STUDIE

Informationssicherheits-Management-Systeme (ISMS) bei Energieversorgern 2018

Autoren: Dr. Joachim Müller
Dr. Alexander Sänn
Verena Ludwig

Mit Gastbeiträgen von:
MdB Marian Wendt
RA Annett Albrecht
Prof. Dr. Peter Langendörfer

Betriebswirtschaftliches Forschungszentrum für Fragen der mittelständischen Wirtschaft e. V. an der Universität Bayreuth

SEVEN PRINCIPLES AG

Datum: 30. September 2018
Version 1.0

HERAUSGEBER

Betriebswirtschaftliches Forschungszentrum für Fragen der mittelständischen Wirtschaft e. V. an der Universität Bayreuth
Mainstrasse 5 - 95444 Bayreuth

T +49 921 530397 - 0
F +49 921 530397 - 10
E info@bfm-bayreuth.de
I www.bfm-bayreuth.de

Registergericht: Amtsgericht Bayreuth
Registernummer: VR 503

Vorstand: Prof. Dr. Torsten Kühlmann (Vorsitzender),

Prof. Dr. Daniel Baier, Prof. Dr. Klaus Schäfer, Prof. Dr. Friedrich Sommer, Prof. Dr. Kay Windthorst

STUDIE

Informationssicherheits-Management-Systeme (ISMS) bei Energieversorgern 2018

BFM

UNIVERSITÄT BAYREUTH

SEVEN PRINCIPLES
Enabling Your Digital Business

Inhaltsverzeichnis

Abbildungsverzeichnis

Tabellenverzeichnis

Abkürzungsverzeichnis

a. F.	Alte Fassung
APT	Advanced Persistent Threat
BDSG	Bundesdatenschutzgesetz
BNetzA	Bundesnetzagentur
BSI	Bundesamt für Sicherheit in der Informationstechnik
CISO	Chief Information Security Officer
DDOS	Distributed-Denial-of-Service
DMZ	Demilitarized Zone
DS-GVO	Europäische Datenschutzgrundverordnung
EnWG	Energiewirtschaftsgesetz
ESCSWG	Energy Sector Control Systems Working Group
EVU	Energieversorgungsunternehmen
FTP	File Transfer Protocol
ICS	Industrial Control Systems
IPU	Interparlamentarische Union
ISMS	Informationssicherheits-Management-System
ISB	Informationssicherheitsbeauftragter / Information Security Officer (engl. ISO)
ISO	Internationale Organisation für Normung
IT-SiKa	IT-Sicherheitskatalog der BNetzA
KRITIS	Kritische Infrastrukturen
MA	Mitarbeiter
NIS	Netz- und Informationssicherheit
ÖPNV	öffentlicher Personennahverkehr
SWIFT	Society for Worldwide Interbank Financial Telecommunication
TOM	Technische und organisatorische Maßnahmen / Controls nach ISO 27001
UP KRITIS	Öffentlich-private Kooperation zwischen Betreibern Kritischer Infrastrukturen (KRITIS), deren Verbänden und den zuständigen staatlichen Stellen
VLAN	Virtuelles Lokales Netzwerk

1 Management Summary

Das Betriebswirtschaftliche Forschungszentrum für Fragen der mittelständischen Wirtschaft an der Universität Bayreuth entwickelte, gemeinsam mit der BA Security der SEVEN PRINCIPLES AG die vorliegende Untersuchung zum Status-quo der Informationssicherheits-Management-Systeme (ISMS) in der Energieversorgung. Die grundlegende Motivation zur Untersuchung stellt die gesetzliche Vorgabe zur Einführung und Zertifizierung eines ISMS bei Netzbetreibern bis zum 31.01.2018 dar. Bereits zum 30.11.2015 waren die Netzbetreiber in der Pflicht, einen Ansprechpartner für IT-Sicherheit gegenüber der Bundesnetzagentur (BNetzA) zu benennen. Die Studie baut auf den im Jahr 2015 von den Energieforen Leipzig, der Universität Bayreuth und der SEVEN PRINCIPLES AG untersuchten Fragen zur Erwartungshaltung und Prognose der Effektivität des ISMS nach ISO 27001 auf und blickt mit der aktuellen Erhebung auf den Stand der ISMS-Einführung und den gesammelten Erfahrungen zur Zertifizierung.

Im Fokus der ersten Studie standen die Erwartungshaltungen sowie die Umsetzungspläne der Betroffenen zur Einführung und Zertifizierung ihres ISMS. Im Ergebnis stellte die erste Studie den damals aktuellen Wissens- und Umsetzungsstand zum ISMS bei den befragten Energieversorgern in Deutschland dar, erlaubte eine Abschätzung des Aufwands zu dessen Implementierung und gab Umsetzungszeiträume und Meilensteine sowie konkrete Handlungsempfehlungen für die Implementierung eines ISMS an. In Summe hatten 34 % der befragten Unternehmen ein ISMS bereits implementiert und 8 % befanden sich in der Einführungsphase. Es zeigte sich, dass 1) wenige Energieversorgungsunternehmen (EVU) zum damaligen Zeitpunkt bereits über ein ISMS verfügten, 2) die Einführung maßgeblich von der Einbindung der Mitarbeiter abhängt, 3) ein ISMS und insbesondere Notfallübungen als lohnend angesehen werden, 4) zum damaligen Zeitpunkt kaum Erfahrungen mit der Zertifizierung vorhanden waren, 5) die Informationslage für die Betroffenen nicht ausreichend erschien, 6) der IT-Sicherheitskatalog in seinen Regelungen als ausreichend empfunden wurden, 7) Kooperationen zum Thema kaum durch EVU gesucht werden, 8) die Vorgabe des Geltungsbereichs bei der Zertifizierung „minimale“ Mentalität bewirkte sowie 9) Trends in der IT beim damaligen Implementierungsstand des ISMS nicht berücksichtigt wurden. Weiterhin fiel auf, dass bei den Kernthemen des ISMS a) Beitrag eines ISMS zur IT-Sicherheit, b) Beitrag zur Versorgungssicherheit und c) Beitrag zur Optimierung von Prozessen die Erwartungshaltung der Energieversorger ohne ISMS und die tatsächliche Bewertung der Energieversorger mit ISMS weit auseinanderlagen und die tatsächliche Bewertung der Wichtigkeit des ISMS positiver als die Erwartungshaltung bewertet wurden. Auch sekundäre Themen wie die Verbesserung des Images des Unternehmens und der Beitrag zum Marketing und zur Öffentlichkeitsarbeit sowie Begleiteffekte in Form von Sensibilisierung und Transparenz wurden real positiver bewertet als die Erwartungshalt es vermuten ließ. Auf der negativen Seite stand jedoch die Komplexität, welche insbesondere in der Steuerung abteilungsübergreifender Prozesse und Verfahren, dem Ressourcen-Management sowie in der Erstellung praxisnaher Richtlinien und Arbeitsanweisungen als hoch bewertet wurden. In Summe zeigte die erste Studie damit, dass die Unternehmen skeptisch dem ISMS gegenüberstanden und von der tatsächlichen Leistung positiv „überrascht“ wurden.

Die Ergebnisse der aktuellen Studie zeigen, dass sich die Situation zur Umsetzung des ISMS in den Unternehmen der EVU verbessert hat. Bereits 88 % der Studienteilnehmer haben nunmehr ein ISMS implementiert und weitere 10 % befinden sich derzeit in der Phase der Einführung. Hauptgründe waren zu 95 % die gesetzliche Verpflichtung sowie zu 52 % die gezielte Steigerung der Informationssicherheit im Unternehmen. Dabei zeigte sich, dass bei 62 % der Unternehmen bereits vor der Implementierung das Thema Informationssicherheit einen hohen Stellenwert einnahm. Das größte Potenzial zur Wirkung des ISMS besteht demnach bei 38 % der Unternehmen, die dem Thema Informationssicherheit bisher lediglich einen beiläufigen oder gar keinen Stellenwert einräumten. Treiber zur Implementierung waren größtenteils die Fachbeauftragten mit 83 % - die (Chief) Information Security Officer. Die Implementierungen decken mehrheitlich die Leitstelle und die Netzführung ab. Es zeigt sich weiterhin, dass durch die Einführung eines ISMS insbesondere die Sensibilisierung der Mitarbeiter sowie die Reduzierung von Schwachstellen in der Informationssicherheit erreicht werden konnte. Zu Sensibilisierung setzen 92 % der befragten Unternehmen auf regelmäßige Schulungsmaßnahmen, wie es gesetzlich gefordert ist. Immerhin noch die Hälfte der befragten Unternehmen berücksichtigen das Thema Informationssicherheit ebenfalls im Unternehmensnewsletter. In Summe geben 94,9 % der Unternehmen an, dass das ISMS einen Mehrwert für das Unternehmen geleistet hat. Die durch das ISMS erlangten Mehrwerte lassen sich auf folgende Bereiche aufspannen:

Mehrwerte auf Ebene der Anlagen in Form der Bewertung der Anlagen mittels technischen und organisatorischen Maßnahmen bzw. Controls, mittels Stärkung des Verantwortungsbewusstseins auf Ebene der Industriellen Informationstechnik und durch eine (prozessorale) Neustrukturierung der Leitstelle.

Mehrwerte auf Ebene des Personals in Form der Stärkung der Sensibilisierung im Unternehmen, durch die Einführung eines Prozessdenkens sowie durch die Überarbeitung der Handlungsweisen und Anweisungen.

Mehrwerte auf Ebene der Prozesse in Form der Erstellung oder Erneuerung der Prozessdokumentation, durch die Vereinheitlichung der Prozesse, durch die Erhöhung der Prozesstransparenz und durch die Identifikation eines konkreten Handlungsbedarfs.

In der allgemeinen Betrachtung über alle Probanden hinweg zeige sich, dass insbesondere

- die Erwartungen zur Verbesserung im Umgang mit dem Thema Informationssicherheit im Unternehmen,
- die Mitarbeitersensibilisierung,
- die Sicherung der Rechtskonformität sowie
- die Verbesserung der Informationssicherheit auf KRITIS-Ebene (hier Leitsystem-, Produktionssystem-Ebene)

zu größter Zufriedenheit adressiert werden konnten. Diese Punkte werden im Vergleich als die relativ wichtigsten Aspekte in der Implementierung des ISMS und dessen Beitrag zur Informationssicherheit im Unternehmen bewertet. Die Aufdeckung der Sicherheitsrisiken ist sehr zufriedenstellend durch das ISMS umgesetzt.

Durchwachsen ist die Einschätzung zur Identifikation von Sicherheitsvorfällen, zur Annahme des ISMS bei den Mitarbeitern und bei der Sicherstellung der Versorgungssicherheit der Kunden. Hier kann keine vollkommene Zufriedenheit der befragten Unternehmen gemessen werden. Als herausfordernd zeigt sich auch die Festlegung von Entscheidungswegen zur Lösung von Sicherheitsvorfällen, die mit dem ISMS verbundene Verbesserung der Büro-IT, die Qualitätssteigerung und Anpassung der Prozesse sowie die einfache Integration in den Unternehmensalltag. Bei der Zufriedenheit geht die Meinung zwischen Chief Information Security Officer (CISO) und Information Security Officer (ISO/ISB) im Aspekt der Entwicklung operativer Handlungsempfehlungen sowie bei der Annahme des ISMS durch die Mitarbeiter jedoch auseinander. Dennoch besteht weiterhin Verbesserungsbedarf. Dieser kann beim zukünftigen Ausbau des ISMS in den Unternehmen durch die Schulung über das Ziel des ISMS, die Erweiterung des Scopes auf die Büro-IT und auf bisher nicht betroffene Abteilungen sowie in der Vermittlung über die Relevanz von Informationen für die eigene Geschäftstätigkeit und langfristige Unternehmenssicherung liegen. Insgesamt zeigt sich aber, dass die Ziele eines ISMS nach ISO 27001 zur Wahrung von Vertraulichkeit, Integrität und Verfügbarkeit der Informationen und der damit verbundenen Informationssysteme erfüllt werden und wesentlich zur Steigerung der Informationssicherheit beigetragen wird. Dies geschieht insbesondere bei der Risikoanalyse, der Stärkung des Risikobewusstseins und Mitarbeitersensibilisierung sowie der Prozessentwicklung mit Blick auf die drei genannten Schutzziele.

Im Vergleich zur Erstbefragung fällt weiterhin auf, dass 76 % der Unternehmen einen Berater zur Unterstützung bei der Einführung hinzugezogen haben, obwohl im Jahr 2015 noch 92 % der Unternehmen die Hinzunahme eines Dienstleisters postulierten. Die Erfahrungen der Unternehmen bei der Einbindung von Beratern bekräftigt deren Fachkunde und strukturierte Arbeit, welche auf das Ziel der erfolgreichen Zertifizierung ausgelegt ist. Dies ist jedoch fallspezifisch zu sehen und daher äußerten die befragten Unternehmen ebenso Kritik an den Beratern. Die Risikoanalyse, erdachte fachfremde Störszenarien oder mangelhafte Musterdokumente sowie konträre Aussagen der Berater wurden hier genannt. Eine Ursache kann in der zeitlichen Auslastung der Berater zum Thema ISMS liegen, was auch genannte Probleme bzgl. Budgetüberschreitung und Projektcontrolling betreffen kann. Lediglich 39 % der Unternehmen möchten für die kontinuierliche Verbesserung des ISMS einen Berater hinzuziehen. Umso erfreulicher ist die hohe Zahl der erfolgreichen Erstzertifizierungen mit 86 % sowie der konstruktive Dialog mit den Auditoren. Das Aufzeigen von Lücken sowie die Praxisorientierung der Auditoren wurden als positive Einschätzung angegeben. Als problematisch ist hier jedoch die hohe Auslastung der Auditoren, die damit verbundene Terminfindung sowie der von Fall zu Fall unterschiedlich hohe Theoriebezug des Auditors zu nennen.

Ein ähnliches Bild zeigte der ÖPNV, welcher mit der „Ersten Verordnung zur Änderung der BSI-Kritisverordnung“ vom 21. Juni 2017 ebenso in der Pflicht zur Einführung eines ISMS ist. Die Analyse weiterer KRITIS-Bereiche, insbesondere ohne eine Zugehörigkeit zu einem Energieversorger, und deren eigener Umgang zur Implementierung und Zertifizierung eines ISMS sind fortführend die spannenden Themen am Markt und in der Forschung zur Umsetzung.

2 Einleitung

2.1 Der politische Impuls und dessen Effektivität

Gastbeitrag: MdB Marian Wendt

Es ist nun genau drei Jahre her, als im Sommer 2015 der Deutsche Bundestag das IT-Sicherheitsgesetz verabschiedete. Die Notwendigkeit einer einheitlichen bundesgesetzlichen Regelung im Bereich der Cybersicherheit steht heute außer Frage. Zum einen ist der Schutz der IT-Steuerung gegen systemimmanente, also durch Fehler und Mängel der verwendeten Systeme verursachten Ausfälle, ein Ziel. Zum anderen – und dieses Gesetzesziel ist genauso wichtig – ist der Schutz gegen die gezielte Herbeiführung von Fehlfunktionen mit Auswirkungen auf die IT-Prozesse ein Ziel. Wie gefährlich private oder gar staatliche Angreifer sein können, wie tief diese unerwünschten Gäste in die Systeme eindringen können, und wie groß der Schaden sein kann, wurde uns in den letzten Monaten anhand diverser Attacken mehr als deutlich.

Die Sensibilität von Wirtschaft, Verbraucher und Gesetzgeber für den Themenkomplex Cybersicherheit war berechtigt. Gerade aus dem engen Austausch mit Wirtschaft und Gesellschaft, also mit den Betroffenen, entstand das IT-Sicherheitsgesetz. Von Anfang an setzte der Gesetzgeber konstruktiv-kritische Anmerkungen um. Es hatte beispielsweise bereits in der 17. Legislaturperiode einen Anlauf für ein IT-Sicherheitsgesetz gegeben, der maßgeblich wegen Widerstand aus der Wirtschaft nicht umgesetzt wurde. Die Kritik bezog sich vor allem auf die umfassende Meldepflicht. Aber auch lange vor der Verabschiedung des IT-Sicherheitsgesetzes stand das Thema Schutz Kritischer Infrastrukturen weit oben auf der Agenda der Bundesregierung.

Seit 2007 wurde zunächst eine freiwillige kooperative Zusammenarbeit mit den Betreibern Kritischer Infrastrukturen im sogenannten UP KRITIS aufgebaut. Als eine öffentlich-private Kooperation zwischen Betreibern Kritischer Infrastrukturen, deren Verbänden und den zuständigen staatlichen Stellen war der UP KRITIS ein erster Schritt. Auf die verschlechterte Sicherheitslage reagierte die Bundesregierung ab 2014 mit einem weiteren Schritt: Das Prinzip der Freiwilligkeit wurde durch einen verpflichtenden regulatorischen Rahmen erweitert.

Noch bevor die europarechtliche Einheitsregelung mit der Netz- und Informationssicherheitsrichtlinie (NIS-Richtlinie) in Kraft trat, griff der Bundesgesetzgeber den Vorschlag der Europäischen Kommission in der Sache mit dem IT-Sicherheitsgesetz, dem NIS-Richtlinien-Umsetzungsgesetz und der Verordnung des Bundesamts für Sicherheit in der Informationstechnik (BSI KRITIS-Verordnung) auf. Somit waren gerade die zunehmende Bedrohungslage sowie die Abhängigkeit von zuverlässigen und vertrauenswürdigen IT-Systemen der entscheidende Beweggrund für ein erhöhtes Sicherheitsempfinden, welches das IT-Sicherheitsgesetz prägt.

Mit dem IT-Sicherheitsgesetz setzt der Bundesgesetzgeber neue Standards auf dem Gebiet des Sicherheitsrechts. Vor dem Hintergrund des bereits seit 2009 geltenden Gesetzes über das Bundesamt für Sicherheit in der Informationstechnik kommt dieser Bundesbehörde eine zentrale, koordinierende Bedeutung zu. Durch die Festlegung von Pflichten und Mitwirkungsmöglichkeiten seitens der Adressaten bietet das IT-Sicherheitsgesetz einen kooperativen Ansatz. Dabei erhalten die vormals freiwillig mit den Behörden kooperierenden Betreiber Kritischer Infrastrukturen die Möglichkeit, trotz des Pflichtenkanons weiterhin eng und vertrauensvoll zu kooperieren.

Diese Art kooperativer Regulierung spiegelt sich auf allen Ebenen des IT-Sicherheitsgesetzes wider. Sei es durch eine enge Beteiligung der Betreiber bei der Identifizierung durch die BSI KRITIS-Verordnung, sei es durch die Möglichkeit für die Betreiber, die für sie geltenden Sicherheitsstandards aktiv zu gestalten. Beispiel für eine solche aktive Gestaltung ist etwa das Vorschlagsrecht, welches Betreibern Kritischer Infrastrukturen und ihren Branchenverbänden eingeräumt wird, branchenspezifische Sicherheitsstandards zeitnah dem Bundesamt für Sicherheit in der Informationstechnik vorzulegen. Solche und andere Sicherheitsmaßnahmen bringen freilich einen gewissen zusätzlichen Aufwand für die verschiedenen Nachweise und Audits sowie für die Störungsmeldungen mit sich. Von diesem Aufwand profitieren jedoch alle Betroffenen. Aus demselben Grund laden wir als Bundesgesetzgeber die Unternehmen dazu ein, branchenspezifische Standards mitzugestalten.

Dieses enge Zusammenwirken zwischen Staat, Wirtschaft und Verbrauchern und der daraus resultierende kooperative Ansatz haben sich als äußerst fortschrittlich erwiesen. Der angestrebte Kulturwandel gelingt: die Erkenntnis, dass der Aufbau effizienter effektiver Management-Systeme für die Informationssicherheit eine lebensnotwendige Investition in

die Zukunft ist, setzt sich immer stärker durch. Die vorliegende Studie bestätigt, dass das neue IT-Sicherheitsrecht gut angenommen wird. Wenn beispielsweise 95 % der Befragten gerade durch die gesetzliche Verpflichtung zur Einführung ihres Informationssicherheits-Management-Systems motiviert wurden und für 53 % die Steigerung der Informationssicherheit den Beweggrund dafür ausmachte, dann ist dies ein positives Signal an uns Gesetzgeber. Das gemischte Bild, das sich bei der Identifikation von Sicherheitsvorfällen mit einer geringfügigen Mehrerkennung bei professionell aufgestellten Unternehmen ergibt, ist ein genauso bedeutender Befund. Mit dieser „Hand am Puls“, an der Stimmung unter den Adressaten des Gesetzes, leistet die Studie einen wichtigen Betrag.

 Marian Wendt Mitglied des Deutschen Bundestages	Zur Person: Geboren 1985, Abitur, Studium zum Dipl.-Verwaltungswirt (FH) und Master of Laws (Recht der öffentlichen Verwaltung) 2009 Praktikum im US-Kongress in Washington D.C. 2013 und 2017 direkt gewählter Abgeordneter in den Deutschen Bundestag, Ordentliches Mitglied im Petitionsausschuss (Vorsitzender), Innenausschuss und Gremium nach Artikel 13 Abs. 6 GG Mitglied der Deutsch-Italienischen und der Deutsch-Südosteuropäischen Parlamentariergruppen und des parlamentarischen Freundeskreises Berlin-Taipei; stellv. Mitglied der Interparlamentarischen Union (IPU) sowie Funktionen in der CDU/CSU-Bundestagsfraktion Seit 2015 Vorsitzender des Kreisverbandes CDU Nordsachsen, seit 2015 Vorsitzender des Landesfachausschusses „Innere Sicherheit“ der Sächsischen Union Seit 2018 Präsident der THW-Bundesvereinigung e. V.

2.2 Ein Kommentar zur rechtlichen Situation

Gastbeitrag: RA Annett Albrecht

Unsere moderne und vernetzte Gesellschaft ist heute mehr denn je von technischen Systemen abhängig. Nahezu jeder Bereich unseres täglichen Lebens wird durch moderne Technik unterstützt. Jedes Unternehmen sowie auch die Einrichtungen und Organisationen Kritischer Infrastrukturen (KRITIS) sind daher in der Pflicht, Schutzmechanismen zu installieren und kontinuierlich zu pflegen, um Angriffe von außen zu verhindern oder zumindest zu erschweren. Im Falle Kritischer Infrastrukturen drohen bei deren Ausfall oder Beeinträchtigung nachhaltig wirkende Versorgungsengpässe, erhebliche Störungen der öffentlichen Sicherheit oder andere dramatische Folgen. Die IT-Sicherheit steht daher an erster Stelle.

Die DIN EN ISO 27001 regelt die Anforderungen an Informationssicherheits-Management-Systeme und damit die oben genannte Sicherheit. Ohne das ernst gemeinte Bekenntnis der Unternehmensführung, welche die Informationssicherheitspolitik festlegt und deren tatsächliche Anwendung regelmäßig überprüft, ist jede noch so detaillierte wie farbenfrohe Prozessbeschreibung nutzlos.

Die aktuelle Studie zeigt, dass immerhin bereits bei mehr als 88 % der hier befragten Studienteilnehmer ein Informationssicherheits-Management-System (ISMS) vorhanden und sich bei 10 % in der Einführungsphase befindet. Dies stellt klar, dass die erforderliche Informationssicherheit in der Fläche bekannt ist. Hier gilt es nun, den Schritt zur 100 %-Marke zu erreichen.

Bei genauerer Betrachtung ist zu erkennen, dass die Motivation der Unternehmen zur Einführung eines ISMS in erster Linie aus der gesetzlichen Verpflichtung zur Umsetzung resultiert. Die Steigerung der Informationssicherheit und das Bekenntnis der Unternehmensleitung zum ISMS sowie die Mitarbeitersensibilisierung waren erst nachgeordnete Motive zur Implementierung des Systems. Die Aufdeckung von Sicherheitsrisiken wird - ebenso wie die Identifikation von Sicherheitsvorfällen - erstaunlicherweise weniger erwartet, obwohl der Schutz der Informationen Ziel eines jeden ISMS ist.

Beim Blick über den Tellerrand wird sichtbar, dass die Anforderungen, welche die DIN EN ISO 27001 aufstellt, auch in anderen weit weniger bedeutsamen Branchen mittelbar oder unmittelbar Anwendung finden. So zeigt ein Vergleich mit den „Technischen und Organisatorischen Maßnahmen“ der am 25. Mai 2018 Gültigkeit erlangten Europäischen Datenschutz-Grundverordnung (DS-GVO) durchaus Parallelen zur ISO 27001. Dabei hat sich die DS-GVO an den Standard der ISO 27001 angelehnt. Nach beiden Regularien stehen die Bereiche Vertraulichkeit, Integrität und Verfügbarkeit von Informationen für das Unternehmen im Vordergrund. Sie alle haben im Vorfeld und im Nachgang des 25. Mai 2018 die nunmehr gesetzlich vorgeschriebenen Hinweise zu den Informationspflichten über die Verwendung der personenbezogenen Daten in zahlreicher, mitunter auch falscher Anwendung des neuen Rechts, erhalten. Dennoch wäre es zu dieser Flut an Datenschutzhinweisen ohne die gesetzliche Verpflichtung und die damit verbundenen Bußgelder wohl nicht gekommen. Dabei ist der Datenschutz als Ausprägung des Rechts auf informationelle Selbstbestimmung für den Einzelnen ebenso wichtig wie ein störungsfreies Funktionieren der KRITIS. Die ISO 27001 regelt Referenzmaßnahmenziele und Referenzmaßnahmen zur Informationssicherheit. Die DS-GVO verfolgt in Art. 32 DS-GVO die Sicherheit der Verarbeitung und verlangt technische und organisatorische Maßnahmen, um ein angemessenes Schutzniveau bei der Verarbeitung von Daten sicherzustellen. Um Datenschutzkonformität herzustellen, ist hier die innerbetriebliche Organisation so zu gestalten, dass sie den besonderen Anforderungen des Datenschutzes gerecht wird. Es sind alle erforderlichen technischen und organisatorischen Maßnahmen zum angemessenen Schutz der Daten des Auftraggebers, insbesondere mindestens die Maßnahmen der Zutritts-, Zugangs-, Zugriffs-, Weitergabe-, Eingabe-, Auftragskontrolle zur Auftragsdatenverarbeitung, Verfügbarkeits- sowie Trennungskontrolle zu ergreifen.

Durch die DS-GVO bekommen vor allem die technischen IT-Sicherheitsaspekte der Datenverarbeitung eine größere Bedeutung als sie nach dem Bundesdatenschutzgesetz alter Fassung (BDSG a. F) erlangten. Bei Umsetzung dieser umfangreichen Vorgaben werden jedoch nicht nur die personenbezogenen Daten vor dem unberechtigten Zugriff Dritter geschützt. Diese Maßnahmen schützen auch das Know-how, die Unternehmenswerte und damit das Vertrauen der Kunden in das Unternehmen.

Abschließend bleibt festzuhalten: Gleich, ob es sich um die Implementierung eines ISMS, eines Datenschutzkonzeptes oder eines Compliance-Management-Systems handelt, Nutznießer der Umsetzung werden bei konsequenter Durchführung immer das Unternehmen, deren Mitarbeiter und Kunden sein. Auch der Geschäftsführer, dessen straf- und zivilrechtliche Haftung bei Unterlassen von erforderlichen Schutzmaßnahmen schnell spruchreif werden wird, profitiert von der ernsthaften Identifizierung mit dem Thema der Informationssicherheit. Dass dies in den Köpfen der Verantwortlichen angekommen ist, macht die Studie an mehreren Stellen deutlich. Dennoch oder gerade weil die treibende Kraft die „bloße“ Angst vor Strafe ist, scheint die tatsächliche - nicht nur die rechtliche - Notwendigkeit in den Köpfen der Betroffenen noch nicht vollständig Fuß gefasst zu haben. Der „digitalen Sorglosigkeit“ muss entgegengewirkt werden.

Die Auseinandersetzung mit den kritischen Fragen bringt stets einen Mehrwert für die Firma, da erst dadurch Schwachstellen im Unternehmen oder in Bereichen des Unternehmens aufgedeckt werden. Dies zu erkennen, ist die Herausforderung für die Unternehmensführung.

Annett Albrecht

Rechtsanwältin,
Certified Risk Manager,
Datenschutzbeauftragte

Zur Person:

Geboren in Leipzig

Studium der Rechtswissenschaften in Leipzig

Erstes Staatsexamen 2002, Zweites Staatsexamen 2004 (beides in Sachsen)

Wahlstation bei Rechtsanwaltskanzlei KORBION & Kollegen in Düsseldorf

2005 Rechtsanwältin bei Haug Rechtsanwälte in Leipzig

2006 Gründung der Anwaltskanzlei Albrecht in Leipzig

Seit 2007 Certified Risk Manager

Mitgliedschaften im Deutscher AnwaltVerein e. V., in der Rechtsanwaltskammer Sachsen, im Förderverein VKU Abfallwirtschaft und Stadtreinigung VKS e. V. sowie im Leipzig 2015 e. V. und Gemeinsam für Leipzig e. V.

2.3 Zielstellung und Aufbau der Studie

In der heutigen digitalisierten Gesellschaft ist eine funktionierende Energieversorgung unausweichlich. Wird die Strom- und Gasversorgung durch mögliche Hackerangriffe beeinträchtigt, steht das öffentliche Leben in kürzester Zeit still. Beispielsweise können öffentliche Transportmittel nicht mehr genutzt werden und lebensnotwendige Dienstleistungen (wie Krankenhäuser) fallen durch einen Zusammenbruch der allgemeinen Informationstechnik aus. Darüber hinaus hängt eine funktionsfähige Energieversorgung von einer stabilen Informations- und Kommunikationstechnologie ab. Um die Sicherheit einer funktionierenden Energieversorgung gewährleisten zu können, ist es erforderlich ein Informationssicherheits-Management-System (ISMS) gemäß den Sicherheitsanforderungen zu etablieren. Hierfür hat der Deutsche Bundestag im Juni 2015 das IT-Sicherheitsgesetz verabschiedet.

Damit der Schutz gegen potenzielle Bedrohungen bei Energieversorgern sichergestellt werden kann, müssen die Anforderungen des IT-Sicherheitskataloges gemäß § 11 Absatz 1a Energiewirtschaftsgesetz (EnWG) eingehalten werden. Diese Anforderungen mussten bis zum 31. Januar 2018 von allen Strom- und Gasbetreibern in Deutschland eingehalten und erfüllt werden. Somit schreibt der Sicherheitskatalog vor, dass ein ISMS gemäß ISO 27001 von allen Energieversorgern implementiert wird und eine Zertifizierung des Management-Systems durch eine unabhängige zulässige Stelle erfolgt.

Die vorliegende Studie knüpft an die Studie Informationssicherheits-Management-System bei Energieversorgern aus dem Jahr 2016 der SEVEN PRINCIPLES AG in Zusammenarbeit mit den Energieforen Leipzig sowie dem Lehrstuhl für Innovations- und Dialogmarketing der Universität Bayreuth an und fragt den Status quo in der Zielgruppe ab.

Ziel ist es, den praktischen Nutzen sowie die Erfüllung der Erwartungshaltungen an ein ISMS zu hinterfragen. Hierzu wurden einzelne Vertreter aus dem Bereich der Informationssicherheit in der Energieversorgung befragt und ihre Erfahrungen im Unternehmen mit dem ISMS zusammengetragen. Die Studie untersucht damit den Erfüllungsgrad des ISMS an rechtliche und unternehmerische Erwartungen und ermittelt die konkreten Auswirkungen auf die Fachabteilungen in der Energieversorgung, welche nicht immer unmittelbar mit der Leittechnik verbunden sind. Weiterhin werden die Rahmenbedingungen diskutiert, welche herausfordernd und / oder kontraproduktiv zu den politischen Zielen (politische Effektivität des §11 Abs. 1a EnWG) waren.

Auf den nachfolgenden Seiten gibt die vorliegende Studie einen Überblick zur Informationssicherheit in der Energiewirtschaft anhand ausgewählter Beispiele und beschreibt relevante Ereignisse. Weiterhin führt das dritte Kapitel in die beiden exemplarischen Herausforderungen zur Implementierung des ISMS in Bezug auf die Netzwerktrennung und die Berücksichtigung der Informationssicherheit bei Lieferantenbeziehungen ein und beschreibt sie grundlegend. Das darauffolgende vierte Kapitel zeigt die ersten Ergebnisse der empirischen Untersuchung auf. Hierzu befragt die Studie Vertreter aus dem Bereich der Informationssicherheit bei Energieversorgern bzgl. Details zur Motivation zum ISMS, dem Unternehmens-eigenen Umgang mit dem ISMS und den besonderen Erfahrungen mit Blick auf die erwartete Service-Qualität des ISMS in seinen Auswirkungen. Das fünfte Kapitel beschreibt einleitend auf theoretischer Basis aus Sicht des Marketings und Innovations-Managements ein grundlegendes Vorgehen zur Orchestrierung und Zusammenwirkung Unternehmens-interner Projektteams sowie die daraus resultierenden organisatorischen Hürden eines ISMS-Projektteams. Der zweite Teil dieses Kapitels geht auf die Ergebnisse der empirischen Untersuchung zur Zusammenarbeit mit externen Dienstleistern ein. Das sechste Kapitel ist dem Thema der Auditierung und Zertifizierung gewidmet. Im ersten Teil geht die Studie auf die Erfahrungen aus Sicht eines Auditors ein, stellt das Ökosystem und die verschiedenen Rollen im Zuge von Audits vor und gibt Tipps für bevorstehende Auditierungen. Der zweite Teil präsentiert die Ergebnisse der empirischen Untersuchung zu den Erfahrungen der befragten Unternehmen mit Auditierungen und Zertifizierungen. Der dritte Teil thematisiert die Nachbehandlung von Haupt- und Nebenabweichungen bei den befragten Unternehmen. Das siebente Kapitel geht insbesondere auf den Bereich des öffentlichen Personennahverkehrs (ÖPNV) ein. Im Zuge der Erweiterung der KRITIS-Definition generiert eine spezielle Auswertung für Betreiber des ÖPNV erste Erkenntnisse zum ISMS in diesem Bereich. Das Fazit zur Studie gibt einen Ausblick zu zukünftigen Trends und Marktentwicklungen zum Thema.

Insbesondere Bedanken sich die Autoren der Studie für die Gastbeiträge von MdB Marian Wendt, RA Annett Albrecht sowie Prof. Dr. Peter Langendörfer.

3 Herausforderungen der Informationssicherheit in der Energieversorgung

3.1 Der aktuelle Stand

Seit Juli 2015 besteht bei Sicherheitsvorfällen eine Meldepflicht für Betreiber von KRITIS. Laut dem Bundesamt für Sicherheit in der Informationstechnik (BSI) konnten seit der Einführung der Meldepflicht bis zum 30. Juni 2017 34 Meldungen verzeichnet werden (BSI 2017 a, S. 10).

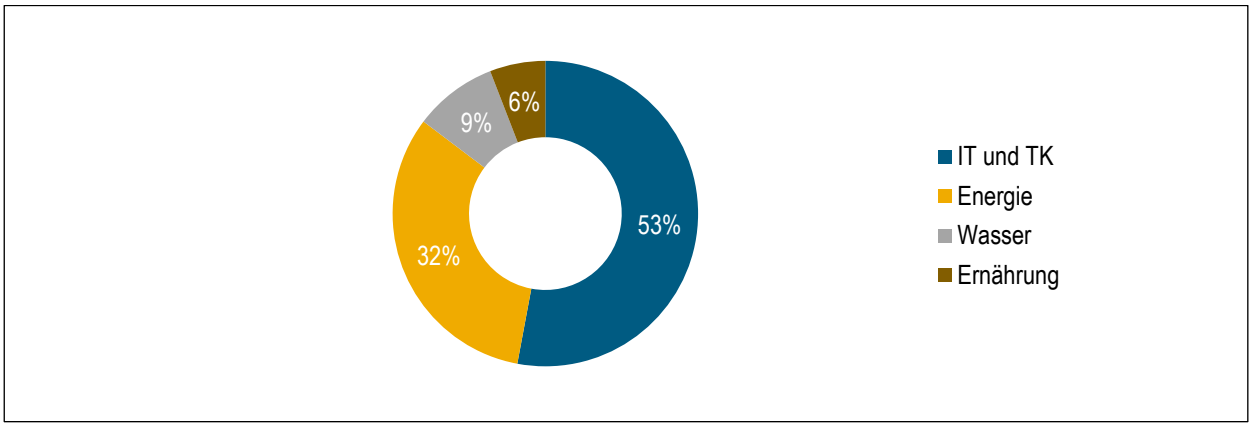


Abbildung 1: Eingegangene Meldungen beim BSI

Quelle: Eigene Darstellung in Anlehnung an BSI (2017 b), S. 10.

Abbildung 1 zeigt die Verteilung der Meldungen nach den Sektoren der KRITIS. Demnach sind 18 Meldungen im Bereich der Informationstechnik und Telekommunikation aufgenommen worden. Die häufigste Ursache der eingegangenen Meldungen sind menschliche Fehler, wie bspw. falsche Konfigurationen, welche anschließend eine IT-Störung auslösen. Weitere Ursachen waren Hardwarefehler oder eine fehlerhafte Software, welche die Folge eines fehlerhaften Updates war (BSI 2017 a, S. 10).

Abbildung 2 zeigt die Anzahl der Sicherheitsvorfälle ab dem Jahr 2014 im Zeitverlauf. Pro Jahr wird dabei insbesondere ein besonders wichtiger Sicherheitsvorfall, welcher in den Medien präsent war, hervorgehoben. Zur Recherche wurden hauptsächlich die Lageberichte des BSI von 2014 bis 2017 herangezogen. Darüber hinaus ist die Anzahl auf Deutschland beschränkt und beinhaltet nur Sicherheitsvorfälle im Bereich der KRITIS. Seit Juli 2015 besteht die Pflicht, Sicherheitsvorfälle zu melden. Des Weiteren sind Betreiber von Telekommunikations- und elektronische Datenverarbeitungssysteme, die für einen sicheren Netzbetrieb notwendig sind, seit dem 17. Juli 2015 nach § 11 Absatz 1a EnWG dazu verpflichtet, ein ISMS gem. IT-SiKa bis zum 31. Januar 2018 zu zertifizieren (Bundesnetzagentur 2015, S. 15). Dies könnte die erhöhte Anzahl im Jahr 2016 erklären. Denn mit der Etablierung eines ISMS werden vermutlich mehr Sicherheitsvorfälle erkannt und dokumentiert. Da nur Sicherheitsvorfälle bis Anfang Juni 2018 verzeichnet wurden, ist die Anzahl im Jahr 2018 noch sehr gering.

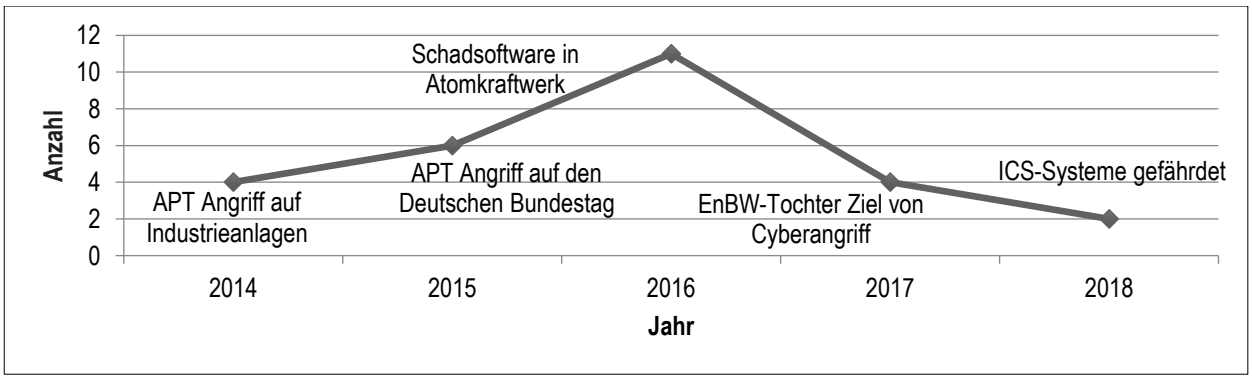


Abbildung 2: Anzahl der Sicherheitsvorfälle im Zeitverlauf

Herausforderungen der Informationssicherheit in der Energieversorgung

Im Folgenden werden aktuelle Sicherheitsvorfälle kurz näher erläutert. Generell ist das Thema Hackerangriffe auf deutsche Energieversorger extrem präsent. Aktuell warnt das Bundesamt für Informationssicherheit vor gezielten Cyberangriffen auf deutsche Energieversorgungsunternehmen. Dabei wären die Energieversorger laut dem BSI Ziel einer großen Cyber-Kampagne. Den Angreifern soll es in einigen Fällen gelungen sein, in die Büro-IT von Energieversorgern einzudringen. Weitere Schäden sind allerdings nicht bekannt. Zudem sei es nur noch eine Frage der Zeit, bis KRITIS-Betreiber erfolgreich angegriffen werden, was durch ein hohes Sicherheitsniveau bisher vermieden wurde (SZ 2018). Tabelle 1 listet aktuelle Sicherheitsvorfälle von 2015 bis 2018 auf. Hierbei wurden nur Sicherheitsvorfälle berücksichtigt, welche in Deutschland stattfanden und Betreiber von KRITIS betroffen waren. Basis bilden die Lageberichte des BSI.

Sicherheitsrelevante Zwischenfälle	Jahr
Ransomware-Attacken auf Krankenhäuser	2015
Social Engineering per Telefon	2015
Advanced Persistent Threat (APT) Angriff auf den Deutschen Bundestag	2015
Distributet-Denial-of-Service (DDoS)-Angriffe auf Webseiten der Bundesregierung und des Deutschen Bundestages	2015
DDoS-Angriffe auf KRITIS-Unternehmen	2015
Spear-Phishing gegen KRITIS-Unternehmen im Energie-Sektor	2015
Cyberangriff auf Society for Worldwide Interbank Financial Telecommunication (SWIFT)-System	2016
Ransomware-Attacke auf Krankenhaus (Neuss)	2016
Schadsoftware in Atomkraftwerk (Ramnit)	2016
Cyber-Spionage bei Rüstungsunternehmen	2016
Social Engineering: CEO Betrug	2016
Routerausfall, Deutsche Telekom	2016
Manipulierbare Baustellenampeln und Wasserwerke	2016
WannaCry	2016
Ransomware in Personalabteilungen	2016
Botnetz Infrastruktur Avalanche	2016
Spear-Phishing gegen Spitzenpersonal	2017
UP KRITIS verhindert Schadcode-Ausbreitung	2017
EnBW-Tochter Ziel von Cyberangriff	2017
Hackerangriff auf Regierungsnetz	2018
ICS-Systeme gefährdet	2018

Tabelle 1: Übersicht von Sicherheitsvorfällen im Bereich der KRITIS

Quelle: Eigene Darstellung in Anlehnung an Blank und Dernbach (2018); BSI (2015, 2016, 2017 a); Schirrmacher (2018)

Herausforderungen der Informationssicherheit in der Energieversorgung

Bisher konnten insgesamt drei bekannte Hackerangriffe verzeichnet werden, welche einen physikalischen Schaden ausgelöst haben. Hierzu zählt der Computerwurm „Stuxnet“. Der zweite bekannte Fall ist der Angriff auf ein deutsches Stahlwerk, welcher 2014 im Lagebericht des BSI veröffentlicht wurde. Der dritte Fall ist ein Hackerangriff auf einen ukrainischen Stromversorger. Letzterer löste den ersten durch einen Hackerangriff initiierten Stromausfall aus (Heller 2016). Im Folgenden werden die beiden letzteren sowie weitere bekannte Hackerangriffe beschrieben.

Angriff auf ein deutsches Stahlwerk

Im Jahr 2014 griffen Hacker ein Stahlwerk in Deutschland gezielt an (BSI 2014, S. 31). Nach dem Bericht des BSI wurde die Steuerung eines Hochofens in Besitz genommen und die Anlage zerstört. Infolgedessen legten die Hacker ganze Systeme des Hochofens lahm. Darüber hinaus konnte das Stahlwerk den Hochofen nicht mehr selbständig herunterfahren. Hackern erlangten durch Spear-Phishing Zugriff auf das Büronetz des Stahlwerks. Danach arbeiteten sie sich bis an die Produktionsnetze voran. Dabei bewertet das BSI die Kenntnisse der Hacker als sehr fortgeschritten. Die Kenntnisse erstrecken sich hierbei nicht nur auf die klassische IT-Sicherheit, sondern auf ausgeprägtes Fachwissen in der Industrie und die Produktionsprozesse des Stahlwerkes (BSI 2014, S. 31).

Hackerangriff auf ukrainische Stromversorger

Im Dezember 2015 sorgte ein Cyberangriff für einen immensen Stromausfall in der Ukraine. Infolgedessen waren hunderttausende Menschen mehrere Stunden ohne Strom. Insgesamt waren 27 Umspannwerke von dem Hackerangriff betroffen. Dabei sind sich Experten sicher, dass es sich um einen Cyberangriff aus Russland handelt (Tanriverdi 2016). IT-Sicherheitsfirmen konnten die Schadsoftware „Black-Energy“ ausfindig machen (Heller 2016). Der Angriff begann damit, dass Mitarbeiter des Stromversorgungsunternehmen E-Mails mit Word-Dateien im Anhang erhielten. Als Mitarbeiter den Anhang öffneten, konnten sich die Hacker einen Zugriff auf die Netzwerke verschaffen. Danach hatten die Angreifer die Möglichkeit, eine Schadsoftware hochzuladen, um die Netzwerke weiter zu infizieren und aus der Ferne zu kontrollieren (Tanriverdi 2016). Festzuhalten ist, dass dieser Fall der erste durch einen Hackerangriff verursachte Stromausfall ist (Heller 2016). Darüber hinaus ist dieses Ereignis in Deutschland ebenfalls denkbar (Hannoversche Allgemeine 2018) und aus diesem Grund ist der Hackerangriff ebenfalls für Deutschland und die Sicherheit der Betreiber von KRITIS relevant.

Schadsoftware in Atomkraftwerk

In einem Kernreaktor in Gundremmingen ist 2016 eine Schadsoftware entdeckt worden. Hierbei handelte es sich um einen Computervirus (Spiegel Online 2016). Es wird vermutet, dass die Schadsoftware über einen Datenträger verbreitet wurde (Beer 2016). Bei Vorbereitungen auf die Revision ist die Schadsoftware aufgefallen. Dennoch wurde eine Gefährdung des Personals und der Gesamtbevölkerung ausgeschlossen, da die sensiblen Anlagen des Kernkraftwerkes nicht mit dem Internet verbunden sind. Das BSI wurde dahingegen entsprechend informiert. Als angemessene Gegenmaßnahmen wurde die Schließung des Atomkraftwerkes verlangt (Spiegel Online 2016).

EnBW-Tochter Ziel von Cyberangriff

Bereits im Juni 2017 warnte das BSI die Energieversorger vor Cyberangriffen. Grund dafür war der Hackerangriff auf die deutsche Tochterfirma des Stromkonzern EnBW (SZ 2018). Es handelte sich dabei um den regionalen Internetanbieter Netcom BW. Die Gefahr eines Stromausfalls bestand nicht, dennoch ist nicht auszuschließen, dass es sich um einen größeren ausgefeilten Hackerangriff handelte. Die Hacker nutzten Schwachstellen der Router des Herstellers Cisco aus, worauf sie anschließend ein Programm installierten. Der Zugriff konnte aufgrund dessen beschafft werden, da die Hacker das Mitarbeiterkonto eines externen Dienstleisters erwarben. Dadurch besteht die Möglichkeit, dass die Hacker Webseiten ausfindig machen können, welche die Mitarbeiter besuchen. Infolgedessen können die Angreifer diese Webseiten so manipulieren, dass sie Zugriff auf Passwörter erlangen. Dabei spricht man von den sogenannten „Waterholing“-Angriffen. Nach Aussagen des Unternehmens EnBW kam es allerdings nicht soweit. Die Angreifer befanden sich noch im Anfangsstadium und es konnte potenzieller Schaden abgewandt werden. Der Hackerangriff wurde rechtzeitig aufgrund der Warnung des BSI erkannt (Krause und Tanriverdi 2018).

3.2 Exemplarische Herausforderungen in der Praxis

Gastbeitrag: Prof. Dr. Peter Langendörfer – IHP – Leibniz-Institut für innovative Mikroelektronik

Netzwerksegregierung als Grundproblem

Das grundlegende Problem von Produktionsanlagen aus IT-Sicherheitssicht ist, dass diese Anlagen lange isoliert betrieben wurden und erst in den letzten Jahren immer häufiger in Unternehmensnetzwerke und damit auch ins Internet integriert werden. Damit sind Produktionsanlagen für Angreifer auch aus großen Distanzen erreichbar geworden und können mit „State-of-the-art"-Methoden angegriffen werden. Es können beispielsweise inhärent unsichere Protokolle wie FTP und telnet verwendet werden, um einen Angriff zu starten. Die File Transfer Protocol (FTP)-Server sind u. U. so konfiguriert, dass sie einen Gast-Account oder einen Anonymous Login erlauben, d. h. ein Angreifer braucht sich nicht zu authentifizieren, um Zugang zu einem Teil des Systems zu bekommen. Im Anschluss kann er die Tatsache, dass der FTP-Server Teil des Netzwerkes ist, nutzen, um weitere Informationen für seine Angriffe zu erhalten. Mit Hilfe von Sniffing-Werkzeugen wie Wire-Shark können Informationen wie Netzwerkadressen erhalten werden, die dann für weitere Angriffe wie IP-Spoofing genutzt werden.

Die Verwendung von „State-of-the-art" IT-Sicherheitslösungen ist hingegen aus folgenden Gründen meistens nicht möglich:

- Der Lebenszyklus von Produktionsanlagen ist in der Regel sehr viel länger als der von IT-Systemen. Das bedeutet, dass in Produktionsanlagen häufig nicht mehr unterstützte Softwarevarianten verwendet werden und dass die Rechenleistung häufig für aktuelle Sicherheitslösungen nicht ausreichend ist.
- Produktionsanlagen unterliegen u. U. rechtlichen Auflagen für Zertifizierungen, z. B. im Hinblick auf Umweltbedingungen. Aktualisierungen von Teilsystemen erfordern Re-Zertifizierungen, die die Aktualisierung der verwendeten Software extrem aufwendig machen, sodass diese nur selten durchgeführt werden kann.
- Veränderungen der Systemkonfiguration können Auswirkungen auf die Sicherheitseigenschaften und Produktqualität haben, was bedeutet, dass alle Aktualisierungen vor ihrer Umsetzung im Produktivsystem sehr gründlich getestet werden müssen.
- Veränderungen von Produktionsanlagen können negative Auswirkung auf die Herstellergarantie haben.

Um die Anzahl erfolgreicher Angriffe möglichst klein zu halten, bleibt also nur eine realistische Lösung: Produktionsanlagen müssen so gut wie möglich vom Internet und damit von potenziellen Angriffen abgeschirmt werden. Da eine kontrollierte Kommunikation mit den Produktionsanlagen aus betriebswirtschaftlicher Sicht sinnvoll und wichtig ist, ist eine vollständige physikalische Separierung nicht möglich. Die hier diskutierte Lösung ist folglich die logische Separierung des Unternehmensnetzwerkes in Teilnetze. Hierfür können allerdings Standardtechnologien wie Firewalls und Virtuelle Lokale Netzwerke (VLAN) verwendet werden.

Der entscheidende Punkt bei der Aufteilung eines komplexen Netzwerkes ist die Definition unterschiedlicher „Sicherheitszonen" oder „Sicherheitslevel". Einen Startpunkt kann die Struktur der Produktionsnetzwerke bilden:

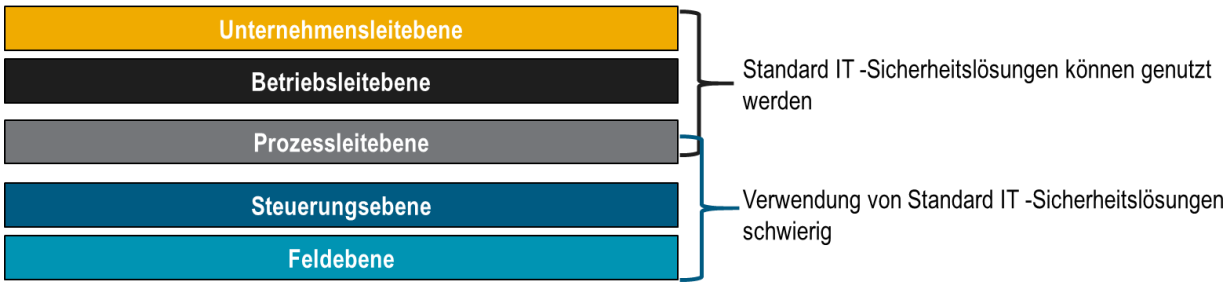


Abbildung 3: Grundprinzip der Netzwerksagregierung

Die Kritikalität der Angriffe ist zumindest teilweise abhängig von der betroffenen Ebene. Das begründet sich sowohl aus dem Einfluss, den ein erfolgreicher Angriff auf den laufenden Betrieb und das Unternehmensergebnis hat und aus den verfügbaren IT-Sicherheitsmechanismen, die auf der entsprechenden Ebene eingesetzt werden können.

Als generelle Leitlinie kann gelten, dass die Systeme, die eher aus dem Bereich der Informationstechnologie kommen, besser zu schützen sind, weil für diese entsprechend aktuelle Softwareversionen verfügbar sind. Das bedeutet, dass die Feld- und Steuerungsebene strikter abgeschirmt werden sollten als z. B. die Betriebs- und Unternehmensleitebene.

Die unterschiedlichen Ebenen eines Produktionssystems sollten z. B. durch „demilitarized zones“ (DMZ) voneinander getrennt werden. Dies erschwert potenziellen Angreifern den Zugriff auf Geräte, z. B. in der Feldebene. DMZs können mit Hilfe von Firewalls eingerichtet werden und helfen den Netzwerkverkehr einzuschränken. Die eingesetzten Firewalls müssen drei oder mehr Schnittstellen bereitstellen, eine zum Office-Netzwerk, eine zum Produktionsnetzwerk und die dritte für gemeinsam genutzte bzw. nicht vertrauenswürdige Geräte. Mit einem wohldurchdachten rule-set (Regelwerk) kann der Netzwerkverkehr zwischen den unterschiedlichen Netzwerkzonen sehr gut kontrolliert und eine klare Trennung der Netzwerke realisiert werden. Hierbei ist allerdings Vorsicht geboten, DMZs sind kein Allheilmittel. Falls ein Angreifer ein Gerät in der DMZ kompromittieren kann, wird der folgenden Angriff evtl. erleichtert, da diesem Gerät ein höheres Vertrauen entgegengebracht wird, das der Angreifer entsprechend ausnutzen kann.

Neben DMZs können VLANs eingerichtet werden, die helfen, das Netzwerk in logisch separierte Teilnetze aufzuteilen. So kann beispielsweise auch auf der Feldebene eine weitere Unterteilung des Netzwerkes umgesetzt werden. Eine Feldebene beinhaltet hierbei Systeme, die zur Überwachung und Steuerung unter anderem in Umspannwerken, Trafostationen oder Pumpstationen installiert sind, sich also im „Feld“ befinden. Auf diese Weise kann der Effekt von erfolgreichen Angriffen weiter begrenzt werden. Hierbei muss beachtet werden, dass keine physikalische, sondern nur eine logische Trennung in den Switches erfolgt. Wichtig ist, dass bei der Konfiguration der Switches keine Standardeinstellungen verwendet werden, die Ports als „static“ definiert und insbesondere „trunk“ Ports deaktiviert werden. Mit diesen Maßnahmen können Angriffe wie „switch-spoofing“, vermieden werden.

Zusätzlich können Regeln definiert werden, die festlegen, von welchem Sicherheitslevel aus eine Kommunikation initiiert werden darf. So kann z. B. festgelegt werden, dass Kommunikation mit der Feldebene immer nur von der Feldebene selbst initiiert werden kann. Das verhindert, dass Angreifer von sich aus Nachrichten in die Feldebene einbringen können.

Informationssicherheit als Bestandteil der Lieferantenbeziehung

Die Informationssicherheit ist ein komplexes Thema und mit den Forderungen eines ISMS nach Einbringung dieser in die Beziehung zu Lieferanten vergleichsweise neu im Beschaffungsprozess. Hier treffen u. U. Experten aus unterschiedlichen Gebieten aufeinander: Automatisierungsexperten sowie Informations- und IT-Sicherheitsspezialisten zusammen mit Einkäufern. Das kann leicht dazu führen, dass Missverständnisse entstehen und im Rahmen der Beschaffung die Lieferantenbeziehung und das zu beschaffende Produkt nicht primär auf Informationssicherheitsbedürfnisse hin ausgewählt werden. Trotzdem, oder gerade deswegen, wird der Lieferantenbeziehung im Annex A.15 der ISO 27001 eine bedeutsame Rolle zugeschrieben.

Risiken im Zusammenhang mit dem Zugriff von Lieferanten auf Informationen müssen demnach dokumentiert und geregelt werden. Doch auch die Informationssicherheit bei den beschafften Leistungen und Produkten sollte als Thema so frühzeitig wie möglich im Beschaffungsprozess adressiert werden. Hierbei ist wichtig, dass zunächst die Anforderungen an die Informationssicherheit erhoben werden, sodass diese auch in den Anforderungskatalog integriert werden können. Selbst wenn innerhalb eines Unternehmens die IT-Sicherheitsexperten und die Automatisierungsexperten eine gemeinsame Vorstellung der gewünschten Eigenschaften neuer (Teil-)Systeme haben, bleibt das Problem der Kommunikation mit potenziellen Lieferanten. Hier können weiterhin Missverständnisse entstehen, da deutlich weniger Zeit für die Entwicklung eines gemeinsamen Verständnisses der Begrifflichkeiten und damit der Anforderungen zur Verfügung steht als innerhalb eines Unternehmens.

Für den Bereich der Informationssicherheit in Produktionsanlagen gibt es mindestens zwei Ansätze zur Definition eines gemeinsamen Vokabulars sowie der zugrundeliegenden Technologien: die Cyber Security Procurement Language for Control Systems, 2009, veröffentlicht vom Department of Homeland Security, und die Cybersecurity Procurement Language for Energy Delivery Systems, 2014, veröffentlicht von der Energy Sector Control Systems Working Group (ESCSWG). Beide Dokumente erläutern IT-Sicherheits-Aspekte sowie geeignete Formulierungen dieser im Beschaffungsprozess. Das Dokument des Department of Homeland Security ist deutlich umfangreicher und erläutert auch Fragen der Abnahme der Systeme im Sinne von Tests. Das Dokument der ESCSWG bietet einen leichteren Einstieg und ermöglicht durch Formulierungsbeispiele eine schnelle Anwendung. Ähnliche Dokumente für den deutschsprachigen Raum wären erforderlich.

Prof. Dr. Peter Langendörfer

Team Leader System Design / Sensornets & Middleware Platform an der IHP – Leibniz-Institut für innovative Mikroelektronik

Zur Person:

Prof. Dr. Peter Langendörfer absolvierte sein Diplom und seine Promotion im Bereich der Informatik. Am IHP - Leibniz-Institut für innovative Mikroelektronik leitet er die Gruppe "Sensornetzwerke und mobile Middleware". Seit dem Jahr 2012 ist er Inhaber der Professur für Sicherheit in pervasiven Systemen an der Brandenburgischen Technischen Universität Cottbus. Im Laufe seiner wissenschaftlichen Entwicklung publizierte Prof. Langendörfer mehr als 140 referierte Artikel, brachte 10 Patente im Bereich der Sicherheit/Privacy auf den Weg und arbeitete als Gasteditor für eine Vielzahl anerkannter Journals, wie z. B. Wireless Communications and Mobile Computing, publiziert von Wiley. Hauptgegenstand der Forschung ist die Sicherheit in drahtlosen Sensornetzwerken und Cyber-Physical-Systems.

4 Erkenntnisse aus der Sicherheitsbefragung

4.1 Methodik

Das methodische Vorgehen in dieser Studie beruht auf dem Ansatz der Messung der Dienstleistungsqualität. Mit der Applikation eines ISMS ist die Erbringung einer Dienstleistung durch das ISMS gegenüber dem Unternehmen verknüpft. Diese Dienstleistung beschreibt die Aufrechterhaltung und den Schutz von Informationen in Bezug auf Integrität, Vertraulichkeit und Verfügbarkeit in Verbindung mit dem Risiko-Management. Daher wurde die SERVIMPERF-Methode (ursprünglich Matilla und James 1977) herangezogen und in ihrer Umsetzung an das Anwendungsfeld literaturbasiert angepasst, welche wissenschaftliche und praxisorientierte Beiträge zum Thema ISMS untersuchte und Beiträge zu anderen Management-Systemen berücksichtigte.

Autor und Jahr	Problemstellung	Ergebnis
Schlienger (2007)	Systematische Vorgehensweise zur Sensibilisierung der Mitarbeiter bezüglich der Informationssicherheit	Informationssicherheitskultur ist relevant; Mitarbeiter sollten bei Fragen zur Informationssicherheit integriert werden
Rumpel (2011)	Erfahrungen zur Betreibung eines ISMS aus der Praxis	Manager sollten sich persönlich um Datensicherheit und Datenschutz kümmern; ausreichendes Budget und Ressourcen notwendig; regelmäßige Überwachung des Zustands und des Fortschritts des ISMS
Jendrian (2014)	Darstellung der wesentlichen Änderungen des Standards ISO/IEC 27001:2013 gegenüber der letzten Version	Angleichung an andere ISO-Managementsysteme; bessere Gliederung; Anpassung an aktuelle Erfordernisse der Informationssicherheit
Dürig, Fischer (2018)	Zusammenfassende Darstellung der Inhalte und Zusammenhänge des Regulierungsrahmens im Bereich der Informationssicherheit für KRITIS	Pflicht für Betreiber von KRITIS Sicherheitsmaßnahmen umzusetzen; zweijährige Umsetzungsfrist endet für KRITIS am 02.05.2018
Autor und Jahr	**Adaptierte Fragestellung aus der Quelle**	**Umsetzung in vorliegender Studie**
Thomson und Solms (1998)	Es wird sichergestellt, dass sich die Mitarbeiter immer ausloggen, wenn sie ihren Arbeitsplatz verlassen.	Bildung Konstrukt Auswirkungen des ISMS
Stanton et al. (2005)	Die Passwort-Richtlinie wird eingehalten.	Bildung Konstrukt Auswirkungen des ISMS
Brodin (2015)	Alle persönlichen mobilen Geräte sind im Unternehmen registriert.	Bildung Konstrukt Auswirkungen des ISMS
Psomas und Antony (2015)	Die Commitment des Managements führt zur Annahme und Akzeptanz des ISMS bei Mitarbeitern.	Bildung Konstrukt Kompatibilität
Barki und Hartwick (1994)	Wurden Sie stetig über den Fortschritt und/ oder über Probleme während des Zertifizierungsaudits informiert?	Bildung Konstrukt Auditor

Tabelle 2: Auszug zur literaturbasierten Entwicklung der Fragestellungen und Konstrukte

Die literaturbasierten Fragen und Konstrukte modifizierten die Basis der ersten Studie und wurden um Praxiserfahrungen fortführend ergänzt. Die Vorgehensweise der Implementierung eines ISMS wurde in einem Service Blueprint dargestellt (Pastowski 2004). Basierend auf diesem Ansatz sind Fragegruppen aggregiert und in die Abfrage der Wichtigkeit mittels MaxDiff-Ansatz (Chrzan und Golovashkina 2006) eingebunden worden. Es bestätigte sich der Konsens, dass zwischen dem Umgang mit Informationssicherheitsrisiken, der Verbesserung der Unternehmensprozesse sowie der Kompatibilität eine Vergleichbarkeit hinsichtlich der Beurteilung der Wichtigkeit nicht gegeben ist. Im Resultat ergibt sich eine 6-Felder-Matrix zur Darstellung der Performance aller Items und zur Wichtigkeit dieser in Gruppenbezug.

In der Betrachtung der Ergebnisse wurde neben dem speziellen Augenmerk auf den Bereich öffentlicher Personennahverkehr (ÖPNV) auch zwischen Unternehmen mit bereits vor dem ISMS hohen Stellenwert an Informationssicherheit sowie den anderen Unternehmen. Dies ist dem Ansatz des Lead Users (vgl. Sänn 2017) geschuldet. Lead User stellen führende Nutzer dar und bindet die Erwartung, dass Unternehmen, welche heute als „normale Nutzer“ einzustufen sind, im Umgang mit dem Thema ISMS mit den „führenden Nutzern“ gleichziehen und die Aspekte in ähnlicher Art und Weise behandeln werden.

4.2 Zielgruppe der Befragung

Der Fragebogen startete am 30. Mai 2018. Kontaktiert wurden telefonisch CISOs bzw. ISO/ISBs von 230 Energieversorgungsunternehmen. Nach dem telefonischen Gespräch wurde der nicht-personalisierte Link zur Umfrage per E-Mail an die ermittelten Ansprechpartner versandt. Da Einige schon beim Telefonat die Teilnahme an der Umfrage verneinten, wurden 137 Probanden angeschrieben. Am 29. Juni 2018 wurde die Umfrage geschlossen. Insgesamt nahmen 71 Probanden an der Umfrage teil, wovon insgesamt 42 Probanden den Fragebogen vollständig ausfüllten. Dies entspricht nach Bereinigung der Fragebögen einer Rücklaufquote von 18 %.

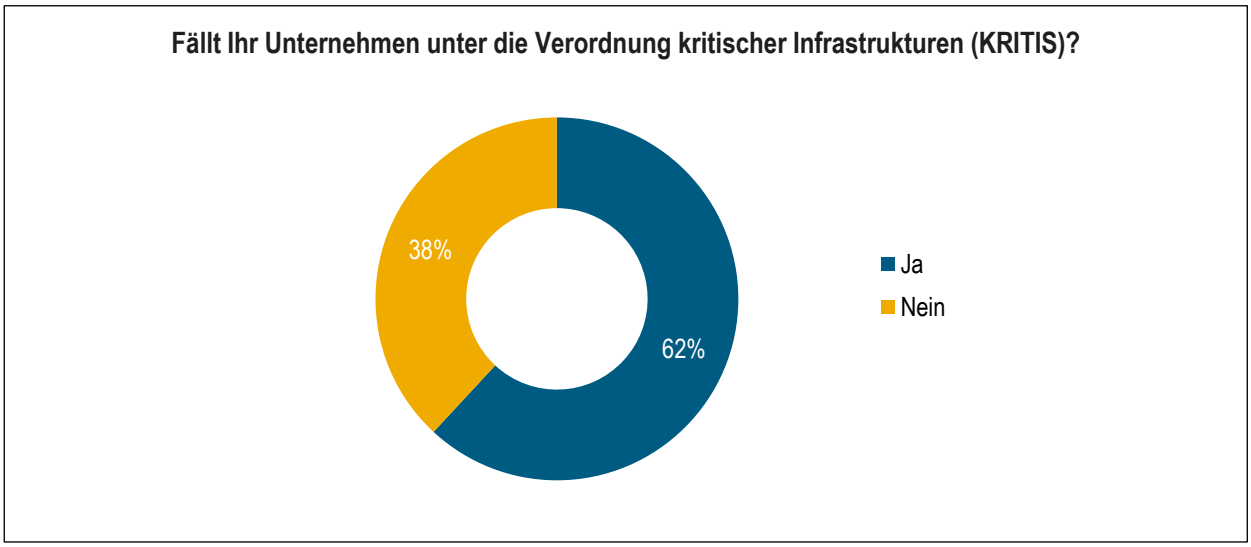


Abbildung 4: Zugehörigkeit als KRITIS

Mehr als die Hälfte der teilnehmenden Energieversorgungsunternehmen zählen unter die Verordnung Kritischer Infrastrukturen (KRITIS). Nur 38 % geben an, nicht als KRITIS eingestuft zu sein. Die Zuordnung ergibt sich aus der Selbstbewertung der Probanden hinsichtlich der Verordnung zur Bestimmung Kritischer Infrastrukturen nach dem BSI-Gesetz (BSI-Kritisverordnung - BSI-KritisV) in dessen Anhang 1. Die entsprechenden Schwellenwerte als Netto-Nennleistung in Megawatt sind zum Auszug in nachfolgender Tabelle für die Stromversorgung angegeben:

Bereich Stromerzeugung		
Erzeugungsanlage	Installierte Netto-Nennleistung (elektrisch) in MW	420
Erzeugungsanlage mit Wärmeauskopplung (KWK)	Installierte Netto-Nennleistung (direkt mit Wärmeauskopplung verbundene elektrische Wirkleistung bei Wärmenennleistung ohne Kondensationsanteil) in MW	420
Dezentrale Energieerzeugungsanlage	Installierte Netto-Nennleistung (elektrisch) in MW	420
Speicheranlage	Installierte Netto-Nennleistung (elektrisch) in MW	420
Steuerung / Bündelung elektrischer Leistung	Installierte Netto-Nennleistung (elektrisch) in MW	420
Bereich Stromübertragung		
Übertragungsnetz	Durch Letztverbraucher und Weiterverteiler entnommene Jahresarbeit in GWh p.a.	3.700
Zentrale Anlage für den Stromhandel	Handelsvolumen an der Börse in TWh p.a.	200
Bereich Stromverteilung		
Verteilernetz	Durch Letztverbraucher und Weiterverteiler entnommene Jahresarbeit in GWh p.a.	3.700
Messstelle	Leistung der angeschlossenen Verbrauchsstelle beziehungsweise Einspeisung in MW	420

Tabelle 3: Schwellenwerte zur Zuordnung in der BSI-Kritisverordnung für den Sektor Energie

Quelle: Verordnung zur Bestimmung Kritischer Infrastrukturen nach dem BSI-Gesetz (BSI-Kritisverordnung - BSI-KritisV)

Erkenntnisse aus der Sicherheitsbefragung

Schlüsselt man die Unternehmen nach Branchenzugehörigkeit auf (siehe Abbildung 5), ist ein Großteil der Unternehmen in den Branchen Strom (95 %), Gas (88 %) und / oder Wasser (76 %) angesiedelt. Mehrfachnennungen waren hier möglich. Die wenigsten Unternehmen befinden sich auch im Bereich des Nahverkehrs (31 %) und der Entsorgung (14 %). Eine Mehrfachauswahl war möglich und unterstreicht die Relevanz des Samples als Einrichtungen mit kritischen Dienstleistungen im Sinne des BSI. Es ist anzunehmen, dass bei den befragten Unternehmen auch einzelne Bereiche eines Konzernverbundes vorhanden sind.

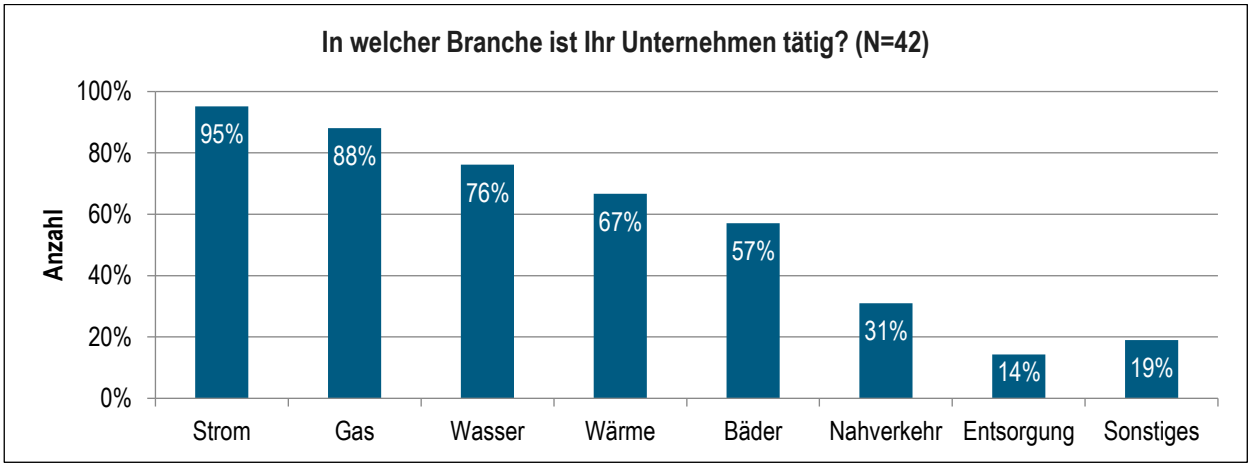


Abbildung 5: Branche des Unternehmens

(Mehrfachantworten möglich)

Von den befragten Unternehmen ist der Großteil der Unternehmen in der Verteilung von Energie tätig (88 %), gefolgt vom Vertrieb von Energie (79 %). Unternehmen mit Schwerpunkt „Handel von Energie“ (14 %) sowie „Erzeugung und Gewinnung von Energie“ (41 %) ergänzen die funktionalen Bereiche. Unternehmen als Betreiber eines Übertragungsnetzes und Fernleitungsnetzes stellen lediglich 5 % der befragten Unternehmen dar.

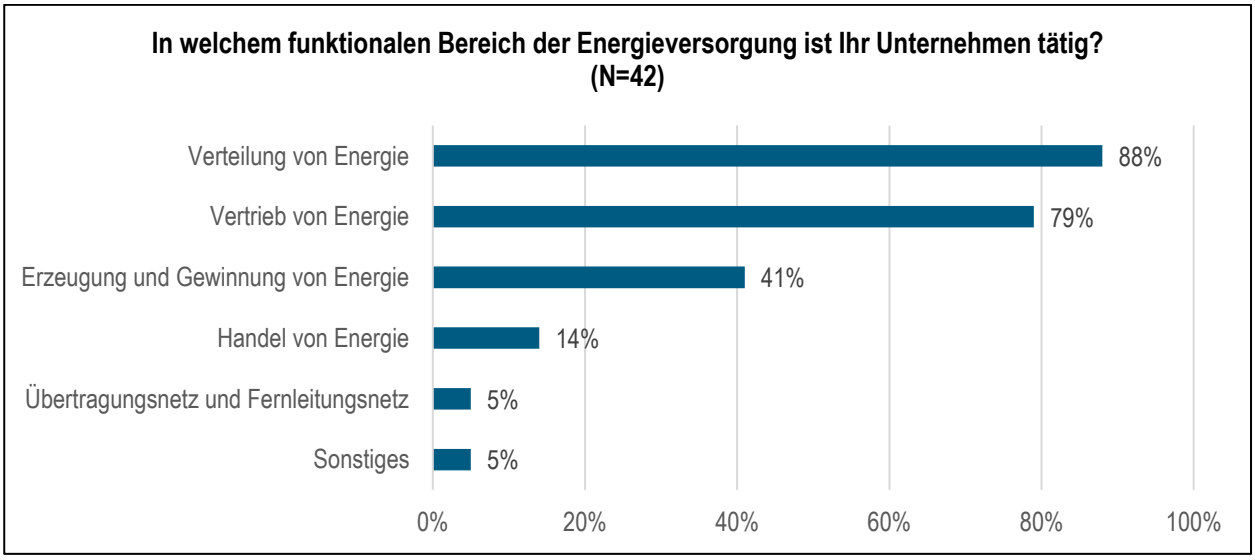


Abbildung 6: Funktionaler Bereich des Unternehmens

(Mehrfachantworten möglich)

Die Kennzahlen-basierte Betrachtung der befragten Unternehmen zeigt, dass 66 % der Unternehmen über 50 bis 250 Mitarbeiter verfügen. Weitere 27 % der befragten Unternehmen geben an, dass sie mehr als 250 Mitarbeiter beschäftigen. Auch die Darstellung des Jahresumsatzes zeigt, dass 21 % mehr als 50 Mio. EUR erwirtschaften. Mit 41 % geben vergleichsweise viele Unternehmen hierzu keine Antwort. Weiterhin geben 52 % keine Angabe zu der Bilanzsumme. Dies scheint aus der Analyse der vorliegenden Daten Gründe in der Anonymität zu haben.

Ein ähnlicher Schluss lässt sich bei der Betrachtung der Zählpunkte zu, welche von 29 % der befragten Unternehmen nicht beziffert wurde. Auffällig ist, dass 63 % der Unternehmen angeben, unter 100.000 Zählpunkte zu bedienen.

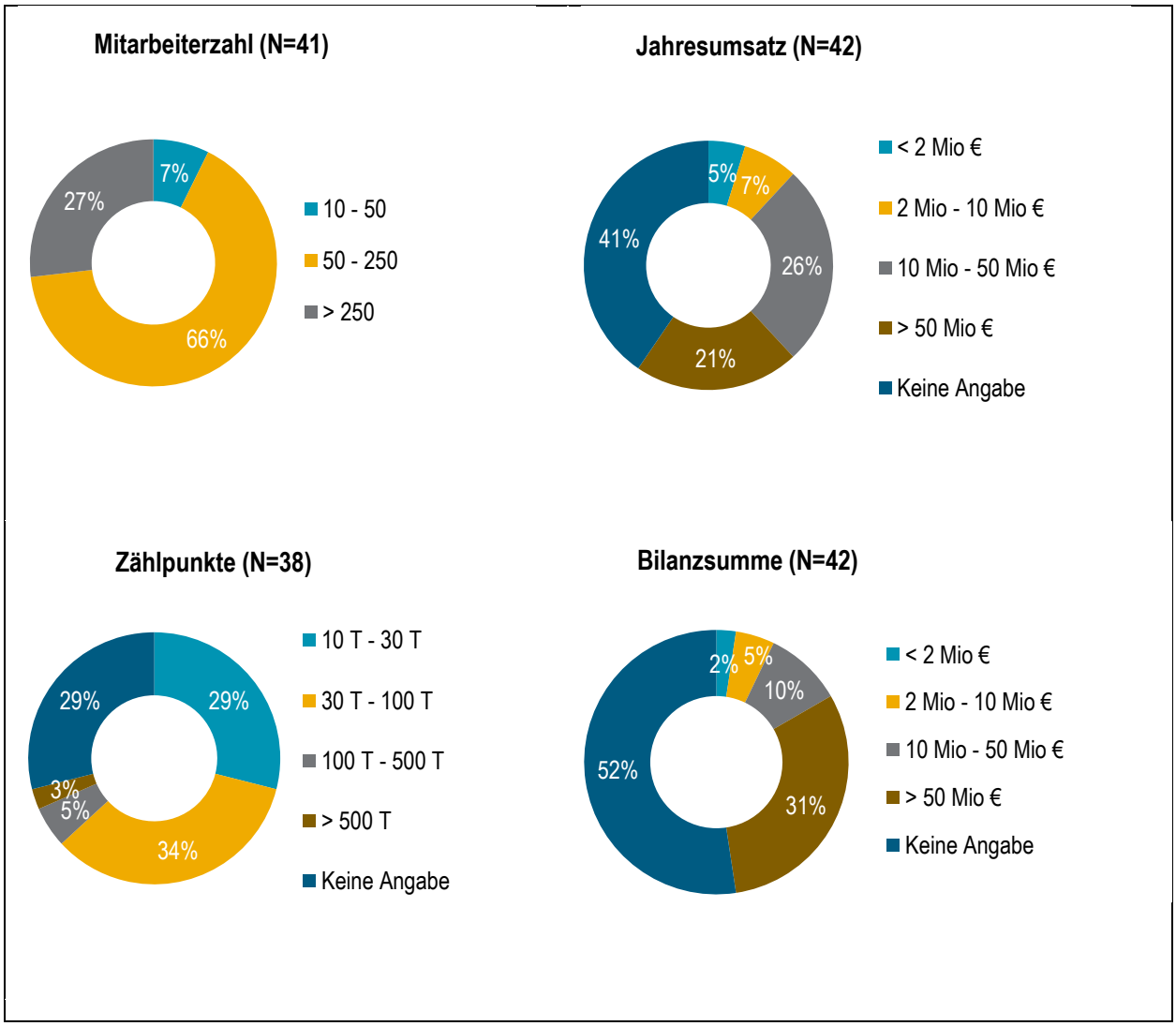


Abbildung 7: Unternehmensdaten des Samples

Von den insgesamt 42 Studienteilnehmern sind 17 % als Chief Information Security Officer (CISO) im Unternehmen beschäftigt. CISOs leiten in der Regel die Koordination der Information Security Officer (ISO/ISB) und das Projekt-Management für bspw. ISMS-Projekte im Konzernverbund. Sie sind hierarchisch in der Regel direkt der Geschäftsführung unterstellt bzw. zugeordnet, besitzen damit Weisungsbefugnis sowie Verantwortlichkeit.

Mehr als die Hälfte (61 %) der Befragten ist als Information Security Officer tätig (siehe Abbildung 8). Sie setzen damit in der Regel das Projekt-Management für einzelne Projekte um und sind operativer als der CISO in die IT-Landschaft eingebunden. Typische Aufgaben der ISO/ISBs umfassen die Implementierung des ISMS nach ISO 27001.

Nach der Projektphase zur Implementierung des ISMS übernehmen sowohl CISO wie auch ISO/ISB die Betreuung des Regelbetriebs des ISMS. Nach der Erstellung der Dokumentation und dem Aufbau der Prozesse verschiebt sich der Fokus des Tätigkeitsfeldes auf den Betrieb und die kontinuierliche Verbesserung des ISMS.

In Summe 12 % der befragten Personen gaben an, dass sie im Unternehmen weder CISO noch ISO/ISB sind, jedoch eine andere Rolle zum Thema Informationssicherheit bekleiden. Diese können bspw. der hauseigene Ansprechpartner für das BSI, Mitglieder im ISMS-Team, der IT-Sicherheits- und Datenschutzbeauftragte, IT-Leiter oder die Administration des eigenen Security Operations Centers sein.

Lediglich 10 % der Befragten verfügen über keine spezifische Rolle im Hinblick auf Informationssicherheit in ihrem jeweiligen Unternehmen. Damit sind sie nicht zwangsweise mit fachfremden Personen gleichzusetzen und sind u. a.

in der Praxis als Personalunion wiederauffindbar. Diese Rollen sind bspw. in ihrer Hauptaufgabe bspw. für die IT-Planung verantwortlich und decken in ihrer Funktion einzelne Projekte der Informationssicherheit mit ab.

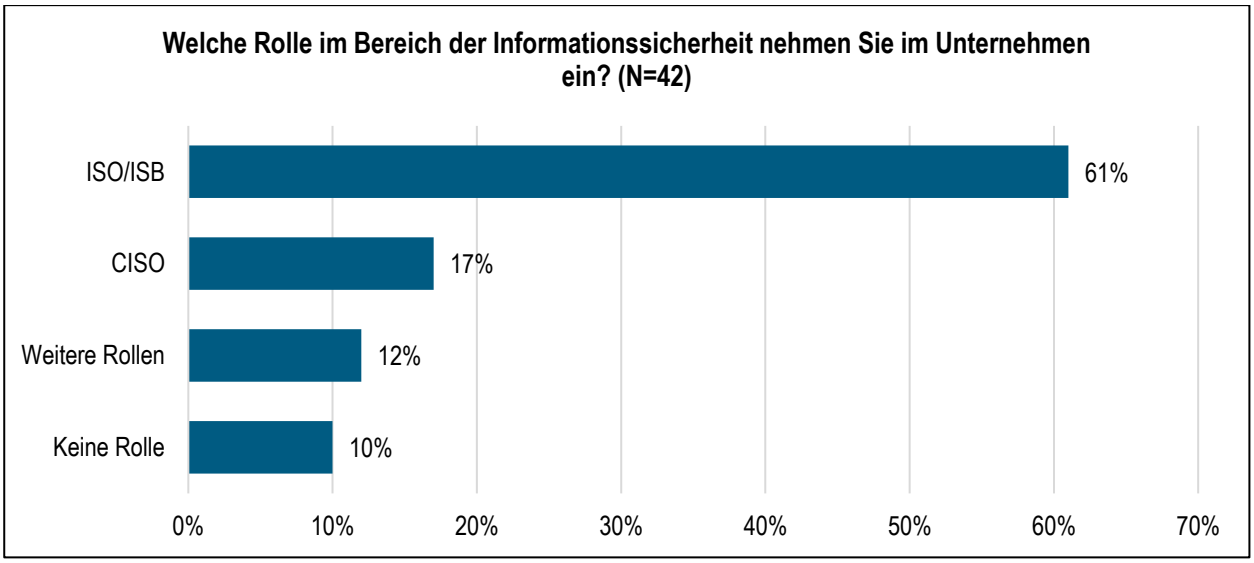


Abbildung 8: Rolle der Befragten in der Informationssicherheit

Umso interessanter gestalten sich die Ergebnisse zum Status eines ISMS nach ISO 27001 in den Unternehmen. Im Vergleich zur Vorläuferstudie aus dem Jahr 2016 ist der Anteil der Energieversorgungsunternehmen, die eine ISMS eingeführt haben, deutlich angestiegen. Hatten 2016 nur 38 % der befragten Energieversorger ein ISMS eingeführt, sind es in diesem Jahr bereits 88 %.

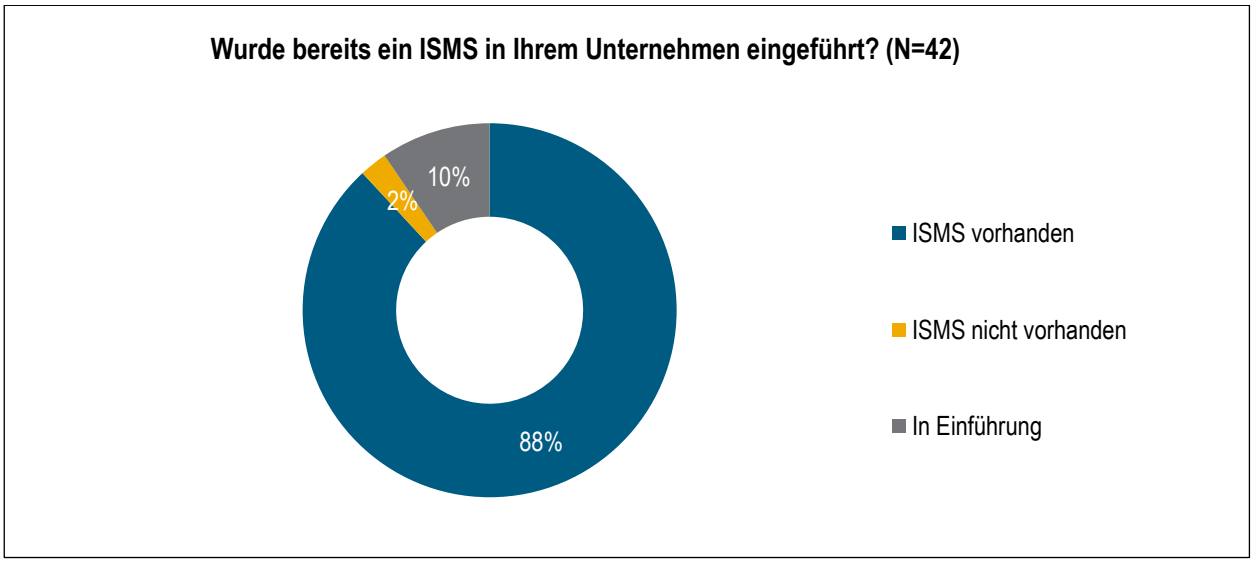


Abbildung 9: Wurde bereits ein ISMS in Ihrem Unternehmen eingeführt?

Bei 10 % der Befragten ist das ISMS in der Phase der Einführung. Das Ergebnis umfasst auch Unternehmen, welche nicht als KRITIS eingestuft sind. Dies zeigt, dass Unternehmen, welche keinen gesetzlichen Zwang zur Einführung eines ISMS aus der BSI-Kritisverordnung besitzen, das Konzept für sich anwenden.

Nur 2 % der befragten Unternehmen gaben an, dass ein ISMS nicht vorhanden ist und noch nicht mit der Einführung begonnen wurde. Nach Analyse der qualitativen Angaben dieser Unternehmen werden sie weiterhin in der Auswertung berücksichtigt, da das Thema im Unternehmen vorangetrieben wird und punktuelle Regelung, die mit dem Anhang A der ISO 27001 (Referenzmaßnahmen und –ziele) vergleichbar sind, bereits umgesetzt werden.

4.3 Motivation zum ISMS

Der Fragebogen befasste sich insbesondere mit den Gründen zur Einführung eines ISMS. Mit den vorliegenden Ergebnissen lassen sich zwei Hauptaspekte zur Einführung eines ISMS ausmachen.

Als vordergründiger Aspekt drängte die gesetzliche Verpflichtung 95 % der Unternehmen zur Einführung eines ISMS. Der hohe Prozentsatz der gesetzlichen Verpflichtungen lässt sich damit erklären, dass seit Mitte 2015 das IT-Sicherheitsgesetz sowie der IT-Sicherheitskatalog für Energieversorger Pflicht ist. Der Grund der gesetzlichen Verpflichtung ist umso interessanter, da bspw. keine expliziten Strafen in Summe vorgegeben sind. Dies ist ein deutlicher Unterschied zur bspw. DS-GVO. Darauf fußt der Umstand, dass die gesetzliche Verpflichtung nicht bei 100 % der befragten Unternehmen als Grund genannt wird. In der Praxis spekulieren Unternehmen durchaus mit dieser gesetzlichen Verpflichtung und warten die ersten Strafen zur Nichteinführung sowie die ersten Reaktionen der BNetzA zu dem Thema ab. Im konkreten Sample scheint dies bei zwei Unternehmen der Fall zu sein. Im Gegensatz dazu ist anzumerken, dass mit dem Ergebnis von 95 % bei dem KRITIS-Anteil von 62 % in diesem Sample auch die Signalwirkung der gesetzlichen Verpflichtung für andere Bereiche der Energieversorgung ausgedrückt wird. Insgesamt 87,5 % der Unternehmen, welche nach eigenen Angaben nicht unter die Kritisverordnung fallen, geben an, ein ISMS auf Basis der gesetzlichen Forderung eingeführt zu haben. Dies unterstreicht die Signalwirkung.

Als zweiter Hauptaspekt wird die Steigerung der Informationssicherheit (52 %) genannt. Andere Gründe, wie beispielsweise einen Wettbewerbsvorteil zu erzielen oder die explizite Forderung der Unternehmensleitung im Rahmen der Digitalisierung sowie der Stakeholder, spielen eine untergeordnete Rolle. Bei 5 % der Unternehmen wurde das Bewusstsein zur Relevanz des Themas Informationssicherheit durch die DS-GVO vorangetrieben.

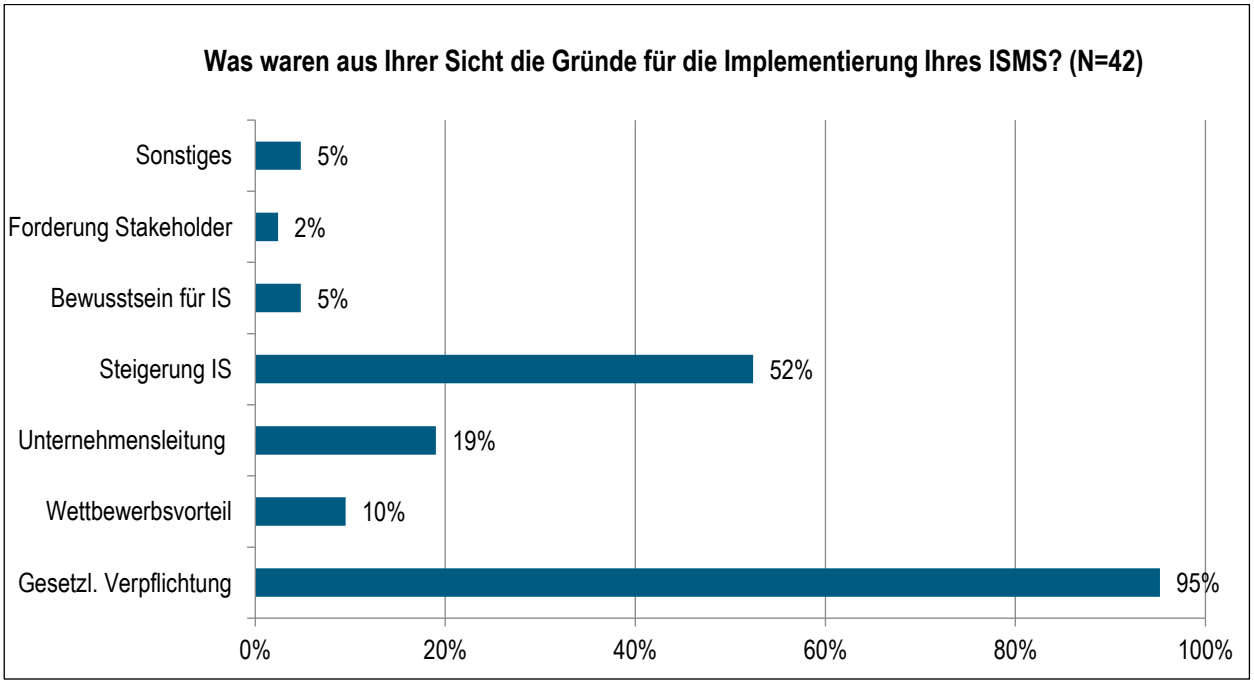


Abbildung 10: Gründe für die Implementierung eines ISMS

(Mehrfachantworten möglich)

Um diese Ergebnisse in dem richtigen Kontext zu interpretieren, ist ein Blick auf den vorherigen Stellenwert der Informationssicherheit im Unternehmen lohnenswert. Wie aus nachfolgender Abbildung ersichtlich, hatte das Thema Informationssicherheit bereits vor der Einführung des ISMS 62 % der befragten Unternehmen einen hohen Stellenwert. Insgesamt gaben 53,8 % der Unternehmen mit einem bereits hohen Ausgangs-Level an Informationssicherheit an, dass das ISMS zur weiteren Steigerung eingeführt wurde. Jedes dritte Unternehmen (29 %) gab an, dass die

Informationssicherheit vor der Implementierung ein beiläufiges Thema gewesen sei. Lediglich bei 9 % der Unternehmen hatte die Informationssicherheit keinen Stellenwert.

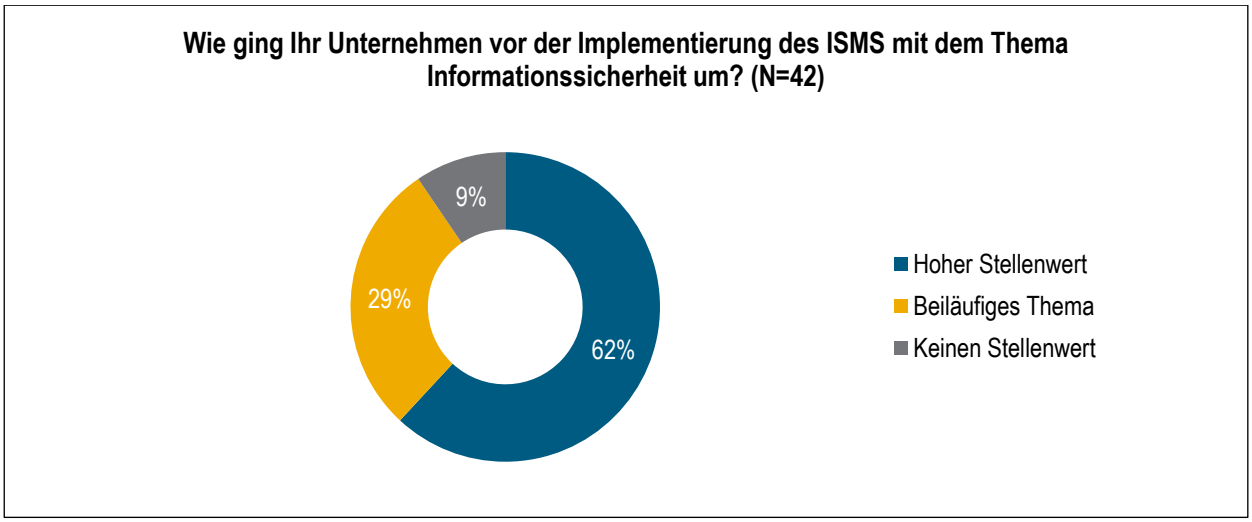


Abbildung 11: Stellenwert von Informationssicherheit vor der Implementierung des ISMS

Die Gründe für die Einführung eines ISMS unterscheiden sich zum Teil bei den befragten Unternehmen je nach Stellenwert. Bei Unternehmen, in denen die Informationssicherheit vor der Einführung beiläufig behandelt wurde, spielten das Bewusstsein für Informationssicherheit und die Forderung von Stakeholdern keine Rolle bei der Einführung des ISMS. Im Gegensatz dazu stellte der Wettbewerbsvorteil einen verhältnismäßig stärkeren Grund zur Einführung dar.

Die dahinterstehenden Treiber zur Einführung des ISMS stellen die Unternehmensleitung, Mitarbeiter mit Fachwissen sowie die Beauftragten für Informationssicherheit dar. Es zeigt sich, dass in 62 % der Fälle die Unternehmensleitung die Implementierung stark befürwortete. In 83 % der Fälle trieb der Beauftragte für Informationssicherheit den Prozess voran. In weiteren 21 % der Fälle engagierte sich ein Mitarbeiter mit Fachwissen als Antreiber. Sonstige Treiber zur Einführung waren laut Aussagen der befragten Unternehmen die IT-Leitung durch den gesetzlichen Zwang sowie externe Berater. Mehrfachantworten waren hierbei möglich. In 12 % der Fälle wurde das Thema durch den Beauftragten für Informationssicherheit, der Unternehmensleitung sowie dem Mitarbeiter mit Fachwissen vorangetrieben. In leidglich 38 % der betrachteten Fälle wirkten die Unternehmensleitung und der Beauftragte für Informationssicherheit als Treiber zusammen. Auch bei dem Unternehmen, welches bisher mit der ISMS-Einführung nicht begonnen hat, treibt der Beauftragte für Informationssicherheit das Thema weiterhin voran.

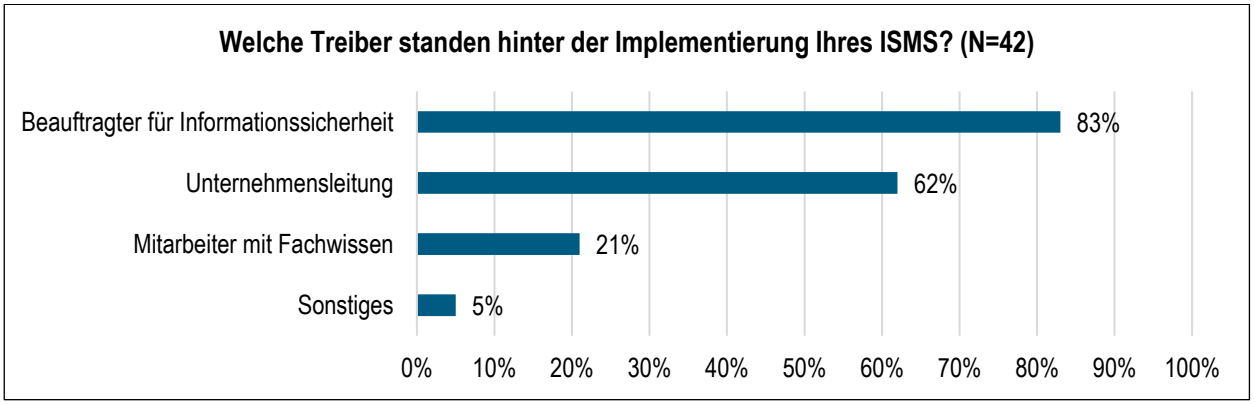


Abbildung 12: Welche Treiber standen hinter der Implementierung Ihres ISMS?

(Mehrfachantworten möglich)

Die Aufteilung der Unternehmen zeigt, dass in 61 % der Unternehmen mit einem bereits zuvor hohen Stellenwert an Informationssicherheit, die Unternehmensleitung der Treiber war. Noch stärker wirkte jedoch der Beauftragte für die Informationssicherheit, welcher in 84,6 % dieser Unternehmen als Treiber agierte.

4.4 Unternehmens-eigener Umgang mit dem ISMS

Insgesamt geben 85 % der befragten Unternehmen an, dass sich der Geltungsbereich auf die Leitstelle und Netzführung bezieht. Bei nur 20 % der Energieversorger deckt das ISMS das Gesamtunternehmen ab und bei weiteren 22 % die IT und das Rechenzentrum. Der Hauptfokus der Unternehmen liegt dabei also auf der Leitstelle und der Netzführung. Ein ISMS sollte sich über das komplette Unternehmen erstrecken und ebenfalls in die korrespondierenden Management-Systeme von assoziierten Unternehmen greifen. Da jedoch gesetzliche Vorgaben existieren, die festlegen, in welchen Geltungsbereichen ein ISMS eingeführt und zertifiziert werden muss, entsteht eine Fokussierung auf eben diese Bereiche. Weitere Bereiche, die ebenfalls von einer Einführung profitieren würden, werden vernachlässigt. Dies zeigt sich insbesondere im Unternehmensvergleich mit dem vorherigen Umgang zum Informationssicherheit. Von den Unternehmen mit einem hohen Stellenwert sagen 27 % aus, dass ihr ISMS das Gesamtunternehmen abdeckt. Weitere Bereiche zum Geltungsbereich stellt das Geoinformationssystem dar. Im Vergleich zu der Studie aus dem Jahr 2016, in der die Geltungsbereiche noch sehr viel breiter aufgestellt waren, fokussieren sich die Geltungsbereiche in dieser Erhebung sehr stark auf die Leitstelle und Netzführung. An dieser Stelle muss zwischen dem Geltungsbereich und dem Zertifizierungsbereich unterscheiden werden. Ein unternehmensweiter Geltungsbereich und ein Netz-bezogener Zertifizierungsbereich wurden genannt (weiterführend der auditierte Geltungsbereich im Kapitel 6.1)

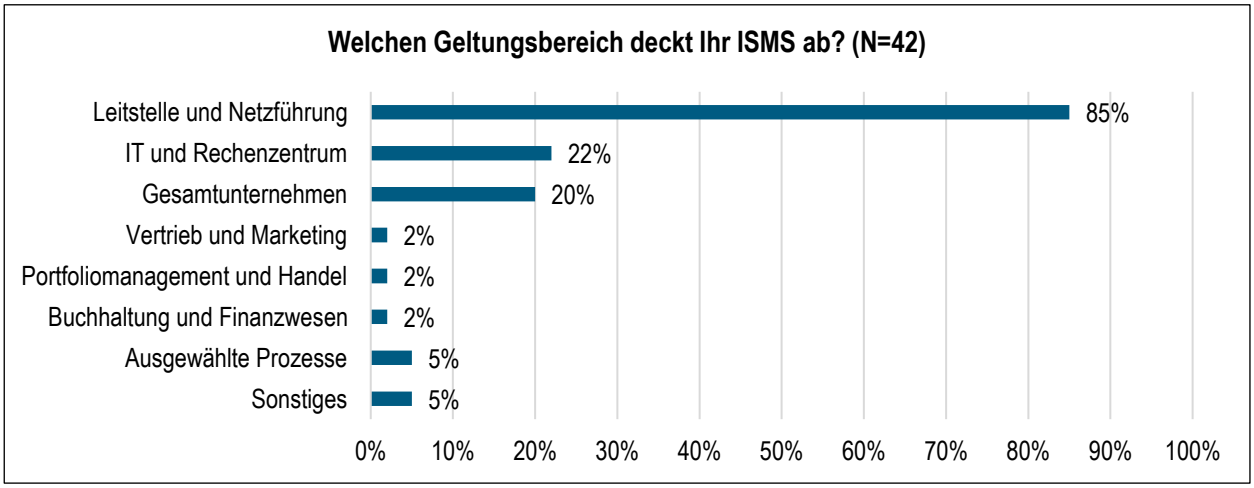


Abbildung 13: Geltungsbereich des ISMS

(Mehrfachantworten möglich)

Im individuellen Umgang mit dem ISMS und dessen Implementierung wurde die Kombination mit anderen Management-Systemen von 51 % der befragten Unternehmen berücksichtigt. Die Kombination mit anderen ISO-Normen und Standards[1] erscheint sinnvoll und insbesondere die Kombination mit einem Datenschutz-Management-System und dem technischen Sicherheits-Management zeigen einen inkludierenden Ansatz in der Behandlung der Informationssicherheit. Die Kombination mit einem Qualitäts-Management-System nach ISO 9001 zeigt, dass das Thema ISMS weiterhin kein reines IT-Thema ist, sondern ein Organisationsthema darstellt.

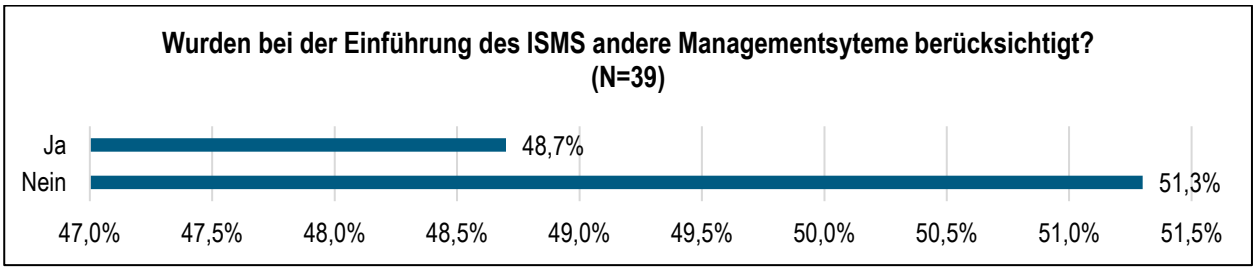


Abbildung 14: Berücksichtigung anderer Management-Systeme bei der Einführung des ISMS

[1] Genannt wurden ISO 9001 Qualitäts-Management-System, ISO 14001 Umwelt-Management-System, ISO 50001 Energie-Management, ISO 45001 Arbeitsschutz-Management, Datenschutz-Management und dem Technisches Sicherheits-Management und Business Continuity Management nach ISO 22301

Behält man die Aufteilung nach ISMS in der Kombination mit anderen Management-Systemen bei, so zeigt sich, dass diese Kombination allerdings keinen entscheidenden Einfluss auf den generierten Mehrwert des ISMS besitzt. So konnten zwar anhand einzelner Kommentare der Beitrag zur Senkung der Einführungskosten monetärer Art sowie die Senkung der Arbeitslast als Ansatzpunkte identifiziert werden, doch wurde insgesamt der hohe Aufwand für kleine Verteilnetzbetreiber (im konkreten Fall mit sechs Mitarbeitern) als unwirtschaftlich im Vergleich zum Nutzen kritisiert. Dieser Aspekt unterstreicht die organisationale Relevanz und Auswirkung des ISMS, die mehr als nur die IT prägt und damit punktuelle Redundanzen mit anderen Management-Systemen aufweist.

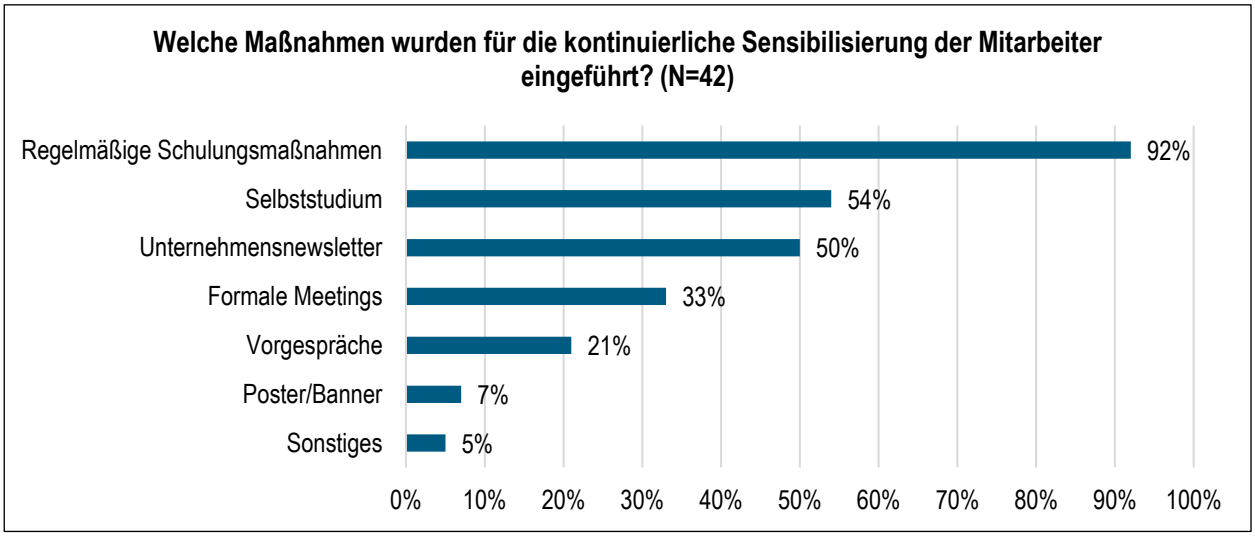


Abbildung 15: Maßnahmen für die kontinuierliche Sensibilisierung der Mitarbeiter

(Mehrfachantworten möglich)

Um die Mitarbeiter für ein ISMS und das Thema Informationssicherheit zu sensibilisieren, führten die Unternehmen verschiedene Maßnahmen durch. Die am häufigsten verwendeten Maßnahmen, waren mit 35 % die Durchführung regelmäßiger Schulungen und mit 21 % das Selbststudium der Mitarbeiter. Insgesamt 19 % wendeten den Unternehmensnewsletter an, um das Thema bei den Mitarbeiten präsent zu halten und 12 % führten formale Meetings durch. Maßnahmen wie Vorgespräche oder Poster / Banner fanden eher weniger Verwendung. Unter „Sonstiges“ wurden u. a. themenbezogene Bildschirmschoner und die Kommunikation im Intranet genannt.

Die Implementierung eines ISMS brachte in der Gesamtbetrachtung ca. 95 % der Unternehmen einen Mehrwert. Auffällig ist, dass 94,7 % der Unternehmen, welche das ISMS mit einem vorhandenen Management-System kombinierten, ebenso den Mehrwert bestätigten.

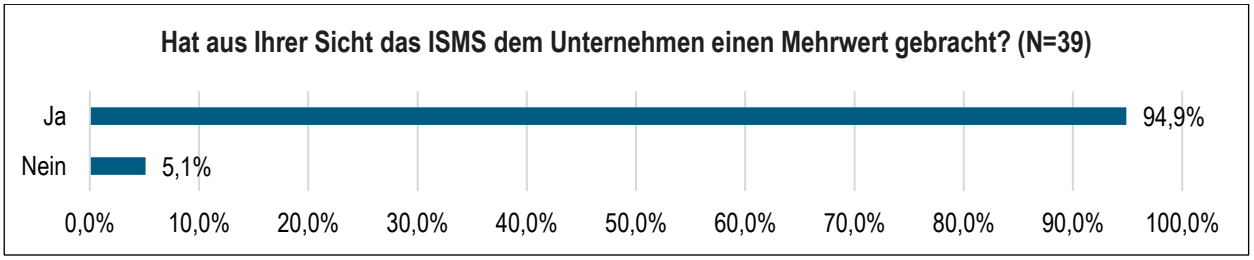


Abbildung 16: Hat aus Ihrer Sicht das ISMS dem Unternehmen einen Mehrwert gebracht?

Aus Sicht der Unternehmensleitung wurde vor allem das Sicherheitsniveau erhöht, dieses kontinuierlich verbessert sowie das Bewusstsein der Mitarbeiter in Bezug auf Informationssicherheit geschärft. Einzelne Statements fasst die nachfolgende Tabelle zusammen:

Mehrwert auf Ebene der Anlagen
Anlagenbewertung nach technischen und organisatorischen Maßnahmen (TOM/Controls), Umgang mit kritischen Daten, Verantwortungsbewusstsein wurde gestärkt.
Führte zur Neustrukturierung der Leitstelle
Mehrwert auf Ebene des Personals
Die Mitarbeiter wurden erneut und intensiver mit dem Thema konfrontiert. Schulungen wurden ausgebaut. Die Regelmäßigkeit bringt immer wieder eine "Erinnerung".
Dokumentation von Prozessen, Erhöhung des Mitarbeiterbewusstseins für Informationssicherheit.
Erhöhung der Informationssicherheit, insbesondere Schärfung des Bewusstseins der Mitarbeiter (MA).
Es wurden Handlungsweisen identifiziert, über die nicht mehr nachgedacht und die nicht in Frage gestellt wurden, die aber definitiv falsch und nicht mehr zu vertreten waren.
Primär die Sensibilisierung der Mitarbeiter.
Schaffung Bewusstsein für Informationssicherheit in allen Geschäftsbereichen und auf allen Ebenen.
Steigerung des Sicherheitsbewusstseins, weitere Implementierung auch in Bereichen, welche nicht im Scope liegen.
Verbessertes Sicherheitsbewusstsein der Mitarbeiter
Mehrwert auf Ebene der Prozesse
Dokumentation wurde erneuert.
Prozessdokumentation und Prozessoptimierung
Prozesse wurden vereinheitlicht.
Sensiblerer Umgang mit Zugangsrechten, Zutrittskontrollen, Datenweitergabe etc.
Stabile IT mit geordneten IT-Prozessen
Steigerung der Qualität im IT-Betrieb
Transparenz über Risiken durch den Einsatz von IT. Steuerung der Risiken durch das ISMS. Prozesse und Aufzeigen von Handlungsbedarf
Umsetzung gezielter Maßnahmen anstatt Ad-Hoc Maßnahmen
Allgemeine Statements zum Mehrwert
Da wir bereits seit 2006 zertifiziert sind, haben wir [einen] ausführlichen Überblick über alle von der IT-Sicherheit betroffenen Themen.
Das Sicherheitsniveau wurde insgesamt erhöht und wird kontinuierlich verbessert.
Optimierung der Prozesse. Steigerung der Sicherheit. Strukturierte Nutzung von Management Systemen.
Schwachstellen wurden aufgedeckt, Prozesse geschärft, Awareness erhöht.
Wettbewerbsvorteil, Datensicherheit
Workflow Risikobetrachtung - Ableitung von Maßnahmen - Verfolgung der Maßnahmen

Tabelle 4: Welcher Mehrwert wurde durch das ISMS im Unternehmen generiert?

Mit der außerordentlich deutlichen Meinung zum Mehrwert des ISMS stellt sich die Frage nach der Unternehmens-internen Unterstützung durch das Management. Wie zeigt sich in der Praxis der konkrete Beitrag der Unternehmensleitung und des Managements bei den Befragten?

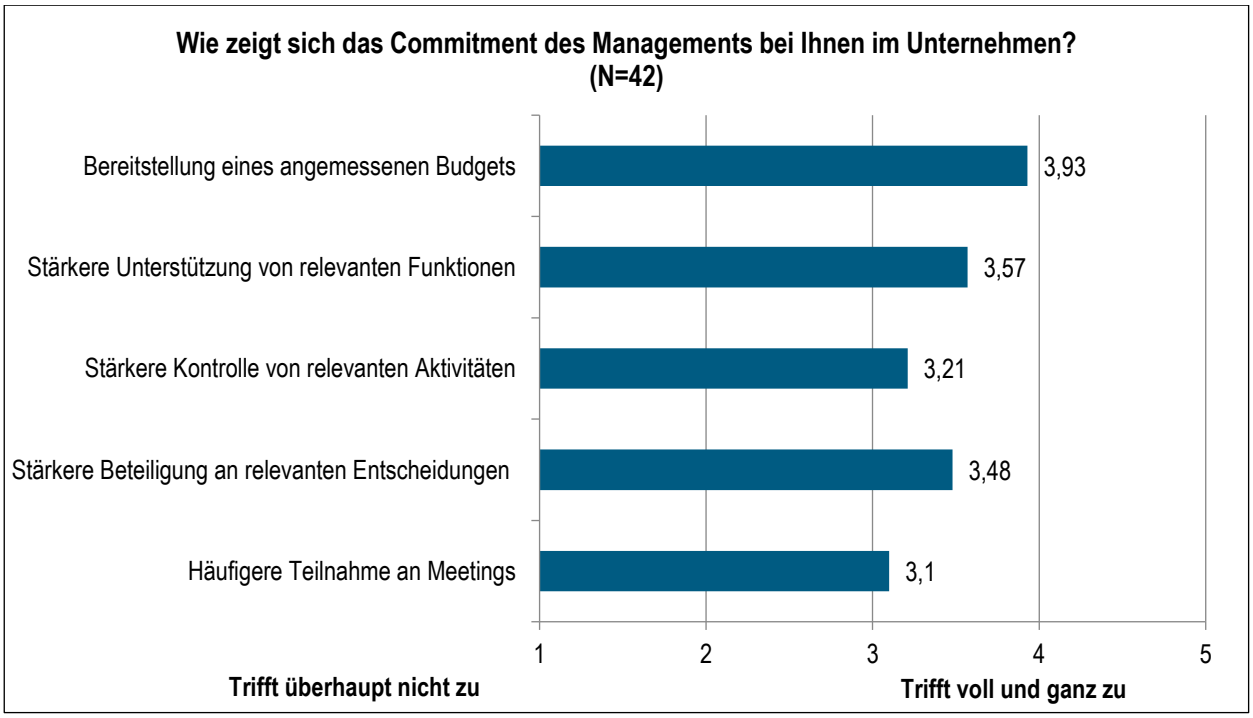


Abbildung 17: Commitment des Managements

Hinsichtlich des Commitment des Managements wurde vor allem ein angemessenes Budget bereitgestellt und die Unterstützung von relevanten Funktionen gewährleistet. Ebenso wurde eine stärkere Beteiligung des Managements an relevanten Entscheidungen festgestellt. Eine stärkere Kontrolle von relevanten Aktivitäten sowie eine häufigere Teilnahme an Meetings hat sich entwickelt, wenn auch nicht in einem so hohen Ausmaß, wie die anderen genannten Aspekte (siehe Abbildung 17).

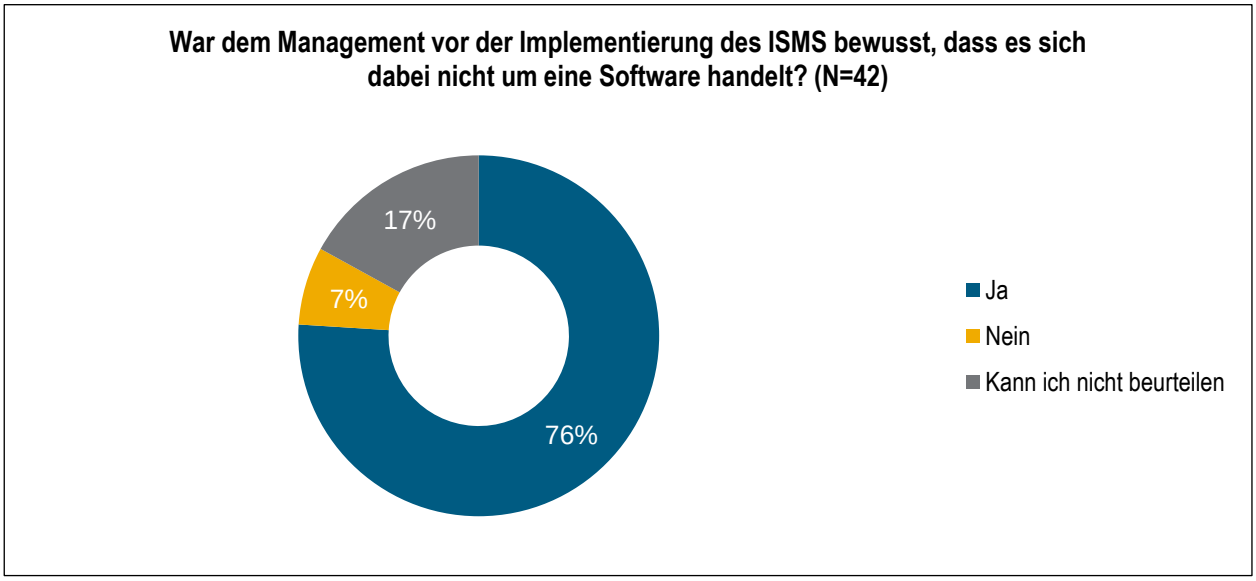


Abbildung 18: Kenntnisstand des Managements zu ISMS

Insgesamt 76 % der Studienteilnehmer gaben an, dass dem Management vor der Implementierung des ISMS bewusst gewesen sei, dass es sich dabei nicht um eine Software handle. Im Gegensatz dazu sei dies bei etwa 7 % der Befragten dem Management in ihrem Unternehmen nicht bewusst gewesen (siehe Abbildung 18).

4.5 Besondere Erfahrungen in der Implementierung

Die Implementierung eines ISMS beinhaltet besondere Herausforderungen für das damit betraute Projektteam. Die einzelnen Prozesse müssen hierzu erfasst, dokumentiert und ggf. an die Forderung der Norm angepasst werden. Dies bedingt die Aufnahme der Assets und die passende Risikoanalyse vor dem Hintergrund der Schutzziele Vertraulichkeit, Integrität und Verfügbarkeit von Informationen. Weitere Schutzziele können vom Unternehmen individuell hinzugefügt werden und müssen dann in der Implementierung des ISMS Berücksichtigung finden.

Die Vorläuferstudie im Jahr 2016 ermittelte insbesondere die Erwartungshaltung gegenüber des ISMS. Welcher Beitrag wird zur IT-Sicherheit im Unternehmen erwartet? Wie hoch ist der erwartete Beitrag des ISMS zur Optimierung der Prozesse? Welche Erwartungen besitzen die Befragten an das Management eines ISMS? Im Ergebnis (siehe Hänel und Wohlfart 2016) zeigte sich zu dem damaligen Zeitpunkt, dass, a) der Beitrag des ISMS zur IT-Sicherheit im Unternehmen tatsächlich wichtiger als erwartet war, b) der Beitrag zur Optimierung der Prozesse ebenso die Erwartungshaltung überstieg und c) damit der Beitrag zur Versorgungssicherheit der Endkunden für wichtiger als erwartet angesehen wurde. Im Vergleich dazu stellten sich der Themenbereich des Managements des ISMS in Form einer einfachen Bedienbarkeit, einer aufwandsarmen Pflege und einer leichten Integration in das Alltagsgeschäft für schwieriger als erwartet heraus.

Die nachfolgenden Darstellungen zeigen die Zufriedenheit mit der Erfüllung der Erwartungshaltung zum jetzigen Stand. Die berücksichtigten Gruppen an Wirkungsbereichen stellen folgende dar:

1) Umgang mit Informationssicherheitsrisiken bestehend aus 6 Teilbereichen zu 2 Gruppen (Identifikation von Sicherheitsvorfällen, Verbesserung Umgang mit Informationssicherheit, Aufdeckung von Sicherheitsrisiken - Mitarbeitersensibilisierung, Operative Handlungsempfehlungen, Entscheidungswege zur Lösung),
2) Verbesserung der Unternehmensprozesse bestehend aus 6 Teilbereichen zu 2 Gruppen (Versorgungssicherheit der Kunden, Verbesserung Büro-IT, Verbesserung KRITIS - Rechtskonformität, Qualitätssteigerung, Transparenz)
3) Kompatibilität (Einfache Integration im Unternehmensalltag, Annahme des ISMS bei Mitarbeitern, Anpassung der Prozesse

Es wird die Bewertung der Zufriedenheit zur Erfüllung der Erwartungen und die Wichtigkeit gegenübergestellt.

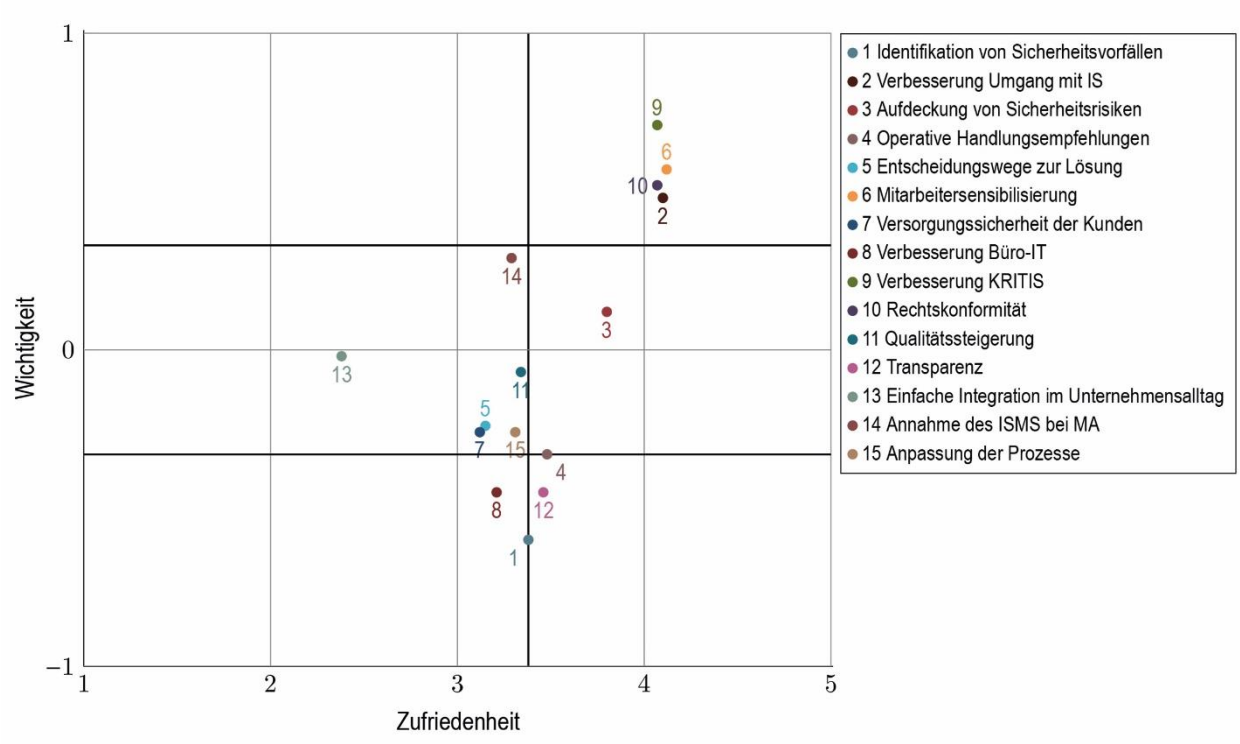


Abbildung 19: Allgemeine Zufriedenheit mit dem ISMS und Wichtigkeit zur Implementierung

Über alle Probanden (N=42)

Erkenntnisse aus der Sicherheitsbefragung

Die Zufriedenheit wurde auf einer 5-Punkte-Likert-Skala (1… äußerst unzufrieden bis 5... vollkommen zufrieden) abgefragt und die Wichtigkeit relativ über den MaxDiff-Ansatz ermittelt (siehe dazu Martilla und James 1977 und Chrzan und Golovashkina 2006). Hierzu mussten die Probanden die einzelnen Ausprägungen der Gruppen miteinander vergleichen, da es prinzipiell keine unwichtigen Aspekte im ISMS gibt.

In der allgemeinen Betrachtung über alle Probanden hinweg zeigt sich, dass insbesondere die Erwartungen zur Verbesserung im Umgang mit dem Thema Informationssicherheit im Unternehmen, die Mitarbeitersensibilisierung, Sicherung der Rechtskonformität sowie die Verbesserung der Informationssicherheit auf KRITIS-Ebene (hier Leitsystem-, Produktionssystem-Ebene) zu größter Zufriedenheit adressiert werden konnten. Diese Punkte wurden im Vergleich als die relativ wichtigsten Aspekte in der Implementierung des ISMS und dessen Beitrag zur Informationssicherheit im Unternehmen bewertet.

Es zeigt sich in obiger Abbildung insbesondere, dass die Zufriedenheit mit einer einfachen Integration in den Unternehmensalltag deutlich negativer bewertet wurde als die restlichen Aspekte. Die Wichtigkeit dieses Punktes ist für die Leistung des ISMS allerdings als relativ hoch anzusehen und steht noch vor den eigentlichen Verbesserungen zur Identifikation von Sicherheitsvorfällen bzw. im Allgemeinen der Wirkung des ISMS im Unternehmen. Der Aspekt der einfachen Integration und der Handhabbarkeit im Unternehmensalltag stellt eine wichtige Größe zur Akzeptanz des ISMS und damit auch zur Einhaltung der Verfahren und Prozesse im Unternehmensalltag dar. Ist das ISMS im Alltag nicht handhabbar, werden die im Scope befindlichen Mitarbeiter alternative Wege finden, um am ISMS „herum kommen“ zu können (BYOD) (Cram et al. 2017).

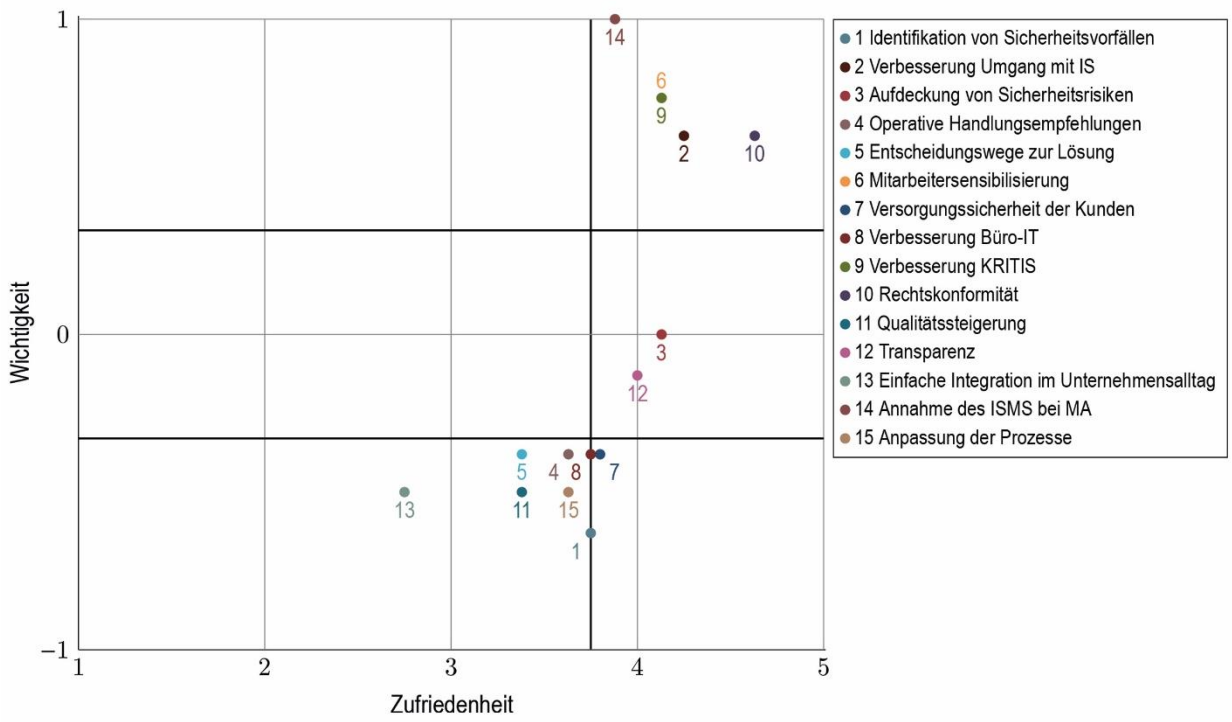


Abbildung 20: Zufriedenheit und Wichtigkeit zur Implementierung aus Sicht des CISOs

Nur CISO (N=8)

Die Annahme des ISMS bei den Mitarbeitern als entscheidender Aspekt zeigt sich bei der speziellen Betrachtung der Probanden mit der Rolle CISO in den Unternehmen. Die Annahme des ISMS bei den Mitarbeitern wird in der Zufriedenheit als zutreffend bewertet. Die Wichtigkeit dieses Punktes zur Leistungsentfaltung des ISMS wurde bei den CISOs als relativ am wichtigsten bewertet.

Bei den ISO/ISBs (nachfolgende Abbildung) zeigt sich der deutliche Unterschied in der Bewertung der Wichtigkeit zur einfachen Integration in den Unternehmensalltag. Hier wird im Vergleich zu den CISOs die Zufriedenheit negativer gesehen und die Wichtigkeit zur Entfaltung der Wirkungen eines ISMS höher bewertet. Dies kann bspw. an einer eher strategischen Sichtweise des CISOs und einer eher operativen Sichtweise des ISO/ISBs auf das Thema ISMS liegen.

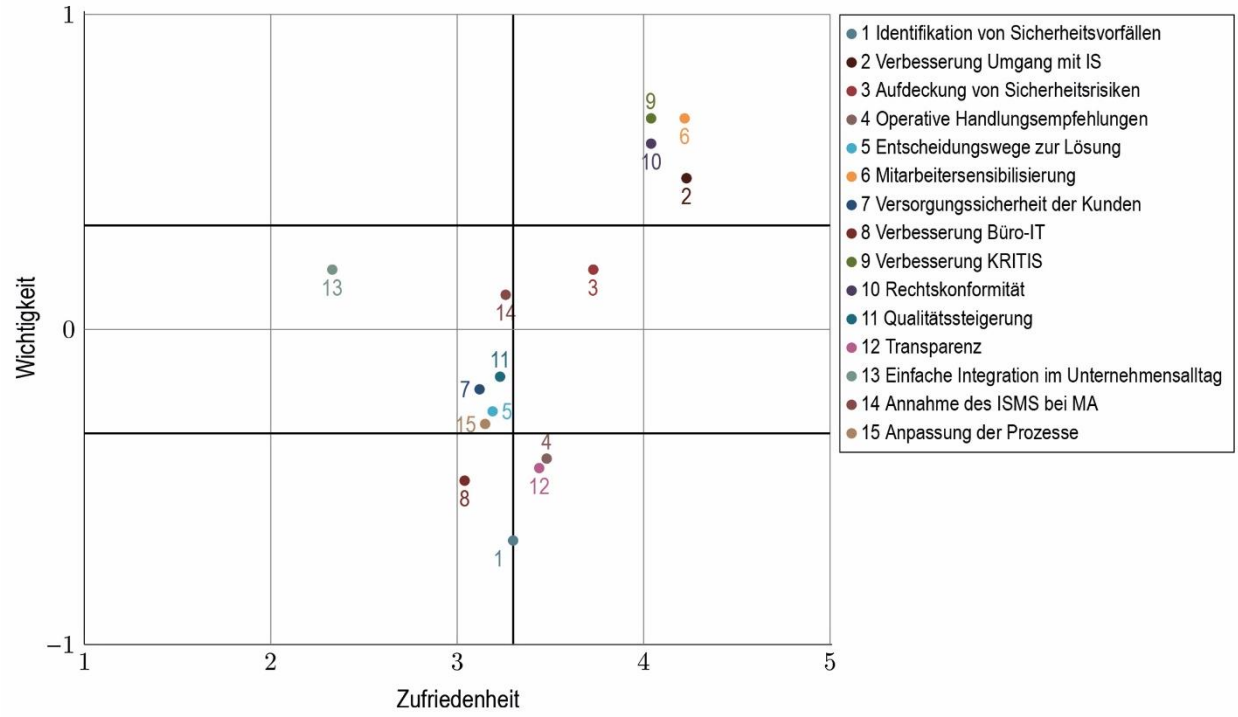


Abbildung 21: Zufriedenheit und Wichtigkeit zur Implementierung aus Sicht des ISO/ISBs

Nur ISO/ISB (N=27)

Die Implementierung eines ISMS hat Auswirkungen auf eine Vielzahl an Abteilungen im Unternehmen. Wie obige Abbildungen zeigen, ist hier auch die Office-IT (Unternehmensleitebene) betroffen. Nachfolgende Abbildung zeigt, welchen operativen Impact das ISMS in den Fachabteilungen entwickelte.

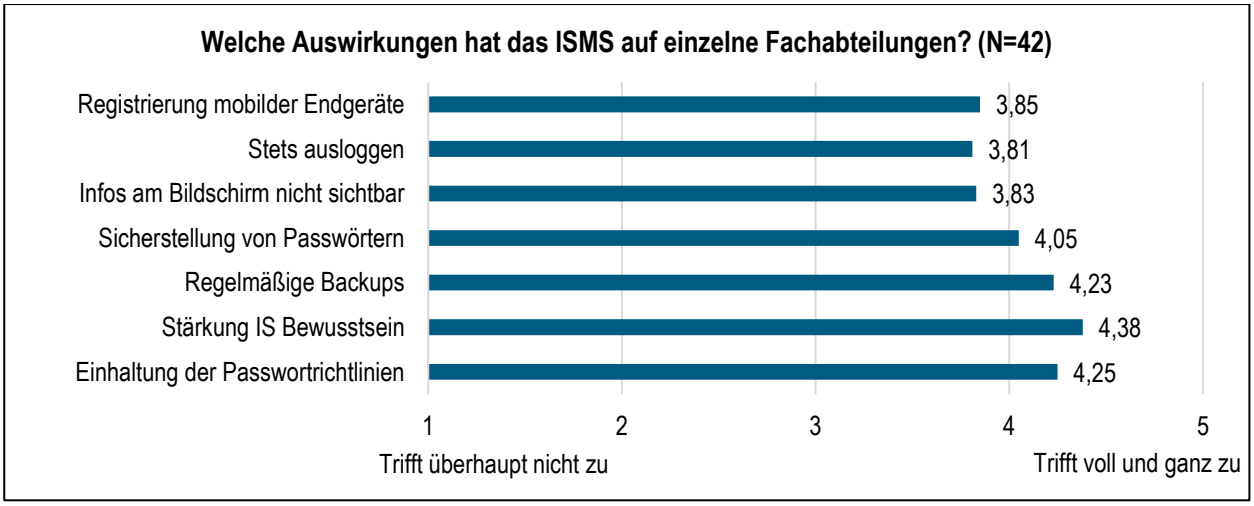


Abbildung 22: Operative Auswirkungen des ISMS in den Fachabteilungen

Es zeigen sich Ähnlichkeiten in den Einschätzungen der CISOs und ISO/ISBs zum Beitrag des ISMS für das Bewusstsein der Mitarbeiter. Damit verbunden sind die Einhaltung der Passwortrichtlinie sowie die Durchführung von regelmäßigen Backups in den Fachabteilungen. Die Interpretation der Ergebnisse zeigt, dass die grundlegenden Verhaltensweisen, wie z. B. die Registrierung mobiler Endgeräte im Unternehmen, der Log-out der Mitarbeiter beim Verlassen des Arbeitsplatzes sowie die sorgfältige Aufbewahrung von Passwörtern adressiert werden. Die Fragestellung lässt jedoch auch die Interpretation zu, dass bspw. die Durchführung regelmäßiger Backups in den Fachabteilungen vor der Einführung des ISMS nicht allumfänglich gegeben war und damit teils gesetzliche Anforderungen missachtet wurden.

5 Detailbetrachtung zur Führung in Organisationsprojekten

5.1 Unterstützung organisatorischer Veränderungen

Autor: Dr. Alexander Sänn

Eine der größten Hürden für Veränderungen im Unternehmensalltag ist die Annahme neuer Regelungen bei den Betroffenen – eben den Mitarbeitern in den jeweiligen (Fach-)Bereichen. Verfahrensanweisungen und Regelwerke eines ISMS erscheinen wenig sinnhaft, wenn die Mitarbeiter sich im Alltag nicht an diese halten und das ISMS damit nicht gelebt wird. Entwickeln die Betroffenen nicht den Grundgedanken der Informationssicherheit für sich und verinnerlichen sie diese nicht als oberste Direktive, droht das ISMS im Alltag zu scheitern.

Der Erfolg eines ISMS zeichnet sich bereits in der Einführungsphase ab. Verläuft die Implementierung erfolgreich und konnten in dieser Phase bereits die relevanten Personen sensibilisiert und für das Thema „mitgenommen" werden, kann das ISMS tatsächlich zum Leben im Unternehmensalltag erweckt werden. Scheitert diese Mitnahme, droht das ISMS auf ein Dasein als Dokumentation begrenzt zu sein.

Damit steht ein Unternehmen vor ähnlichen Herausforderungen wie in einem Innovationsprojekt mit mehreren Beteiligten. Im Rahmen des Projekts muss über Abteilungsgrenzen oder sogar Unternehmensgrenzen hinweg zusammengearbeitet werden und Mitarbeiter aus unterschiedlichen Abteilungen, Hierarchiestufen und Unternehmen (die in einem Zusammenhang durch die Wertschöpfungskette stehen) sensibilisiert und koordiniert werden. Damit beginnt die Herausforderung bei der Zusammenstellung des Innovationsteams.

Die Basis dazu verdeutlicht die nachfolgende Darstellung der Ebenen des Not-invented-here Syndroms (vgl. Anton und Piller 2015). Je nach Unternehmensart stößt ein Projekt „ISMS" auf einen oder mehrere Typen des Not-invented-here Syndroms, welches die Ablehnung der ISMS-Regularien auf operativer Ebene interpretieren kann. Typ 1 repräsentiert den gestörten internen Wissenstransfer, Typ 2 beschreibt den gestörten Transfer zwischen Individuen unterschiedlicher Firmen(-Standorte) innerhalb eines Projektteams, Typ 3 beschreibt die Symptome zwischen Hierarchieebenen, Typ 4 beschreibt dies für Wissen von externen Quellen, Typ 5, 6, 7 und 8 beschreiben dies zusätzlich für Wissen außerhalb des Kontexts der Informationssicherheit, z. B. bei Integration von Regularien aus der Informationssicherheit in andere Domänen, wie z. B. die Regelung innerhalb des ISMS zu Themen des Arbeitsschutzes oder des Lieferanten-Managements.

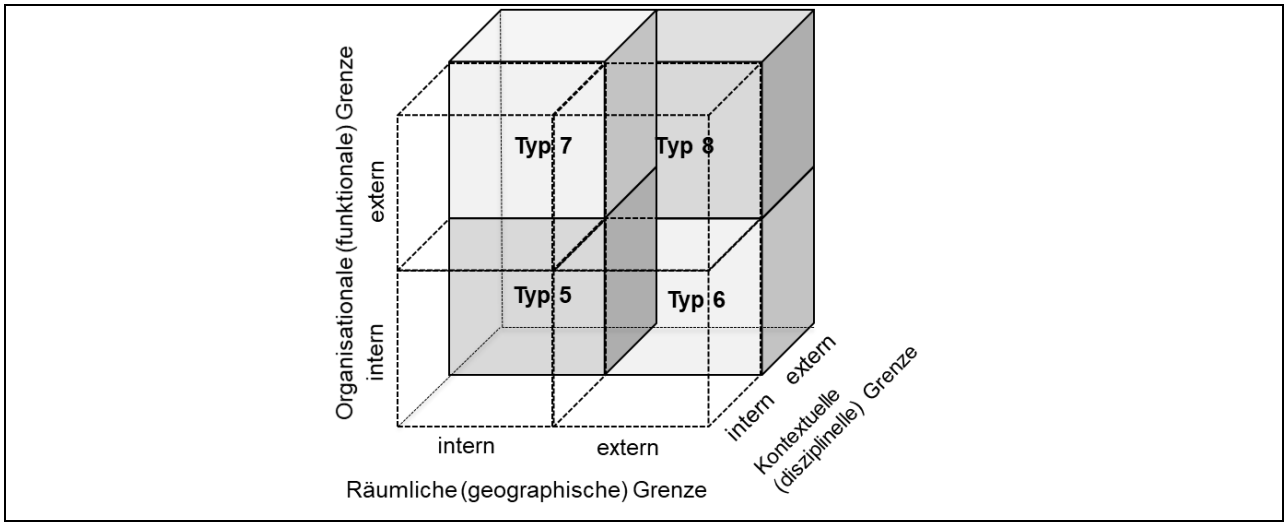


Abbildung 23: Typisierung des Not-Invented-Here Syndroms

Quelle: Darstellung nach Antons und Piller (2015)

Die Theorie des Promotoren-Modells soll Barrieren und Opponenten als „… beeinflussender Faktor, der eine Innovation verhindert, verzögert oder umformt" (Mirow, Hölzle und Gemünden 2007) unterbinden und damit für eine erfolgreiche Einführung sorgen. In der Grundlage beschreibt es, dass für die Überwindung jeder spezifischen Barriere eine spezifische Energie benötigt wird, welche von unterschiedlichen Personen bereitgestellt wird und durch die unterschiedlichen Personen im Rahmen ihrer Zusammenarbeit koaliert und koordiniert werden muss. Die Koalition und

Detailbetrachtung zur Führung in Organisationsprojekten

Koordination der Energien geschehen durch die besondere Beachtung verschiedener Rollen: dem Fach-, Macht-, Prozess- und Beziehungspromotor.

Die Rollen der Promotoren sind im Unternehmen zu finden und bei der Projektinitialisierung einzubeziehen. Grundlage dabei ist die Annahme, dass ein (größeres) Unternehmen einem Netzwerk gleichzusetzen ist und als Innovations Community angesehen werden kann. Die Rollen der Promotoren sind nachfolgend aufgezeigt.

In der Anwendung resultiert der Beziehungspromotor aus einem inter-organisationalen Innovations-Netzwerk. Seine Rolle überlappt mit dem Prozesspromotor, welchem eine intra-organisationale Rolle zugesprochen wird. Im Kontext großer Organisationen kann der Beziehungspromotor anhand der geografischen Barrieren – Abteilungen an unterschiedlichen geografischen Standorten - vom Prozesspromotor, welcher Abteilungen innerhalb des Hauses an einem Standort innovationsfördernd koordiniert, differenziert werden.

Die unterschiedlichen Promotorenrollen werden über diverse Wege zusammengeführt. Im Champion-Konzept entspricht der Promotor / Champion einem Generalisten. Ein einziges Individuum bildet die zentrale, treibende Kraft im Innovationsprozess und vereinigt mindestens zwei verschiedene Promotorenrollen in seiner Person. Ist der Fachpromotor gleichzeitig der Machtpromotor, ist dieser Weg vorliegend. Innerhalb einer Gespann-Struktur stellt der Promotor den jeweiligen Spezialisten dar. Bei diesem Weg wirken der Fach- und Machtpromotor ohne zwingende Verpflichtung zusammen. Diese Struktur ist das Idealbild in Bezug auf effiziente Entscheidungsprozesse, einem hohen Innovationsgrad und einer hohen Problemlösungskompetenz. Die Troika-Struktur sieht den Promotor ebenfalls als Spezialisten an und beschreibt das Zusammenwirken des Fach-, Macht- und Prozesspromotors. Es dient der besseren Überwindung von Opponenten (bspw. fest im Unternehmen eingesessene Gegner, fest etablierte gegenläufige Prozesse), der effizienteren Informationsakquirierung sowie einem höhere(r) Innovationsgrad und -fähigkeit. Es ergibt sich der Interpretationsschluss, dass ein ISMS-Projekt, bei welchem im Vorfeld ein Projektteam per Order bestimmt wird (zusätzliche Beauftragung eines verfügbaren Mitarbeiters als Informationssicherheitsbeauftragter), augenscheinlich wenig Erfolgsaussichten besitzt. Die Orientierung als Champion einer einzelnen Person (Chief Information Security Officer (CISO) / Information Security Officer (ISO/ISB) als Champion bzw. Generalist) erscheint bei der Erfüllung der beiden Rollen des Fach- und Machtpromotors erfolgsversprechend, doch fehlt es ihm womöglich an der Prozess- und Beziehungskenntnis im Unternehmen. Auch eine Zusammenstellung des Themas im Unternehmen mit ausschließlich homogenen Rollen erscheint diskutabel. Die Aufstellung des Projektteams als Troika erscheint erfolgsversprechender.

Der Fachpromoter

Der Fachpromotor löst die Fähigkeitsbarriere auf. Die Rolle besitzt objektspezifisches Fachwissen und eine direkte Nähe zum Thema. Die Rolle besitzt die Fähigkeit, nicht involvierte Akteure mit ihrem Fachwissen anstecken zu können und zeichnet sich durch die Bereitstellung fachspezifischer Informationen an alle Akteure aus. Er ist weder Spitzenmanager, noch rein ausführende Arbeitskraft, zeichnet sich durch seine Neugier, Risikofreudigkeit und Technikorientierung aus. Aus diesen Eigenschaften entwickelt er Ideen zur Bewältigung fachspezifischer Fragestellungen, beurteilt und entwickelt alternative Problemlösungsvorschläge und führt Problemlösungen bis hin zu einem Entschluss. Diesen Entschluss bereitet er fachlich kompetent vor, trifft den Entschluss aber nicht.

Der Machtpromoter

Der Machtpromotor löst die Willensbarriere und Hierarchiebarriere auf. Die Quelle seiner Macht resultiert aus seiner hierarchischen Stellung im Unternehmen bzw. im Projekt. Die Rolle ist Mitglied der höchsten Führungsebene bzw. liefert totale Unterstützung aus der höchsten Ebene für das Projekt. Er zeichnet sich durch modernen Führungsstil mit Überzeugungskraft und Begeisterungsfähigkeit aus, nutzt Belohnungs- und Anreizsysteme, ist Adressat und Unterstützer des fachlichen Experten bezüglich fachspezifischer Wünsche und Beschwerden. Die Rolle gewährleistet Hilfe, überbrückt Schwierigkeiten und scheut keine Auseinandersetzung. Er legt die Ziele des Projekts fest, stellt die Ressourcen bereit und schützt vor Opponenten. Fachpromotoren können sich auf die Unterstützung des Machtpromotors verlassen. Dieser fällt den Entschluss.

Der Prozesspromoter

Der Prozesspromotor löst fachübergreifende Fähigkeits- und Abhängigkeitsbarrieren auf. Er besitzt Organisationskenntnis und Kommunikationsfähigkeit, diplomatisches Geschick und Fähigkeit zur Ansprache und Gewinnung unterschiedlicher Menschen, Charisma und Fähigkeit zur Inspiration und Stimulierung. Mittels seiner

zentralen Position im Kommunikationsnetzwerk hat er Kenntnis von Betroffenen, deren Bedenken und versteht es, rationale Argumente präsentationsgerecht aufzuarbeiten. Damit wirbt die Rolle für das Neue und verhindert Insellösungen durch eine Konsensfindung. Dies resultiert auch durch die bei der Rolle anliegenden Aufgaben zur Koordination anfallender Tätigkeiten (Prozesssteuerung), zur Zusammenführung von betriebsinternen Interaktionspartnern und zur Sammlung, Filterung, Übersetzung / Interpretierung und Kommunikation von Informationen aller Beteiligten.

Der Beziehungspromoter

Der Beziehungspromotor löst organisationsübergreifende Fähigkeits- und Abhängigkeitsbarrieren auf. Die Rolle besitzt ein Beziehungsportfolio, Netzwerkwissen und Sozialkompetenz. Er besetzt Grenzstellen als Förderer innovationsorientierter Geschäftsbeziehungen, ist einem starken Informationseinfluss aus der Umwelt ausgesetzt und entwickelte bisher eine besondere Sensibilität, sein Netzwerk persönlicher Beziehungen zu Externen sowie die Fähigkeit, dieses zu entwickeln. Die Rolle fördert den Austauschprozess zwischen Unternehmen, sammelt, filtert übersetzt Umweltinformationen für die Beteiligten und bringt Interaktionspartner zusammen. Verhandlungen mit und zwischen Interaktionspartnern (Konflikt-Management), die Koordinierung von Tätigkeiten von Interaktionspartnern (Prozesssteuerung) und die Konsensfindung sind sein Metier.

Dr. Alexander Sänn

Geschäftsführer BF/M-Bayreuth

Zur Person:

Dr. Alexander Sänn studierte Wirtschaftsinformatik (eBusiness) an der Brandenburgischen Technischen Universität Cottbus-Senftenberg und promovierte dort unter Prof. Dr. Daniel Baier im Bereich Marketing und Innovations-Management zur Entwicklung von Informationssicherheits-technologien mittels der Einbindung von Lead Usern. In seinem Schwerpunkt berät und unterstützt er Klein- und Mittelständische Unternehmen bei Innovationsprozessen zur Umsetzung Kunden-integrierender Methoden sowie bei Fragen der Sensibilisierung zur Informationssicherheit. Weiterhin ist er zertifizierter ISO 27001 Lead Auditor und Dozent zum Thema Open Innovation an der Universität Bayreuth.

5.2 Zusammenarbeit mit externen Dienstleistern

Im Jahr 2016 gaben noch 92 % der Energieversorger an, die Unterstützung eines Dienstleistungsunternehmens in Anspruch genommen zu haben. In dieser Befragung sind es nur noch 76 %. Der hohe Prozentsatz aus dem Jahr 2016 kann durch die damals erst kurzfristige Einführung des Gesetzes im Jahr 2015 erklärt werden. Mangelnde Erfahrung und eine damals noch nicht finalisierte Norm sorgte für Unsicherheit bei den Unternehmen. Die Anzahl an Unternehmen, die 2018 die ISMS Beratung von Dienstleistern in Anspruch nahmen, ist zwar mit 76 % geringer, aber immer noch hoch. Es scheint weiterhin eine Unsicherheit seitens der Unternehmen im Umgang zu herrschen.

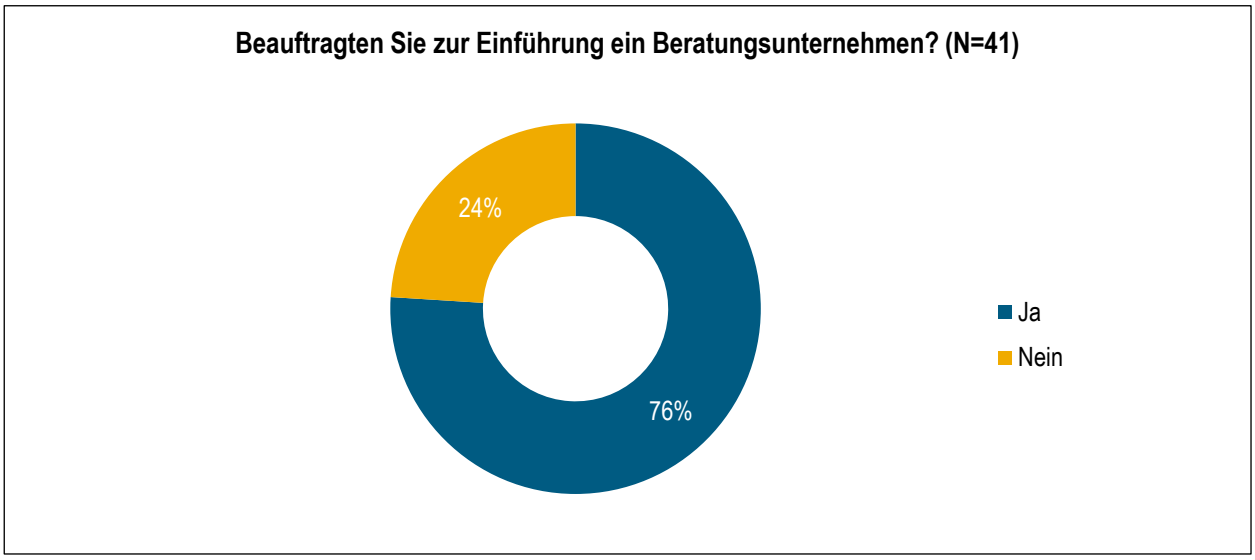


Abbildung 24: Beauftragung eines Beratungsunternehmens

Die Unterteilung der Unternehmen nach dem vorherigen Umgang mit dem Thema Informationssicherheit zeigt, dass die Einbindung eines Beraters abhängig davon scheint. Bei den Unternehmen mit vorherigem hohen Stellenwert der Informationssicherheit gaben 73 % an, ein Beratungsunternehmen beauftragt zu haben. Bei Unternehmen, welche bisher Informationssicherheit als beiläufiges Thema ansahen, geben ca. 92 % die Beauftragung eines Beratungsunternehmens an.

Die Berater wurden von den Unternehmen in allen Phasen der Einführung eines ISMS benötigt, beginnend mit der Initiierung, dem Scoping, gefolgt von der Implementierung und dem internen Audit. Im Mittel waren 1,4 Berater für 34,8 Tage bei den Unternehmen zur Einführung eines ISMS vor Ort.

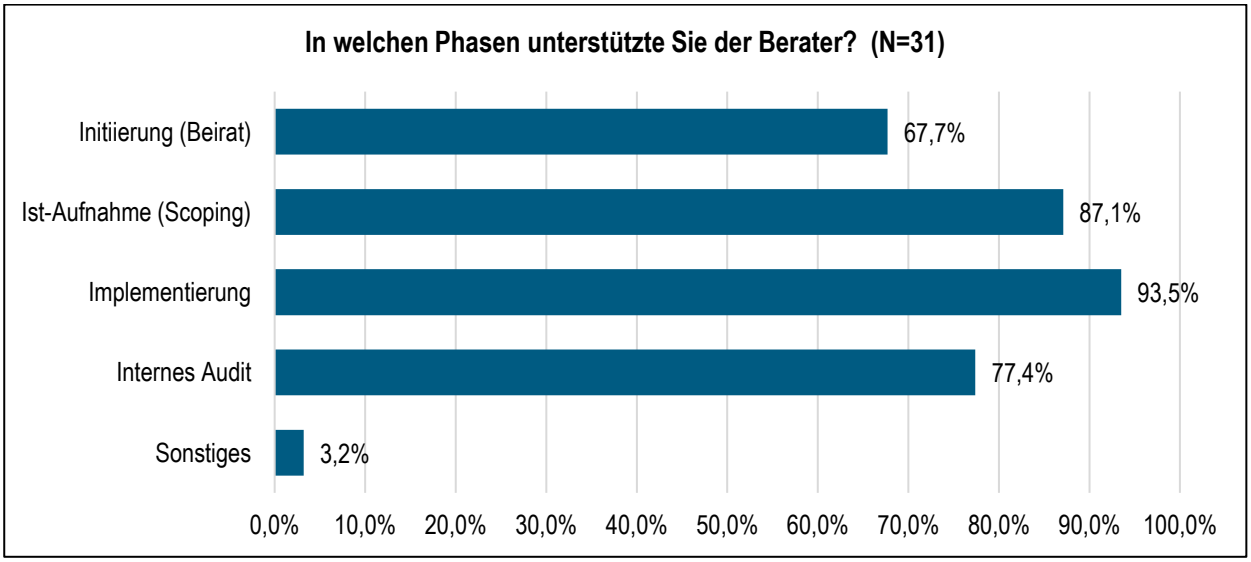


Abbildung 25: Phasen der ISMS-Implementierung mit Beratungsunterstützung

Detailbetrachtung zur Führung in Organisationsprojekten

Die Erfahrungen, welche die Befragten hierbei mit den Beratern sammelten, waren durch eine Heterogenität geprägt. Insgesamt wurden 22 positive und 20 negative Kommentare zu den in Anspruch genommenen Beratern geäußert. Nachfolgende Tabelle gibt einen Überblick hierzu:

Positive Erfahrungen mit dem Berater	Negative Erfahrungen mit dem Berater
Aufdeckung von Problemen	Das Unternehmen hat in Bezug auf die Risikoanalyse falsch beraten.
Fachkunde und Zielerreichung hinsichtlich erfolgreicher Zertifizierung	Keine ausreichenden Musterdokumente; internes Audit, das sämtliche Dokumente der Beraterfirma beanstandete (Internes Audit wurde von gleichem Unternehmen, wie Dokumente durchgeführt).
Grundsätzlich positiv zu bewertende Vorbereitung der fachlichen Themen	Manchmal etwas verwirrende Aussagen unterschiedlicher Berater
Gutes Know-how	Praxisfremd, langatmige Besprechungen von erdachten Störszenarien
Kompetent und hilfsbereit. Eine sehr gute und erfolgreiche Zusammenarbeit; es hat sich ein gutes Team entwickelt.	Schlechtes Projektcontrolling, hohe Kosten, Budgetüberschreitung
Hohe fachliche und soziale Kompetenz	Zeitliche Auslastung der Berater
Richtige Struktur aufgebaut; Zeiteinsparung für das Unternehmen	Zu hohe Aufwände wurden generiert

Tabelle 5: Erfahrungen mit dem Berater

Für die kontinuierliche Verbesserung des ISMS zogen nur noch 39 % der Energieversorger einen Berater hinzu; 61 % verwendeten dafür eigene Kompetenzen.

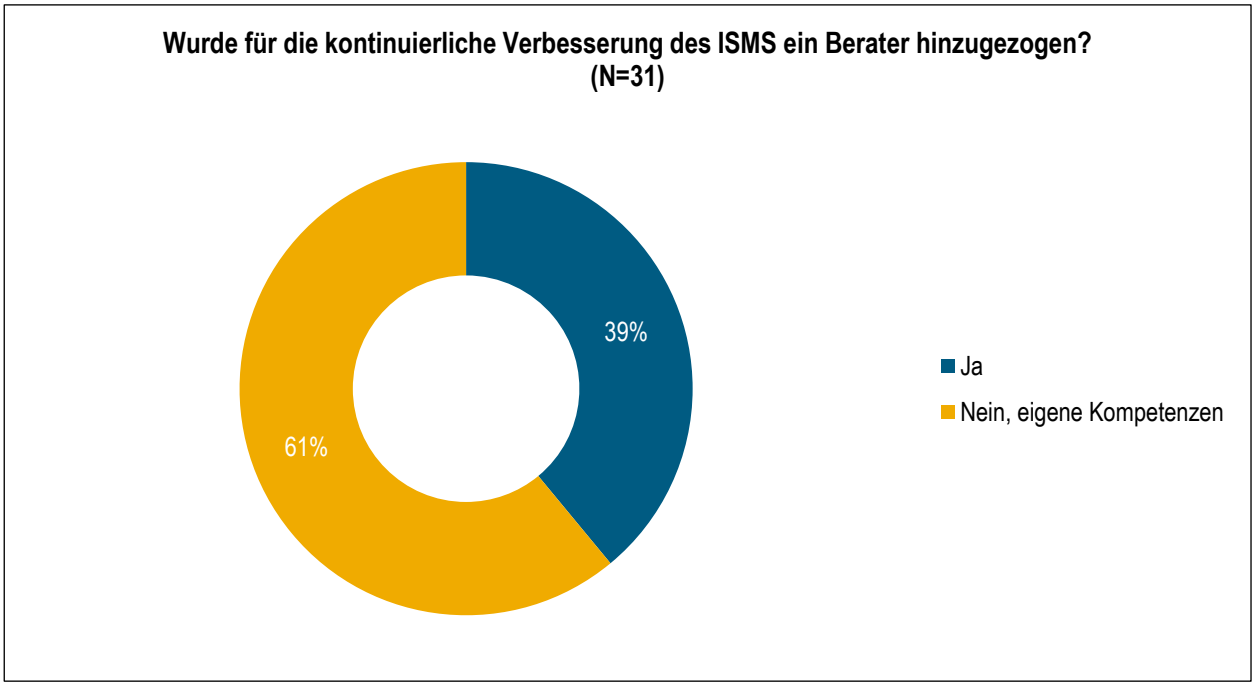


Abbildung 26: Wurde für den KVP des ISMS ein Berater hinzugezogen?

6 Detailanalyse zur Auditierung und Zertifizierung

6.1 Das Ökosystem eines Audits

Autor: Dr. Joachim Müller

Die deutsche Volkswirtschaft ist in hohem Maße von der ordnungsgemäßen Funktion der Strom-, Wasser- und Gasversorgung abhängig. Versorgungsunternehmen sind in der besonderen Verantwortung, die Versorgungssicherheit für Endkunden, Verwaltungen und Unternehmen sicherzustellen. Doch durch die immer stärker werdenden technologischen Abhängigkeiten vor allem durch All-IP[2], nimmt die Zahl der alternativen Dienste ab. Da alle Dienste digital verarbeitet werden, sind bei All-IP auch alle bekannten (und bisher nicht bekannten) IT-Risiken zu betrachten, da die Telekommunikationsunternehmen u. a. analoge Leitungen und Dienste, wie auch ISDN-Leitungen und Dienste sukzessive abkündigen.

Spätestens seit dem Einzug kommerzieller Betriebssysteme in der Fernwirk- und Steuerungstechnik (SCADA, MSR, u.a.) war abzusehen, dass es Auflagen durch Prüfungen und Zertifizierungen geben wird[3]. Rahmenwerke und Management-Systeme zur Steuerung eines sicheren und ordnungsgemäßen IT-Betriebes waren schon seit den 90ern[4] bekannt, wurden aber nur selten etabliert.

Getrieben durch den kontinuierlichen und schnellen technologischen Wandel bleiben Konzeption, Planung, Projektierung, Test, Freigabe und Dokumentation vor, während und nach der Produktivsetzung oft in unterschiedlichem Maße auf der Strecke. Die Folgen sind Risiken, denen sich die Unternehmen, ihren Mitarbeitern, Kunden und Lieferanten gleichermaßen aussetzen. Tagtäglich gibt es gefühlt gravierende Meldungen zu erheblichen Ausmaßen aus IT-Sicherheitsschwachstellen.

Haben wir den Überblick verloren? Diese Frage hat die Politik (weltweit) in den vergangenen Jahren stark beschäftigt und zu unterschiedlichen Ansätzen in der Herangehensweise an das Thema digitale Sicherheit geführt.

So war es auch aufgrund des EU-weiten Vorgehens absehbar, dass die gesetzlich-regulatorische Anforderung an Sicherheit auch für das Informationssicherheits-Management von Steuerungssystemen der Energieversorgung kommen musste.

Mit dem IT-Sicherheitskatalog, resultierend aus dem Energiewirtschaftsgesetz (EnWG) und dem IT-Sicherheitsgesetz sowie dessen Rechtsverordnungen hat die Politik den ersten Schritt gemacht, konkrete Anforderungen für Informations- und IT-Sicherheit an KRITIS-Unternehmen5 zu stellen. In weiteren Schritten ist geplant: *Eine erfolgreiche Digitalisierungsstrategie setzt Datensicherheit voraus. Wir wollen, dass gemeinsam zwischen Bund und Ländern, möglichst sogar in ganz Europa, Sicherheitsstandards für die IT-Strukturen und den Schutz der kritischen Infrastruktur entwickelt werden. Den mit dem IT-Sicherheitsgesetz eingeführten Ordnungsrahmen werden wir in einem IT-Sicherheitsgesetz 2.0 weiterentwickeln und ausbauen. In diesem Zusammenhang werden wir die Herstellerinnen und Hersteller sowie Anbieterinnen und Anbieter von IT-Produkten, die neben den kritischen Infrastrukturen von besonderem nationalem Interesse sind, stärker in die Pflicht nehmen* (Koalitionsvertrag 2018, Zeile 5868 ff.)

---

[2] All-IP. Moderne (rein digitale) All-IP-Netze (AIPN) stellen alle Dienste, wie z. B. Internettelefonie (VoIP, Voice over Internet Protocol), Internetfernsehen (IPTV), Online-Spiele, Datenübertragung usw. jedem Benutzer zu jeder Zeit an jedem beliebigen Ort zur Verfügung.

[3] Die verwendete Netzleittechnik muss deshalb technisch, baulich und organisatorisch konsequent ausfallsicher ausgelegt werden. {…} ist eine TÜV-Zertifizierung für solche Umgebungen eine adäquate Antwort auf die meist offene Frage nach dem tatsächlichen Sicherheitsstatus (Healthy State) und gewährleistet damit einen nachhaltigen und sicheren Versorgungsbetrieb.“ (Schartner/Taeger 2011)

[4] Z. B. COBIT (Control Objectives for Information and Related Technology) oder BS 7799 (Information Security Management Systems – Specification with guidance for use), welches die Grundlage für ein Informationssicherheits-Management-System (ISMS) nach ISO 27001 darstellt.

[5] KRITIS. Für Betreiber Kritischer Infrastrukturen im Sinne des BSI-Gesetzes und des Energiewirtschaftsgesetzes ist das IT-Sicherheitsgesetz mit den Pflichten zur Absicherung ihrer IT nach dem Stand der Technik und zur Meldung erheblicher IT-Sicherheitsvorfälle durch die Rechtsverordnung (sog. KRITIS-Verordnung) des Bundesministerium des Innern am 03.05.2016 in Kraft getreten.

Detailanalyse zur Auditierung und Zertifizierung

Der Grundgedanke geht dabei auf die Forderungen der Politik aus dem Jahre 2012 zurück, als der damalige Innenminister Hans-Peter Friedrich den Anspruch nach einem IT.-Sicherheitsgesetz erhob, „da die Erfahrung gezeigt habe, dass man allein mit freiwilligen Maßnahmen hinter unseren Zielen zurückgeblieben“[6] sei.

Verantwortung ist nicht delegierbar. Und so ist das Unternehmen in der Pflicht und die Unternehmensleitung nebst Management in der Haftung, die Anforderungen aus dem IT-Sicherheitskatalog zu erfüllen und die geforderten Maßnahmen aus den zugrundeliegenden Normen (DIN ISO/IEC 27001 und ISO/IEC TR 27019 in der jeweils gültigen Fassung) umzusetzen. Die Normen der ISO sind international anerkannt und weltweit inhaltlich, wie auch von Zertifizierungsverfahren her, identisch und somit vergleichbar.

Oft wird bemerkt, dass die Norm nur inhaltliche Vorgaben mache und wenig Konkretes beinhalte, insbesondere technische Vorgaben seien darin nicht zu finden. Das ist gut so, denn so liegt die Ausgestaltung beim Unternehmen und zwingt das Unternehmen nicht in ein Korsett an Vorschriften, die die Wettbewerbsfähigkeit negativ beeinträchtigen würden. Je nach Branche, Größe, betriebswirtschaftlicher Ausrichtung, Unternehmensstrategie und Organisation können Maßnahmen im Sinne des Unternehmens an Aufbau- und Ablauforganisation sowie zu den Unternehmens-prozessen angepasst und stetig verbessert werden. Die Norm als Management-System ist prozessorientiert, nicht technisch. Das ist der Grund, warum sich viele Unternehmen mit der Projektumsetzung schwertun. Projekte von Management-Systemen, auch zur Informationssicherheit, sind Organisationsprojekte. Das Aufsetzen und Steuern solcher Projekte bedarf seitens der Managementberatung nicht nur Erfahrung im Thema selbst, sondern auch im Umgang und im Aufbau von Organisationen und abteilungsübergreifenden Prozessen.

In den Zertifizierungsaudits gemäß IT-Sicherheitskatalog hat sich immer wieder gezeigt, dass eine bereits vorhandene Zertifizierung nach dem Technischen Sicherheits-Management (TSM) unter geschickter Einbindung in das Informationssicherheits-Management nicht nur zu kürzeren Vorbereitungszeiten zur Zertifizierungsreife führen konnte, sondern auch erhebliche Rationalisierungs- und Effizienzgewinne bei der Erstellung der Dokumentation zur Folge hatte. Die Einbindung des Technischen Sicherheits-Managements in den Geltungsbereich des Informationssicherheits-Managements war dabei offenkundig stark abhängig von den eingesetzten Beratern für die Einführung des Management-Systems. Es konnten mitunter zwei völlig voneinander unabhängig laufende Stränge (eines für ISO 27001 und eines für TSM) festgestellt werden. Hier können künftig noch erhebliche Effizienzgewinne gehoben werden, die die Abläufe und Prozesse und vor allem die Dokumentation deutlich erleichtern und somit Ressourcengewinne für die Abteilungen der Unternehmen erbringen.

Wesentliche Rationalisierungs- und Effizienzgewinne können durch den Abgleich gleichgelagerter Anforderungen aus anderen Gesetzen, Verordnungen, regulatorischen Anforderungen oder vertraglichen Vereinbarungen erreicht werden. So ist ein Datenschutz-Management-System gemäß der Datenschutzgrundverordnung (DS-GVO) optimal mit einem Informationssicherheits-Management-System zu verknüpfen, da hier umfangreiche Rationalisierungs- und Effizienzgewinne zu erreichen sind, denn die DS-GVO hat durch den vorgenommenen Paradigmenwechsel die Prozessorientierung und die Dokumentation (Rechenschaftspflicht) von Gesetzes wegen verordnet.

Die Zertifizierung

Eine Zertifizierung ist ein Verfahren, mit dem durch eine unabhängige dritte Partei die Überprüfung nach einem gültigen Anforderungskatalog (Prüfkatalog) eines Produktes, eines Verfahrens oder einer Betriebsorganisation überprüft und dessen Zertifizierungsreife nachgewiesen wird. Im Zusammenhang mit Zertifizierungen ist grundsätzlich zu beachten, in wessen Hoheit die Ausstellung eines Zertifikates vorgenommen wird. Zertifikate werden u. a. von akkreditierten Zertifizierungsstellen, Bundesämtern, Prüfverbänden, Prüfinstituten, Prüflaboren, Gutachtern und Wirtschaftsprüfungsgesellschaften ausgestellt.

Die Zertifizierung ist für ein Unternehmen in zweierlei Hinsicht ein Positivum. Ein Zertifikat ist ein Alleinstellungsmerkmal gegenüber den Marktbegleitern einerseits, anderseits ist die dahinterstehende Umsetzung im Unternehmen ein wichtiger Beitrag zur betriebswirtschaftlichen Grundmotivation des Unternehmens. Durch geregelte, dokumentierte und gelebte Unternehmensprozesse und den kontinuierlichen Verbesserungsprozess ist der reibungslose Ablauf innerhalb der Organisation ein wichtiger Beitrag zur Ressourceneffizienz.

---

[6] Bundesinnenminister Dr. Hans-Peter Friedrich, 08.11.2012

Detailanalyse zur Auditierung und Zertifizierung

Zertifizierungen für Management-Systeme, wie die der ISO 27001, sind (im Gegensatz zu früher in den 90ern) prozessorientiert und erfordern seitens der Organisation, die die Zertifizierung anstrebt, deutliche Aufwände zur Erreichung der Zertifizierungsreife. Aus diesem Grund ist die Verpflichtung des Managements aus der Norm heraus ein wesentlicher Faktor. Anders ausgedrückt: Steht die Geschäftsleitung nicht aufrichtig zur internen Umsetzung und Verbesserung, sondern stellt fälschlicherweise nur das (Papier-)Zertifikat in den Vordergrund, haben die innere Organisation und die Mitarbeiter alle Not mit der Erreichung der Normziele und somit auch mit dem Erhalt des Zertifikates. Auch wenn im Falle des IT-Sicherheitskataloges die Zertifizierung gesetzlich vorgeschrieben ist, die Umsetzung des Management-Systems erfolgt für das Unternehmen, nicht für das Papier(-Zertifikat).

Die Deutsche Akkreditierungsstelle GmbH (DAkkS)

Die Deutsche Akkreditierungsstelle GmbH (DAkkS) ist die nationale Akkreditierungsstelle der Bundesrepublik Deutschland auf Basis der Verordnung (EG) Nr. 765/2008 und dem Akkreditierungsstellengesetz (AkkStelleG). Sie ist eine nicht gewinnorientierte Gesellschaft, die auf Beleihung des Bundes ihre hoheitlichen, nationalen und alleinigen Akkreditierungsaufgaben innerhalb des Staatsgebietes der Bundesrepublik Deutschland wahrnimmt und somit das deutsche Verwaltungsrecht anwendet. Die DAkkS ist eine GmbH, deren Gesellschafter die Bundesrepublik Deutschland, die Bundesländer Bayern, Hamburg, Nordrhein-Westfalen und der Bundesverband der Deutschen Industrie e. V. (BDI) sind. Der gesetzliche Auftrag der DAkkS ist die Akkreditierung von Konformitätsbewertungsstellen. Dazu gehören u. a. Inspektions- und Zertifizierungsstellen, Laboratorien und andere Prüfungseinrichtungen. Angabe gemäß sind ca. 4.300 Akkreditierungsverfahren durch die DAkkS begutachtet, bestätigt und überwacht. Mit einer Akkreditierung bestätigt die DAkkS, dass diese Stellen ihre Aufgaben fachkundig und nach geltenden Anforderungen erfüllen. Kurz: Die DAkkS prüft die Prüfer (und die Auditoren; Anm. des Autors).

Die Zertifizierungsstelle

Die Zertifizierungsstelle ist eine Organisation (ein gewinnorientiertes, betriebswirtschaftlich geführtes Unternehmen), welches auf Basis der Akkreditierungen bei der DAkkS Zertifizierungsaudits durchführt, einen Auditbericht erstellt und bei Erfolg ein Zertifikat oder Testat ausstellt und ein Prüfzeichen vergibt, z. B. TÜV-Gesellschaften wie TÜV Nord, TÜV Süd, TÜV InterCert und andere Zertifizierungsstellen wie Deutsche Zertifizierung (DeuZert), DQS, FOX-Certification, Dekra u. a. Wichtig im Zusammenhang mit gesetzlich geforderten Zertifizierungen ist, dass die prüfende Zertifizierungsstelle eine Akkreditierung bei der Deutschen Akkreditierungsstelle innehat (nationales Verwaltungsrecht). Die Zertifizierungsstelle beruft Auditoren, die entsprechend den normativ festgelegten Regularien ausgewählt und aufgrund ihrer Fach- und Sachkunde, ihrer Berufserfahrung, ihrer Schulung und erfolgreichen Prüfung zur Norm sowie der vorgeschriebenen Anzahl an Traineetagen in Zertifizierungsaudits, zum Einsatz kommen.

An dieser Stelle erscheint es zielführend, die Thematik der geregelten und ungeregelten Zertifizierungen einzuführen. Man spricht von geregelten Zertifizierungen, wenn es sich um normkonforme Zertifizierungsverfahren handelt, die von der Akkreditierungsstelle des jeweiligen Landes auf Basis international anerkannter Normen als solche anerkannt sind. Ungeregelte Zertifizierungen sind solche, die durch Zertifizierungsstellen selbst auf Basis verschiedener anerkannter Prüfkriterien ein eigenes Prüfverfahren entwickelt haben, welches mit einem (freiwilligen) Prüfzeichen zum Ausdruck gebracht wird, z. B. „TÜV geprüftes Rechenzentrum“, basierend auf Anforderungen aus dem Grundschutzkompendium des BSI (Bundesamt für Sicherheit in der Informationstechnik), der ISO 27001 und der EN 50600 (Einrichtungen und Infrastrukturen von Rechenzentren).

Das Witness-Audit

Das Witness-Audit ist eine der Grundvoraussetzungen für eine Zertifizierungsstelle, die Akkreditierung für den geregelten Zertifizierungsbereich zu erhalten. Voraussetzung für ein Witness-Audit ist zunächst die genaue Beschreibung des Zertifizierungsverfahrens und der Verfahrensabläufe innerhalb der beantragenden Zertifizierungsstelle. Diese werden durch Begutachter der DAkkS im Rahmen eines Geschäftsstellen-Audits überprüft. Sind die Dokumente, Prüflisten, Verfahrensbeschreibungen, das Auditoren-Management und dessen Auswahlkriterien als entsprechend der Normanforderungen von den Begutachtern anerkannt, so ist der Weg frei für die Durchführung eines Witness-Audit durch die Auditoren, die von der Zertifizierungsstelle benannt und die ebenfalls im Rahmen der Begutachtung geprüft wurden.

Die Rolle des DAkkS-Begutachters im Witness-Audit ist die eines stillen Beobachters. Der Begutachter muss entsprechend den Anforderungen und der Stellenbeschreibung der DAkkS über die berufliche und fachliche Kompetenz verfügen. Er muss mindestens vier Jahre Berufserfahrung und über umfangreiche Normenkenntnisse im

jeweiligen Fachgebiet mitbringen. Außerdem sind persönliche Eigenschaften wie Unparteilichkeit, Aufrichtigkeit, Diskretion, Diplomatie, Selbstsicherheit und andere Merkmale gefordert.

Es menschelt. Und so finden sich auch bei Begutachtern (wie auch bei Auditoren) unterschiedliche menschliche und persönliche Charaktere. Damit muss ein Unternehmen, welches ein Witness-Audit bei sich durchführen lässt, umgehen. Erfahrungen von Unternehmen, insbesondere solcher, die bisher keine Auditerfahrung haben, führen mitunter zu der Aussage Witness-Audits eine Absage zu erteilen. Aber: Wird kein Witness-Audit der Zertifizierungsstelle durchgeführt (weil sich niemand bereit erklärt dies bei sich durchführen zulassen), ist die Konsequenz, dass die Zertifizierungsstelle keine Akkreditierung erhält. Erhält die Zertifizierungsstelle keine Akkreditierung, kann diese keine Zertifizierungen in dieser Norm durchführen. Erfahrungsgemäß findet sich aber meistens ein Unternehmen für ein Witness-Audit. Die Anzahl der akkreditierten und damit zugelassenen Zertifizierungsstellen die am Markt verfügbar sind, hängt somit auch ein Stück an der Bereitschaft zur Durchführung eines Witness-Audits seitens der Unternehmen. Natürlich ist in einem solchen Audit die Anspannung aller Beteiligter besonders hoch, denn alle müssen und wollen ihre Aufgabe möglichst gut erledigen – das kann schon mal recht spannend werden. Der Begutachter kann im Audit an den leitenden Auditor Fragen zu dessen Vorgehen oder Entscheidungen stellen, um seinerseits die Korrektheit zur angewandten Norm und den definierten Verfahren der Zertifizierungsstelle feststellen zu können. Diese Fragen sind vom Auditor zu beantworten, während das Unternehmen hier im Allgemeinen nicht involviert ist, denn der Begutachter prüft den Auditor und die Verfahren der Zertifizierungsstelle, nicht das Unternehmen, das macht nach wie vor das Auditteam. Und so ist es wichtig, dass man erfahrene Berater oder Auditoren im Witness-Audit zur Seite hat, die in sachlicher, ruhiger und lösungsorientierter Art mögliche Befindlichkeiten erörtern und auflösen.

Der Auditor

Wie machen Sie das? Wo steht das? Dann möchte ich das jetzt sehen? Und nun bitte noch einen Nachweis. Vielen Dank – Ihr Auditor.

Auditoren sind häufig externe Mitarbeiter oder Mitarbeiter aus Unternehmen, können aber auch fest angestellte Mitarbeiter (der Zertifizierungsstelle), die die Audits und Bewertungen im Auftrag der jeweiligen Zertifizierungsstelle durchführen, sein. Bei der Auswahl sind entscheidende Merkmale die Qualifikation, die Kompetenz im Fachgebiet, die kontinuierliche Weiterbildung und eine hohe Qualität der erbrachten Dienstleistung. Die Auswahlkriterien für Auditoren unterscheiden sich zwischen den Zertifizierungsstellen in Deutschland nur minimal, da auch hier Regelungen der Norm und der DAkkS greifen.

Für die Berufung zum Auditoren sind also zunächst fachliche Eigenschaften, wie Berufsausbildung oder vergleichbarer Abschluss, mehrjährige Berufserfahrung, hierzu mindestens 2 Jahre im Bereich Informationssicherheit nötig. Gefordert ist auch die erfolgreiche Teilnahme (Nachweis durch bestandene Prüfung) an einer anerkannten Auditorenausbildung der ISO 19011, ISO 17021, ISO 27001 und IT-Sicherheitskatalog. Darüber hinaus sind persönliche Eigenschaften gefordert, wie: soziale Kompetenz, Objektivität und Neutralität, schnelle Auffassungsgabe, effektive Kommunikation, kritisches Urteilvermögen und weitere.

Bevor die Berufung zum Auditor durch die Zertifizierungsstelle erfolgt, muss der angehende Auditor a priori Auditerfahrung von mehreren vollständigen Audits mit mindestens 20 Tagen Umfang, davon mindestens 11 Tage vor Ort unter der Aufsicht und Anleitung eines erfahrenen (leitenden) Auditors gesammelt haben, um die Qualifikation als Auditor erhalten zu können. [gekürzter und zusammengefasster Auszug aus den internen Unterlagen der DeuZert® – mit freundlicher Genehmigung der Zertifizierungsstelle der DeuZert - Deutsche Zertifizierung in Bildung und Wirtschaft GmbH]

Der angehende Auditor ist also zunächst als „Trainee“ begleitend bei den Audits dabei, eine Berechnung oder eine Zuweisung von Audittätigkeiten ist in der Regel nicht zulässig, Fragen stellen darf der angehende Auditor selbstverständlich. Nun folgt ein Monitoring Audit, welches erfolgreich absolviert werden muss.

Sofern Auditoren bereits bei einer Zertifizierungsstelle berufen sind[7], können sie bei anderen Zertifizierungsstellen unter Vorlage und Prüfung aller Dokumente (Lebenslauf, Zeugnisse, Personenzertifizierungen, Aus- und Fortbildungsnachweise, Auditorenberufungen und Führungszeugnis) berufen werden, denn die entsprechenden

[7] Auditorenberufungen von nicht akkreditierten Zertifizierungsstellen werden nicht anerkannt

Anforderungen sind erfüllt. Es folgt immer eine Einweisung in die Abläufe und Verfahren der Zertifizierungsstelle, da sich diese, wie bereits erwähnt, unterscheiden. Die Berufung zum Auditor erfolgt schriftlich.

Auditoren müssen an den regelmäßigen, meist jährlich stattfindenden Erfahrungsaustausch der Zertifizierungsstelle teilnehmen. Erfolgt diese Teilnahme nicht nachvollziehbar regelmäßig, kann der Auditor abberufen werden, da er sich nicht mehr ausreichend mit den Verfahren und Anweisungen der Zertifizierungsstelle und möglicherweise den aktuellen Entwicklungen im Fachgebiet auskennt.

Das Auditorenverhalten lernt man und im Laufe der Berufserfahrung verbessert sich auch der Auditor. Frische Auditoren sind oft sehr genau und formal, man will schließlich keine Fehler machen. Natürlich bringt jeder Auditor fachspezifisches Wissen mit. Und so hält jeder Auditor sich an seinem persönlichen Spezialthema länger auf, weil er sich sicher fühlt. Eine Expertise im Energiesektor ist nicht nur wichtig, sondern gefordert, aber auch hier kann das Umgekehrte passieren; normative organisatorische Management-Themen werden möglicherweise nicht umfangreich genug betrachtet. Es gibt derzeit in der ISO 27001 keine EA-Codes, wie dies bei der Akkreditierung zur ISO 9001 festgelegt ist. Der EA-Code[8] legt fest, in welcher Branche ein Auditor Zertifizierungsaudits durchführen darf. Die Festlegung erfolgt auf Basis seiner Berufserfahrung und Qualifikationen (siehe zuvor).

Der Auditor kann Angestellter oder Mitarbeiter eines Unternehmens sein, durchaus auch aus einem Beratungsunternehmen. Aber: Berater dürfen Unternehmen, bei denen sie tätig waren, zwei Jahre nach Abschluss der Beratungstätigkeiten nicht auditieren, sind also als Auditor ausgeschlossen. Auch dieser Umstand wird durch die DAkkS strikt geprüft. Beratung und Audit schließen sich aus! D.h., dass Auditoren während ihrer Audittätigkeiten, im Audit, in den Pausen (wann auch immer) das auditierte Unternehmen nicht beraten dürfen. Aber: Auditoren dürfen Verbesserungspotenziale aufzeigen, die gängige Praxis, andere Normen oder Vorschriften reflektieren. Kleiner Tipp: Lassen Sie den Auditor ausreden und hören Sie aufmerksam zu, das kann hilfreich sein.

Nun kommt er (der Auditor) in das Unternehmen und es funktioniert so gar nicht, wie man sich das gedacht hat. Grundsätzlich kann man den Auditor abweisen oder gar Hausverbot erteilen. Aber auch hier gilt: Reden hilft. Sprechen Sie bei Vorbehalten gegen den Auditor mit der Zertifizierungsstelle (z. B. Leiter der Zertifizierungsstelle) über Ihre „Bauchschmerzen“ und fragen Sie nach Möglichkeiten eines Wechsels oder eines zusätzlichen Auditors / Fachexperten als begleitende (vermittelnde) Person (beachten sie den Kostenaspekt und klären sie diesen im Vorfeld).

Oft sind die Diskussionspunkte im Audit zwischen Auditor und Unternehmen auf sehr formaler Basis. Das ist sicherlich bis zu einem gewissen Punkt richtig und wichtig. Aber es geht darum, dass das Unternehmen normativ mit dem Management-System in die richtige Richtung gebracht wird – der Sinn des Audits. Unerfahrene Auditoren sind manchmal sehr formalistisch, das kommt oft aus einer eigenen Unsicherheit heraus, denn der Auditor muss schnell und umfassend ein sehr komplexes Thema in einem ebenso komplexen Unternehmen mit einer eigenen Kultur erfassen. Das ist an sich schon eine Herausforderung und da gilt durchaus der Satz eines guten Freundes und Auditorenkollegen: „Da die meisten Auditoren nicht richtig zuhören, ist es ein Wagnis, das, was sie heraushören, eine Beurteilung zu nennen.“ (Hermann J. Paul, Management eines Auditprogrammes, qmserve)

Der Fachexperte

Da das zu prüfende Themenfeld häufig sehr spezielle Fachkenntnisse erfordert, können Auditoren während des Auditprozesses durch Fachexperten der Zertifizierungsstelle unterstützt werden. Analog zu den Anforderungen an Auditoren werden auch von Fachexperten entsprechende Qualifikationen gefordert. Dies umfasst eine entsprechende Ausbildung (i. d. R. ein erfolgreich abgeschlossenes Studium einer passenden Fachrichtung), spezifische Weiterbildungen und Personenzertifikate sowie mehrjährige Berufserfahrung im jeweiligen Fachgebiet.

Für die Zertifizierung gemäß IT-Sicherheitskatalog können die akkreditierten Zertifizierungsstellen Fachexperten benennen, nachdem diese von der Bundesnetzagentur (BNetzA) für geeignet befunden wurden. Hierzu sind alle relevanten Unterlagen vorab zur Prüfung bei der BNetzA einzureichen. Insbesondere die Berufserfahrung wird geprüft, eine Tätigkeit bei einem Energieversorgungsunternehmen qualifiziert nicht automatisch für die Fachexpertentätigkeit.

[8] ISO Certification Scope, EA Code, European Accreditation Codes, z.B. EA 33 = Datenverarbeitung / Dienstleistungen; EA 25 = Elektrizitätsversorgung (vgl. Bundesverband der Auditoren e.V. 2018)

Detailanalyse zur Auditierung und Zertifizierung

Es wird geprüft, ob tatsächlich die geforderten Erfahrungen und Qualifikationen in der leitungsgebunden Strom- und Gasversorgung und insbesondere der zugehörigen Fernwirk- und SCADA-Technik vorliegen.

Das zugrundeliegende Zertifizierungsverfahren sieht vor, dass ein Auditor, der die Anforderungen an einen Fachexperten nicht selbst erfüllt, bei den ersten fünf Audits durch einen Fachexperten begleitet wird. Bei den weiteren Audits kann der Auditor auf diese Unterstützung verzichten.

Das Monitoring-Audit

Das Monitoring-Audit dient der Überwachung und Kontrolle der berufenen Auditoren der jeweiligen Zertifizierungsstelle. Jede Zertifizierungsstelle muss ihre Auditoren in regelmäßigen Abständen durch einen weiteren Auditor des gleichen Normgebietes und ggf. mit der entsprechenden Branchenkenntnis in einem Zertifizierungsaudit überprüfen lassen. Dabei fertigt der prüfende Auditor über seinen Auditorenkollegen/in auf Grundlage des Verfahrens und der Formvorgaben der jeweiligen Zertifizierungsstelle einen Bericht an. Die Berichte werden in der Zertifizierungsstelle gegenprüft und archiviert. In den Geschäftsstellen-Audits durch die DAkkS werden diese durch die Begutachter der DAkkS stichprobenhaft geprüft und im Bedarfsfall mit dem Leiter der Zertifizierungsstelle besprochen.

Das Unternehmen

Wichtig ist selbstbewusstes Auftreten, nicht arrogant und nicht rechthaberisch. Das Unternehmen entscheidet über die getroffenen Maßnahmen und begründet diese. Die Begründung muss Normkonform sein und die Risiken müssen dokumentiert bewertet worden sein. Die im Auditprozess involvierten Mitarbeiter müssen „sattelfest“ sein, in dem was sie tun, in dem wie es dokumentiert ist und in dem was die Norm fordert. Der Auditor entscheidet nicht über die Korrektheit der Maßnahmen, er schaut, ob diese normkonform, plausibel, durchführbar, praktikabel, zukunftsorientiert und vor allem wirksam sind.

Der Berater

Die Auswahl des Beraters ist wohl eine der schwierigsten Disziplinen in der gesamten Normumsetzung – könnte man doch nur vorher erkennen, wer der Richtige ist. Doch es gibt ihn nicht, auch Berater sind wie Auditoren und Begutachter Menschen und haben ihre Stärken, Schwächen, Vorlieben und Abneigungen. Wichtige Merkmale sind Erfahrung des Beraters in der Management-Beratung zum geforderten Management-System sowie Branchenkenntnis und bestenfalls auch Erfahrung als Auditor[9].

Der Berater sollte beim Audit dabei sein, vor allem beim Stufe 2 Audit (gemeinsam mit der Geschäftsführung). Während des Audits darf der Berater maßvoll und angemessen unterstützen. Wichtig: Es ist ein Management-System und auditiert wird das Unternehmen. Also müssen die Mitarbeiter (auch Manager, Geschäftsführer und Vorstände sind Mitarbeiter des Unternehmens), die das Management-System des Unternehmens betreiben, die Fragen beantworten. Die Antworten müssen von den jeweiligen Fachverantwortlichen kommen. Es wird schnell eng, wenn der Berater übermäßig antwortet, in das Audit eingreift oder womöglich den Auditor maßregelt. Hier reagieren Auditoren menschlich, jeder auf seine Art und Weise, jeder in seinem eigenen Stil. Da das Unternehmen das Ansinnen hat, das Audit erfolgreich zu durchlaufen, geht man hier sinnvollerweise diplomatisch vor, z. B. mit der Frage „Wo in der Norm steht das?“ Kommunikationskultur spielt hier eine wichtige Rolle, anhören, ausreden lassen, Fragen stellen. Hat man das Gefühl festgefahren zu sein, kann man auch um eine kurze (angemessene) Beratungspause bitten, um sich intern zu der Fragestellung oder dem Diskussionspunkt abzustimmen. Formal ist das keine Auditzeit, d. h. es gibt dafür „Nachspielzeit“.

Der auditierte Geltungsbereich

Man unterscheidet zwischen dem Geltungsbereich des Management-Systems und dem Geltungsbereich für die Zertifizierung, also der Bereich, der auf dem Zertifikat beschrieben/aufgeführt ist. Sinnvoller Weise gilt das Management-System, in vorliegenden Fall ISO 27001 (IT-Sicherheitskatalog), für das gesamte Unternehmen. Den Scope für den zu zertifizierenden Bereich legt man zunächst auf ein gefordertes Mindestmaß fest. Dies ermöglicht es,

---

[9] Die Bezeichnung Auditor kann durch Schulung und erfolgreiche Prüfung erlangt werden. Für die Durchführung von Audits sind weitere Schritte notwendig, für die Durchführung von Audits für DAkkS-akkreditierte Zertifizierungsstellen ist das Durchlaufen des Traineeprogrammes und die Akkreditierung des Auditors für jeden einzelnen Normbereich notwendig sowie ggf. weitere Schulungen und Prüfungen.

die reine Auditierung im ersten Schritt möglichst klein zu halten. Später kann man das Zertifikat auf weitere Geltungsbereiche sukzessive ausweiten, bis das ganze Unternehmen zertifiziert ist.

Es wird dringend empfohlen, in einem Unternehmen oder Unternehmensgefüge (Konzern) nur ein einheitliches Informationssicherheits-Management-System (gilt auch für andere Management-Systeme gleichermaßen) einzuführen. Dabei ist es unbenommen, wenn Unternehmenseinheiten mit speziellen branchenspezifischen Anforderungen, Ergänzungen oder Ausschlüsse zu dem unternehmens-/konzernweiten Informationssicherheits-Management-System vornehmen. Diese sind schriftlich zu dokumentieren und von der jeweiligen Geschäftsführung für verbindlich zu erklären.

Die Festlegung des zu zertifizierenden Bereiches erfolgt durch das Unternehmen selbst. Die beauftragte Zertifizierungsstelle überprüft die Scope-Festlegung auf Basis der gültigen Normen und unter Hinzuziehung eines fachkundigen Auditors, in vorliegendem Fall eines berufenen Auditors und Fachexperten für IT-Sicherheitskatalog und ISO 27001 (in einer oder auch mehreren Personen). Beim „Scope schneiden“ ist zu beachten, dass es sich um wesentliche, für die Geschäftserbringung notwendige Organisationseinheiten, Standorte und Prozesse/Verfahren handelt. Der Scope ist also organisatorisch und technisch zu betrachten, wobei der Schwerpunkt die Organisation ist, denn es handelt sich um ein Management-System. Dies ist auch die Basis für die Prüfung durch die Zertifizierungsstelle. Erscheint den prüfenden Personen der Geltungsbereich als unschlüssig, so wird im Allgemeinen Rücksprache genommen und in gemeinsamer Abstimmung der Scope ggf. verändert. Auf dieser Basis erfolgt die Angebotsstellung für das Zertifizierungsaudit.

Das interne Audit

Die ISO 27001 schreibt im normativen Teil unter Kapitel 9.2 „Internes Audit“ die Durchführung eines internen Audits vor. „Intern“ bedeutet dabei, dass es sich nicht um ein Audit im Rahmen der Zertifizierungsaudit handelt, sondern um ein durch das Unternehmen in Eigenregie organisiertes Audit. Da ein in der Auditierung unerfahrenes Unternehmen schwer die Anforderungen der Norm erfüllen kann, muss sichergestellt sein, dass das Unternehmen selber einen fachkundigen und personenzertifizierten Mitarbeiter zur Verfügung hat, der das interne Audit durchführen kann. Hier werden auch Berater mit entsprechender Zertifizierung zur Durchführung des internen Audits beauftragt. Diese können auch von dem mit dem Einführungsprojekt beauftragen Beratungsunternehmen oder einem anderen Beratungshaus sein. Wichtig dabei ist, dass die Objektivität und Unabhängigkeit sichergestellt ist.

Wichtig ist aber an dieser Stelle, dass durch das interne Audit und zwar vor dem Stage 1, vgl. nachfolgend, die gesamten Controls des Anhangs A der ISO 27001 einmal durchgeprüft wurden. Es ist nicht zwingend erforderlich die Controls alle innerhalb eines Audits durchzuprüfen. Es ist aber sicherzustellen, dass sie vor dem weiteren Verfahren alle einmal durchgeprüft worden sind.

Innerhalb des auf das Erstzertifizierungsaudit folgenden Zertifizierungszyklusses ist es erst wieder zum Rezertifizierungsaudit, entsprechend im dritten Jahr nach der Erstzertifizierung, notwendig, die erneute vollumfängliche Prüfung des Anhanges A nachzuweisen.

Das Voraudit

Das optionale Voraudit ist ein Audit, in dem die Zertifizierungsreife des Unternehmens festgestellt wird. Das Voraudit an sich ist kein Bestandteil des regulären Zertifizierungsverfahrens. Der Ablauf des Voraudits ist in den Verfahrensbeschreibungen der jeweiligen Zertifizierungsstelle beschrieben. Grundsätzlich kann ein Voraudit empfohlen werden, denn es gibt insbesondere dem auditierten Unternehmen die Möglichkeit, einen „Trockenlauf“ vor dem Zertifizierungsaudit durchzuführen und auch ein Gefühl für die Schwerpunkte der Prüfung an sich zu bekommen. Darüber hinaus lernt man Auditor und Regularien der Zertifizierungsstelle kennen und kann sich natürlich auch mit dem Auditor im zugelassenen Rahmen austauschen.

Detailanalyse zur Auditierung und Zertifizierung

Das Erstzertifizierungsaudit

Die Verfahren für die Durchführung der Erstzertifizierung sind in der dazugehörigen Norm[10] und den Verfahrensanweisungen der jeweiligen Zertifizierungsstelle beschrieben. Im Letzteren gibt es Unterschiede, die meist formaler Natur innerhalb der Zertifizierungsstelle sind. Dazu gehören der Umgang mit den Unterlagen, wie Beauftragungen zu erfolgen haben, welche Bestätigungen benötigt werden und vor allem der Prüfkatalog. Der Prüfkatalog wird auf Basis der zu zertifizierenden Norm von der Zertifizierungsstelle erstellt und im Rahmen der Begutachtung durch die DAkkS abgenommen. Der Prüfkatalog für den IT-Sicherheitskatalog umfasst also inhaltlich immer die DIN ISO/IEC 27001, die ISO/IEC TR 27019 und die Anforderungen aus dem Konformitätsbewertungsprogramm der BNetzA. In den Abläufen der Prüfung und dem Umgang der inhaltlichen Fragen bestehen Unterschiede. Die Auditzeiten sind in der ISO 27006 und dem Konformitätsbewertungsprogramm des IT-Sicherheitskataloges geregelt und berechnen sich an der Anzahl der Mitarbeiter im Zertifizierungsbereich (Scope), Anzahl der Standorte und der (nicht) dauerhaft besetzten Betriebsstätten sowie Komplexität und weiteren Faktoren. Nicht zu den Auditzeiten zählen Pausen sowie Fahrzeit zwischen Standorten/Betriebsstätten. Das Erstzertifizierungsaudit besteht aus dem Audit Stufe 1 und dem Audit Stufe 2.

Das Stufe-1 Audit

Das Stufe 1 Audit dient überwiegend der Prüfung der Dokumente, Unterlagen, Verfahrensanweisungen etc. des zu zertifizierenden Unternehmens im Vorfeld zum Stufe 2 Audit und dem Kennenlernen der Gegebenheiten vor Ort. Im Stufe 1 Audit erfolgt die Überprüfung der Art und der Vollständigkeit der Dokumentation (digitale und Papierdokumente, Aufzeichnungen, interne Auditberichte, Pentest-Berichte etc.). Die Dokumentenprüfung erfolgt nicht komplett vor Ort. Es ist aber festgelegt, dass Teile des Audits der Stufe 1 vor Ort durchgeführt werden, um die Auditziele entsprechend prüfen zu können. Die Dauer der anzuwendenden Zeit ist festgelegt. Dies ergibt sich aus den Vorgaben der Zertifizierungsstelle und den normativen Vorgaben.

Bei der Bereitstellung der Dokumente durch das Unternehmen ist unbedingt die Vertraulichkeit der Informationen sicherzustellen. Der Austausch der Dokumente zwischen dem Unternehmen und der Zertifizierungsstelle muss auf einem gesicherten Weg erfolgen - also sicher nicht der einfache E-Mailverkehr, das wäre gleichbedeutend einer Postkarte. Die Dokumente könnten bspw. in gedruckter Form in einem verschlossenen Einwurfeinschreiben übersandt werden, das ist der altmodische Weg. Heute ist die Bereitstellung digitaler Dokumente üblich. Hierbei ist unbedingt zu beachten, dass die Übertragung verschlüsselt ist. Dies ist oft in Abhängigkeit mit der Zertifizierungsstelle zu regeln. So gibt es Zertifizierungsstellen, welche S/MIME-Verschlüsselung anbieten oder https-verschlüsselte Upload-Server (private Cloudspeicher) bereitstellen, auf die der Kunde exklusiven Zugang erhält. Das Unternehmen selbst kann natürlich auch verschlüsselte Downloadbereiche für die Auditoren bereitstellen oder den Versand in passwortgeschützten ZIP-Verzeichnissen vornehmen (hierzu sollte das dazugehörige Passwort auf anderem Weg bereitgestellt werden, z. B. SMS). Wichtig: Wenn Sie Ihre Dokumente „mal eben per Mail übersenden“ ohne diese nach Stand der Technik zu verschlüsseln, dann kommt der Auditor zum Stufe 1 Audit bereits mit einer Nichtkonformität ins Haus.

Die Vorbereitung des Auditors auf den Besuch vor Ort erfolgt anhand der vorab bereitgestellten Dokumente. Dabei ist eines der Kerndokumente die Anwendbarkeitserklärung (Statement of Applicability, SoA). Die Norm lässt hier Ausschlüsse (dazu weiter unten) zu. Diese müssen stichhaltig begründet werden. Der Auditor wird sich dieser Punkte als erstes und mit besonderer Hingabe widmen. Es besteht durchaus die Möglichkeit, keine Ausschlüsse zu definieren und stattdessen im Maßnahmenplan solche Controls aufzuführen, die für das Unternehmen derzeit nicht in Frage kommen. Beispiel: Sie haben keinen Anlieferungsbereich in ihrem Unternehmen. In Control A.11.1.6 (Anlieferungs- und Ladebereiche) lautet die Fragestellung, wie Sie diesen Bereich gegen unbefugten Zutritt absichern. Statt des Ausschlusses in der SoA definieren Sie im Maßnahmenplan eine regelmäßige (also mindestens jährliche) Prüfung, ob durch bauliche Änderung, Umzug, Neuanmietung etc. Liefer- oder Ladebereiche entstanden/geplant/gebaut wurden. Die Maßnahme definiert dabei im positiven Fall (Lieferbereich jetzt neu), dass die Maßnahmen aus dem Control der

[10] ISO/IEC 17021-1:2015-06 - Konformitätsbewertung - Anforderungen an Stellen, die Management-Systeme auditieren und zertifizieren - Teil 1: Anforderungen; ISO/IEC 17021-2:2016-12 - Konformitätsbewertung – Anforderungen an Stellen, die Management-Systeme auditieren und zertifizieren - Teil 2: Anforderungen an die Kompetenz für die Auditierung und Zertifizierung von Umwelt-Management-Systemen; ISO/IEC 17021-3:2017-03 - Teil 3: Anforderungen an die Kompetenz für die Auditierung und Zertifizierung von Qualitäts-Management-Systemen

Norm beschrieben, bewertet (Risiko), behandelt und überprüft werden. Das Stufe 1 Audit ist eine Konformitätsprüfung des Systems mit den Auditkriterien und eine Überprüfung der Plausibilität dieser.

Kleiner Tipp: Die SoA ist auch ein Kerndokument für den Auditor. Je besser und übersichtlicher dieses Dokument gestaltet ist, desto schneller findet sich der Auditor in ihrem Management-System zurecht.

Das Stufe-2 Audit

Das Stufe 2 Audit ist das alles Entscheidende. Und nun schon wieder: Wie machen Sie das? Wo steht das? Dann möchte ich das jetzt sehen. Und nun bitte noch einen Nachweis. Vielen Dank!

Ziel des Stufe 2 Audits ist es, die Umsetzung und Wirksamkeit des Management-Systems des Kunden / Unternehmens zu beurteilen. Das Stufe 2 Audit muss vollständig an dem bzw. den Standort(en) des Kunden stattfinden. Welche Standorte besucht werden, wird im Vorfeld durch den Auditplan festgelegt. Die Anzahl der zu begutachtenden Ort ist in der Norm bzw. dem Konformitätsbewertungsprogramm des IT-Sicherheitskataloges geregelt.

Auditierung beruht grundsätzlich auf einem Stichprobenverfahren und stellt hinsichtlich der zur Verfügung gestellten Informationen immer ein gewisses Unsicherheitselement in Bezug auf die Auditnachweise dar. Darüber müssen sich alle Beteiligten im Klaren sein, denn darauf werden die Auditergebnisse und die Schlussfolgerungen (Maßnahmen) getroffen. Das auditierte Unternehmen tut gut daran, sich seiner Verantwortung bewusst zu sein und im Rahmen des kontinuierlichen Verbesserungsprozesses alle Auditergebnisse zu verifizieren.

Der vom Auditor erstellte Auditplan enthält die zu prüfenden Management-Systemanforderungen, benennt die involvierten Organisationseinheiten / Abteilungen des Kunden / Unternehmens und betrachtet den Prüfpunkt. Der leitende Auditor hat stets den Auditplan im Auge und achtet auf das Zeit-Management. Entsprechend der ISO/IEC 17021-1:2015 kann das Audit neuerlich auch Aktivitäten des Remote Auditing beinhalten. Diese dürfen maximal 30 % der vorgegebenen Auditzeit betragen.

Wichtig: Das Unternehmen muss den Auditor in die Sicherheitshinweise des Unternehmens einweisen: Fluchtwege, Notrufnummern, Helmpflicht, Tragen von Arbeitsschuhen. Ist der Auditor nicht dafür gerüstet, kann das Unternehmen passende Arbeitskleidung bereitstellen. Dieser Punkt ist im Vorfeld zum Audit unbedingt zu klären, damit es nicht zu unerwarteten Verschiebungen in der Auditplanung kommt.

Nachdem das offizielle Eröffnungsgespräch erfolgt ist und das Audit offiziell vom leitenden Auditor eröffnet wurde, kommen auch schon die ersten Fragen zum normativen Teil des Management-Systems, den organisatorischen Faktoren.

In diesem Audit muss das Management und die oberste Leitung ihr Commitment zum Management-System und die Wahrnehmung ihrer Verantwortung deutlich aufzeigen und Geschäftsführer und zuständige Vorstände sind bei der Auditeröffnung und dem Auditabschluss anwesend. Führungskräfte mit Leitungsfunktion sind auch sonst gern gesehen, z. B. bei den täglichen Abschlussgesprächen.

Das eine Einladung in die Kantine zum Mittagessen oder Getränke nicht als Bestechung anzusehen sind, sondern zum guten Ton in einer Geschäftsbeziehung gehören, kann als gängige Praxis angesehen werden; aber: Fragen Sie den Auditor vorher, ob er sich in die Kantine einladen lässt und akzeptieren Sie seine Entscheidung.

Im Vorfeld zum Audit sind die Kommunikationskanäle und die Sprache zu klären, denn direkte und sofortige Kommunikation zwischen Auditierten und Auditor bei Feststellungen tragen erheblich zur Transparenz des Audits bei und vermeiden Missverständnisse im Nachgang.

Im Vor-Ort-Audit, das auch als Zertifizierungsaudit bezeichnet wird, prüft der Auditor mit geeigneten Mitteln (einer Checkliste, einem Prüfkatalog, seinem Wissen, seiner Erfahrung) die Konformität (oder Nichtkonformität) des vorliegenden aktuellen Prüfkataloges der Norm, in unserem Fall des IT-Sicherheitskatalogs mit dem umfangreichen Teil der DIN ISO/IEC 27001 und der sektorspezifischen ISO/IEC TR 27019. Die Durchführungszeit ist in der jeweiligen Prüfungsordnung zum Zertifikat geregelt (siehe auch Stufe 1).

Die Fragen der Checkliste sind als geschlossene Fragen formuliert, sodass sie mit „ja“ oder „nein“ beantwortet werden. Wobei "ja" für "konform" und "nein" für "nicht konform" anzusehen sind.

Dabei ist die Nachvollziehbarkeit zu beachten: diese entspricht weitgehend der gesetzlichen Rechenschaftspflicht der Datenschutzgrundverordnung (Koreng und Lachenmann 2018). Dies ist der Nachweis, dass eine Auditfrage durch Dokumente oder Sichtprüfung vor Ort erfüllt wurde.

- MUSS = Diese Anforderung ist immer zu erfüllen.
- SOLL = Diese Anforderung sollte erfüllt werden können, wenn das Unternehmen durch Mittel und Ressourcen dazu in der Lage ist, einfach ausgedrückt: Sollte ist müssen, wenn man kann.
- KANN = Diese Anforderung muss nicht zwangsläufig erfüllt sein. Ihre Erfüllung wirkt sich jedoch positiv auf die Gesamtbeurteilung aus.

Man unterscheidet zwischen diesen drei Kriterien, da nicht immer alle Anforderungen von allen Unternehmensgrößen im Sinne der Wahrung der Verhältnismäßigkeit erfüllt werden können.

Im Auditablauf der Erstzertifizierung nimmt sich das Auditteam zunächst des Management-Systems an. Wie funktioniert das System, sind die Führungskräfte in ihrer Vorbildfunktion sichtbar und unterstützen das System? In der Folge kommt man zu den Maßnahmen, die das Unternehmen zur Umsetzung und Aufrechterhaltung des ISMS und den Anforderungen des IT-Sicherheitskatalog implementiert hat und wie die Umsetzung zu den bereits in Stufe 1 geprüften Leitlinien, Konzepten, Richtlinien, Prozessbeschreibungen und Arbeitsanweisungen passt. Es folgen die Begehungen, um sich ein Gesamtbild des Zusammenspiels zwischen „Theorie“ (Beschreibungen der Mitarbeiter und der vorliegenden Dokumentation) und der „Praxis“ (Umsetzung und gelebte Praxis) zu machen. Es empfiehlt sich für die auditierten Unternehmen, immer bei Darstellung und Beschreibung an der Realität und Wahrheit zu bleiben. Die Norm will das Unternehmen nicht umbauen, das Unternehmen muss wissen, was es tut. Und wenn das Unternehmen dem Auditor stichhaltig nachweisen kann, dass die implementierten und umgesetzten Maßnahmen aus Sicht des Unternehmens und unter Heranziehung der Risikobewertung die derzeit beste und sinnvollste Maßnahme darstellen, ist daran nur wenig zu kritisieren, trotzdem gilt: Verbesserungen gibt es immer, diesen muss man sich annehmen.

Mit der Einführung der ISO/IEC 17021-1:2015 wurde das bisherige Wording Haupt- und Nebenabweichung (allgemeine Bezeichnung) verändert:

- Wesentliche Nichtkonformität = Haupt-Nichtkonformität
- Untergeordnete Nichtkonformität = Neben-Nichtkonformität

Es gilt also zu beachten, ob die Fähigkeit des Management-Systems, die beabsichtigten Ergebnisse zu erreichen, derart durch die festgestellte wesentliche Nichtkonformität beeinträchtigt ist, dass erhebliche Zweifel daran bestehen, dass eine wirksame Prozesslenkung besteht. Dabei können aber auch mehrere Neben-Nichtkonformitäten (siehe nachfolgend), die sich auf dieselbe Anforderung beziehen, eine Haupt-Nichtkonformität ergeben. Das Unternehmen ist bei derartigen Nichtkonformitäten aufgefordert, Ursachenanalysen durchzuführen. Es müssen Korrekturen und Korrekturmaßnahmen unter Beachtung von Fristen festgelegt, dokumentiert und umgesetzt werden. Die durchgeführten Ursachenanalysen und die festgelegten Korrekturen und Korrekturmaßnahmen sowie deren Wirksamkeit, müssen innerhalb der im Audit festgelegten Zeiträume in der Zertifizierungsstelle vorliegen sowie von ihr bewertet, angenommen und (durch einen Auditor) verifiziert worden sein.

Eine wesentliche Nichtkonformität kann auch zu einem Abbruch des Audits durch den Auditor führen, muss es aber nicht – seien Sie in solchen Stellen kooperativ und suchen Sie gemeinsam mit den Anwesenden (im Rahmen des Erlaubten wird auch das Auditteam lösungsorientiert sein) nach Lösungsmöglichkeiten - mangelnde Kooperation seitens des Auditierten ist hier eher kontraproduktiv.

Bei der untergeordneten Nichtkonformität ist die Fähigkeit des Management-Systems als Ganzes, die beabsichtigten Ergebnisse zu erreichen, nicht derart beeinträchtigt wie bei der wesentlichen Nichtkonformität, aber es wird eine einzelne Anforderung nicht erfüllt. Auch hier müssen Ursachenanalysen durchgeführt und Korrekturmaßnahmen unter Beachtung von Fristen festgelegt, dokumentiert und umgesetzt werden. Auch hier obliegt die Bewertung der eingereichten Korrekturen der Zertifizierungsstelle (siehe zuvor).

Nachaudit

Ein Nachaudit kann vom Auditor festgelegt werden, sofern Abweichungen im Audit festgestellt wurden, die das System (und damit das Zertifikat) in Frage stellen. Das Unternehmen bekommt eine angemessene Zeit, um Korrekturmaßnahmen umzusetzen, die dann im Nachaudit auf ihre Wirksamkeit geprüft werden.

Überwachungsaudit

Entsprechend den Regelungen der Zertifizierungsstelle für eine bestimmte Zertifizierung erfolgt ein Überwachungsaudit in dem festgestellt werden muss, ob die Zertifizierung weiter aufrechterhalten werden kann, in der Regel vor Ablauf eines Jahres nach dem vorangegangenen externen Audit.

Wiederholungsaudit / Rezertifizierungsaudit

Entsprechend den Regelungen der Zertifizierungsstelle für eine bestimmte Zertifizierung erfolgt ein Wiederholungsaudit vor Ablauf des Zertifikates, in der Regel vor Ablauf des dritten Jahres nach einem Erst- oder Rezertifizierungsaudit.

Das Unternehmen tut also gut daran, sich umgehend nach den Audits immer um die weitere Fortführung und Verbesserung des Management-Systems zu kümmern. Das ist deutlich entspannter, als wenige Wochen vor dem Überwachungsaudit mit der Umsetzung der Maßnahmen zu beginnen. Erfahrungsgemäß ist dies ein Lernprozess im Unternehmen, der sich mit jedem weiteren Audit verbessert und schließlich auch zu den von der Norm gewünschten Effekten innerhalb der Organisation führt: das lernende Unternehmen.

Tipps für das Audit

Der Auditor darf bei der Durchführung des Audits nicht in das Unternehmensgeschehen eingreifen oder dieses durch sein Verhalten beeinflussen. „Und wenn ich jetzt diesen Knopf drücke, funktioniert alles wie hier dokumentiert?!“ Hände weg! Der Auditor kann in die Haftung oder Schadenersatzpflicht kommen. Und auch dies wäre ein unzulässiger Eingriff: „Wenn diese Frage nur von Mitarbeiter Meyer beantwortet werden kann, dann muss er sofort hier erscheinen!“ „Nein, kann er nicht, Ihre Forderung kann den Betrieb des Unternehmens stören! Wollen Sie das?“ Gemach, gehen Sie die Dinge ruhig an. Suchen Sie Lösungsmöglichkeiten und beraten Sie in einer kurzen Pause, ob ein adäquater Vertreter des so vehement geforderten Kollegen die Fragen des Auditors beantworten kann oder vertagen Sie das Thema auf den Nachmittag oder den Folgetag.

Der Auditor darf zwar in die Personalabteilung gehen und sich z. B. Vertraulichkeitsvereinbarungen oder Fortbildungsnachweise im Rahmen der Norm anschauen, er darf aber keine Gehaltsdaten oder Krankendaten einsehen. Er darf vor allem nicht einfach in die Personalakten greifen, nach dem Motto: Mal sehen, wen wir ziehen. Gehen Sie als Geprüfter bei solchen Anfragen wie folgt vor: Bei digitalem Zugriff auf Personaldaten, erst das Dokument aufrufen und dann den Monitor zur Ansicht dem Auditor freigeben! Auditoren sind auch nur Menschen, deshalb können auch sie in Gedanken schon mal unbeabsichtigt vorpreschen. Freundliche, klare Ansagen verdeutlichen die Souveränität mit dem entsprechenden Prozess.

In Auditsituationen neigen Mitarbeiter des Kunden mitunter dazu, in der Ausformulierung der Vorgehensweise zu schwelgen und eventuell sogar den Pfad der Realität zu verlassen. Die Mitarbeiter sollten vor dem Audit deshalb auf die Nachvollziehbarkeit der Nachweise, Belege und Umsetzungsdokumentationen fokussiert werden. Besser nicht zu viel Prosa erzählen, bei den Tatsachen und Dokumenten bleiben, Auditor fragen lassen und angemessene kurze und klare Antworten geben.

Und immer ehrlich antworten, auch wenn das möglicherweise eine Abweichung wird: das schafft Vertrauen und kommt bei den meisten erfahrenen Auditoren gut an, denn man kennt sich aus und weiß, wo es weh tut.

Grundlage des prozessorientierten Audits ist eine Checkliste mit Fragen und / oder Prüfpunkten. Die Fragen für die Checkliste ergeben sich aus Vorgaben, die für den Prozess notwendig sind. Dazu zählen beispielsweise Prozess-und Funktionsbeschreibungen sowie Verfahrens- und Arbeitsanweisungen.

Ausschluss von A.14.1.3 Schutz der Transaktionen bei Anwendungsdiensten: Hierbei handelt es sich nicht um Banktransaktionen, Überweisungen oder ähnliches: dies ist eine allgemeine Formulierung. Der Ausschluss ist schwierig, denn seit über 20 Jahren haben alle Datenbanken eine transaktionsbasierte Speicherung (alle Änderungen werden zuerst in die Log-Dateien geschrieben, dann in die Datenbankdatei). Es handelt sich also um eine Technologie

nach Stand der Technik, die in allen datenbankbasierten Standardsoftwareprodukten Anwendung findet und möglicherweise auch in anderen Anwendungen, also noch mal genau drüber nachdenken.

A.18.1.5 Regelungen bezüglich kryptographischer Maßnahmen: Lässt sich überhaupt nicht ausschließen, denn zum einen findet Verschlüsselung nach dem Stand der Technik in jedem Verzeichnisdienst (z. B. Active Directory) und bei jeder VPN-Verbindung (oder https-Verbindung) statt. Zum anderen ist Verschlüsselung gesetzlich bei der Übermittlung personenbezogener Daten vorgeschrieben. Dies ist aktuell in der Datenschutzgrundverordnung Art. 32 Abs. 1 lit. a DS-GVO, übrigens vorher ebenfalls gesetzlich vorgeschrieben gewesen, in Anlage zu § 9 S. 2 Nr. 2 bis 4 BDSG a.F. und eine Normanforderung aus A.18 Compliance.

Schlusswort

Normen haben sich aus Best Practices entwickelt und stellen somit eine ausgereifte und sichere Methodik und Verfahrensweise dar, die als etabliert und nachhaltig angesehen werden muss. Stellt sich ein Unternehmen normkonform auf, so heißt dies nicht, dass man die bisherige gelebte Praxis abschaffen und alles ändern muss. Normative Vorgaben sind eine Orientierung, um die bisherige Vorgehensweise zu verbessern und nachhaltig durchzuführen. Das geht nur mit angemessener Dokumentation und Schulung der Mitarbeiter. Dabei sind Normen für Management-Systeme stets vordergründig prozessorientiert und nachrangig technisch unterstützt und umgesetzt. Bereits bei einer Erstzertifizierung stellt sich dies positiv dar, denn die Mitarbeiter bekommen die notwendige Weitsicht durch die Prozesse, die durch das gesamte Unternehmen laufen und nicht an der „Abteilungsgrenze“ aufhören. Ein gesamtheitlicher Blick aller Mitarbeiter im Unternehmen führt zu strukturierten und effizienten Arbeitsweisen, die sich nachgewiesenermaßen positiv auf die zertifizierten Unternehmen auswirken, sobald man die ersten Jahre einer Zertifizierung durchlaufen hat. Eine Zertifizierung des Informationssicherheits-Managements reduziert deutlich die Risiken dieses Themenumfeldes, heißt aber nicht, dass es diese grundsätzlich verhindert. Das Unternehmen aber ist in der Lage, organisiert und strukturiert vorzugehen, da man proaktiv festgelegte Vorgehensweisen und Maßnahmen definiert und implementiert hat.

Dr. Joachim Müller

Leiter Business Area SECURITY der SEVEN PRINCIPLES AG

Akkreditierter Auditor für ISO 27001

Zur Person:

Dr. Joachim Müller ist als akkreditierter Auditor für ISO 27001, beurkundeter Lead-Auditor IT-Sicherheitskatalog (BNetzA) und TÜV-zertifizierte (TÜV InterCert GmbH – Group of TÜV Saarland) „Data Center Security“ für die Prüfung und Zertifizierung von Netzleitstellen und Kraftwerken im IT-Umfeld im Einsatz. Gemeinsam mit nationalen und internationalen Zertifizierungsstellen (DeuZert, TÜV InterCert SAAR; Fox-Certification) entwickelt er aktuelle und bedarfsgerechte Audit- und Prüfkataloge für offene Zertifizierungen. Er verantwortet als Head of Security die Informations- und IT-Sicherheit der SEVEN PRINCIPLES GROUP und führt als Chief Information Security Officer (CISO) die Informationssicherheit nach einer eigens entwickelten holistischen Methodik durch. Mit seinem Team aus langjährig erfahrenen Beratern werden Kunden bei der Einführung und Absicherung ihrer Unternehmen und Systeme beraten und auditiert. Die Verknüpfung von Großprojekten bekannter internationaler Unternehmen im Bereich ISO 27001 und Sarbanes Oxley (SOX) gehören ebenso zu seinem Wirkungskreis, wie auch die Durchführung von Due Diligence bei Merger and Acquisition Projekten. Als Dozent an der Steinbeis Hochschule Berlin (SMI) und der ADG Business School unterrichtet Herr Müller Studenten bei ihrem berufsbegleitenden Studiengang mit den Themen IT-Recht und Management betrieblicher Systeme.

** Dieser Beitrag von Dr. Joachim Müller wurde anlässlich des VDE Jahresforums für Technische Führungskräfte und TSM-Verantwortliche in der Energieversorgung vom 19. bis 20. Juni 2018 in Offenbach/M. erstellt.*

6.2 Erfahrungen der befragten Unternehmen mit der Auditierung

Ausgehend von der Vorläuferstudie im Jahr 2016 zeigt sich, dass der Anteil der zertifizierten Energieversorgungsunternehmen deutlich gestiegen ist. Im Jahr 2016 waren vom befragten Sample mit eingeführtem ISMS lediglich ca. 30 % zertifiziert. Im gegenwärtigen Sample haben sich 100 % der befragten Unternehmen mit bereits eingeführtem ISMS der Zertifizierung gestellt.

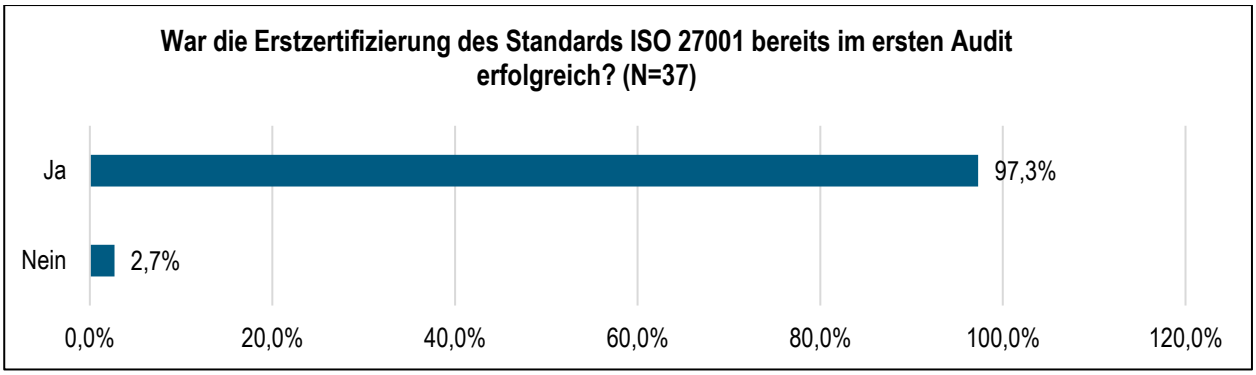


Abbildung 27: War die Erstzertifizierung bereits im ersten Durchlauf erfolgreich?

Wie die Ergebnisse zeigen, war die Erstzertifizierung bereits zu mehrheitlichen Teilen beim ersten Audit erfolgreich. In Bezug auf Herausforderungen und Probleme im Audit gaben 59,5 % der Unternehmen an, dass keine Probleme aufgetreten sind. Bei 32,4 % der befragten Unternehmen ergaben sich vor allem Herausforderungen durch fehlende Ressourcen, sowohl zeitlich als auch personell sowie die fehlende Kompetenz des Auditors (13,5 %). Nur 8,1 % gaben an, mit Kommunikationsproblemen konfrontiert worden zu sein. Mehrfachantworten waren möglich. Generell war die Zufriedenheit mit dem Vorgehen des Auditors jedoch recht hoch.

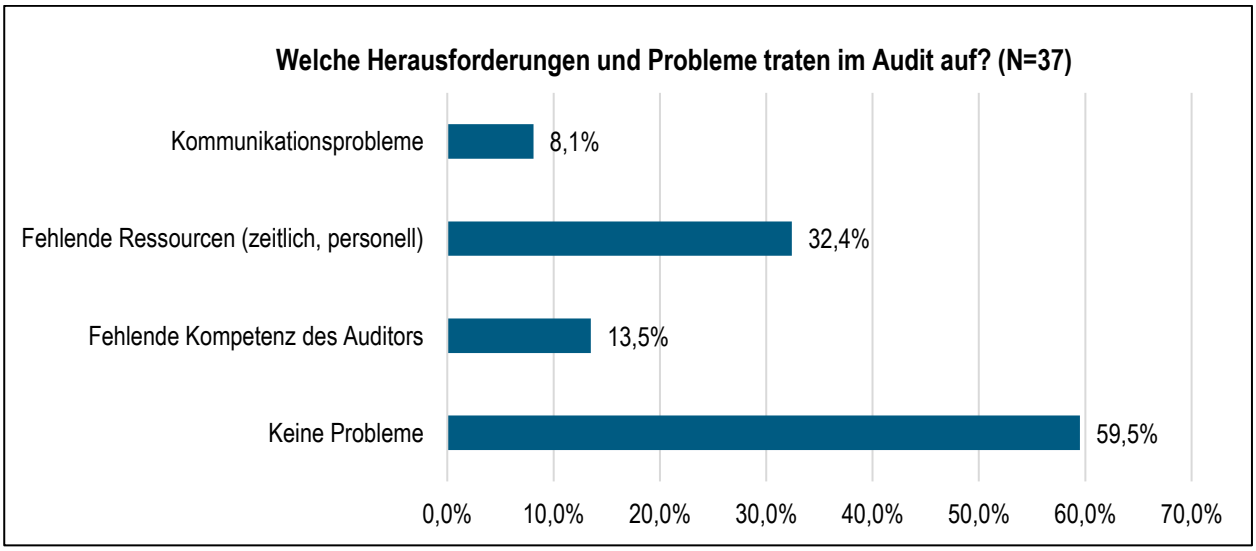


Abbildung 28: Herausforderungen und Probleme im Audit

(Mehrfachantworten möglich)

Insgesamt konnte jedoch ein zufriedenes Bild der Auditoren und deren Vorgehensweise aufgezeigt werden. In den einzelnen Phasen der Vorbereitung auf die Zertifizierung (Dry Run), der Abschätzung des Zertifizierungsbereiches und des Aufwands (Scoping) sowie der Analyse der Implementierung und des sich anschließenden Zertifizierungsprozesses konnten zufriedene bis sehr zufriedene Ergebnisse gesammelt werden.

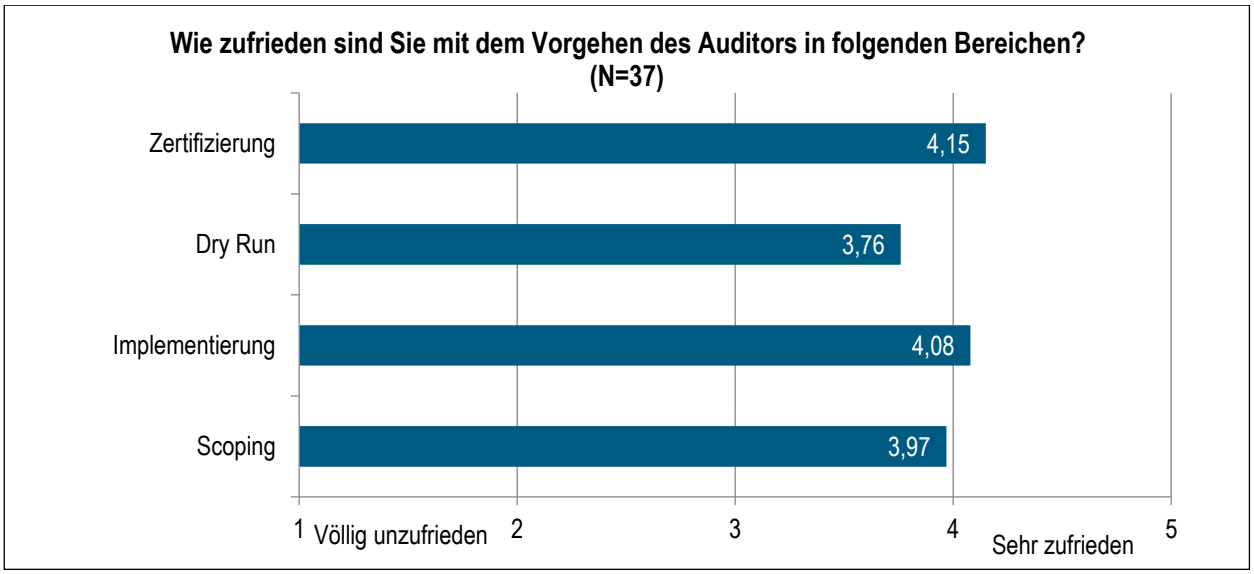


Abbildung 29: Zufriedenheit mit dem Vorgehen des Auditors

Dies steht in Korrelation mit der Kommunikation zwischen dem Auditor und dem zu auditierenden Unternehmen. Insgesamt gaben 92 % der Unternehmen an, dass sie stetig über den Fortschritt und / oder Probleme während des Zertifizierungsaudits informiert wurden und somit in Interaktion mit dem Auditor standen.

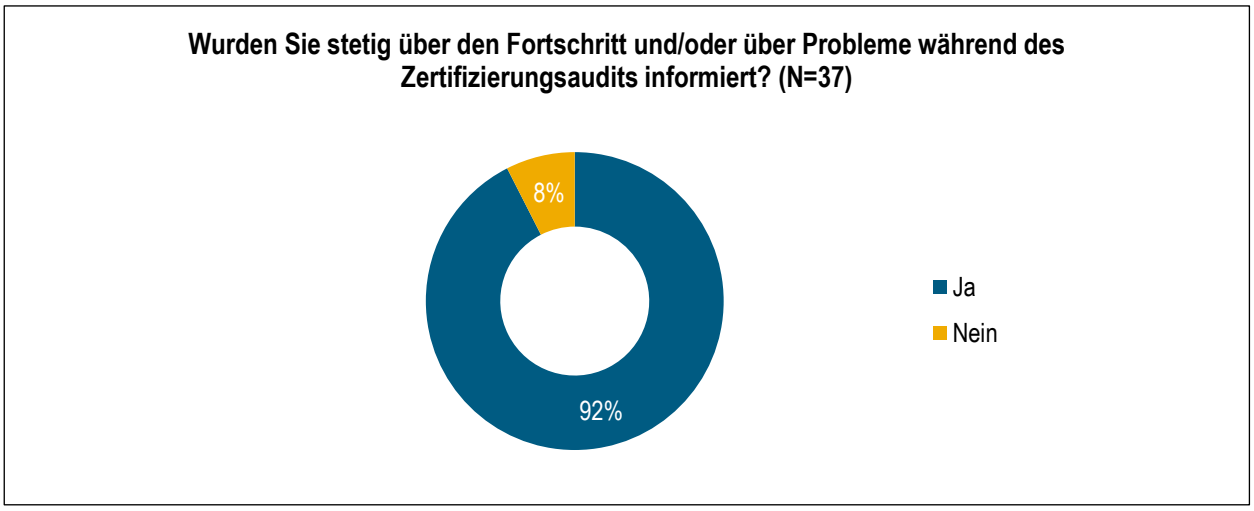


Abbildung 30: Kommunikation im Audit

Im Mittel wurde durch den Auditor eine Auditzeit von 11,5 Tagen geplant. Die tatsächliche Auditzeit wurde im Mittel mit 11,1 Tagen angegeben. Die Einhaltung der Zeitplanung durch den Auditor stellt für die befragten Unternehmen eine am wenigsten wichtige Eigenschaft des Auditors dar. Viel wichtiger sind die Eigenschaften der Unparteilichkeit und Objektivität sowie die Nachvollziehbarkeit der Schlussfolgerungen des Auditors als wichtigste Eigenschaft. Dies deutet auf eine nicht zu unterschätzende Problemstellung in der Praxis hin, da Abbildung 28 die fehlende Kompetenz des Auditors als Problemstellung aufzeigt. Nachfolgende Abbildung zeigt ergänzend, dass 11 % der Probanden die Einschätzung der mangelnden Fach- und Sachkenntnis teilen.

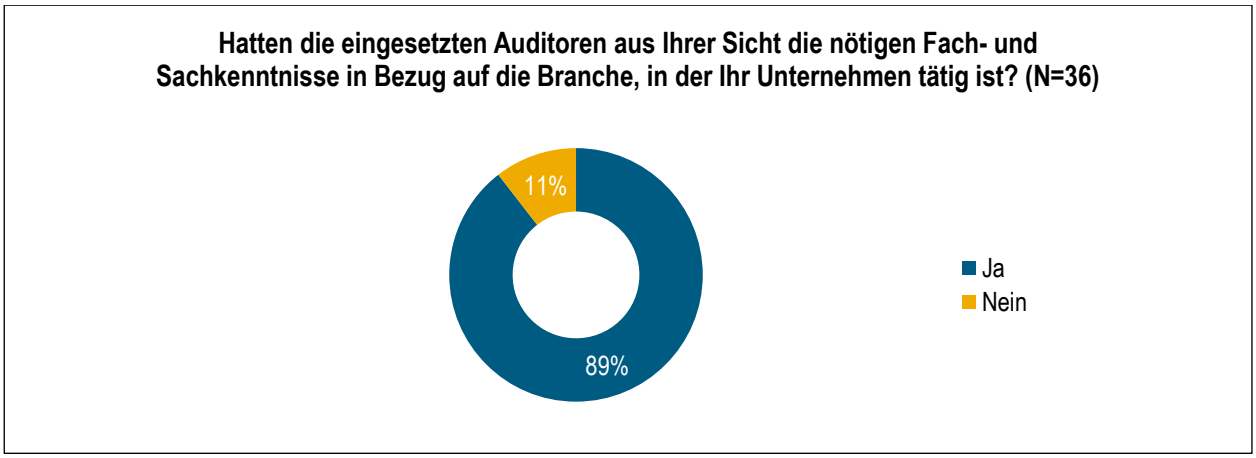


Abbildung 31: Einschätzung der Fach- und Sachkenntnisse der Auditoren

Einen Überblick zu den positiven und negativen Erfahrungen mit Auditoren im Kontext der ISO 27001 geben die nachfolgenden Tabellen:

Positive Erfahrungen mit dem Auditor
Der Auditor ist auf die integrierte Dokumentation eingegangen, obwohl ihm eine dezidierte besser gefallen hätte.
Aufzeigen von Lücken
Der Auditor ging pragmatisch und maßvoll ins Audit.
Der Auditor war ein Praktiker, konnte also durchaus die Verhältnismäßigkeit von Maßnahmen einschätzen.
Ehrliche, konstruktive Kritik mit Anregungen für den Verbesserungsprozess.
Eine Art von Ratgeber und Coach.
Eher praxisorientiert
Es werden Mehrwerte zur Verbesserung durch die Erfahrung und den externen Blick generiert.
Es wurde viel Wert auf Praktikabilität der von der Norm geforderten Maßnahmen gelegt.
Es wurden sehr detailliert alle möglichen Gefahrenpotenziale durchgegangen.
Externe Sicht auf unsere Abläufe
Fachkompetenter Blick von extern auf das eigene Unternehmen, konstruktiver Dialog.
Fachkunde des Auditors
Für unseren langjährigen Auditor ist es auch ein willkommener Informationsaustausch.
Sehr gute konkrete Hinweise bei der Umsetzung der ISO 27001 Maßnahmen.
Hilfestellung im Umgang mit dem ISMS
Hilfreiche Hinweise zur Verbesserung
Interesse am Unternehmen
Offene Diskussion über die "richtige" Auslegung von Normanforderungen.
Schärfung des Blicks auf scheinbar das Unwesentliche.
Strenge Vorgaben
Verständnis für die Größe des Unternehmens, im Verhältnis zu den geforderten Prozessen.
Von Anfang bis Ende war alles positiv.
Zu jedem Kritikpunkt eine Lösung vorgeschlagen

Tabelle 6: Positive Kommentare zur Umsetzung des Audits

Negative Erfahrungen mit dem Auditor
Die Aufforderung, verpflichtende Sicherheitsüberprüfungen durchzuführen und Führungszeugnisse einzufordern, obwohl dies nicht zulässig ist.
Hohe Auslastung der Auditoren, somit schwierige Terminfindung
Hoher Zeitaufwand
Persönliche Dissonanzen zwischen Auditor und Auditbeteiligten
Sehr theoretisch, praxisfremde Störszenarien, Kommunikation sehr normbezogen und theoretisch
Teilweise recht hohe Ansprüche
Termine wurden nicht eingehalten, Auditplan war so gut wie nicht vorhanden
Unerfahrenheit in der Umsetzung
Wir haben an einen Witness-Audit teilgenommen. Der Vertreter einer Akkreditierungsgesellschaft hat alles verkompliziert. Nie mehr freiwillig.
Witness-Audit - der Vertreter einer Akkreditierungsgesellschaft hat sich zu stark eingemischt.
Zu dem Zeitpunkt war das Thema IT-Sicherheitskatalog noch brandneu und noch nicht alles "klar"; das ist aber nicht dem Auditor anzukreiden.

Tabelle 7: Negative Kommentare zur Umsetzung des Audits

Wie sich innerhalb der Kommentare zeigt, ist das Thema der Witness-Audits interessant zu vertiefen und der Umgang mit Witness Auditoren zu hinterfragen. Die befragten Probanden gingen teilweise distanziert mit ihnen um. Statements wie „Diese muss man ignorieren. Keine Fragen zulassen“ und „Witness-Auditor [hat] zu stark in das Zertifizierungs-Audit eingegriffen“ weisen auf Problemstellungen in der Konstellation eines Witness-Audits hin. Ein Statement „[Die Teilnahme des Witness-Auditors] war kein Problem. Dieser nahm stillschweigend am Audit teil“ wurde ebenfalls benannt.

6.3 Nachbereitung der Auditergebnisse seitens der befragten Unternehmen

Mit Blick auf das Resultat des ersten Zertifizierungsaudits (vgl. Abbildung 27) sowie mit Blick auf den Anteil von festgestellten Hauptabweichungen in der nachfolgenden Abbildung zeigt sich, dass die befragten Unternehmen sehr gut vorbereitet in das Audit gegangen sind.

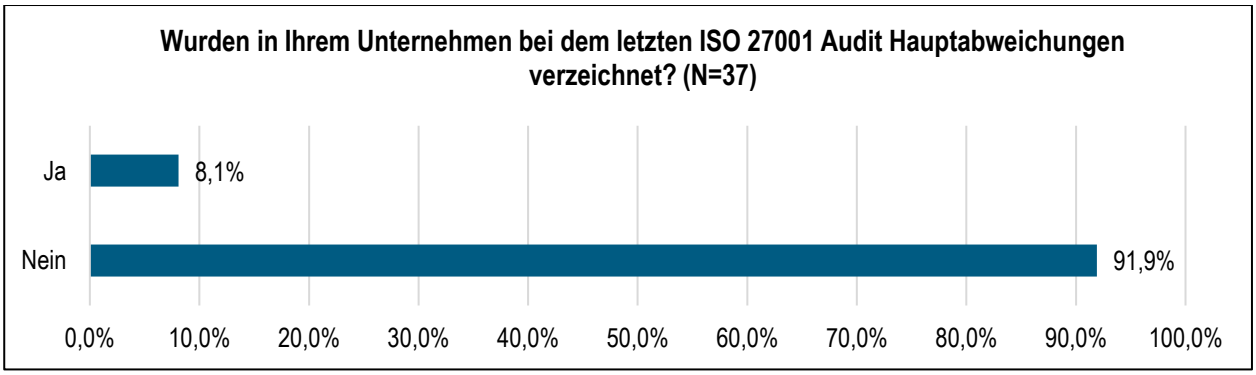


Abbildung 32: Wurden in Ihrem Unternehmen Hauptabweichungen verzeichnet?

Hauptabweichungen, welche im Audit verzeichnet wurden, betreffen a) die Verbesserung der End-Point-Security, b) den Detaillierungsgrad des Netzstrukturplans, c) eine nicht ausreichende Matrix der Norm-Controls zur Management-Dokumentation (zzgl. einer zu geringen Berücksichtigung der Norm-Controls bei integrierten internen Audits) sowie d) den Prozess des Notfall-Managements.

Nebenabweichungen wurden hierbei ebenfalls festgestellt. Diese lassen sich in folgende Ausführungen der Probanden auflisten:

- Business Continuity Management: Dokument erstellen, Verfahren festlegen
- Dokumentation verbessern
- Fehlende Dokumente, Formalien waren zu korrigieren, Ergänzungen und Erläuterungen ausführlicher darzustellen
- Härtung der Leitstellensoftware notwendig
- Lieferantenrichtlinien, Sicherheitsbereiche und Zutrittskontrolle
- Umsetzung des IT-Sicherheitsgesetzes beim internen Audit
- Verantwortlichkeiten waren nicht ausreichend den Assets zu geordnet
- Verbesserung einzelner Prozesse, einzelne Maßnahmen noch nicht komplett umgesetzt
- Verbesserungspotenzial beim Mapping von Assets und Risiken

Im allgemeinen zeigt sich, dass die Empfehlungen des Auditors zur Behebung von Haupt- und Nebenabweichungen umgesetzt werden. Dies zeigt sich auch in der nachfolgenden Abbildung zur Behebung der Nebenabweichungen mit den Empfehlungen des Auditors. Insgesamt mehr als 69 % der Befragten gaben an, dass für gewöhnlich oder immer allen Empfehlungen gefolgt wurde.

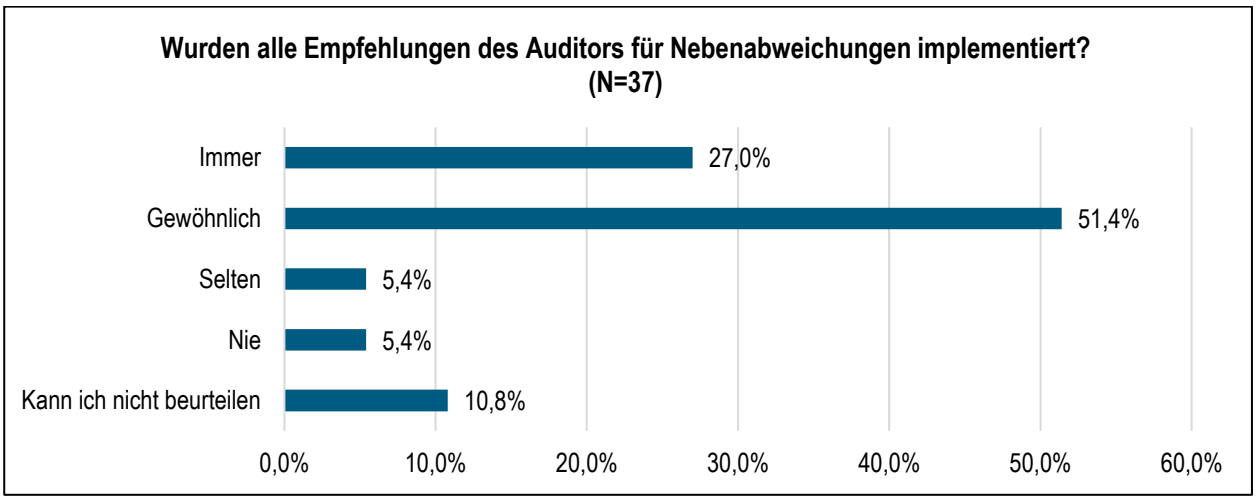


Abbildung 33: Wurden die Empfehlungen des Auditors für Nebenabweichungen implementiert?

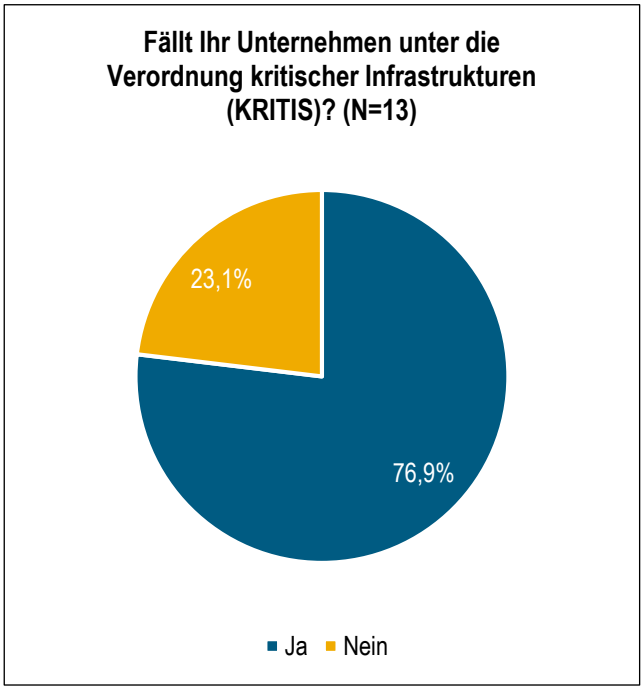
Im Mittel benötigten die Unternehmen 74,2 Tage, um Haupt- oder Nebenabweichungen zu beheben.

7 Gesonderte Betrachtung des Nahverkehrs (ÖPNV)

7.1 Unternehmensstruktur

Die nachfolgende Auswertung blickt insbesondere auf die befragten Unternehmen, welche den Nahverkehr als Branche angaben. Damit wird der Teil aus dem gesamten Sample im Details betrachtet und an ausgewählten Stellen Parallelen im Vergleich zum gesamten Sample gezogen. Die Auswertung der Unternehmen im Personennahverkehr umfasst in Summe 13 befragte Unternehmen. Es ist dabei anzumerken, dass im Sample kein reiner ÖPNV-Betrieb enthalten war und diese nach eigenen Angaben mindestens dem Verbund mit Strom und Gas angehören.

Diese fallen in der Gesamtbetrachtung nach eigener Klassifizierung zu 76,9 % unter die BSI-Kritisverordnung. Es ist davon auszugehen, dass das Verbundunternehmen damit unter die Verordnung zu kritischen Infrastrukturen zählt.



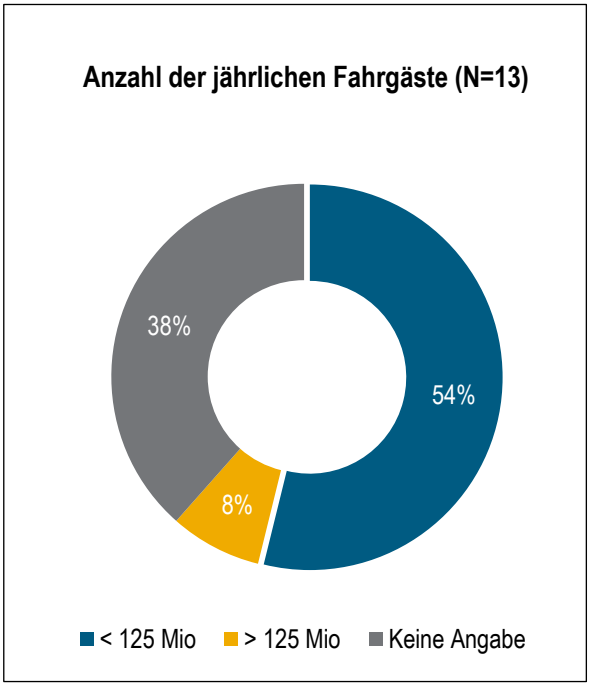


Abbildung 34: Zugehörigkeit als KRITIS

Betrachtet man den Bereich des Nahverkehrs in der BSI-Kritisverordnung nach 2. Korb genauer, lässt sich festhalten, dass ÖPNV-Betreiber mit mehr als 125 Mio. jährlichen Fahrgästen als KRITIS klassifiziert sind.

Schwellenwerte im öffentlichen Personennahverkehr. BSI-Kritisverordnung		
Schienennetz und Stellwerke des öffentlichen Straßenpersonenverkehrs (ÖSPV)	Anzahl Fahrgäste/Jahr	125 000 000
Verkehrssteuerungs- und Leitsystem des ÖPNV	Anzahl Fahrgäste/Jahr	125 000 000
Leitzentrale des ÖSPV (Betreiber, Verkehrsunternehmen)	Anzahl Fahrgäste/Jahr	125 000 000

Tabelle 8: Schwellenwerte zur Zuordnung in der BSI-Kritisverordnung für den Sektor ÖPNV

Quelle: Verordnung zur Bestimmung Kritischer Infrastrukturen nach dem BSI-Gesetz (BSI-Kritisverordnung - BSI-KritisV)

Lediglich 7,7 % der Befragten gaben in der direkten Abfrage an, mehr als 125 Mio. Fahrgäste pro Jahr tatsächlich zu befördern. Mit 38,5 % liegt die Anzahl der enthaltenen Angaben hierzu relativ hoch. Die restlichen 53,8 % der Befragten zählen nach den Kriterien der vorherigen Tabelle nicht als KRITIS. Damit zeigt sich, dass diese Unternehmen im Konzernverbund agieren und somit prinzipiell auf das Know-how innerhalb des Konzerns zurückgreifen können. Wie der Tabelle weiterhin zu entnehmen ist, stehen das Verkehrssteuerungs- und Leitsystem des ÖPNV sowie das Schienennetz und die Stellwerke des öffentlichen Straßenpersonenverkehrs (ÖSPV) im Fokus. Weiterhin geben 53,8 % der Unternehmen an, zwischen 50 und 250 Mitarbeiter zu beschäftigen. 46,2 % beschäftigen mehr als 250 Mitarbeiter. Zu dem Umsatz machten 38,4 % keine Angabe. Jeweils 23,1 % geben an, zwischen 10 Mio. und 50 Mio.

sowie über 50 Mio. EUR Umsatz zu erwirtschaften. Jeweils 7,5 % geben an, unter 2 Mio. EUR sowie zwischen 2 Mio. und 10 Mio. EUR Umsatz zu erwirtschaften. In Bezug auf die Bilanzsumme machten 61,5 % keine Angabe. Mehr als 50 Mio. EUR gaben 23,1 % an und jeweils 7,7 % gaben zwischen 2 Mio. und 10 Mio. EUR sowie zwischen 10 Mio. und 50 Mio. EUR an. Für die Einstufung als KRITIS ist dies jedoch unerheblich.

Mit Blick auf die erreichten Probanden zeigt sich, dass vorwiegend die Information Security Officer erreicht wurden. Von den Befragten im Bereich des Nahverkehrs geben 23,1 % an, als CISO tätig zu sein. Als ISO/ISB sind 46,2 % tätig. Als weitere Rolle bzw. mit keiner speziellen Rolle definiert sind jeweils 15,4 % der betrachteten Probanden. Eine weitere Rolle stellt hier bspw. der IT-Leiter dar.

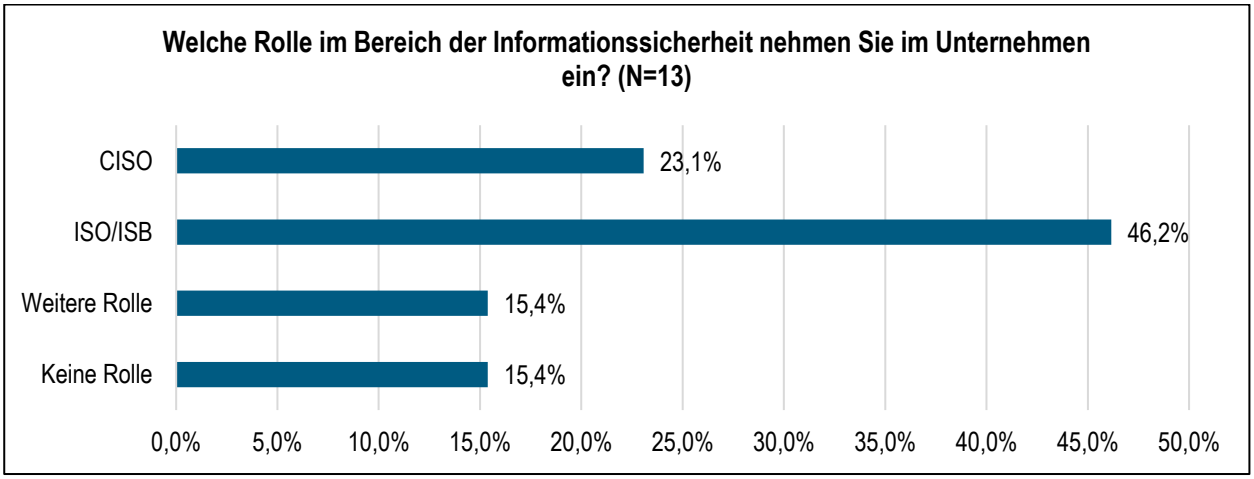


Abbildung 35 Rolle der Befragten in der Informationssicherheit - ÖPNV

Ein ISMS ist zu 92,3 % bereits in den betrachteten Unternehmen bzw. Konzernverbund vorhanden.

7.2 Motivation zum ISMS

Die Motivation zur Einführung eines ISMS entstammt zu 100 % aus der gesetzlichen Forderung. 92,3 % geben weiterhin an, dass die Steigerung der Informationssicherheit eine ausschlaggebende Motivation war. Es lässt sich festhalten, dass der aktuelle Trend der Sensibilisierung zur Informationssicherheit sowie die parallele gesetzliche Forderung zu einem ISMS scheinbar positiven Zusammenwirken führten. Ein ISMS als Forderung der Stakeholder wurde im Bereich den ÖPNV gar nicht geäußert. Interessante Aspekte zeigt hier jedoch auch die DS-GVO, welche von den Befragten zu 15,4 % als Grund für die Implementierung genannt wurde. Die DS-GVO verweist auf ein Datenschutz-Management-System und die technischen und organisatorischen Maßnahmen (TOMs) zeigen punktuelle Parallelen zu den Controls aus der bekannten ISO 27001. Daher scheint es sinnvoll, dies zu kombinieren.

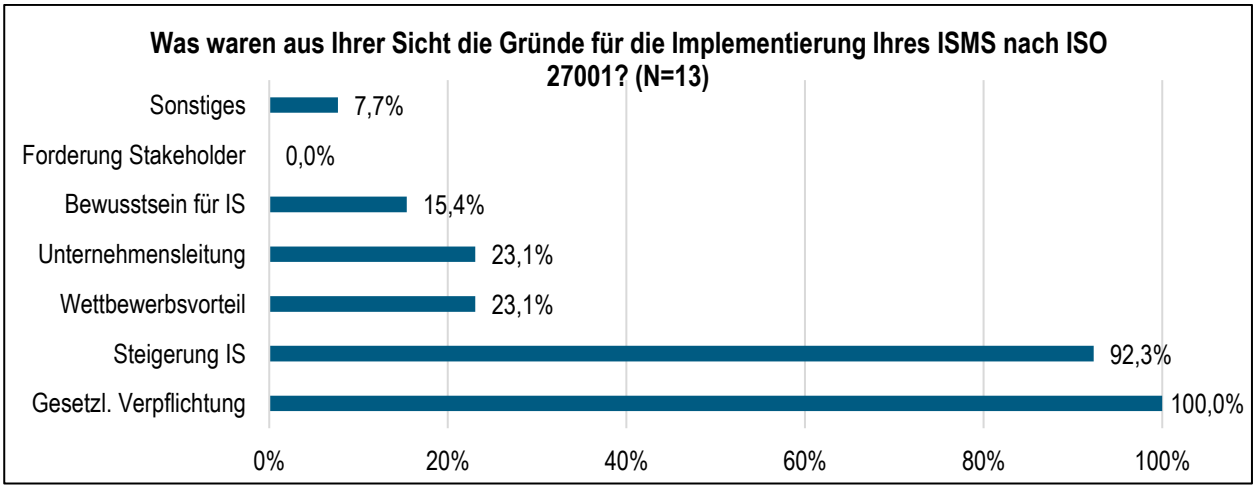


Abbildung 36: Gründe für die Implementierung eines ISMS

Dabei zeigt sich, dass das Thema Informationssicherheit, im Vergleich zum gesamten Sample (69 %), einen relativ hohen Stellenwert vor der ISMS-Einführung hatte. Es gaben 76,9 % der befragten Unternehmen mit ÖPNV-Aktivitäten

an, dass das Thema Informationssicherheit bereits einen hohen Stellenwert hatte. Einen beiläufigen Stellenwert räumten noch 23,1 % der Befragten ein. Kein Unternehmen mit ÖPNV-Bereich gab an, dass Informationssicherheit bisher keinen Stellenwert im Unternehmen hatte. Im gesamten Sample gaben dies 9,9 % der Unternehmen an.

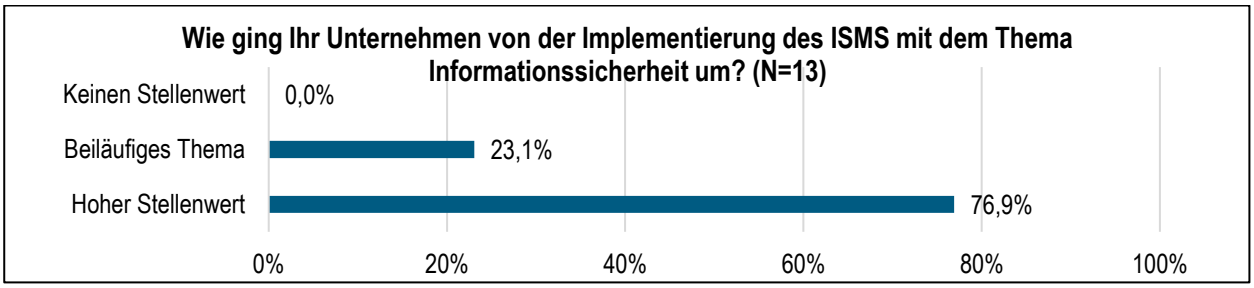


Abbildung 37: Stellenwert von Informationssicherheit vor der Implementierung des ISMS im ÖPNV

Als Treiber der Einführung wurde zu 84,6 % die Unternehmensleitung sowie der Beauftragte für Informationssicherheit genannt. Spezifische Mitarbeiter mit Fachwissen waren lediglich zu 15,4 % genannt. Dies ist ein wesentlicher Unterschied zum gesamten Sample, welches die Unternehmensleitung mit lediglich 62 % als Treiber des Themas angab. Mitarbeiter mit Fachwissen wurden im Vergleich beim gesamten Sample mit 21 % als treibende Kraft angegeben. Mehrfachnennungen waren möglich.

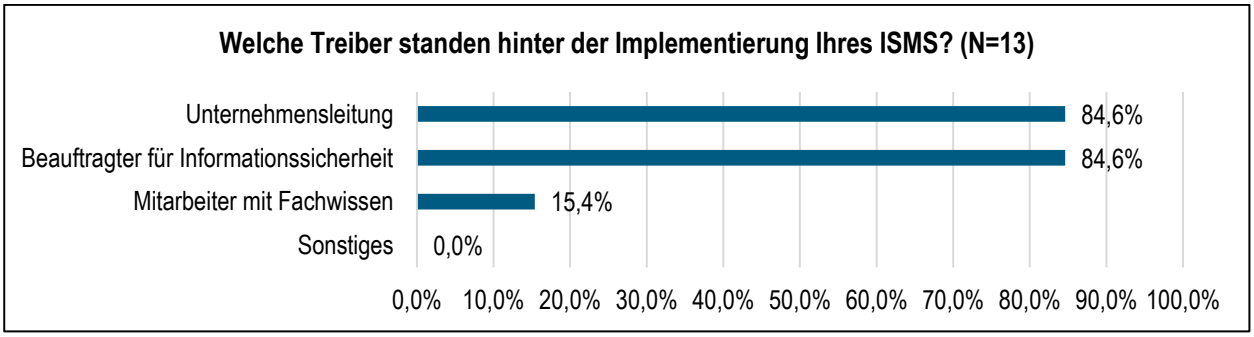


Abbildung 38: Welche Treiber standen hinter der Implementierung Ihres ISMS im Bereich ÖPNV?

(Mehrfachantworten möglich)

7.3 Unternehmens-eigener Umgang mit dem ISMS

Im Vergleich zur Gesamtbetrachtung der befragten Unternehmen der Energieversorgung zeigt sich, dass der Bereich des Nahverkehrs im Unternehmensverbund an dem generellen Geltungsbereich des Verbunds partizipiert.

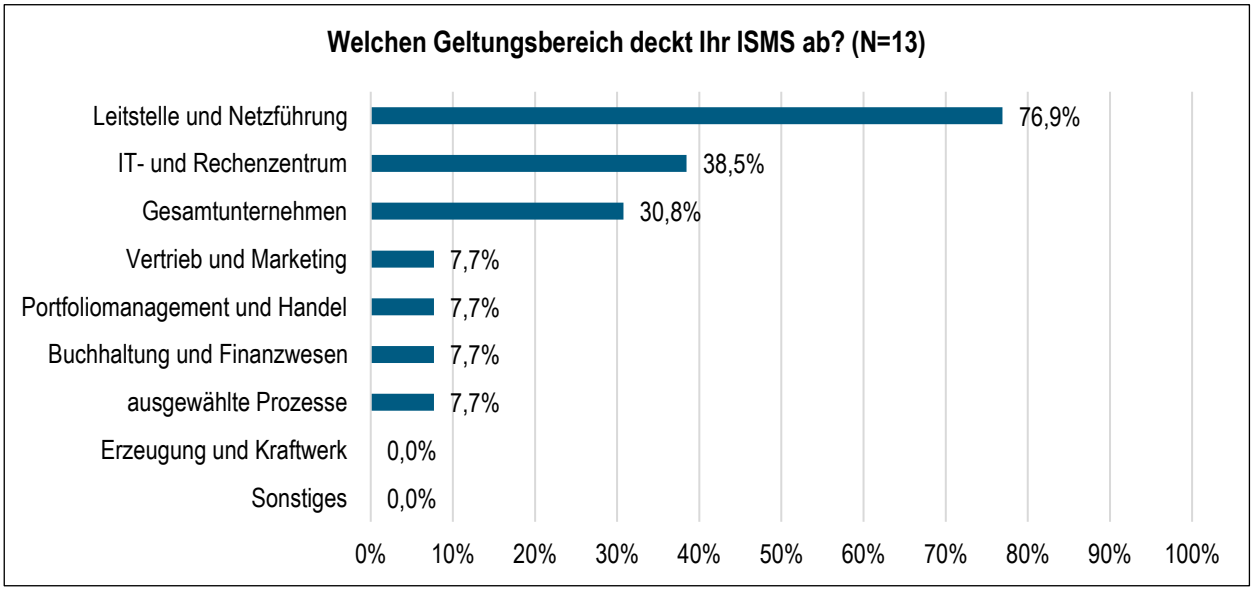


Abbildung 39: Geltungsbereich des ISMS im Bereich des ÖPNV

Gesonderte Betrachtung des Nahverkehrs (ÖPNV)

Die Leitstelle sowie das IT- und Rechenzentrum als Geltungsbereich des ISMS werden mehrheitlich von den Probanden im Nahverkehr angegeben.

Die Berücksichtigung anderer Management-Systeme bei der Einführung des ISMS wurde von den 13 Probanden zu 46,2 % verneint und zu 53,8 % bejaht. Dies stellt ein konträres Bild zu dem gesamten Sample dar. Berücksichtigung fanden bspw. Datenschutz-Management-Systeme, das technische Sicherheits-Management sowie die ISO 9001:2015 mit dem TSM. Verbunden wurde dies durch ein Integriertes Management-System.

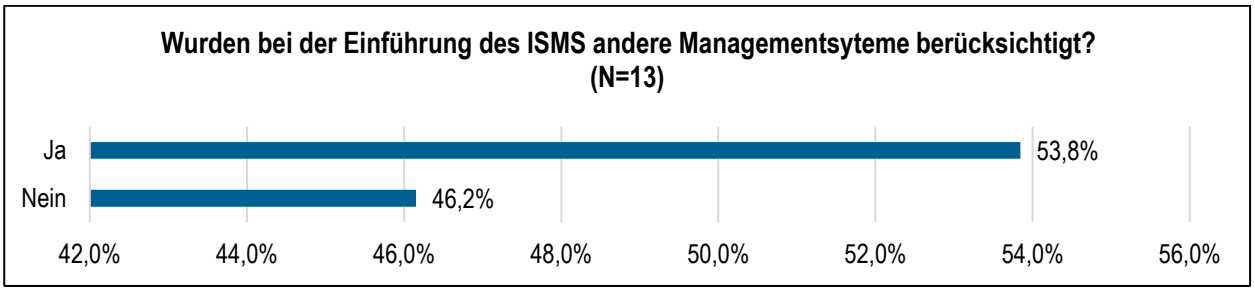


Abbildung 40 Berücksichtigung anderer Management-Systeme bei der Einführung des ISMS im Bereich ÖPNV

In 84,6 % der Unternehmen wurden im Nahverkehrsbereich regelmäßige Schulungsmaßnahmen umgesetzt. Unternehmensnewsletter, Selbststudium etc. sind nachrangig genannt und dienen eher als ergänzende Maßnahmen.

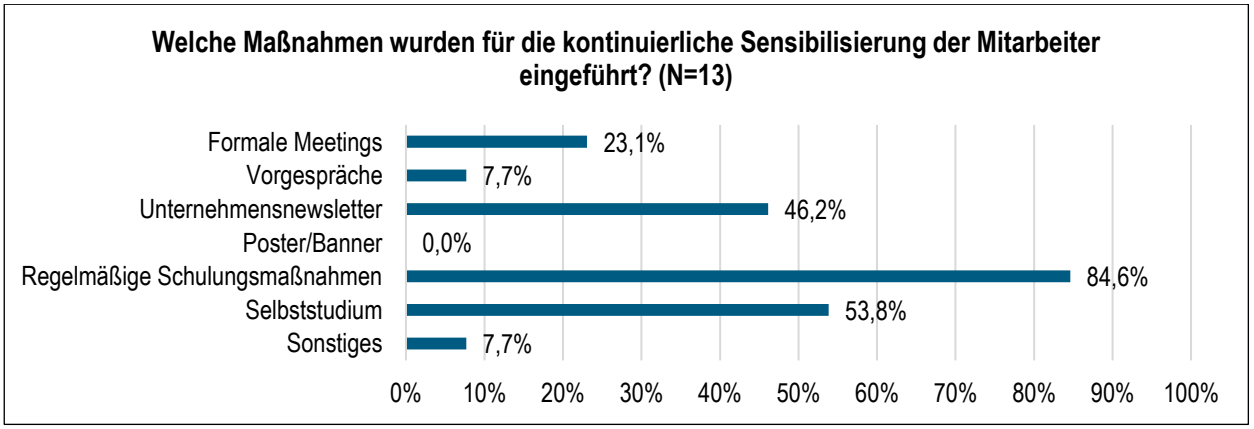


Abbildung 41: Maßnahmen für die kontinuierliche Sensibilisierung der Mitarbeiter im Bereich ÖPNV

Mehrfachnennung möglich

Insgesamt lässt sich festhalten, dass 100 % der Befragten im Bereich des Nahverkehrs den Mehrwert für das Unternehmen durch das ISMS bestätigen.

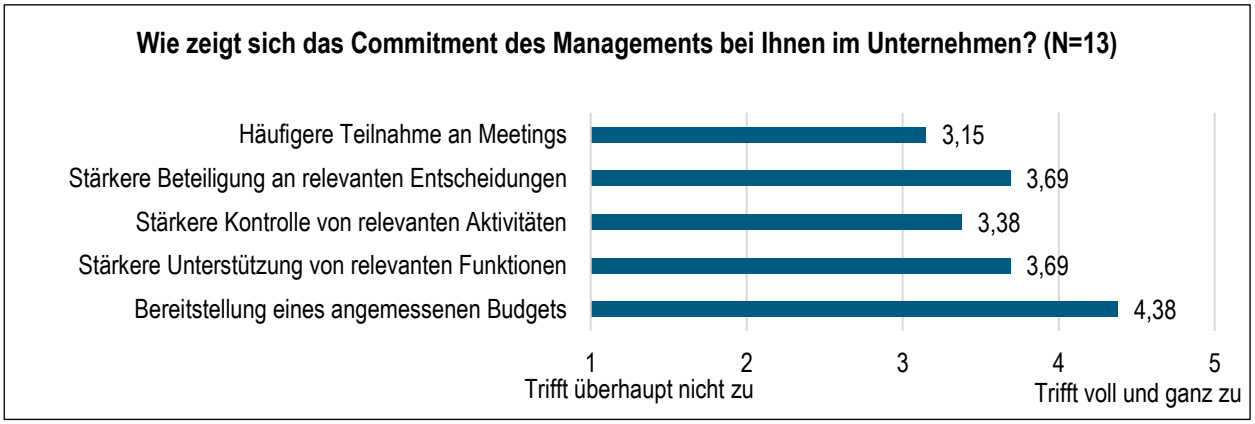


Abbildung 42: Commitment des Managements

Im Vergleich zur Gesamtbetrachtung zeigt sich, dass das Commitment des Managements im Mittel positiver im Bereich des Nahverkehrs gesehen wird. Insbesondere die Bereitstellung eines angemessenen Budgets ist positiver bewertet.

7.4 Zusammenarbeit mit externen Dienstleistern

Zur Einführung des ISMS beauftragten 53,8 % ein Beratungsunternehmen, was im Vergleich zu der Gesamtbetrachtung der Unternehmen in der Energieversorgung mit 76 % ein deutlich geringerer Wert ist. Beratungsunternehmen unterstützten vergleichsweise weniger bei der Initiierung und nahmen in den Phasen des Scopings, der Implementierung und des internen Audits eine bedeutendere Rolle ein. Das Gesamtniveau des Einsatzes in den einzelnen Phasen ist deutlich geringer als im gesamten Sample. Es lässt sich vermuten, dass im Bereich des Nahverkehrs bei der Einführung eines ISMS zuerst nach In house-Kompetenzen im Unternehmensverbund gesucht und diese zur Initiierung genutzt wird.

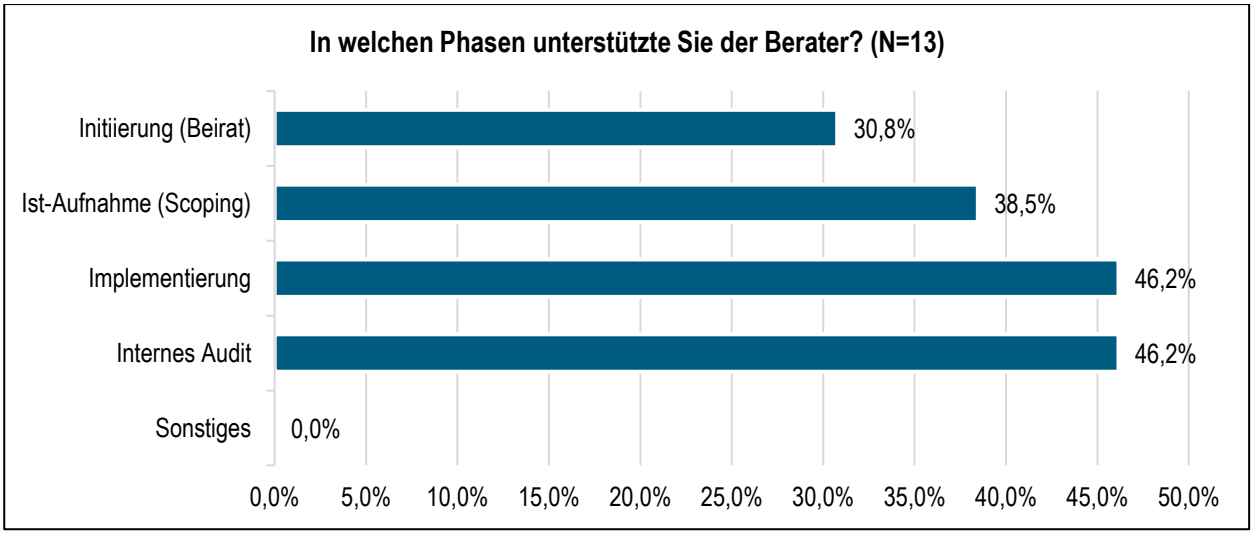


Abbildung 43: Phasen der ISMS-Implementierung mit Beratungsunterstützung im Bereich ÖPNV

Als positive Erfahrungen mit dem Berater wurden a) die gute Einführung in das Thema, b) der Zugriff auf die Erfahrung sowie c) Praxisorientierung und d) der Aufbau des notwendigen Drucks zur Durchführung genannt. Weiterhin partizipierten die Unternehmen an den vorhandenen Hilfsansätzen für Dokumentationen. Als negative Erfahrungen wurden a) verwirrende Aussagen unterschiedlicher Berater, b) die langatmige Besprechung von erdachten Szenarien sowie c) die Praxisferne einiger Berater genannt.

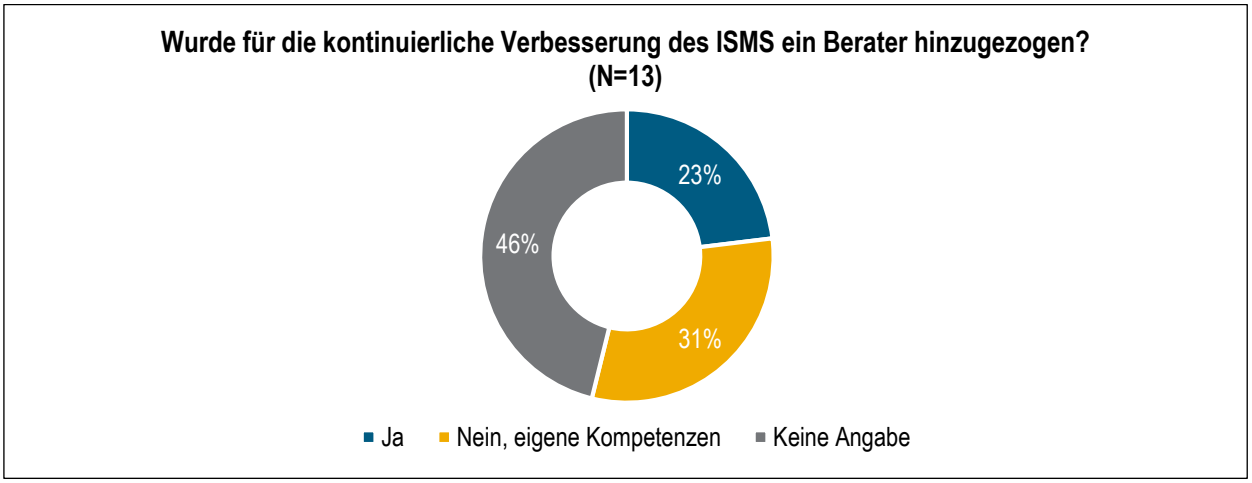


Abbildung 44: Wurde für den KVP des ISMS ein Berater hinzugezogen?

Auch zeigt sich bei der Betrachtung der Hinzunahme eines Dienstleisters für den Kontinuierlichen Verbesserungsprozess des ISMS, dass lediglich 23,1 % der Befragten hierzu auf externe Unterstützung setzen. Vernachlässigt man die Probanden, welche keine Angabe hierzu machten, zeigt sich, dass 57,1 % auf die eigenen Kompetenzen für die kontinuierliche Verbesserung setzen. Dies ist auf vergleichbarem Niveau im gesamten Sample.

7.5 Besondere Erfahrungen in der Implementierung

Bei der Betrachtung der besonderen Erfahrungen in der Implementierung und der damit verbundenen Zufriedenheit mit dem Wirken des ISMS im Sample des ÖPNV zeigt sich, dass insbesondere die einfache Integration in den Unternehmensalltag nur schlecht umgesetzt werden kann. Dieser Punkt ist gleichzeitig relativ wichtig.

Eine positive Wirkung entfaltet das ISMS in den Aspekten der Verbesserung der eigenen Kritischen Infrastruktur, in der Verbesserung im Umgang mit dem Thema Informationssicherheit, der Mitarbeitersensibilisierung sowie der Rechtskonformität. Hier äußern sich die Probanden sehr zufriedenstellend und mit hoher Wichtigkeit. Im direkten Vergleich mit dem gesamten Sample ist auffällig, dass der Verbesserung des Schutzes der Büro-IT eine höhere Wichtigkeit zugeordnet wird. Das Aufzeigen konkreter Entscheidungswege zur Lösung von Sicherheitsvorfällen sowie die Unterstützung der Versorgungssicherheit für die Kunden werden im Vergleich hier als weniger wichtig bewertet.

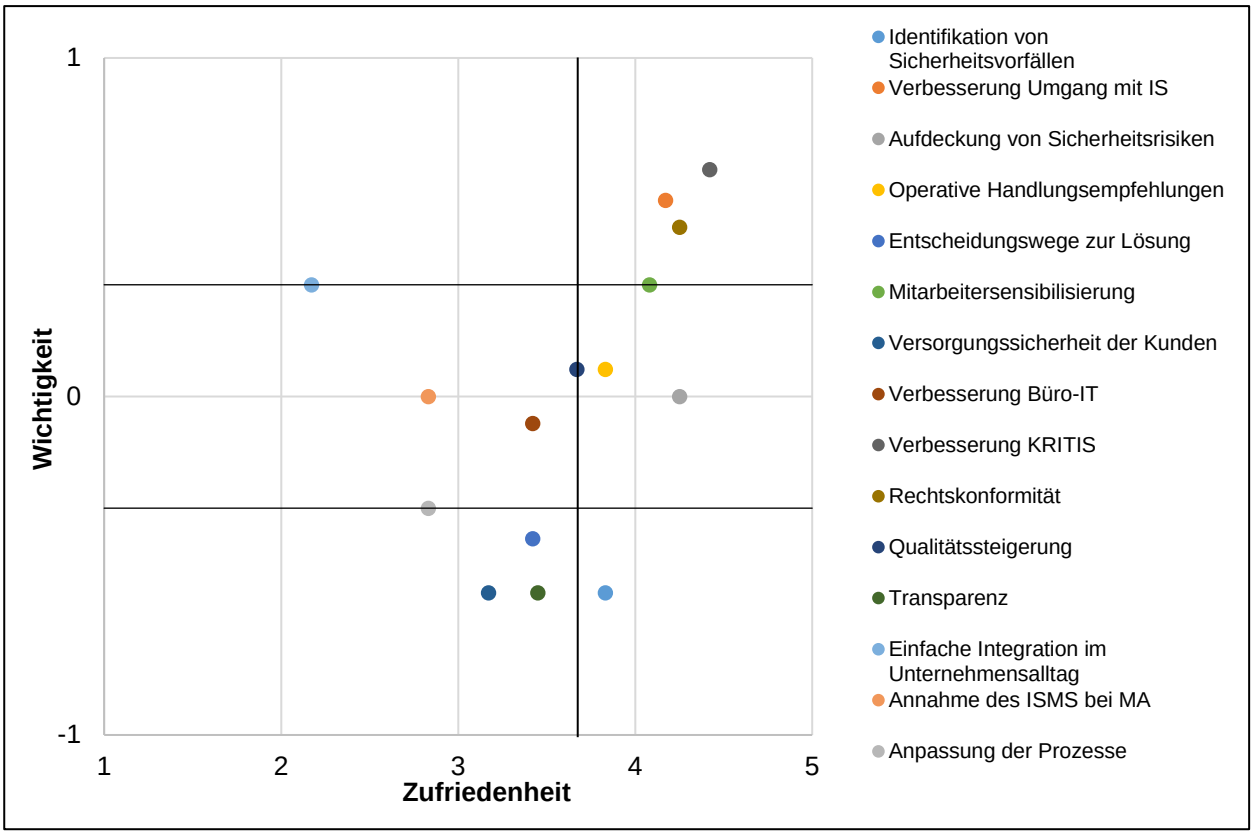


Abbildung 45: SERVIMPERF im Bereich ÖPNV

Die Auswirkungen auf die Fachabteilungen wurden wie folgt bewertet. Hier fällt insbesondere im Vergleich zum gesamten Sample auf, dass die regelmäßigen Backups als positivste Auswirkung bewertet wurden.

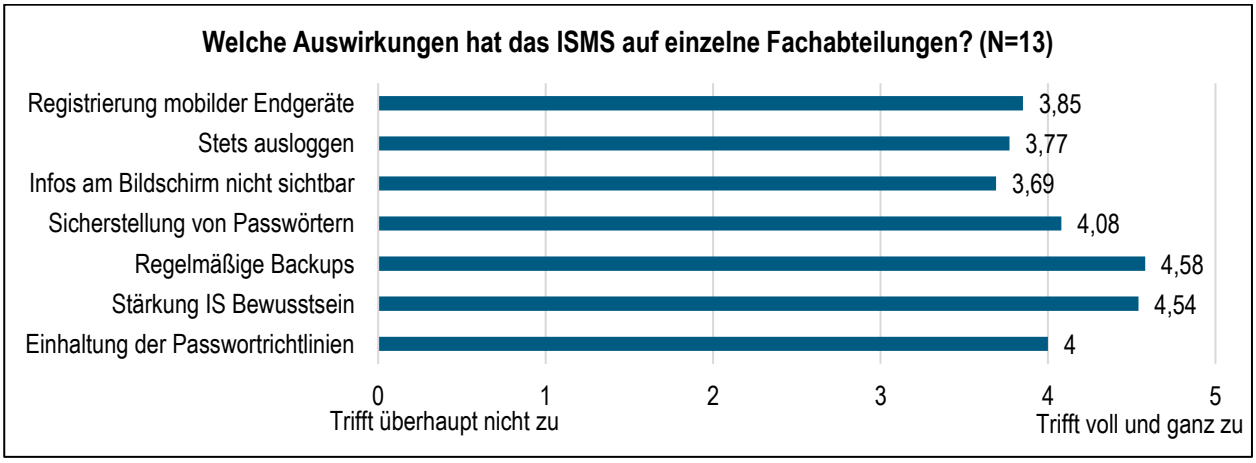


Abbildung 46: Auswirkungen auf die Fachabteilungen im Bereich ÖPNV

7.6 Erfahrungen in der Auditierung und Nachbereitung

Die Erfahrungen in Bezug auf das Audit geben ein konsistentes Bild zu den Ergebnissen des gesamten Samples. Es gaben 84,6 % der Unternehmen mit ÖPNV-Bereich an, dass ihr ISMS – inkl. dem ISMS des Verbundes – bereits beim ersten Audit zur Erstzertifizierung erfolgreich war. Dies steht im Einklang mit den 86 % der Unternehmen aus dem gesamten Sample, die dies ebenfalls angaben.

Auffällig ist jedoch der Grad der Verteilung zu den Herausforderungen und Problemen im Audit. Es gaben 69 % der Unternehmen mit ÖPNV-Bereich an, dass es keine Probleme im Audit gab, während im gesamten Sample lediglich 58 % der Unternehmen diese Auffassung teilten. Im Gegenzug wurden die fehlenden Ressourcen häufiger als Problembereich genannt und stellen die größte der vorgegebenen Herausforderungen für das Audit dar. Kommunikationsprobleme hingegeben wurden gar nicht als Problem genannt.

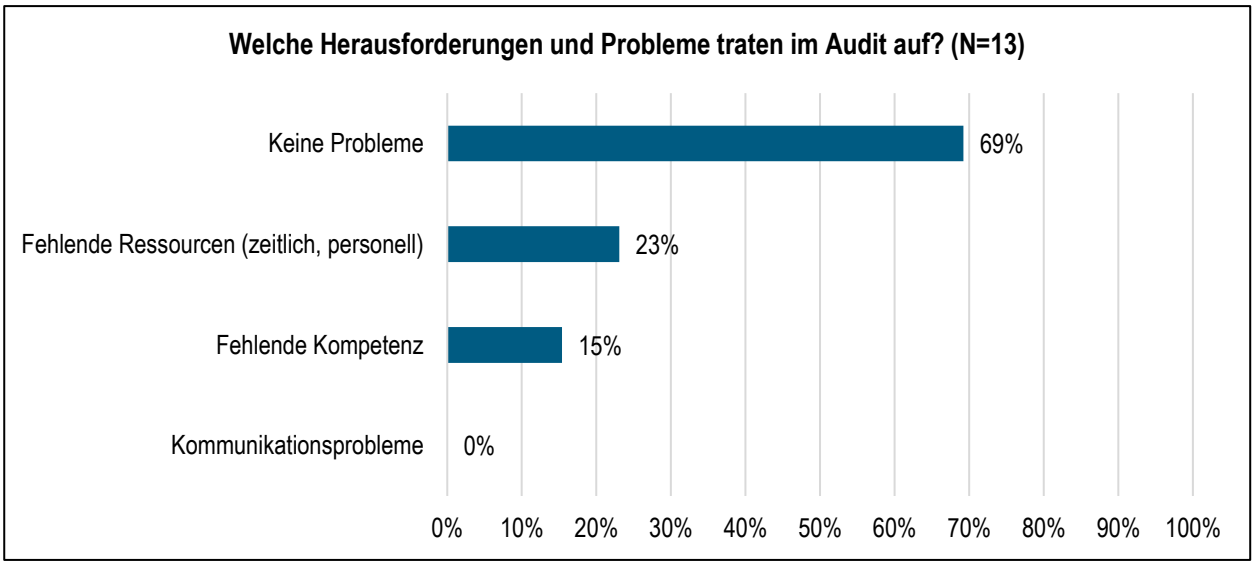


Abbildung 47: Herausforderungen und Probleme im Audit bei ÖPNV

(Mehrfachantworten möglich)

Die Empfehlungen des Auditors wurden in der Regel umgesetzt. Einen deutlichen Überhang zum gesamten Sample besitzt die Kategorie „gewöhnlich“ mit 69 % im Vergleich zu 45 %. Die Antwortoption „immer“ nutzten 7,7 % der Unternehmen mit ÖPNV-Bereich, im Vergleich zu 21 % im gesamten Sample.

8 Fazit

Die vorliegende Studie zum Status-quo des ISMS nach dem ISO 27001 gemäß § 11 Absatz 1a EnWG bei Energieversorgern untersuchte den Einführungs- und Zertifizierungsstand und behandelt die Fragen, welche Auswirkungen ein ISMS auf einzelne Abteilungen der Energieversorger ausübt und ob das ISMS der Erwartungshaltung der Energieversorger gerecht wird. Insbesondere wird untersucht, ob die Energieversorger mit den Leistungen des ISMS zur Wahrung der Informationssicherheit über Sicherstellung der Integrität, der Vertraulichkeit und Verfügbarkeit zufrieden sind. Hierbei wird aufgezeigt, welchen Impact ein ISMS in der Praxis besitzt und welche Herausforderungen mit der Einführung bis hin zur Zertifizierung einhergehen. Dies wurde mittels einzelner Items, wie beispielsweise die Identifikation von Sicherheitsrisiken, detailliert. Die Studie analysiert weiterhin die Erfahrungen der Unternehmen mit der Auditierung und Zertifizierung. Die Basis zu den Untersuchungen bilden jeweilige textuelle Ausführungen zur theoretischen Betrachtung ausgewählter Herausforderungen und Erfahrungen.

Die Ergebnisse der vorliegenden Studie richten sich zum einem an Ansprechpartner zum ISMS bei Energieversorgungsunternehmen, an Unternehmen, welche freiwillig ein ISMS implementieren wollen, und an Interessierte aus dem Bereich der Informationssicherheit und der organisationalen Veränderung. An der empirischen Studie nahmen 42 Energieversorger teil, welche die Erwartungshaltung an ein ISMS hinsichtlich der Zufriedenheit und Wichtigkeit bewerteten. Die Grundlage der Ergebnisse bildete die SERVIMPERF-Analyse. Die Analyse der Daten ergab, dass sich das ISMS positiv auf die Abteilungen der Energieversorger auswirkt und insbesondere die Informationssicherheit mittels Stärkung des Bewusstseins, Vorgaben für Passwörter und regelmäßiger Datensicherung unterstützt. Weiterhin wird das ISMS hinsichtlich der Mitarbeitersensibilisierung, der Verbesserung zur Informationssicherheit bei den eigenen kritischen Infrastrukturen im Unternehmen und der Rechtskonformität zufriedenstellend ab. Ebenso konnte nachvollzogen werden, dass die Leistung des ISMS zur Identifikation von Sicherheitsrisiken äußerst zufriedenstellend ist – das Hauptanliegen des politischen Impulses.

Deutliches Verbesserungspotenzial besteht in der Integration des ISMS in den Unternehmensalltag. Mit Blick auf die Norm und den Anhang A zeigt sich, dass das Business Continuity Management (Notfall- und Krisen-Management) in den Fokus rückt und nach Angaben der befragten Unternehmen noch nicht vollumfänglich zufriedenstellend gem. den Kommentaren der Auditoren implementiert ist. Hier müssen die Unternehmen intern nacharbeiten und die externen Berater das Thema in ihrem Portfolio in den Fokus stellen.

Die Bedeutung der Informationssicherheit ist für den Energiesektor von hoher und weiterhin zunehmender Bedeutung. Vor diesem Hintergrund hat die Bundesnetzagentur nach § 11 Abs. 1b EnWG den Auftrag, einen Katalog von Sicherheitsanforderungen zum Schutz gegen Bedrohungen für Telekommunikations- und elektronische Datenverarbeitungssysteme, die für einen sicheren Betrieb von Energieanlagen notwendig sind, zu erstellen (sog. „IT-Sicherheitskatalog“). Kernforderung des IT-Sicherheitskatalogs ist die Verpflichtung der Betreiber der betroffenen Energieanlagen, ein Informationssicherheits-Managementsystem zu implementieren.

In Zukunft wird das Thema ISMS nach ISO 27001 für weitere Bereiche der Kritischen Infrastrukturen relevant werden. Der 2. Korb der BSI-Kritisverordnung umfasst u. a. den öffentlichen Personennahverkehr. Energieversorgungsunternehmen mit ÖPNV-Bereich wurden in der vorliegenden Studie gesondert betrachtet.

Für zukünftige Untersuchungen stellt das Thema „Schnittstellen zwischen ISMS-Implementierungen“ eine Basis dar. Das Ziel ISMS-Implementierungen beim Informationsaustausch zwischen Unternehmen ineinandergreifen zu lassen wurde gegenwärtig noch nicht thematisiert. Erste Herausforderungen hierzu, wie bspw. die Einbindung von Lieferanten in das ISMS, wurden aber bereits in dieser Studie angesprochen. Im zukünftigen Fokus sollten auch Unternehmen stehen, welche im Bereich der Datenanalyse aktiv sind. Daten und Informationen sind das Öl der gegenwärtigen Zeit und damit ist der Schutz dieser vor unberechtigtem Zugriff - egal ob nur lesend, schreibend und damit vernichtend - umso wichtiger. Ein ISMS mit dem Ziel der Sicherstellung der Integrität von Daten ist ein wichtiger Schritt bevor Big Data und Business Intelligence-Überlegungen im Unternehmen greifen. Geschäftliche Entscheidungen auf Basis von Datenanalysen können nach Ansicht der Autoren nur gewinnbringend sein, wenn die Integrität der Daten sichergestellt ist und eine Datenmanipulation durch Dritte vor der Analyse ausgeschlossen werden kann. Dabei ist die Einführung eines ISMS gerade bei Start-Ups zu diskutieren. Einerseits bringt es in einer frühen Phase des Unternehmens Struktur und Prozessdenken ein und sorgte für einen dokumentierten und geregelten Wachstumsprozess des Unternehmens. Andererseits ist der Aufwand ein ISMS zu implementieren scheinbar sehr hoch, da Prozesse erst vom Unternehmen entwickelt und dokumentiert werden müssen. Im Paradigma ist dies nur teilweise mit einem agilen Ansatz im Unternehmensalltag und der Unternehmensführung vereinbar – schlanke Lösungswege sind zu entwickeln.

Literaturverzeichnis

Antons, David und Frank T. Piller (2015), "Opening the black box of “Not Invented Here”: Attitudes, decision biases, and behavioral consequences", Academy of Management Perspectives, 29 (2), 193-217.

Barki, Henri und Jon Hartwick (1994) “Measuring user participation, user involvement, and user attitude”, MIS Quarterly, 18 (1) 59–82.

Beer, Kristina (2016), „Schadsoftware im Atomkraftwerk Gundremmingen“, https://www.heise.de/newsticker/meldung/Schadsoftware-im-Atomkraftwerk-Gundremmingen-3186045.html, (Zugriff am 30.06.18)

Blank, Jörg und Christoph Dernbach (2018), „Sicherheitskreise: Hacker drangen in deutsches Regierungsnetz ein“, https://www.heise.de/newsticker/meldung/Sicherheitskreise-Hackerdrangen-in-deutsches-Regierungsnetz-ein-3983510.html“, (Zugriff am 02.07.18).

Brodin, Martin (2015) “Combining ISMS with strategic management: the case of BYOD“, 8th IADIS International Conference on Information Systems (IS 2015), Funchal, Madeira, Portugal.

BSI (2014), „Die Lage der IT-Sicherheit in Deutschland 2014“, Bonn: Bundesamt für Sicherheit in der Informationstechnik.

BSI (2015), „Die Lage der IT-Sicherheit in Deutschland 2015“, Bonn: Bundesamt für Sicherheit in der Informationstechnik.

BSI (2016), Die Lage der IT-Sicherheit in Deutschland 2016“, Bonn: Bundesamt für Sicherheit in der Informationstechnik.

BSI (2017a), „Die Lage der IT-Sicherheit in Deutschland 2017“, Bonn: Bundesamt für Sicherheit in der Informationstechnik.

BSI (2017b), „Schutz Kritischer Infrastrukturen durch IT-Sicherheitsgesetz und UP KRITIS“, Bonn: Bundesamt für Sicherheit in der Informationstechnik.

Bundesnetzagentur (2015), IT-Sicherheitskatalog gemäß § 11 Absatz 1a Energiewirtschaftsgesetz, Bonn.

Bundesverband der Auditoren e.V. (2018): „IAF/EA- und NACE-Code“, https://www.bvd-auditoren.de/nace-code.html, (Zugriff am 16.09.18).

Chrzan, Keith und Natalia Golovashkina (2006), "An Empirical Test of Six Stated Importance Measures", International Journal of Market Research, 48 (6), 717-740.

Cram, W. Alec; Proudfoot, Jeffrey und John D'Arcy (2017), "Seeing the forest and the trees: A meta-analysis of information security policy compliance literature", Proceedings of the 50th Hawaii International Conference on System Sciences.

Cyber Security Procurement Language for Control Systems (2009), veröffentlicht vom Department of Homeland Security.

Cybersecurity Procurement Language for Energy Delivery Systems (2014), veröffentlicht von ESCSWG.

Dürig, Markus und Matthias Fischer (2018), „Cybersicherheit in Kritischen Infrastrukturen", Datenschutz und Datensicherheit, 42 (4), 209-213.

Hänel Andreas und Fabian Wohlfart (2016), „Informationssicherheits-Managementsystem (ISMS) bei Energieversorgern“, Studie im Auftrag der SEVEN PRINCIPLES AG in Zusammenarbeit mit Energieforen Leipzig GmbH.

Hannoversche Allgemeine (2018), „Hacker greifen deutsche Energieversorger an“, http://www.haz.de/Nachrichten/Wirtschaft/Deutschland-Welt/Hacker- greifen-deutsche-Energieversorger-an, (Zugriff am17.06.18).

Heller, Piotr (2016), „Die Häckerdämmerung“, http://www.faz.net/aktuell/wissen/physik-mehr/ukrainischer-stromausfall-war-ein-hacker-angriff-14005472.html, (Zugriff am16.05.18).

Jendrian, Kai (2014), „Der Standard ISO/IEC 27001: 2013", Datenschutz und Datensicherheit, 38 (8), 552-557.

Koalitionsvertrag (2018), „Ein neuer Aufbruch für Europa - Eine neue Dynamik für Deutschland - Ein neuer Zusammenhalt für unser Land – Koalitionsvertrag zwischen CDU, CSU und SPD“, 19. Legislaturperiode

Koreng, Ansgar und Matthias Lachenmann (2018), „Formularhandbuch Datenschutzrecht“, 2. Auflage, C.H.BECK ISBN 978-3-406-69542-1.

Krause, Till und Hakan Tanriverdi (2018), „Hacker haben deutschen Energieversorger angegriffen“, www.sueddeutsche.de/digital/enbwtochter-hacker-haben-deutschen-energieversorger-angegriffen-1.3980625, (Zugriff am 17.06.18).

Martilla, John A. und John C. James (1977), “Importance – Performance Analysis”, Journal of Marketing, 41 (1), 77-79.

Mirow, Christoph, Katharina Hölzle und Hans Georg Gemünden (2007), „Systematisierung, Erklärungsbeiträge und Effekte von Innovationsbarrieren", Journal für Betriebswirtschaft, 57 (2), 101-134.

Pastowski, Sven (2004), Messung der Dienstleistungsqualität in komplexen Marktstrukturen: Perspektiven für ein Qualitätsmanagement von Hochschulen, Wiesbaden: Deutscher Universitäts-Verlag.

Psomas, Evangelos und Jiju Antony (2015) "The effectiveness of the ISO 9001 quality management system and its influential critical factors in Greek manufacturing companies." International Journal of Production Research 53 (7), 2089-2099.

Rumpel, Rainer (2011), „Planung und Betrieb von Informationssicherheits-Managementsystemen", Datenschutz und Datensicherheit, 35 (1), 12-15.

Sänn, Alexander (2017), “The preference-driven lead user method for new product development: A comprehensive way to stimulate innovations with internal and external sources”. Springer.

Schartner, Peter und Jürgen Taeger (2011), Proceedings DACH Security 2011, 20. und 21. September 2011, IT-Quartier Oldenburg, 594 Seiten.

Schirrmacher, Dennis (2018), „ICS-Systeme von Schneider Electric: Angreifer könnten Fabriken übernehmen“, https://www.heise.de/security/meldung/ICS-Systeme-von-Schneider-Electric-Angreifer-koennten- Fabriken-uebernehmen-4041363.html, (Zugriff am 29.06.18).

Schlienger, Thomas (2007), „Informationssicherheitskultur", Datenschutz und Datensicherheit, 31 (7), 487-491.

Spiegel Online (2016), „Schadsoftware in bayerischem Atomkraftwerk entdeckt“, http://www.spiegel.de/netzwelt/web/grundremmingencomputervirus-im-atomkraftwerk-entdeckt-a-1089248.html, (Zugriff am 29.06.18).

Stanton, Jeffrey M., Kathryn R.Stam, Paul Mastrangelo und Jeffrey Jolton (2005) “Analysis of end user security behaviors“, Computers & Security, 24 (2), 124–133.

SZ (2018), „Warnung vor Hackerangriffen auf deutsche Energieversorger“, http://www.sueddeutsche.de/digital/itsicherheit-warnung-vor-hackerangriffen-auf-deutsche-energieversorger-1.4015345, Süddeutsche Zeitung, (Zugriff am 17.06.18).

Tanriverdi, Hakan (2016), „Bundesamt geht von Hackerangriff auf ukrainisches Stromnetz aus“, http://www.sueddeutsche.de/digital/ ukrainebundesamt-geht-von-hackerangriff-auf-ukrainisches-stromnetz-aus-1.2830197, (Zugriff am 22.05.18).

Thomson, M.E. und R. von Solms (1998) “Information security awareness: educating our users effectively”, Information Management & Computer Security, 6 (4), 167-173.

Wir danken den Mitautoren und Bearbeitern dieser Studie!

Maren Ahlborn

David Bartela

Christian Book

Sven Braam

Thomas Ebel

Jörg Jaenichen

Jonas Kahon

Verena Ludwig

Katharina Pflügner

Simon Rath

Friederke Sporer

Betriebswirtschaftliche Forschungszentrum für Fragen der mittelständischen Wirtschaft e. V. an der Universität Bayreuth
Mainstrasse 5
95444 Bayreuth

T +49 921 530397 - 0
F +49 921 530397 - 10
E info@bfm-bayreuth.de
I www.bfm-bayreuth.de

SEVEN PRINCIPLES AG
Erna-Scheffler-Strasse 1a
51103 Köln

T +49 221 92007 - 0
F +49 221 92007 - 77
E info@bfm-bayreuth.de
I www.bfm-bayreuth.de

Zu den Unternehmen:

Das Betriebswirtschaftliche Forschungszentrum für Fragen der mittelständischen Wirtschaft e. V. (BF/M) an der Universität Bayreuth ist ein gemeinnütziger Verein, der 1979 gegründet wurde und es sich zum Ziel gesetzt hat, Wissenschaft und Wirtschaft miteinander zu verzahnen, indem betriebswirtschaftliche Forschungsergebnisse in Unternehmen transferiert werden und empirische Untersuchungen stattfinden können. Das Hauptaugenmerk liegt dabei ganz klar auf kleinen und mittleren Unternehmen (KMU).

Der Organisationsform als eingetragener Verein folgend, finanziert sich das BF/M außerhalb des Universitätshaushalts ohne jede Gewinnerzielungsabsicht. Die Finanzierung erfolgt dabei zu einem bedeutenden Anteil über unterschiedlichste eigene Projekte im betriebswirtschaftlichen Kontext. Dazu werden sowohl mehrjährige Forschungsprojekte als auch kurzfristige Projekte im Unternehmensauftrag durchgeführt. Weitere Finanzierungsquellen stellen zudem Mitgliedsbeiträge, Spenden sowie eine Fehlbedarfsförderung des Bayerischen Staatsministeriums für Wirtschaft, Infrastruktur, Verkehr und Technologie dar.

Das Institut arbeitet an der Erforschung, Entwicklung und Einführung von effizienten Methoden und Instrumenten der Unternehmensführung. Vor dem Hintergrund der zunehmenden Globalisierung der Wirtschaft, der zunehmenden Bedeutung des Dienstleitungssektors wie auch moderner Informations- und Kommunikationstechnologien fokussiert das BF/M-Bayreuth in seiner Forschung die Themenschwerpunkte Unternehmensnetzwerke, Internationalisierung von KMU, Kompetenzmanagement in KMU, Digitalisierung des Mittelstandes, Unternehmensfinanzierung und –controlling.

SEVEN PRINCIPLES AG (7P): Dienstleistungen rund um die Digitalisierung von Geschäftsmodellen

Das Leistungsspektrum umfasst die gesamte Wertschöpfungskette von der Prozess- und Architekturberatung über Systemintegration bis hin zu einem Managed Service Angebot. Innovative Themen wie BI/Big Data, Cloud, SAP-Beratung & Entwicklung, Security und agile Softwareentwicklung stehen dabei im Fokus der 7P-Kunden, die primär aus den Branchen Telecommunication, Automotive, Energy sowie Travel, Transport & Logistics kommen.

Die 7P mit Hauptsitz in Köln und weiteren Standorten, u. a. in München, beschäftigt bundesweit über 500 Mitarbeiter.

Der Unternehmensbereich 7P Security

Informationssicherheit dient dem Schutz vor Gefahren bzw. Bedrohungen, der Vermeidung von wirtschaftlichen Schäden und der Minimierung von Risiken.

Mit der internationalen Norm ISO/IEC 27001:2013 existiert ein weltweit anerkanntes und durch unabhängige Stellen zertifizierungsfähiges Informationssicherheits-Management-System (ISMS), mit dessen Hilfe Informationssicherheit in Unternehmen jeder Größe und Branche etabliert werden kann.

Eine ISO/IEC 27001:2013-Zertifizierung dient somit nicht nur der Vermarktung, sondern fördert insgesamt die Unternehmenskultur, die Transparenz und die Prozessteuerung. Viele zertifizierte Unternehmen erwarten bereits von Lieferanten und Partnern, dass auch diese ein zertifiziertes ISMS betreiben.

7P unterstützt dabei mit erfahrenen, zertifizierten Beratern beim Aufbau eines gemeinsamen Verständnisses zur Informationssicherheit, IT-Sicherheit, Datenschutz und Compliance, um gemeinsam mit seinen Kunden die wesentlichen Umsetzungen zu implementieren.