen Linienaufgaben einführt, schwer, die Einführungsaufgaben in einer angemessenen Zeit umzusetzen. Wenn Sie Ihre Themen definiert haben, die aus Ihrer Sicht eine Relevanz für die Informationssicherheit haben, müssen Sie etwa 1-2 Tage für eine Risikoanalyse je Thema einplanen. Zusätzlich müssen Sie die Maßnahmenziele aus dem Anhang A für alle Ihre Themen ebenfalls einer Risikoanalyse unterziehen, um sicherzugehen, dass Sie kein offensichtliches Risiko übersehen. Planen Sie also etwa 3-5 Monate für die Umsetzung von Kapitel 6 ein.

Wenn Sie Ihre Risiken und Ziele kennen, können Sie mit der Umsetzung der Richtlinien beginnen. Eine Richtlinie sollte einen Titel, den Geltungsbereich, das Verhalten bei Informationssicherheitsvorfällen und die Verantwortlichkeiten beinhalten. Die Richtlinien müssen außerdem gelenkt werden. Das bedeutet, dass die Richtlinie vor ihrer Veröffentlichung von einer zweiten Person geprüft und freigegeben werden muss. Und die Richtlinie muss eine Versionsnummer besitzen und den Mitarbeitern zugänglich sein.

Der Inhalt einer Richtlinie richtet sich nach dem Wert, der mit dieser Richtlinie geschützt werden soll. Wenn bspw. Mobilgeräte geschützt werden sollen, muss die Richtlinie alle Aspekte beinhalten, die dem Schutz von Mobilgeräten dienen können. Es hat sich dabei als hilfreich gezeigt, bei der Erarbeitung von Richtlinien gezielt an dieser Stelle auch im BSI-Grundschutzkatalog nachzulesen, welche Maßnahmen vom BSI für die jeweiligen Themen vorgeschlagen werden. In der Richtlinie müssen die Mitarbeiter angesprochen werden.

Bei der Einführung eines ISMS sollten regelmäßige Treffen der Verantwortlichen stattfinden. In größeren Organisationen ist die Etablierung eines Informationssicherheitszirkels/IT-Sicherheitskreis sinnvoll.

Welche Themen müssen Sie außerdem beachten? Sie müssen die notwendigen Kom-

petenzen für Informationssicherheit aufbauen, Sie müssen mittels Awareness-Schulungen Ihre Mitarbeiter für Informationssicherheit sensibilisieren, Sie müssen die Kommunikationsketten definieren und Ihre Dokumentation lenken.

Weiterhin müssen Sie Prozesse einrichten, mit denen Sie Informationssicherheitsverstöße erkennen, beurteilen und behandeln können. Diese Phase wird als RISK MANAGEMENT bezeichnet.

Die Überprüfung der Einhaltung von Regelungen und Gesetzen wird auch COMPLIANCE genannt.

Bei Ihnen bedeutet das, dass Sie einen internen Auditor benennen müssen, der in regelmäßigen Abständen bspw. Ihre Richtlinien überprüft und bewertet, ob diese Richtlinien der aktuellen Gesetzeslage entsprechen und ob die Mitarbeiter sich an diese Richtlinien halten. Darüber hinaus muss der Auditor Ihr IT-System prüfen. Dazu ist Berufserfahrung in der IT unerlässlich. Die Ergebnisse der Audits fließen in einen Auditbericht ein und werden der obersten Leitung zur Prüfung übergeben.

In der Managementbewertung wird die oberste Leitung die Ergebnisse aus den Audits für die Neujustierung des ISMS verwenden und neue Informationssicherheitsziele vorgeben. Durch die neuen Zielvorgaben wird die PLAN-Phase bzw. GOVERNANCE wiederholt angestoßen und das ISMS kontinuierlich verbessert.

Risiken bei der ISMS-Einführung

Eine falsche Reihenfolge, beispielsweise die ISMS-Einführung mit BSI-Maßnahmen zu starten, kann dazu führen, dass Ihr ISMS über viele Jahre lang eingeführt werden muss, da Sie sich nicht fokussieren können. Ein weiteres Risiko besteht darin, dass die oberste Leitung die Verantwortung für die ISMS-Einführung vollständig einem Mitarbeiter überträgt und sich selbst komplett heraushält. Dieses Vorgehen kann dazu führen, dass keine einzige Maßnahme von anderen Mitarbeitern akzeptiert und angewendet wird. Das ISMS wird so nie vollständig eingeführt.

Ein personelles Risiko kann bestehen, wenn ausgebildete Fachkräfte in den Bereichen ISMS und interne Audits die Organisation verlassen und keine Vertreter aufgebaut wurden. Auch die finanziellen Ressourcen können zu einem Risiko werden, wenn beispielsweise nicht in sichere Hardware oder Software, in externe Beratung oder interne Weiterbildung investiert werden kann.

In den meisten Bundesländern gibt es für informationssicherheitsrelevante Projekte Fördertöpfe des Bundes. Die Beantragung muss schriftlich bei der jeweiligen Förderbank erfolgen. Die Prüfung und Bearbeitung dauert in der Regel etwa 8 Wochen. Bis zur Entscheidung der Förderbanken darf das Projekt natürlich noch nicht begonnen werden, was wiederrum ein zeitliches Risiko birgt.

Wenn Sie jetzt mit der ISMS-Einführung beginnen möchten oder müssen, klären Sie intern alle Verantwortlichkeiten und machen Sie die Entscheidung zur Einführung eines ISMS in einer Mitarbeiterversammlung allen bekannt.

Holen Sie sich bei allen Themen immer die richtigen Ansprechpartner aus den jeweiligen Fachabteilungen hinzu, die Ihnen die aktuelle Umsetzung in der Organisation erklären können. So können Sie schnell entscheiden, an welchen Stellen Sie externe Berater benötigen, und diese ganz gezielt für ISO-27001-Themen beauftragen. ■

JACQUELINE NAUMANN,
M.Sc. Praktische Informatik, Information Security Officer (TÜV), Information Security Auditor (TÜV), Qualitätsmanagementbeauftragte (TÜV)

Frau Naumann ist Dozentin, Beraterin & Auditorin für Informationssicherheit und Qualitätsmanagement.

Sie ist seit 2015 Inhaberin der iXactly IT- und Systemberatung Naumann. Zuvor hat sie über 16 Jahre in der IT-Branche gearbeitet und bspw. als Projektmanagerin für die Stadt Dresden das SAP-SD-Modul in den Fachämtern und das Dresdner Kitaplatz-Vergabesystem eKita eingeführt.

Ihre langjährigen Erfahrungen in der IT-Branche fließen in ihre Seminar- und Beratungstätigkeiten ein. Sie ist Expertin in den Bereichen ISO 27001, ISO 9001, Dokumentation, Softwareentwicklung, Datenbanken, SAP®, Testmanagement, Projektmanagement, Berechtigungsmanagement sowie Change- und Releasemanagement.

Sie ist vom TÜV Süd zertifizierte Qualitätsmanagementbeauftragte (QMB-TÜV, ISO 9001:2015), zertifizierter Information Security Officer sowie Information Security Auditor (ISO 27001:2013) und seit 2016 Vertragspartnerin der TÜV Süd.

Frau Naumann ist Autorin des Fachbuches „Praxisbuch eCATT" (Verlag: Rheinwerk-Verlag (ehem. Galileo Press), 2009)

Fußnoten

- *[1] Organisationen mit kritischen Infrastrukturen und wesentlicher Bedeutung für das staatliche Gemeinwesen, Betreiber von Kritischen Infrastrukturen*
- *[2] ISO 27001: ISO 27001:2013 Norm für Informationstechnik – IT-Sicherheitsverfahren – Informationssicherheits-Managementsysteme – Anforderungen, Original-Ausgabe 2013, deutsche Ausgabe 2015*
- *[3] Verordnung Bestimmung Kritischer Infrastrukturen nach dem BSI-Gesetz*
- *[4] ISO High Level Structure: übergeordnete Struktur, um zukünftige ISO-Normen zu vereinheitlichen und gemeinsame Kernthemen vorzugeben*
- *[5] Bewusstseins-Schulungen für Informationssicherheit*
- *[6] P: PLAN/Planung, D: DO/Umsetzung, C: CHECK/Überprüfung, A: ACT/Entscheidung*