BSI Forum

offizielles Organ des BSI
Bundesamt
für Sicherheit in der
Informationstechnik

Industrial IT meets Cyber-Security meets Safety

Cyber-Sicherheit für Produktionssysteme und die damit verbundenen Herausforderungen

Security im Sinne der Abwehr von Bedrohungen aus der IT- und Cyber-Welt ist ein Thema, welches zunehmend im Bereich der Fabrikautomation und Prozesssteuerung angenommen wird. Hierbei geht es nicht nur wie in der konventionellen IT um den Schutz vor Spionage oder Datendiebstahl, sondern auch um die Gewährleistung der Verfügbarkeit und Integrität von Produktionsanlagen. Bislang wenig berücksichtigt wird jedoch der Aspekt der funktionalen Sicherheit im Kontext von Cyber-Bedrohungen.

Von Holger Junker, BSI

IT-basierte Angriffe auf Produktionsanlagen haben eine sehr lange Historie. Häufig wird der unter dem Namen Stuxnet bekannt gewordene Angriff auf die iranische Urananreicherungsanlage in Natanz als erster Vorfall dieser Art beschrieben. Tatsächlich aber gab es bereits sehr viel früher solche Vorfälle, auch wenn diese weniger Potenzial für eine umfassende mediale Abdeckung hatten.

So wurde beispielsweise im Jahr 2000 die Wasser-/Abwasserversorgung im australischen Queensland über zwei Monate hinweg immer wieder manipuliert. Glaubte man anfangs noch an sporadische Ausfälle und Fehlfunktionen, so war doch sehr schnell ein Muster zu erkennen: Immer wieder wurden Pumpen unter Volllast gefahren, Ventile verstellt oder Anzeigen in der Leitwarte manipuliert. Schließlich kam man dem Mitarbeiter eines externen Dienstleisters auf die Spur, der mit diesen Manipulationen dafür Rache nehmen wollte, dass er keine Anstellung beim lokalen Versorger bekommen hatte.

Cyber-Sicherheitsvorfälle in Produktionsanlagen müssen überdies nicht immer auf zielgerichtete Angriffe zurückzuführen sein. Schon vor mehr als zehn Jahren haben verschiedene nicht-zielgerichtete Würmer wie Blaster oder Slammer massive Produktionsausfälle in den

Inhalt

Impressum

Redaktion:
Matthias Gärtner (verantwortlich)
E-Mail: matthias.gaertner@bsi.bund.de

Sebastian Bebel
E-Mail: sebastian.bebel@bsi.bund.de

Bundesamt für Sicherheit
in der Informationstechnik (BSI)
Referat Öffentlichkeitsarbeit und Presse
Postfach 20 03 63
53133 Bonn

Hausanschrift:
Godesberger Allee 185–189
53175 Bonn

Telefon: +49 228 999582-0
Telefax: +49 228 999582-5455

Web: www.bsi.bund.de
www.bsi-fuer-buerger.de

Das BSI-Forum, Organ des Bundesamtes für Sicherheit in der Informationstechnik in Bonn, ist Bestandteil der <kes> – Die Zeitschrift für Informations-Sicherheit
23. Jahrgang 2015

unterschiedlichsten Branchen verursacht. Ihre einzige Funktionalität bestand darin, sich zu verbreiten, was in vielen Fällen zu einer Überlastung der Produktionsnetze führte.

Aktuelle Bedrohungslage

Auch heute gibt es immer wieder solche Kollateralschäden: Zu den bekannt gewordenen Fällen der letzten Jahre zählen beispielsweise Maschinenbauer oder auch die Lebensmittelindustrie. Man stelle sich etwa die Auswirkungen vor, wenn in einer Molkerei plötzlich sämtliche Bedienterminals nur noch einen Bluescreen anzeigen, die speicherprogrammierbaren Steuerungen ihren Dienst verweigern und diese Situation nicht zeitnah behoben werden kann. Die Schadsoftware Conficker aus dem Jahre 2008 wird übrigens heute noch immer in Produktionsanlagen gefunden.

Deutschland im Fokus der Angreifer

Zielgerichtete Angriffe auf industrielle Anlagen werden zunehmend professioneller vorbereitet und durchgeführt. Ein prominentes Beispiel aus 2014 ist die Schadsoftware Havex: Hierbei handelte es sich um eine modular aufgebaute Schadsoftware, die insbesondere auch Anlagen in Deutschland zum Ziel hatte. Zunächst wurde Havex über Spear-Phishing verbreitet – einzelne Mitarbeiter beim angegriffenen Unternehmen erhielten eine E-Mail, die recht authentisch wirkte und den Empfänger zum Klicken auf einen Link verleiten sollte oder die teilweise auch direkt mit Schadsoftware behaftet war.

Später kam mit so genannten Waterhole-Attacks ein weiterer Verbreitungsweg hinzu: Dabei wurden die Webseiten von Herstellern von Industriekomponenten gehackt und die darauf zum Download angebotenen Softwarepakete beziehungsweise Firmware-Updates für Industriekomponenten mit dem Schadcode versehen. Jeder Anlagenbetreiber oder Integrator, der anschließend einen entsprechenden Download vornahm, wurde somit infiziert.

Havex spionierte anschließend die auf den befallenen Systemen gespeicherten Zugangsdaten, Verbindungsdaten für VPN-Zugänge und weitere sensitive Daten aus – vermutlich zur Vorbereitung von schwerwiegenden und umfassenden Folgeangriffen. Zudem wurde ein Scan nach verschiedenen Industriekomponenten durchgeführt – hierzu gehörte auch das Mitlesen der Kommunikation auf Basis des industriespezifischen Protokolls OPC.

Zu diesem Zeitpunkt versuchte Havex noch, möglichst nicht entdeckt zu werden, sodass weitere Schadroutinen später nachgeladen werden konnten. Jedoch war die Implementierung des OPC-Protokolls fehlerhaft, was dazu führte, dass verschiedene Industriekomponenten mit OPC-Unterstützung plötzlich abstürzten und den Dienst verweigerten. Havex richtete also bereits Schaden an, ohne dass dies beabsichtigt war.

Havex ist ein Musterbeispiel dafür, wie Angriffe auf Industriekomponenten ablaufen. Repräsentativ ist auch die Tatsache, dass viele Unternehmen längere Zeit infiziert waren, ohne dies selbst zu bemerken.

Stuxnet, der Million-Dollar-Angriff

Viele Anlagenbetreiber fühlen sich auch heute noch recht sicher, da sie sich nicht als attraktives Ziel für die Angreifer verstehen. Schließlich wurde von verschiedenen Stellen für den Stuxnet-Vorfall ein Kostenaufwand seitens der Angreifer jenseits von einer Million US-Dollar geschätzt. Wer also sollte ein kleines oder mittelständisches Unternehmen angreifen und dessen Produktion sabotieren, wenn damit solche Kosten verbunden sind?

Der Angriff auf ein Stahlwerk im Jahr 2013 hat jedoch gezeigt, dass eine signifikante Beschädigung von Produktionsanlagen auch mit weniger Entwicklungsaufwand umgesetzt werden kann. Bei Stuxnet wurde der Prozess der Urananreicherung sukzessive manipuliert, während den Bedienern ein völlig integrer Anlagenzustand visualisiert wurde. Bei Stuxnet musste also detailliertes Fachwissen über die verwendeten Komponenten und die dadurch gesteuerten Produktionsprozesse einfließen.

Was aber, wenn ein Angreifer nicht auf diese schleichende Manipulation aus ist, sondern auf einen „Big Bang“? In praktisch jeder Produktionsanlage findet man Visualisierungskomponenten, speicherprogrammierbare Steuerungen und andere vernetzte Geräte, die aus unterschiedlichen Gründen nicht mit Updates oder Sicherheitspatches versorgt werden. Schafft es ein Angreifer erst einmal in ein solches Produktionsnetz, sind ihm diese Komponenten hoffnungslos ausgeliefert.

So kann beispielsweise ein Angreifer sukzessive das Produktionsnetz unterwandern und zu einem bestimmten Zeitpunkt vorhandene Schwachstellen ausnutzen, die zu einem Ausfall der Steuerungskomponenten führen. Ein Neustart der betroffenen Geräte ist nutzlos, da die Schadsoftware sofort wieder aktiv werden kann. Bis zum Ergreifen erster Maßnahmen wie etwa auf der Netzwerkebene kann schon längst ein signifikanter Schaden eingetreten sein.

Erfahrungen aus der Revision

Cyber-Angriffe sind nicht nur auf funktionale Anlagenteile beschränkt, sondern können durchaus auch

die funktionale Sicherheit betreffen – dies wird durch Erfahrungen aus der Beratung und Revision von Produktionsanlagen immer wieder bestätigt.

So sind häufig die PCs, von denen aus Safety-Steuerungen programmiert oder parametriert werden, entgegen den einschlägigen Empfehlungen nicht vom lokalen Netzwerk getrennt; immer wieder ergibt sich in Revisionsbesuchen, dass diese sogar direkten Internetzugriff haben. Dies öffnet sowohl allgemeiner Schadsoftware als auch zielgerichteten Angriffen Tür und Tor. Da Safety-Steuerungen in der Regel keiner Einbruchsdetektion oder Anomalieerkennung unterliegen, kann ein Angreifer hier ungestört agieren.

Erst vor Kurzem wurde bei einer Revision festgestellt, dass die Not-Aus-Taster in einem produzierenden Betrieb über einen Protokollumsetzer an das allgemeine Produktionsnetz angebunden waren. Eine simple Überlastung des Produktionsnetzes oder die gezielte Manipulation von Netzwerkkomponenten hätte hier zu einer äußerst kritischen Situation führen können.

Für einen Angreifer ist es mitunter keine besondere Herausforderung, verschiedene Steuerungskomponenten gleichzeitig zu manipulieren oder deren Verfügbarkeit zu beeinträchtigen. Bei Herstellungsprozessen mit Gefahrenstoffen, hohen Temperaturen oder anderen kritischen Eigenschaften kann somit sehr schnell eine folgenschwere Situation herbeigeführt werden, wenn sowohl funktionale als auch sicherheitsgerichtete Steuerungen gleichzeitig Ziel des Angreifers sind.

Handlungsempfehlungen

Die Cyber-Sicherheit von sicherheitsgerichteten Komponenten erfordert ein abgestimmtes Handeln von Herstellern, Integratoren und Betreibern, wie dies auch für die Cyber-Sicherheit funktionaler Steuerungssysteme in der VDI/VDE 2182 postuliert wird.

Zunächst sind die Hersteller von sicherheitsgerichteten Steuerungen in der Pflicht, ihre Produkte und Entwicklungsprozesse angemessen zu gestalten. Hierbei geht es nicht darum, ein maximales IT-Sicherheitskonzept umzusetzen, sondern vielmehr um ein solides Basisniveau: So müssen beispielsweise die Anforderungen zu Beginn des Entwicklungsprozesses auch bezüglich der Cyber-Sicherheit definiert werden. Im weiteren Verlauf der Entwicklung müssen auch Codeanalysen, Penetrationstests, Fuzzing-Tests und andere Verfahren im Zuge der Qualitätssicherung zur Anwendung kommen. Besonders wichtig ist die sorgfältige Dokumentation und die Definition von Anforderungen und Empfehlungen für Integratoren und Betreiber.

Integratoren müssen diese Anforderungen und Empfehlungen ebenfalls beachten und ihrerseits darauf hinwirken, dass die sicherheitsgerichteten Elemente in ihrer Maschine oder Anlage einem soliden Basisniveau der Cyber-Sicherheit genügen. Auch sie müssen schließlich Anforderungen und Empfehlungen definieren, die dann seitens der Betreiber zu beachten sind.

Mit Blick auf die aktuelle Bedrohungslage muss es das Ziel eines Anlagenbetreibers sein, die Eintrittswahrscheinlichkeiten und die Schadensfolgen von verbreiteten Angriffsarten zu minimieren. Anlagenbetreiber müssen sich von der Vorstellung eines sicheren „Plug & Produce“ lösen und dies auch bei sicherheitsgerichteten Steuerungen berücksichtigen.

Ein Ansatz hierfür kann sein, zunächst die Mitarbeiter für die Risiken und Bedrohungen im Bereich der Cyber-Sicherheit zu sensibilisieren. Anschließend können die Bedrohungen der Cyber-Sicherheit im Rahmen einer „Hazard and Operability“-Analyse (HAZOP) diskutiert und analysiert werden. Anzustreben ist ein kontinuierliches Sicherheitsmanagement, in welches insbesondere sicherheitsspezifische Informationen von Herstellern und Integratoren sowie aktuelle Informationen zur Bedrohungslage einfließen.

Roadmap für Cyber-Sicherheit von ICS

Das BSI bietet eine Vielzahl von kostenfreien Empfehlungen und Hilfsmitteln im Kontext von Industrial-Control-Systems (ICS) an, die sukzessive auch für den Bereich Safety adaptiert werden.

Für den Einstieg eignen sich insbesondere die „ICS Top 10 Bedrohungen“, die das BSI unter dem Eindruck vielfältiger Erfahrungswerte erstellt hat. Hier werden nicht nur die zehn kritischsten Angriffsvektoren beschrieben, sondern auch geeignete Gegenmaßnahmen aufgezeigt. Bei den betrachteten Bedrohungen liegt der Schwerpunkt auf den Angriffen, mit denen ein Täter in das Unternehmen eindringt und so einen Brückenkopf errichtet, um weitere Folgeangriffe durchzuführen. Die Gegenmaßnahmen zielen aber nicht nur auf einen Schutz am Perimeter ab, sondern auf ein mehrschichtiges „Defense-in-Depth“-Konzept.

Die „ICS Top 10 Bedrohungen“ enthalten auch eine Checkliste für Betreiber und Integratoren. Intention dieser Liste ist nicht die Ermittlung einer konkreten Maßzahl für das aktuelle Sicherheitsniveau. Vielmehr wird es die Beantwortung dieser Fragen erfordern, dass eine Diskussion und ein Austausch im Unternehmen stattfinden – dies deckt häufig schon erste Unzulänglichkeiten und Regelungslücken auf und setzt so einen Startpunkt für weitere Sicherheitsbemühungen.

Nur durch kontinuierliche Überprüfung und Umsetzung von Sicherheitsmaßnahmen seitens der Betreiber kann ein hinreichendes Sicherheitsniveau gewährleistet werden. Bei diesen handelt es sich nicht nur um technische Aspekten, denn Cyber-Sicherheit kann man nicht als ein fertiges Produkt kaufen. Vielmehr spielen gerade organisatorische Regelungen – beispielsweise im Bereich Sicherheitsmanagement, Sensibilisierung oder Notfallvorsorge – eine zentrale Rolle.

Mit einer geeigneten Kombination aus organisatorischen, architekturellen und technischen Maßnahmen kann einer Vielzahl von Bedrohungen effektiv begegnet werden. Da viele Unternehmen nicht gleich auf einen der komplexen Standards für das Sicherheitsmanagement aufsetzen können, hat das BSI mit dem „ICS Security Kompendium“ die wichtigsten Vorgehensweisen und Methoden zusammengefasst. Ergänzend wird mit dem kostenfreien Tool „Light and Right Security for ICS“ (LARS ICS) ein Werkzeug angeboten, welches die wichtigsten Maßnahmen auf eine Referenzarchitektur abbildet und so den leichtgewichtigen Einstieg in das Sicherheitsmanagement ermöglicht.

Ziel eines Anlagenbetreibers muss es sein, langfristig ein ganzheitliches Informationssicherheitsmanagementsystem (ISMS) zu etablieren. Dabei sollte auf ein bewährtes ISMS wie IT-Grundschutz oder IEC 62443 aufgesetzt werden, ohne jedoch die Anforderungen und Beschränkungen des eigenen Unternehmens zu vernachlässigen. Ergänzend dazu muss der Dialog mit Herstellern und Integratoren bezüglich der gegenseitigen Anforderungen geführt werden. Eine Grundlage hierfür liefern beispielsweise die vom BSI erstellten „Anforderungen an netzwerkfähige Industriekomponenten“, die Anlagenbetreiber verwenden können, um die von ihnen erwarteten Sicherheitsanforderungen zu beschreiben.

Herausforderung Industrie 4.0

Während für Bestandsanlagen eine meist überschaubare Menge an Schutzmechanismen genügt, um ein hinreichendes Niveau bezüglich der IT-Sicherheit zu erreichen, müssen für „Industrie 4.0“ neue Konzepte erarbeitet werden.

In erster Linie gilt es, die mit Industrie 4.0 aufgrund der starken Vernetzung einhergehende Komplexität der Systeme beherrschbar zu machen: Die klassische Herangehensweise der Segmentierung und minimalen Kopplung von unterschiedlichen Teilnetzen in der Automatisierungspyramide wird dabei nicht mehr funktionieren. Zudem sehen viele Szenarien für Industrie 4.0 eine unternehmensübergreifende Vernetzung entlang der gesamten Wertschöpfungskette vor. Dies macht es erforderlich, umfassende und dezentralisierte Konzepte für das Management von Identitäten, Rollen und Berechtigungen zu etablieren. Ein händisches Etablieren statischer Vertrauensbeziehungen wird mit Industrie 4.0 nicht mehr praktikabel sein.

Insgesamt stellt das Thema Cyber-Sicherheit eine Herausforderung im Rahmen von Industrie 4.0 dar. So erfordern deren dynamische Prozesse und Abläufe eine Berücksichtigung des Themas Security von Beginn an. Dies betrifft die Planung, Umsetzung und den späteren Betrieb, um die gegebenenfalls automatisierten Konfigurationsänderungen oder Anpassungen an Maschinen sowie ihre Auswirkungen berücksichtigen zu können. Dies ist notwendig, um einen in jeglicher Sicht sicheren und zuverlässigen Betrieb zu ermöglichen. Cyber-Sicherheit ist daher einer der wesentlichen Grundbausteine von Industrie 4.0.

Die genannten Empfehlungen und Hilfsmittel des BSI können über www.bsi.bund.de/ics kostenfrei bezogen werden. ■

Sektorspezifische Zertifikate – Past, Present and Future

Die Normen ISO/IEC 27001 und ISO/IEC 27002 beschreiben ein generisches Informationssicherheitsmanagementsystem (ISMS). Um Besonderheiten bestimmter Branchen zu berücksichtigen, hat sich ergänzend dazu (national, aber auch international) eine Reihe sektorspezifischer Standards und Normen entwickelt, die aber im Rahmen der ISO/IEC 27001 keine zusätzlichen Anforderungen definieren konnten. Um dieser Forderung, auch aus dem regulierten Umfeld (z. B. IT-Sicherheitsgesetz), gerecht zu werden, wird dies durch die ISO/IEC 27009 zukünftig ermöglicht.

Von Dr. Helge Kreutzmann, BSI

Mitte der 90er-Jahre des vergangenen Jahrhunderts wurden in Großbritannien von der BSI Group (British Standard Institute, www.bsigroup.com) eine Serie von Normen für Informationssicherheitsmanagementsysteme (ISMS) herausgegeben, die vom Department of Trade and Industry erstellt wurden.

Der erste Teil hatte den Titel „BS 7799-1 Information security management. Code of practice for information security management“. Seine zweite Ausgabe von 1998 wurde dann beim ISO/IEC JTC1 SC27 WG1 (siehe Abschnitt „Aufbau der Normungsgremien“ für eine Erläuterung des Aufbaus der internationalen Gremien sowie deren Zusammenhang mit den nationalen Normierungsgremien) zur internationalen Normung im „Fast Track“-Verfahren eingereicht und bekam dort die Nummer ISO/IEC 17799. Im Rahmen des Aufbaus der 2700er-Reihe erhielt sie im Jahre 2007 die Nummer 27002 und liegt mittlerweile in der dritten Fassung aus dem Jahre 2013 als ISO/IEC 27002 „Information technology – Security techniques – Code of practice for information security controls“ vor.

Der zweite Teil der Serie der BSI Group wurde 1999 als „Information Security Management Systems – Specifications with Guidance for use“ veröffentlicht und wurde dann 2005 unter dem Titel „ISO/IEC 27001 Information technology – Security techniques – Information Security Management Systems – Requirements“ eine internationale Norm. Auch diese internationale Norm erschien 2013 in einer neuen Fassung. Für beide Normen gibt es mittlerweile technische Korrigenda.

Die 2005er- beziehungsweise 2007er-Fassung hatten die Grundstruktur und Grundidee der ursprünglichen Normen der BSI Group unverändert gelassen; dies änderte sich in den Versionen aus dem Jahre 2013 erheblich. Die Arbeiten an der neuen Fassung waren sehr intensiv, es wurde wirklich jedes Detail intensiv besprochen, was dazu führte, dass pro Arbeitssitzung mehrere hundert bis tausend Seiten an Kommentaren der einzelnen Spiegelgremien diskutiert werden mussten und trotz mehrfacher Fristverlängerung die Arbeiten bis zur letzten Fassung umstritten waren.

Die ISO/IEC 27001 (ohne die Angabe der Jahreszahl bezieht sich die Referenz stets auf die neueste Version aus 2013) beschreibt die Anforderungen, die ein ISMS erfüllen muss, ohne auf die Maßnahmen hierfür en detail einzugehen. Eine mögliche Maßnahmenliste findet sich im Anhang A der Norm. Die Beibehaltung dieses Anhangs, der gleichzeitig das Inhaltsverzeichnis für die ISO/IEC 27002 darstellt und in dem mögliche Umsetzungen dieser Maßnahmen dargestellt werden, war international sehr umstritten.

Die ISO/IEC 27001 folgt, wie alle zukünftigen Veröffentlichungen von Managementsystemnormen der ISO, der Struktur des so genannten „Annex SL“ (aus [1]). Diese gemeinsame Struktur soll es den Anwendern der Normen erleichtern, integrierte Managementsysteme zu erstellen. Für jeden Normenpunkt gibt es stets einen generischen, das heißt grundsätzlich in allen Managementsystemnormen vorkommenden, Text, der dann bei Bedarf der jeweiligen Norm (hier der ISO/IEC 27001) um Disziplinspezifika ergänzt wird.

Implizit folgt der Aufbau der Struktur dem Deming- oder PDCA-Zyklus („Plan-Do-Check-Act“), auch wenn es anders als in älteren Versionen keine expliziten Referenzen mehr darauf gibt.

Das Ziel der Norm ist es, für alle Organisationen (jeder Größe) anwendbar zu sein. Um dies zu erreichen, basiert die Auswahl der Maßnahmen (bzw. Controls auf Englisch) auf einem Risikomanagement gemäß ISO/IEC 31000. Die so ausgewählten Maßnahmen werden in einem „Statement of Applicability" (SoA) dokumentiert. Hierbei ist es auch möglich, ein Risiko zu tragen, ohne dies durch eine Maßnahme zu eliminieren oder zu minimieren (wofür eine Entscheidung der obersten Leitung notwendig ist).

Die ISO/IEC 27001 liegt mittlerweile auch in einer deutschen Fassung vor, die Anfang 2015 veröffentlicht wurde. Auch die Übersetzung, eine Gemeinschaftsarbeit der Normungsgremien Deutschlands, Österreichs und der Schweiz, hatte eine umfangreiche Arbeit verlangt. Dies insbesondere auch, da die Übersetzung der Vorgängerversion schwerwiegende Mängel aufwies.

Die ISO/IEC 27002 wurde gegenüber älteren Fassungen erheblich umstrukturiert: Sie ist eine Art Katalog von Maßnahmen, wobei für jede Maßnahme ein Ziel und eine Umsetzung dargestellt wird. Sie stellt zudem eine Referenz von Maßnahmen dar, da jeder Anwender der ISO/IEC 27001 seine ausgewählten Maßnahmen mit denen der ISO/IEC 27002 vergleichen muss.

Auch bei der ISO/IEC 27002 wurde darauf geachtet, dass sie für alle Organisationen (jeder Größe) anwendbar ist – dies führt zu einer teilweise sehr hohen, abstrakten Darstellung.

Aufbau der Normungsgremien

Während Standards von jeder Organisation geschrieben werden können, ohne diese notwendigerweise mit anderen Marktteilnehmern abzustimmen (z. B. kann eine einzelne Firma oder Organisation einen Standard entwickeln und intern nutzen, ohne diesen Dritten je zu lesen zu geben) müssen bei Normen eine angemessene Beteiligung aller interessierten Kreise und ein Konsens erreicht werden.

Für Normen gibt es daher in jedem Land grundsätzlich eine Organisation, die die Aufgabe der Erstellung und Veröffentlichung von Normen innehat. In Deutschland ist dies das „Deutsche Institut für Normung" (DIN), in Frankreich die „Association française de normalisation" (AFNOR) und in den USA das „American National Standards Institute" (ANSI). Diese Organisationen können national bestimmte Themenbereiche an andere Organisationen delegieren, so wird zum Beispiel in Deutschland der Bereich der Elektrotechnik durch die „Deutsche Kommission Elektrotechnik" (DKE) betreut. Ganz extensiv macht auch die ANSI davon Gebrauch, da es in den Vereinigten Staaten von Amerika eine Fülle von Normungsorganisationen gibt.

Neben der nationalen Normung dienen diese Organisationen auch als Vertreter für die pannationale und internationale Normung: Für Europa sind dies das „Comité Européen de Normalisation" (CEN), das „Comité Européen de Normalisation Électrotechnique" (CENELEC) und das „European Telecommunications Standards Institute" (ETSI). Auf internationaler Ebene sind dies die „International Organisation for Standardization" (ISO), die „International Electrotechnical Commission" (IEC) und die „International Telecommunication Union" (ITU), wobei Letztere strenggenommen eine Standardisierungsorganisation unter dem Dach der Vereinten Nationen ist.

Je nach Themenbereich ist eine der drei internationalen Organisationen zuständig. Allerdings gibt es hier auch eine Reihe von Grenzbereichen, sodass entweder für einzelne Projekte oder für ganze Themenbereiche zusammengearbeitet wird. Im Kontext dieses Artikels ist das insbesondere der Bereich „Informationstechnologie", bei dem die ISO und das IEC im „Joint Technical Committee 1" (JTC1) dauerhaft zusammenarbeiten, einheitliche Regularien entwickelt haben und die so entstehenden Normen als „ISO/IEC", das heißt für beide Organisationen simultan, veröffentlicht werden.

Innerhalb der ISO (bzw. analog dem IEC) gibt es „Technical Committees" (TCs) beziehungsweise „Subcommittees" (SCs). Die Arbeit für den Bereich Informationssicherheit findet im SC27 des JTC1 statt. Jedes TC beziehungsweise SC kann wiederum in „Working Groups" (WGs) untergliedert sein – so ist beispielsweise die WG1 des SC27 für „Information security management systems" und die WG5 für „Identity management and privacy technologies" zuständig. Weitere Informationen zum Aufbau, den Themen und Projekten des SC27 liefert www.jtc1sc27.din.de.

Sektorspezifische ISMS-Zertifizierung

Wie auch bei anderen Anforderungsnormen (z. B. der ISO/IEC 15448 „Information technology – Security techniques – Evaluation criteria for IT security") besteht der Wunsch, die Erfüllung der ISO/IEC 27001 gegenüber Dritten zu dokumentieren.

Die klassische Methodik hierfür stellt die Zertifizierung dar. Hierfür gibt es eine neutrale Stelle (Zertifizierungsstelle), die das System auditiert und bei Erfüllung aller Anforderungen ein Zertifikat ausstellt. Damit Zertifikate weltweit vergleichbar sind und prinzipiell gegenseitig anerkannt werden können, müssen mehrere Bedingungen erfüllt sein:

_____ Die Zertifizierungsstelle muss ihre Unabhängigkeit und Fachkompetenz kontinuierlich nachweisen und

_____ die Nachweise der Unabhängigkeit, der Fachkompetenz sowie das Vorgehen im Rahmen der Zertifizierung müssen selbst wieder international abgestimmt (idealerweise normiert) sein.

Die erste Anforderung wird erfüllt, indem es in jedem Land eine Akkreditierungsstelle gibt, die einheitlich die Zertifizierungsstellen akkreditiert und überwacht. In Deutschland ist dies die DAkkS (Deutsche Akkreditierungsstelle).

Die zweite Bedingung wird durch die Normen der ISO/IEC 170xxer-Serie gewährleistet. Für die Managementsystemzertifizierung ist dies speziell die ISO/IEC 17021, die voraussichtlich 2015 in einer neuen Fassung erscheinen wird. Darauf aufbauend gibt es die ISO/IEC 27006, die speziell für ISMS die internationalen Akkreditierungsanforderungen festlegt. Auch diese Norm wird voraussichtlich im Laufe von 2015 in einer aktualisierten Fassung erscheinen.

Um die gegenseitige internationale Anerkennung der Akkreditierungen kümmert sich die „International Accreditation Foundation“ (IAF) – für jeden Akkreditierungsbereich gibt es hierfür „Multilateral Agreements“ (MLAs). Hierzu gehören ein Satz verpflichtender Anforderungen an die jeweiligen nationalen Akkreditierungsstellen, deren Einhaltung dann in gegenseitigen Überwachungen (Shadowing) überprüft werden. Die DAkkS durchlief beispielsweise 2014 erfolgreich eine solche Überprüfung.

Derzeit (Stand Januar 2015) ist für die ISO/IEC 27001 von Seiten der IAF noch kein MLA finalisiert; die Fertigstellung dieser Vereinbarung, die voraussichtlich die ISO/IEC 27006 referenzieren wird, ist allerdings weit fortgeschritten.

Wie am Anfang des Artikels dargelegt, handelt es sich bei den Normen ISO/IEC 27001 und ISO/IEC 27002 um generische Normen, das heißt sie sind für alle Organisationen (jeder Größe) prinzipiell geeignet. Dieses ist zum einen vorteilhaft, da es ein (einheitliches) Zertifikat gibt und nicht für jede Variante eines ISMS das Rad „neu erfunden“ werden muss.

Andererseits gibt es im Markt ein großes Bedürfnis, dem Kunden gegenüber zu dokumentieren, dass spezielle, sektorspezifische Anforderungen einer Branche erfüllt wurden. Auch können ein Branchenverband oder eine Regulierungsbehörde bestimmte minimale Anforderungen an die Umsetzung eines ISMS stellen, die von den generischen Normen ISO/IEC 27001 und ISO/IEC 27002 so nicht abgedeckt werden.

Bevor in den folgenden Abschnitten auf Beispiele für solche sektorspezifischen Normen eingegangen wird, ist es nochmals wichtig, auf die Rolle des Anhang A der ISO/IEC 27001 zu verweisen: In diesem Anhang steht eine Auflistung von möglichen Maßnahmen – die Organisation, die das ISMS betreibt, kann aber auch (teilweise) andere Maßnahmen(kataloge) verwenden. Am Ende muss die Zertifizierungsstelle nur prüfen, ob das Risikomanagement korrekt durchgeführt und die ausgewählten / definierten Maßnahmen mit den Maßnahmen des Annex A der ISO/IEC 27002 verglichen wurden. Eine vierte Partei (z. B. ein Kunde), die nur das Zertifikat kennt, kann per se nicht erschließen, welche Maßnahmen tatsächlich ausgewählt wurden.

Anhand der folgenden Fallbeispiele ist dargestellt, wie dieses Problem in der Vergangenheit angegangen wurde, im letzten Abschnitt sind dann zukünftige Ansätze dargestellt.

Entwicklung an Beispielen

ISO 27799

Eines der ersten Beispiele für eine sektorspezifische Norm war die ISO 27799:2008 „Health informatics – Information security management in health using ISO/IEC 27002“, die vom ISO TC 215 ohne (intensive) Beteiligung des ISO/IEC JTC1 SC27, das erst kurz zuvor die ISO/IEC 27002 veröffentlicht hatte, erstellt wurde. Mittlerweile liegt diese Norm in einer überarbeiteten Fassung von 2013 vor; auch hier gab es keine intensiven Kontakte zwischen dem SC27 und TC 215.

Diese eigenständige Entwicklung sorgte innerhalb des SC27 für einige Kritik. Neben inhaltlichen Anmerkungen gab es primär drei Kritikpunkte: Die Arbeit lag nicht (federführend) beim SC27, es wurde auf die ISO/IEC 27002 referenziert und die Norm enthielt zusätzliche Anforderungen (die ISO/IEC 27002 ist eine reine Empfehlungsnorm, kein „shall“).

Dem ersten Kritikpunkt wurde durch eine zunehmend stärker werdende Liaison- und Werbe-Aktivität seitens des SC27 begegnet – zeitweilig gab es sehr viele Liaisons, derzeit wird im SC27 versucht, dieses wieder auf ein handhabbares Maß zu reduzieren. Im Rahmen dieser Liaisons wurden später eine Reihe von sektorspezifischen Normen entwickelt, wie zum Beispiel die X.1051|27011 „Information security control guidelines – based on ISO/IEC 27002 for telecommunications organizations“.

Um die Form der sektorspezifischen Normen zu vereinheitlichen (Kritikpunkt 2), wurde zudem eine Vorlage (SD 1 von WG1 des SC27) erstellt, nach der in Zukunft

sektorspezifische Normen aufgebaut sein sollten (woran sich die meisten Normen dann auch hielten).

Der dritte Kritikpunkt tauchte auch bei neueren sektorspezifischen Normen auf: Die Frage, ob die ISO/IEC 27001 stets ausreichend sein könne oder ob (und wenn ja, in welcher Form) es zusätzliche Anforderungen geben dürfe, wurde in den Folgejahren intensiv und immer wieder diskutiert.

IEC-Normenreihe 62443

Auch in der IEC gab es Entwicklungen, sektorspezifische Normen zu erstellen. Das vielleicht prominenteste Beispiel ist die IEC-Normenreihe 62443 „Industrial communication networks – Network and system security", die von dem IEC TC 65 WG10 betreut wird. Faktisch erfolgt die Arbeit in der ISA 99 (Industrial Society for Automation, www.isa.org) und wird dann im „Fast Track"-Verfahren in der IEC normiert.

Im Jahre 2010 sollte die IEC 62443-1 im Rahmen des parallelen Verfahrens automatisch in das CEN-Normenwerk (und damit in das DIN-Normenwerk) übernommen werden. Der für die Norm zuständige DKE-Unterarbeitskreis 0931.1 stimmte wegen Widersprüchen zur ISO/IEC 27001 dagegen. Diese Meinung wurde auch von anderen CEN-Nationen geteilt, sodass schließlich die IEC 62443-1 nicht in das europäische Normenwerk übernommen wurde.

Um alle Normen widerspruchsfrei zu bekommen (wie dies auch von den Regularien der ISO und der IEC gefordert wird), wurde anschließend mittels einer (neuen) Liaison auf SC27-Ebene eine Überarbeitung erreicht, die neben der Beseitigung von Widersprüchen auch zu einer Übernahme der in SC27 angestrebten Darstellungsform (gemäß SD 1, siehe oben) führen soll.

Auch hier taucht wieder das bis dato ungelöste Problem auf, dass die ISO/IEC 27002 keine Anforderungen formuliert, zusätzliche Anforderungen aber in der IEC-Normenreihe 62443 enthalten sind.

World Lottery Association (WLA)

Sektorspezifische ISMS-Anforderungen und -Maßnahmen wurden und werden aber nicht nur in der ISO oder IEC diskutiert, auch Organisationen außerhalb dieser Normungsgremien verwenden die ISO/IEC 27001 und ISO/IEC 27002, ergänzt um branchenspezifische Anforderungen und Maßnahmen.

Ein frühes Beispiel hierfür ist die World Lottery Association (WLA, www.world-lotteries.org), die eine weltweite Vereinigung der Glücksspielunternehmen ist. Nach Erscheinen der ISO/IEC 27002:2007 trat die WLA an SC27 mit der Bitte heran, ihre „Fassung" der ISO/IEC 27002 im Rahmen einer Liason als internationale Norm zu veröffentlichen.

Neben Fragen der zukünftigen Hoheit über das entstandene Dokument (das dann im Rahmen der normalen Gremienarbeit innerhalb von SC27 weitergepflegt wird) war wieder die Frage, ob und wie zusätzliche Anforderungen formuliert werden können, der Blocker für die Übernahme.

Die geforderte zusätzliche Anforderung war in diesem Fall einfach nachzuvollziehen: Der Geltungsbereich des ISMS, das die geplante WLA-Norm erfüllen sollte, müsste zwingend den gesamten Glücksspielbereich umfassen. Die Erfahrung im Bereich der ISMS-Zertifizierung hatte gezeigt, dass einige Firmen nur „periphere" Bereiche zertifizieren ließen, zum Beispiel ein Rechenzentrum nur seine Büro-IT. Der Geltungsbereich ist zwar auf dem Zertifikat vermerkt, aber viele mit der Zertifizierung nicht so vertraute Personen lesen nur „zertifiziert nach XY" und gehen dann davon aus, dass natürlich „alles" der Firma zertifiziert sei, ohne das Zertifikat selbst zu lesen.

Aufgrund dieses Problems schlief der Kontakt zur WLA wieder ein, mittlerweile hat die WLA aber im Rahmen eines „Vienna Workshop Agreements" im zweiten Anlauf die Übernahme ihrer Standards gestartet. Es ist davon auszugehen, dass hier dann die derzeit in SC27 entwickelten Lösungen berücksichtigt werden.

Cloud-Computing

Ganz dringend wurden die bei anderen sektorspezifischen Normen bereits diskutierten Fragen dann im Rahmen der Entwicklung von Normen im Bereich von Cloud-Computing. Auf der internationalen Sitzung des SC27 in Nairobi im Jahre 2011 wurde intensiv diskutiert, wer und was normiert werden sollte.

Im „Cloud"-Bereich gibt es in den Normungsorganisationen mit den ISO/IEC JTC1 SC38, ISO/IEC JTC1 SC27 und der ITU-T SG17 bereits eine Reihe von Gremien, die sich mit dem Thema beschäftigen. Auch eine Reihe von anderen Gremien hat oder wird Standards im Bereich Cloud-Computing entwickeln – als sehr prominentes Beispiel sei hier die „Cloud Security Alliance" (CSA) genannt, die neben den Normen auch ein eigenes (nicht akkreditiertes) Zertifizierungsschema namens „Open Certification Framework / CSA Star" anbietet (siehe https://cloudsecurityalliance.org/star/#_registry). Und schließlich geht es gerade auch im Cloud-Umfeld nicht nur um Informationssicherheit, sondern auch um Datenschutzaspekte, die innerhalb des SC27 von der WG5 betreut werden.

Die Lösung des „wer“ bestand schließlich darin, mit intensiven Liasons und „Joint Projects“ zwischen der ITU-T, SC27 und SC38 inklusive Editoren aus den Gremien für Normen mit Bezug zu SC27 zu arbeiten. Zudem werden Fragestellungen mit Bezug zur Informationssicherheit in SC27 WG1 (Projekt ISO/IEC 27017) und mit Bezug zu Datenschutzaspekten in SC27 WG5 (Projekt ISO/IEC 27018) bearbeitet. Andere Normen und Standards (bspw. im Hinblick auf Terminologie) werden in den jeweils anderen Gremien bearbeitet – auch hier mit den entsprechenden Liaisons zu SC27.

Damit war aber die Frage des „was“ nur teilweise beantwortet, denn die ISO/IEC 27017 und ISO/IEC 27018 sind wieder „nur“ Ergänzungen zur ISO/IEC 27002. Auch im Bereich Cloud-Computing gibt es Forderungen nach zusätzlichen Anforderungen, zentral soll ein Cloud-Anbieter sein „Statement of Applicability“ (SoA) offenlegen – und somit die gewählten Maßnahmen für Außenstehende sichtbar machen.

Auch kam die Frage auf, ob für „Cloud“ ein eigenes Zertifizierungs- und Auditierungsschema notwendig sei, gegebenenfalls sogar eine eigene Fassung der ISO/IEC 27001. Diese Diskussion endete mit der Entscheidung, im ersten Schritt die zwei oben erwähnten sektorspezifischen Maßnahmennormen zu erstellen, aber für die anderen Fragen in zukünftigen Arbeiten innerhalb des SC27 den notwendigen Rahmen zu entwickeln. Diese Entwicklung ist für den Anforderungsteil im Abschnitt „Ausblick“ dargestellt. Ob das Risikomanagement für die Cloud spezifisch geregelt werden muss, ist derzeit Teil einer „Study Period“ in SC27.

ISO/IEC TR 27019

Ein schönes Beispiel, wie eine solche sektorspezifische Norm entwickelt werden kann, stellt die ISO/IEC TR 27019 „Information technology – Security techniques – Information security management guidelines based on ISO/IEC 27002 for process control systems specific to the energy utility industry“ dar.

Hierzu wurde zunächst innerhalb des DKE-Arbeitskreises 952.0.15 (Spiegelgremium zum IEC TC 57/WG 15) und dann zusammen mit dem deutschen Spiegelgremium des SC27 im DIN (dem NIA 27) sowie einer Reihe von weiteren Organisationen im deutschsprachigen Raum die DIN Spec 27009 entwickelt. Hierbei wurden von Anfang an alle im Rahmen von SC27 benannten Anforderungen berücksichtigt. Die fertige DIN Spec wurde dann im „Fast Track“-Verfahren international eingebracht und 2013 als ISO/IEC 27019 veröffentlicht – die als Zwischenstufe erstellte DIN Spec 27009 konnte somit zurückgezogen werden.

Da die ISO/IEC TR 27019 noch auf der 2007er-Version der ISO/IEC 27002 beruht und zudem im „Fast Track“-Verfahren naturgemäß nur ein Teil der Kommentare anderer Nationen berücksichtigt werden konnten, ist die ISO/IEC TR 27019 für die Überarbeitung (im Rahmen des SC27) vorgesehen.

Auch an diesem Beispiel zeigt sich wieder die Problematik der fehlenden Anforderungen: Die ISO/IEC TR 27019 kann zwar regulativ zitiert werden (wie dies beispielsweise im Sicherheitskatalog [2] der Bundesnetzagentur im Rahmen der Regulierung der Energienetze geplant ist), aber da auch sie naturgemäß keine Anforderungen enthalten (kann), müssen diese separat formuliert werden.

Andererseits zeigt dieses Beispiel auch, wie ein (deutscher) Sektor die eigenen Branchenstandards zielstrebig auf den Weg zu einer internationalen technischen Richtlinie (TR) – und gegebenenfalls im Rahmen der anstehenden Überarbeitung schließlich einer Norm – gebracht hat.

Situation in anderen Ländern

Die ISO erfasst jährlich weltweit die Zertifikate für „große“ Managementsystemnormen – darunter auch die ISO/IEC 27001 – in der so genannten ISO Survey (www.iso.org/iso/iso-survey). Demnach wurden 2013 die meisten Zertifikate gemäß ISO/IEC 27001 weltweit mit großem Abstand in Japan vergeben, gefolgt von Indien, UK und China – das stärkste Wachstum erfolgt dabei klar in Italien, gefolgt von Indien, UK und China.

Sektorspezifische Zertifizierungen sind aus dieser Studie nicht zu entnehmen. Für einige ausgewählte Länder, die in der Normung (auch sektorspezifischer Normen) aktiv sind, wurde dies jedoch näher untersucht.

Italien

In Italien wird nur in einigen wenigen Branchen mit sektorspezifischen Standards gearbeitet; dabei werden die sektorspezifischen Normen der ISO (wie die ISO/IEC 27011 für Telekommunikationsunternehmen) nicht eingesetzt, Zertifizierungen erfolgen dabei nicht. In der Vergangenheit gab es ein paar Standards mit Zertifizierungen für ISMS, die nicht auf die ISO/IEC 27001 aufsetzten (z. B. für Websites), die aber mittlerweile keine Rolle mehr spielen. Einzig die „CSA Star“-Zertifizierung (siehe oben) stößt noch auf Interesse im Markt.

Japan

In Japan ist klar eine Sättigung an Zertifizierungen erkennbar (allerdings auf sehr hohem Niveau, [3]). Auch hier spielen sektorspezifische Zertifizierungen derzeit

keine Rolle, wobei ein Interesse an der ISO/IEC 27009 (siehe Abschnitt „Ausblick“) besteht, sodass sich dies in Zukunft ändern könnte. Ähnlich wie in Italien hat auch hier die „CSA Star“-Zertifizierung eine Bedeutung, wobei die Anzahl der derzeit zertifizierten Unternehmen mit zwei noch eher klein ist. Darüber hinaus gibt es enge Behördenanforderungen für viele Branchen, die sich aber nicht zwingend in (sektorspezifischen) Zertifizierungen niederschlagen.

Schweiz

Die Schweiz ist mit 111 Zertifikaten für ISO/IEC 27001 in 2013 eine größere der „kleinen“ Zertifizierungsnationen. Sektorspezifische Zertifizierungen spielen derzeit keine Rolle; lediglich vereinzelte Nachfragen bezüglich der ISO 27799 bestehen. Allerdings gibt es eine „Verordnung über die Datenschutzzertifizierungen“ [4], die unter anderem auf die ISO/IEC 27001:2005 aufsetzt und gemäß derer rund 80 Zertifikate ausgestellt wurden.

Ausblick

Derzeit gibt es eine Reihe von Aktivitäten im Hinblick zu sektorspezifischen Standards und Normen, von denen im Folgenden exemplarisch drei herausgegriffen werden sollen.

Die zukünftige ISO/IEC 27009

Wie weiter oben bereits dargestellt, blieb die Situation bezüglich der sektorspezifischen Normen in SC 27 unbefriedigend, da zwar eine Vielzahl von Liaisons für Kontakte zu anderen Organisationen sorgten (und somit den „Wildwuchs“ etwas begrenzten), aber der eher informelle Charakter des SD 1 und die fehlende Möglichkeit, auch Anforderungen zu spezifizieren, das Konzept nicht wirklich förderten.

Folgerichtig gab es 2012 in der SC27-Sitzung in Rom die Idee, SD 1 durch eine Norm zu ersetzen, die alle offenen Fragen für die Autoren von Standards und Normen klären sollte. Somit wäre dann für eine einheitliche und – soweit möglich – widerspruchsfreie Gestaltung der sektorspezifischen Standards und Normen gesorgt. Dieses Vorhaben stieß auf große Zustimmung. Derzeit befindet sich diese Norm unter dem Namen ISO/IEC 27009 „Information technology – Security techniques – Sector-specific application of ISO/IEC 27001 – Requirements“ in der Entwicklung.

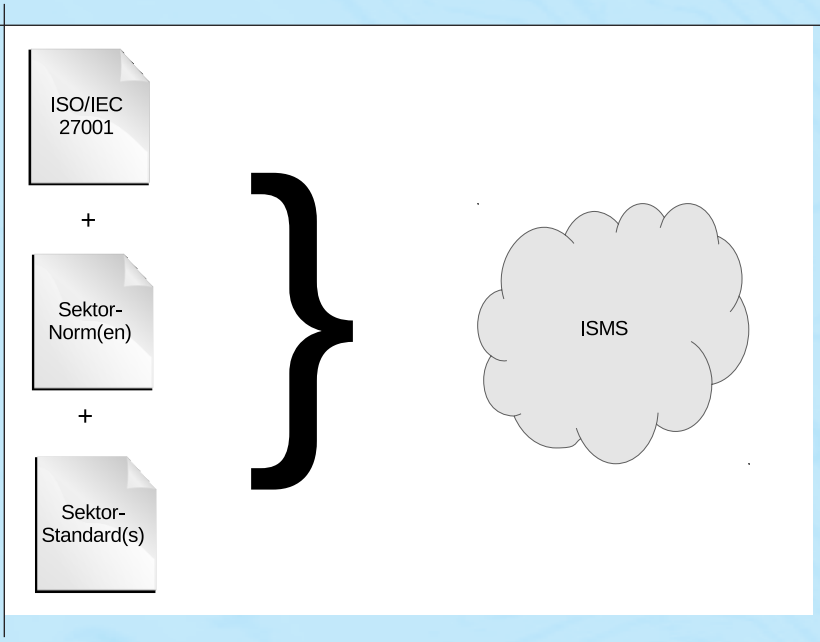

Abbildung 1: Zusammenspiel zwischen der ISO/IEC 27001 und sektorspezifischen Normen und Standards

Die bisherigen Entwürfe wurden zur Diskussion breit innerhalb (möglicherweise) relevanter ISO-Gremien und darüber hinaus gestreut – auch wurde in der internationalen Diskussion von mehreren Delegierten auf die jeweiligen nationalen Diskussionen verwiesen. Zusammen mit einer zusätzlich durchgeführten Befragung vieler Gremien soll sichergestellt werden, dass diese zukünftige Norm auch wirklich die Anforderungen aller relevanten Parteien berücksichtigt. Dazu wurde auch im Geltungsbereich der Norm klar dargelegt, dass sie sowohl für Normen (innerhalb der ISO und IEC) als auch für Standards (z. B. durch Branchenverbände) geeignet sein soll.

Dabei zeigte sich ein Problem in der Terminologie: Die Norm ist auch für branchenübergreifende Anwender gedacht – zum Beispiel haben die Experten aus der WG5 des SC27 großes Interesse, die ISO/IEC 27009 für Datenschutzanforderungen (basierend auf der ISO/IEC 27001) zu verwenden. Hierbei gibt es oft Verständnisprobleme, da sich zum Beispiel der Datenschutz nicht als „Sektor“ versteht. Die Definition von Sektor ist im Rahmen des SD 1 beziehungsweise der zukünftigen ISO/IEC 27009 zwar breiter, sodass auch der Datenschutz darunter fällt, aber Ansätze für einen „breiteren“ Begriff sind bisher gescheitert, als aktueller Kompromiss wird derzeit „sector – and/or service-specific“ verwandt.

Derzeit (Stand Januar 2015) umfasst der aktuelle Entwurf (Committee Draft 2) inklusive aller Anhänge sieben Seiten, wobei fünfeinhalb Seiten wirklich inhaltlich relevant sind. Im Kern der Norm wird festgelegt, dass die Anforderungen der ISO/IEC 27001 nur verfeinert oder sektorspezifisch interpretiert beziehungsweise ergänzt werden dürfen, das heißt Widersprüche nicht möglich sind. Auch werden Anforderungen formuliert, wie sektorspezifische Maßnahmen (als Ergänzung oder

Ersatz der ISO/IEC 27002) formuliert werden müssen.

Im normativen Anhang der ISO/IEC 27009 ist dann generisch dargestellt, wie eine solche sektorspezifische Norm (bzw. ein dergestalter Standard) aufgebaut sein muss. Hierdurch soll sichergestellt werden, dass ein zukünftiger Anwender möglichst leicht diese sektorspezifischen Norm(en) anwenden kann.

Das Zusammenspiel zwischen der ISO/IEC 27001 und einer sektorspezifischen Norm, wie es die ISO/IEC 27009 derzeit vorgibt, ist in Abbildung 1 dargestellt. Denkbar, aber nicht Teil der ISO/IEC 27009, ist, dass eine Zertifizierungsstelle eine solche Zusammenstellung dann zertifiziert, der Kunde dann also ein sektorspezifisches Zertifikat erhält. Hierzu sind von internationaler Seite aber noch eine Reihe von Fragen offen, zum Beispiel ob und wie eine solche Zertifizierung erfolgen soll (reicht hier die bestehende ISO/IEC 27006 aus?) und, natürlich, ob und wie eine internationale Anerkennung möglich wäre.

Die deutsche TR 3145

Auf deutscher Ebene gibt es bereits Ansätze, sektorspezifische Zertifizierungen zu etablieren. Neben dem weiter oben zur ISO/IEC TR 27019 erwähnten Beispiel der Bundesnetzagentur gibt es beim Bundesamt für Sicherheit in der Informationstechnik (BSI) bereits ein Modell für eine sektorspezifische Zertifizierung, konkret für die TR 3145 „Secure CA operation – Generic requirements for Trust Centers instantiating as Certification Authority (CA) in a Public-Key Infrastructure (PKI) with security level ‚high'".

Abbildung 2 zeigt, wie nach einem sektorspezifischen Standard klassisch (hier am Beispiel des BSI) im Markt zertifiziert wird: Eine Organisation entwickelt einen sektorspezifischen Standard (unter möglichst großer Beteiligung aller interessierten Kreise) oder eine sektorspezifische Norm – das heißt die Entwicklung würde in Deutschland dann im Rahmen des DIN oder DKE erfolgen.

Dieser Standard wird dann den beteiligten Kreisen diskriminierungsfrei zur Verfügung gestellt und interessierte Zertifizierungsstellen bieten ihren Kunden dann eine Zertifizierung danach an. Gegebenenfalls erfolgt die Qualifizierung der notwendigen Auditoren bei einer oder mehreren anderen Organisationen. Eventuell spielt auch die nationale Akkreditierungsstelle, die dann die Zertifizierungsstelle überwacht, eine Rolle.

Für die TR 3145 hat das BSI allerdings eine leicht andere Konstruktion gewählt, die in Abbildung 3 dargestellt ist: Hierbei ist die eigentliche Zertifizierung zwischen der (akkreditierten) Zertifizierungsstelle für ISO/IEC 27001 und dem BSI (für den sektorspezifischen Anteil) aufgeteilt. Für den sektorspezifischen Anteil dürfen dabei nur Auditoren eingesetzt werden, die beim BSI dafür als Person zertifiziert sind. Idealerweise findet zudem das Audit beim Kunden für den sektorspezifischen wie auch für den allgemeinen Teil zeitgleich statt.

Ob dieses (komplexere) Modell auch für zukünftige sektorspezifische Zertifizierungen tragbar ist, muss sich zeigen, da damit zwei Zertifizierungsstellen ihre Aktivitäten (eng) verzahnen müssen.

Parallel zur Etablierung der rein nationalen Zertifizierung nach TR 3145 erfolgt in diesem Fall auch die Erarbeitung der internationalen Norm X.842|TR 14516-2 „Guidelines for the use and management of trust service providers – Part 2: Guidelines on information security of PKI trust service providers", welche die TR als Ausgangsbasis verwendet. Mit dem Erscheinen der internationalen Norm ist voraussichtlich 2017 zu rechnen.

Deutsches IT-Sicherheitsgesetz

Auch bei dem zum Zeitpunkt der Erstellung dieses Beitrags diskutierten Entwurf des IT-Sicherheitsgesetzes [5] spielen sektorspezifische Standards, die im Rahmen des Gesetzentwurfes „branchenspezifische Standards" genannt werden, eine wichtige Rolle

Nach dem Entwurf soll es Branchen ermöglicht werden, eigene Standards (bzw. in Zusammenarbeit mit dem DIN sogar Normen) zu entwickeln, die branchenspezifische

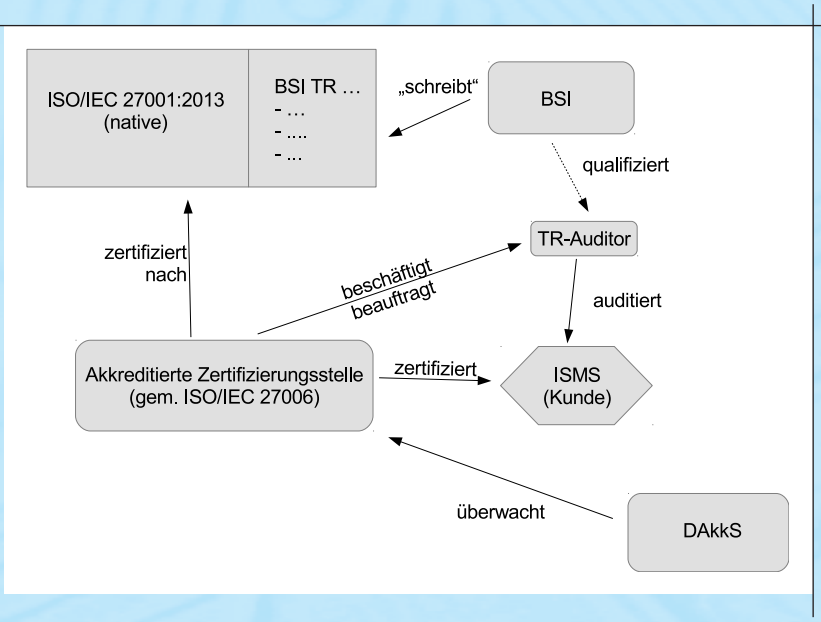

Abbildung 2: Klassisches Zusammenspiel der sektorspezifischen Standarderstellung und Zertifizierung

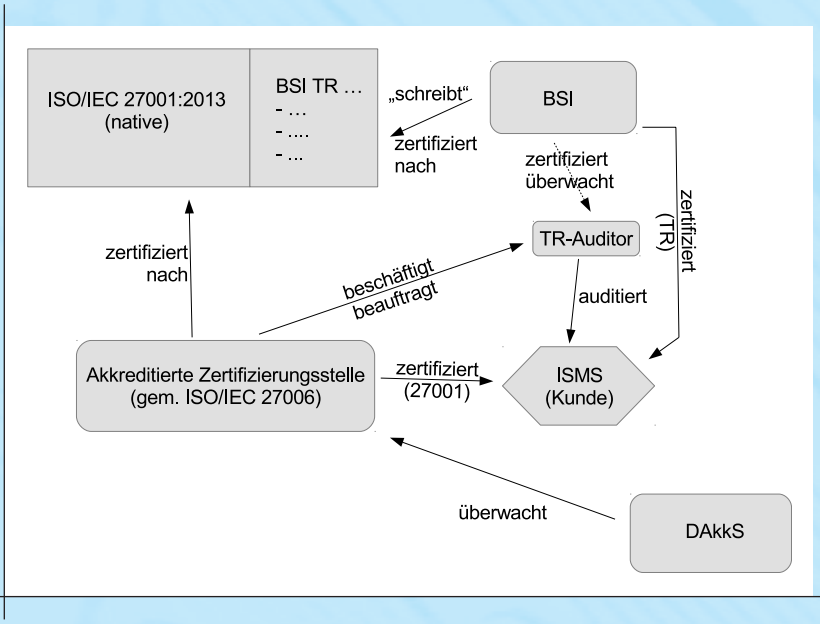

Abbildung 3: Zusammenspiel der Pflege von und Zertifizierung gemäß TR 3145 (aufbauend auf die ISO/IEC 27001)

Sicherheitsanforderungen festlegen. Vom Gesetzgeber ist dabei angedacht, dass diese Standards dann als (mögliche) Grundlage für den Nachweis der IT-Sicherheit in diesen Branchen dienen können.

Um die Eignung solcher Standards zu gewährleisten, kann eine Prüfung beim BSI beantragt werden, das dann im Benehmen mit dem Bundesamt für Bevölkerungsschutz und Katastrophenhilfe sowie im Einvernehmen mit der zuständigen Aufsichtsbehörde des Bundes oder im Benehmen mit der sonst zuständigen Aufsichtsbehörde diese Prüfung durchführt.

Da die ISO/IEC 27001 in einigen der zukünftig als „kritische Infrastruktur“ bezeichneten Branchen bereits etabliert ist, ist davon auszugehen, dass die in diesem Artikel skizzierten Ansätze zur Erstellung sektorspezifischer Normen und Standards (hier auch insbesondere die ISO/IEC 27009) eine Rolle spielen werden.

Die Umsetzung dieser branchenspezifischen Standards in den einzelnen Unternehmen kann zum Beispiel durch Audits oder Zertifizierung nachgewiesen werden. Der Gesetzgeber lässt im Entwurf dabei offen, ob hier eine Ad-hoc-Zertifizierung geschaffen wird (eigenes Schema) oder ob auf etablierte Zertifizierungen nach ISO/IEC 27001 aufgesetzt wird – zum Beispiel analog zu den Modellen, wie sie in Abschnitt für die TR 3145 diskutiert werden.

Gerade für international tätige Firmen bietet somit das geplante IT-Sicherheitsgesetz einen (zusätzlichen) Anlass, branchenspezifische Sicherheitsstandards gemäß den Anforderungen der zukünftigen ISO/IEC 27009 zu entwickeln und eine nationale Umsetzung als Norm zu forcieren. Sollte dann noch ein „Mutual Recognition Agreement“ (MRA) für die ISO/IEC 27001 finalisiert sein, könnten dann weltweit sektorspezifische Zertifikate anerkannt werden, wobei streng genommen nur der generische „27001-Anteil“ unter die gegenseitige Anerkennung fällt, aber wahrscheinlich der sektorspezifische Anteil in vielen Situationen „de facto“ auch anerkannt würde.

Damit hätten deutsche Firmen neben dem Sicherheitsgewinn auch noch einen Image-Gewinn zu verzeichnen (ähnlich der Situation bei der ISO/IEC 27019). ■

Literatur

[1] ISO/IEC Directives, Part 1, Consolidated ISO Supplement – Procedures specific to ISO, http://isotc.iso.org/livelink/livelink?func=ll&objId=4230452&objAction=browse&sort=subtype

[2] Bundesnetzagentur (BNetzA), Sicherheitskatalog gem. § 11 Abs. 1a EnWG, Entwurf, www.bundesnetzagentur.de/SharedDocs/Downloads/DE/Sachgebiete/Energie/Unternehmen_Institutionen/Versorgungssicherheit/IT_Sicherheit/IT_Sicherheitskatalog.pdf

[3] JIPDEC, The Numbers of ISMS Certificates, www.isms.jipdec.or.jp/english/lst/ind/org2.html verfügbar.

[4] Schweizerische Eidgenossenschaft, Der Bundesrat, Verordnung über die Datenschutzzertifizierungen (VDSZ), www.admin.ch/opc/de/classified-compilation/20071826/

[5] Bundesministerium des Innern, Entwurf eines Gesetzes zur Erhöhung der Sicherheit informationstechnischer Systeme (IT-Sicherheitsgesetz), Dezember 2014, www.bmi.bund.de/SharedDocs/Downloads/DE/Nachrichten/Kurzmeldungen/entwurf-it-sicherheitsgesetz.pdf

Amtliche Mitteilungen

1. Im Vergleich zur letzten Ausgabe dieser amtlichen Mitteilungen sind inzwischen folgende Zertifizierungen des BSI gemäß Common Criteria und ITSEC abgeschlossen worden:

Hersteller/Vertreiber	Produkt	Produkt-Typ	Ergebnis ID Zertifizierungsdatum
NXP Semiconductors Germany GmbH	NXP Secure PKI Smart Card Controllers P5CD128V0v/ V0B(s), P5CC128V0v/ V0B(s), P5CD145V0v/ V0B(s), P5CC145V0v/ V0B(s), P5CN145V0v/ V0B(s), each including IC Dedicated Software	Smartcard Controller	EAL 5+ BSI-DSZ-CC-0858-V2-2015 2015-04-27
NXP Semiconductors Germany GmbH	NXP Secure Smart Card Controllers P5CD016/021/041/051 and P5Cx081V1A/ V1A(s)	Smartcard Controller	EAL 5+ BSI-DSZ-CC-0857-V2-2015 2015-04-27
Giesecke & Devrient GmbH	Sm@rtCafé® Expert 7.0 C1	Smartcard Controller	BSI-DSZ-CC-0868-2014-MA-01 2015-04-23
Sophos Technology GmbH	Sophos UTM V9 Packet Filter Version 1.000	Paketfilter	EAL 4+ BSI-DSZ-CC-0942-2015 2015-04-21
Infineon Technologies AG	SLB9670_1.2, V. 6.40.0190.00	Smartcard Controller (TPM)	EAL 4+ BSI-DSZ-CC-0958-2015 2015-04-16
Panasonic Semiconductor Solutions Co., Ltd.	MN67S150 Smart Card IC Version RV08 including IC Dedicated Software	Smartcard Controller	EAL 6+ BSI-DSZ-CC-0935-2015 2015-04-16
Continental Automotive GmbH	Digital Tachograph DTCO 1381, Release 2.2	Fahrtenschreiber	EAL 4+ BSI-DSZ-CC-0936-2015 2015-04-16
Red Hat, Inc.	JBoss Enterprise Application Platform 6, Version 6.2.2	Anwendungsserver	EAL 4+ BSI-DSZ-CC-0909-2015 2015-04-13
IBM Corporation	RACF Element of z/OS, Version 2, Release 1	Serveranwendungen	EAL 5+ BSI-DSZ-CC-0875-2015 2015-04-13
IBM Corporation	z/VM Version 6, Release 3	Betriebssystem	EAL 4+ BSI-DSZ-CC-0903-2015 2015-03-30

Anmerkung:

– Die zugehörigen Zertifizierungsreporte mit Zertifikaten sind auf der Web-Seite www.bsi.bund.de/zertifizierungsreporte einzusehen.

2. Im Vergleich zur letzten Ausgabe dieser amtlichen Mitteilungen ist inzwischen für folgende Produkte eine Zertifizierung beantragt worden:

Antragsteller	Produktname	Produkttyp	Zertifizierungs-ID
intellic GmbH	Digital Tachograph EFAS-4.5 Version 03.00	Digitaler Tachograph	BSI-DSZ-CC-0980
Giesecke & Devrient GmbH	STARCOS 3.6 COSGKV C1	Smartcard Betriebssystem (eHealth G2)	BSI-DSZ-CC-0976
F5 Networks, Inc.	F5 Networks BIG-IP® Application Delivery Controller (ADC-AP) version 11.5	Netzwerk- und Kommunikationsprodukte	BSI-DSZ-CC-0975

Anmerkungen:

- Eine Veröffentlichung dieser Angaben erfolgt hier nur, sofern der Antragsteller damit einverstanden ist *und* die Evaluierung begonnen wurde. In der Liste vorhandene Nummerierungslücken betreffen beantragte Zertifizierungen, für die die genannten Voraussetzungen fehlen.
- Bei einigen Produkten handelt es sich um eine Re-Zertifizierung eines bereits zertifizierten Produktes wegen Änderungen am Produkt oder Wechsel der Prüfkriterien.

3. Vom BSI erteilte Standortzertifikate

Antragsteller	Entwicklungs-/ Produktionsstandorte	ID Ausstellungsdatum	gültig bis
Dream Chip Technologies GmbH Germany	Dream Chip Technologies GmbH Germany	BSI-DSZ-CC-S-0040-2015 2015-04-16	2017-04-15

4. Vom BSI erteilte ISO-27001-Zertifikate auf der Basis von IT-Grundschutz

Zertifikatsnummer	Institution	Untersuchungsgegenstand	gültig bis
BSI-IGZ-0196-2015	TÜV NORD Service	Am Standort Hannover betreibt die TÜV NORD GROUP ihr zentrales Hochverfügbarkeits-Rechenzentrum. Der Untersuchungsgegenstand umfasst das Gebäudemanagement sowie die Betriebsprozesse zur Überwachung der IT-Infrastruktur und zentraler Anwendungen.	2018-03-29
BSI-IGZ-0169-2015	Versatel GmbH	Das „uniCore“ ist eine deutschlandweite, nicht öffentliche Netzwerkinfrastruktur der Versatel GmbH auf Basis der Multiprotocol Label Switching Vermittlungstechnologie (MPLS). Hierüber werden VPN-Dienste für Sprache, Daten und Multimedia zur Erfüllung von Kundenanforderungen bzgl. des sicheren Informationsaustauschs bereitgestellt. Der Untersuchungsgegenstand umfasst den Verbund der MPLS-Core-Router mit realisierter Netzbetreibergrenze (Provider Edge), sowie die für deren Betrieb notwendigen infrastrukturellen, organisatorischen, personellen und technischen Komponenten und Prozesse. Aus Netzwerksicht beinhaltet der Informationsverbund die MPLS-Core-Router an den Standorten Hamburg, Berlin, München, Ulm, Stuttgart, Frankfurt, Essen und Dortmund sowie den Betrieb des „uniCore“ durch das Network Operation Center am Standort Essen.	2018-03-19
BSI-IGZ-0197-2015	SysEleven GmbH	Die SysEleven GmbH ist ein Full Managed Hosting Dienstleister und betreibt für diesen Zweck eine Hostingplattform, die die technische und organisatorische Grundlage für die Erbringung der Dienstleitung „Managed Hosting“ darstellt. Der Untersuchungsgegenstand umfasst alle dafür notwendigen IT-Komponenten und Betriebsprozesse. Im Speziellen sind dies einerseits die Infrastrukturkomponenten (Server-, Speicher- und Netzwerkkomponenten) und die Räume und Gebäude, in denen diese Komponenten betrieben werden, anderseits die Adminstrationsumgebung, in der die Plattform betrieben wird. Die Anbindung an das Internet, die projektspezifischen Anpassungen der bereitgestellten Systeme und Services, die administrative Verwaltung der Domains sowie die Systeme und Prozesse zur Abrechnung der Dienstleistungen sind nicht Teil des Untersuchungsgegenstandes.	2018-03-08
BSI-IGZ-0187-2015	Kommunales Rechenzentrum Minden-Ravensberg/Lippe	Der Untersuchungsgegenstand ist der Verbund des Kommunalen Rechenzentrums Minden-Ravensberg/Lippe (KRZ) in Lemgo. Dieses System bezieht sich auf den vollständigen Betrieb des Rechenzentrums, alle selbst genutzten oder für Kunden zur Verfügung gestellten Anwendungen oder IT-Systeme einschließlich der dafür erforderlichen Infrastruktur.	2018-03-05