ISMS nach ISO 27001 Blaupause für den Einsatz in Unternehmen

Ein ISMS erhöht den Reifegrad einer Sicherheitsorganisation und hilft Compliance-Anforderungen mehrerer Gesetze zu erfüllen – ISO-Zertifizierung bestätigt Sicherheitslevel

Nadine Hofmann
Dr. Waldemar Grudzien
Daniel Augustin

April 2020
Blogpost

Key Facts

- Datengetriebene Ökonomie erhöht Datenvolumen und Wert der Daten stetig
- Fortschreitende Digitalisierung erhöht Angriffsfläche: Angriffe und Schadenssummen steigen
- An ISO 27001 angelehntes Information Security Management System (ISMS) unterstützt den umfänglichen Schutz aller Unternehmensinformationen durch Policies und Prozesse
- ISMS sichert Compliance diverser Anforderungen wie bspw. den sich aus DSGVO ergebenden Schutz personenbezogener Daten ab
- Zertifizierung des eigenen ISMS nach ISO 27001 schafft Verbindlichkeit der Sicherheitsmaßnahmen nach innen und dokumentiert eine umfängliche und resiliente Sicherheitsorganisation nach außen
- Zertifizierung ist durch ein kleines motiviertes Team plan- und durchführ- und für jährliche Re-Zertifizierungen wiederholbar

Informationen der Unternehmen sind wertvoll – für Unternehmen wie für Kriminelle

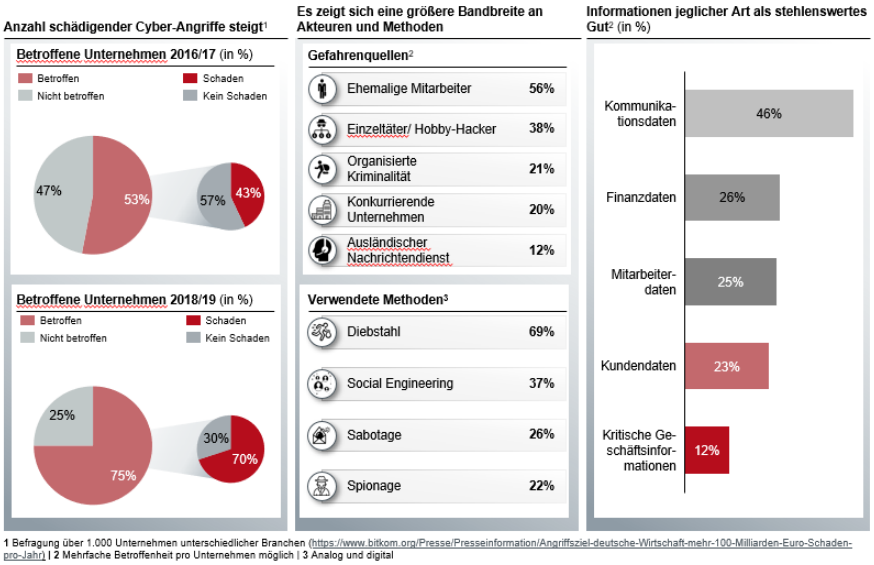
Laut einer Studie des Digitalverbandes Bitkom[1] erlitt die deutsche Wirtschaft im letzten Jahr einen Schaden aus Sabotage, Datendiebstahl oder Spionage von rund 103 Milliarden Euro. Basis dieser Studie ist eine brachenübergreifende Befragung von Geschäftsführern und Sicherheitsverantwortlichen deutscher Unternehmen mit mehr als 10 Mitarbeitern, inwieweit ihre Unternehmen 2018/19 Ziel analoger und digitaler Angriffe wurden. Demnach waren drei Viertel der Unternehmen in diesem Zeitraum tatsächlich von Cyberangriffen betroffen, weitere 13 Prozent vermuten dies.

Das Ausmaß erfolgreicher Angriffeumfasst eine Steigerung von 27 Prozent im Vergleich zu den Vorjahren 2016/17 und sollte jedem Verantwortlichen ein Warnsignal sein. In Abbildung 1 sind die wesentlichen Ergebnisse der Umfrage zusammenfassend dargestellt.

Aus der Analyse der Ergebnisse lassen sich 3 maßgebliche Konsequenzen ableiten

Die wichtigste Erkenntnis der Studie ist: Es wird gemacht, was Erfolg verspricht. Die Angriffe sind mitnichten nur noch „cyber“ oder „digital“. Auch analoge oder gemischt digital-analoge Formen wie Social Engineering, Diebstahl von Dokumenten, Produktionsmitteln und Datenträgern aller Art sowie Sabotage werden eingesetzt.

[1] https://www.bitkom.org/Presse/Presseinformation/Angriffsziel-deutsche-Wirtschaft-mehr-100-Milliarden-Euro-Schaden-pro-Jahr



1 Befragung über 1.000 Unternehmen unterschiedlicher Branchen (https://www.bitkom.org/Presse/Presseinformation/Angriffsziel-deutsche-Wirtschaft-mehr-100-Milliarden-Euro-Schaden-pro-Jahr) I 2 Mehrfache Betroffenheit pro Unternehmen möglich I 3 Analog und digital

Abbildung 1: Anstieg der Fälle von Cyber-Attacken mit distribuierenden Gefahrenquellen und -gut

Die Täter entwenden alle Informationen, derer sie habhaft werden können. Dabei müssen neben dem rein unternehmerischen Schaden zusätzlich der Reputationsschaden und der Schaden aus Compliance-Verstößen beachtet werden – DSGVO bei personenbezogenen Informationen, bei Geschäftsgeheimnissen konkret das dafür konzipierte Gesetz zum Schutz von Geschäftsgeheimnissen.

Des Weiteren zählen inzwischen alle Branchen zum Kreis der Opfer, kein Unternehmen ist mehr gefeit: Wurden früher vornehmlich Unternehmen des Finanzsektors angegriffen, ist heute praktisch die breite Wirtschaft das Ziel. Auch der Täterkreis hat sich gewandelt. Täter sind nicht nur Kriminelle und Nachrichtendienste, sondern auch Mitarbeiter – aktuelle und besonders ehemalige.

Angriffe werden vermehrt gegen Mitarbeiter geführt, da Menschen insgesamt fehlbarer sind als Technik. So verspricht eine personalisierte Mail mit Anhang eher Aussicht auf Erfolg als ein DDoS-Angriff gegen eine Infrastruktur.

Insofern müssen Maßnahmen das breite Angriffsspektrum auf Technik und Personal berücksichtigen. Im Ergebnis der Studie können drei Konsequenzen gezogen werden:

1. Kein Unternehmen kann sich mehr im Schatten der „Großen“ verstecken. Das Risiko von Schäden durch Angriffe ist überall dort konkret, wo Informationen verarbeitet werden, ohne dass eine umfassende Identifizierung und wirksame Schließung von Einfallstoren praktiziert wird.
2. Eine Konzentration allein auf digitale Maßnahmen zum Schutz der Unternehmenswerte reicht nicht aus. Zusätzlich müssen diese durch analoge Maßnahmen flankiert sein, um das breite Spektrum der Angriffe wirksam zu bekämpfen.
3. Alle Mitarbeiter, nicht nur solche mit IT-Sachverstand, bilden den Kern einer funktionierenden Sicherheitsstrategie.

ISMS ist Best Practice für Schutz von Informationen

Zum Aufbau und Erhalt einer Sicherheitsorganisation setzen Unternehmen vermehrt auf Informationssicherheits-Managementsysteme (ISMS), ein Rahmenwerk für den Aufbau, die Überprüfung und die kontinuierliche Verbesserung der Sicherheit von Organisationen.

Gemäß BSI[2] umfasst ein Managementsystem alle Regelungen für die zielgerichtete Steuerung und Lenkung einer Institution. Ein Managementsystem für Informationssicherheit legt somit fest, mit welchen Instrumenten und Methoden die Leitungsebene einer Institution die auf Informationssicherheit ausgerichteten Aufgaben und Aktivitäten nachvollziehbar lenken kann.

Ein ISMS stellt in Dokumenten („Policies“) Ziele als Verfahren und Regeln auf, die den Rahmen für die Umsetzung dieser in der täglichen Praxis durch Prozesse („Arbeitsanweisungen“) vorgeben. Somit unterstützt ein ISMS, das Ambitionsniveau der eigenen Informationssicherheit zu definieren, zu steuern, zu kontrollieren, aufrechtzuerhalten und fortlaufend zu verbessern. Als etablierter Standard der Wahl zum Aufbau und Betrieb eines ISMS gilt ISO 27001[3], ergänzt um die Umsetzungshinweise des ISO 27002[4]-Standards.

Ein ISMS nach ISO 27001 gliedert sich in eine übergeordnete High Level Structure (HLS) und 14 grundlegende Sicherheitsziele (security controls A.5 bis A.18). Sie ordnen sich in vier Dokumentebenen (Level) mit unterschiedlichen Adressaten ein (siehe Abbildung 2).

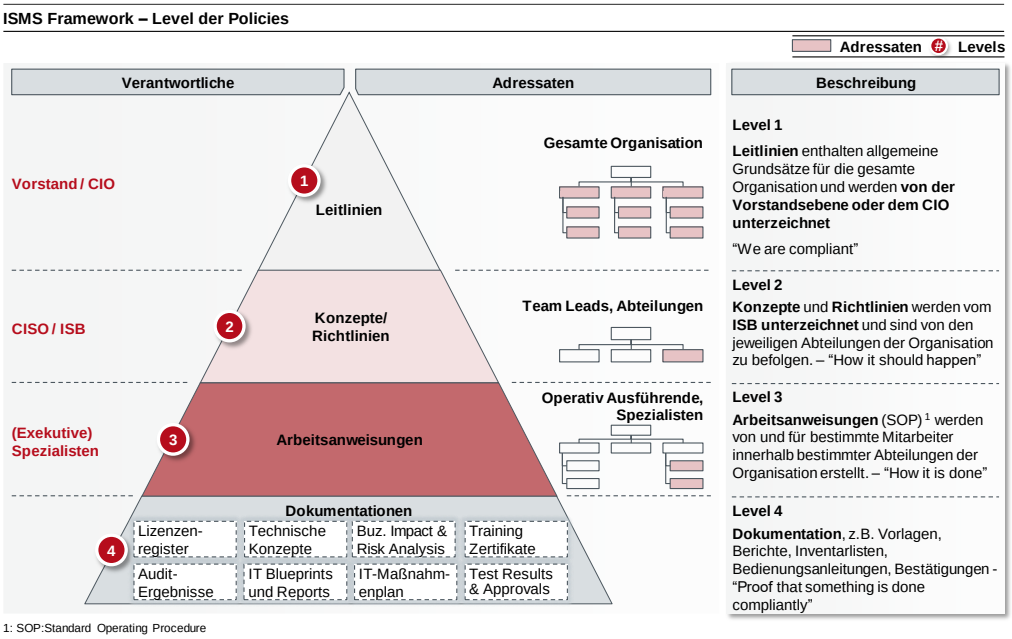


Abbildung 2: ISMS Policy Konvolut

Die Struktur der ISMS-Dokumentation erzeugt ein konsistentes und aktuelles Bild der eigenen Sicherheitsinfrastruktur in Bezug auf Technologie, Organisation, Leitung und Personal. Der Prozess des Zusammentragens aller erforderlichen Informationen zwingt dazu, „jeden Stein

[2] BSI-Standard 200-1: Managementsysteme für Informationssicherheit (ISMS)
[3] Information technology – Security techniques – Information security management systems – Requirements
[4] Information technology – Security techniques – Code of practice for information security controls

umzudrehen“. Durch ihn wird die eigene Infrastruktur durchdrungen – mit ihren potenziellen Schwachstellen wie ihren aktuellen Stärken und Schwächen. Auf der Grundlage dieses Infrastrukturbildes werden Aufgabenkomplexe identifiziert und einer Mitigation zugeführt, zum Beispiel das Wertemanagement (Identifikation und Behandlung von Werten), das Risikomanagement (Identifikation, Klassifikation, Behandlung von Risiken) oder das Notfallmanagement (Incident Management, Notfallhandbuch, Business Impact Analysis BIA, Geschäftsfortführung). Da HLS und security controls alle wesentlichen Themen zum Schutz der Informationen adressieren, gewährleistet ein ISMS nach ISO 27001, dass kein wichtiges Sicherheitsthema vernachlässigt oder gänzlich „vergessen“ wird. So werden nicht nur die „üblichen“ digitalen Sicherheitsanforderungen an die elektronische Kommunikation (A.13), die kryptographischen Verfahren (A.10) oder die Sicherheit im Betrieb (A.12) und der Anwendungsentwicklung (A.14) gestellt, sondern auch an die physische Sicherheit (A.11), Zugang inkl. Rollen & Rechten (IAM) und Zugriff, den physischen Zutritt (A.9) und ebenso an die Mitarbeiter (A.7), wobei auch ehemalige Mitarbeiter berücksichtigt werden.

Durch den Aufbau und die kontinuierliche Pflege eines ISMS ist die Organisation gezwungen, die eigene Infrastruktur in Technik, Personal und Governance zu analysieren und zu dokumentieren. Es führt ferner zu einer Einbindung sämtlicher Mitarbeiter, die Prozesse anhand der in Policies festgelegten Rahmenbedingungen leben, gestalten und dokumentieren. Durch Aufbau des ISMS etabliert sich eine reifere Sicherheitsorganisation, die durch kontinuierliche Pflege verbessert wird.

Die oben genannten drei Konsequenzen werden mit Hilfe der Maßnahmen eines ISMS adressiert:

- Schutzmaßnahmen müssen **analog und digital** sein, und es müssen **alle** Einfallstore gesichert werden – durch Berücksichtigung von HLS und security controls
- Ein **Fokus auf digital verfügbare Informationen** oder gar nur auf die „Kronjuwelen“ **genügt nicht** – Risikobehandlung HLS Nr. 6 und Nr. 8, Informationsklassifizierung (A.8)
- **Technische Maßnahmen allein reichen nicht aus** – sie müssen neben technischer auch organisatorischer (A.6), rechtlicher (A.15, A.18) und personeller (A.7) Art sein
- **Alle Mitarbeiter sind entscheidend** bei der Abwehr, nicht nur die der IT-Abteilung – regelmäßige Schulung (A.7) aller Mitarbeiter

Durch die kontinuierliche Messung der Funktionsfähigkeit des ISMS (HLS Nr. 9) wird die Qualität des Schutzes durch ständige Anpassung von Bedrohungen, Schwachstellen, Risiken und Maßnahmen aufrechterhalten. Eine eindeutige Festlegung von Verantwortlichkeiten der Informationssicherheit (HLS Nr. 5 und Nr. 7, A.6) sowie der Kommunikationsstrukturen bei einem Ereignis (A.16) und im Notfall (A.17) stellt Verbindlichkeit her.

ISMS als Compliance-Werkzeug

Ein funktionsfähiges, gut gepflegtes ISMS stellt nicht nur die Informationssicherheit auf eine höhere Reifestufe, sondern unterstützt mit der Datenschutz-Grundverordnung (DSGVO) und dem Gesetz zum Schutz von Geschäftsgeheimnissen zusätzlich die Einhaltung weiterer regulatorischer und sanktionsbewährter Anforderungen durch Bereitstellung einer sicheren IT-Infrastruktur. In Abbildung 3 wird exemplarisch die Erfüllung von Anforderungen aus der DSGVO durch Umsetzung der Sicherheitsziele aus ISO 27001 gezeigt.

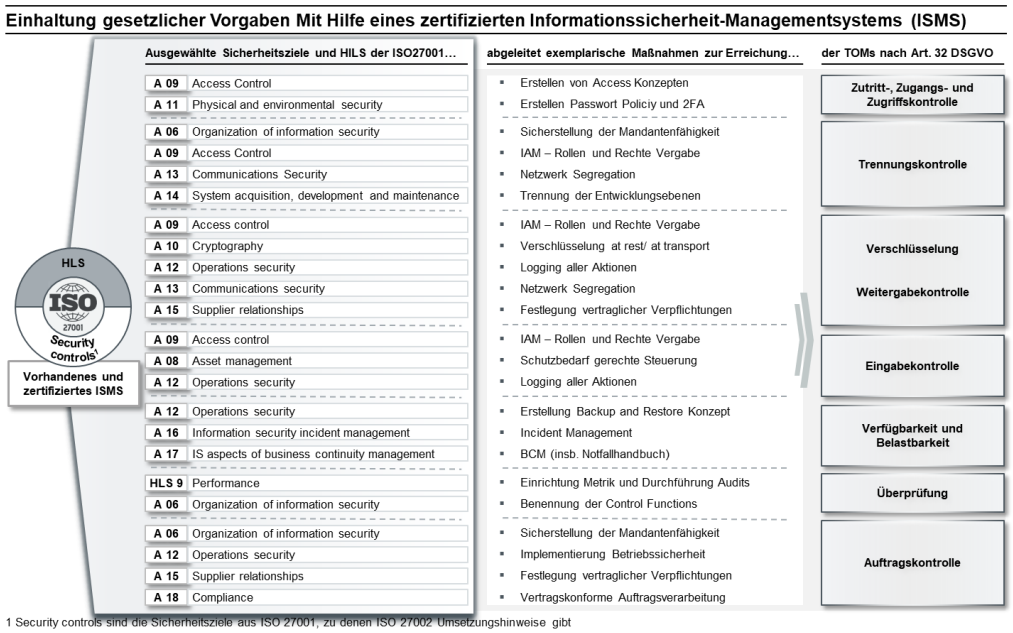


Abbildung 3: Erfüllung von Datenschutzanforderungen mit Hilfe eines ISMS

Die DSGVO verlangt den Einsatz von technischen Sicherheitsmaßnahmen zum Schutz von personenbezogenen Daten. Die einzelnen Techisch-Organisatorischen Maßnahmen (TOM) lassen sich aus Artikel 32 „Sicherheit der Verarbeitung“ wie folgt ableiten:

Artikel 32 Abs. 1	Maßnahme im Gesetz genannt	TOM durch Umsetzung ISMS
Satz 1	Zwecke der Verarbeitung	Trennbarkeit
lit. a	Pseudonymisierung und Verschlüsselung	Pseudonomysierung Verschlüsselung
lit. b	Vertraulichkeit	Benutzerkontrolle Zutrittskontrolle Zugangskontrolle Zugriffskontrolle Transportkontrolle
lit. b	Integrität	Übertragungskontrolle Eingabekontrolle Datenträgerkontrolle Speicherkontrolle Transportkontrolle
lit. b und c	Verfügbarkeit und Belastbarkeit	Zuverlässigkeit Wiederherstellbarkeit
lit. d	Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung	Datenschutz-Management Auftragskontrolle Verfügbarkeitskontrolle

Das Gesetz zum Schutz von Geschäftsgeheimnissen (GeschGehG) dient dem Schutz von Geschäftsgeheimnissen vor unerlaubter Erlangung, Nutzung und Offenlegung. Mit diesem Gesetz werden Unternehmen vor Spionage durch Wettbewerber besser geschützt. Voraussetzung für das Vorliegen eines Geschäftsgeheimnisses und damit der Schutzwirkung des Gesetzes sind allerdings „den Umständen nach angemessene Geheimhaltungsmaßnahmen“ (§2 Abs. 1 lit. b GeschGehG). Zusätzlich hängt nach § 9 lit. 2 GeschGehG ein Anspruchsausschluss bei Unverhältnismäßigkeit u.a. von den (nicht) getroffenen Geheimhaltungsmaßnahmen ab. Hieraus wird ersichtlich, dass die unmittelbare Schutzwirkung eines ISMS zum Erhalt der Schutzwirkung des GeschGehG beiträgt.

Als drittes Beispiel für Vorteile durch ein ISMS wird das Zahlungsdiensteaufsichtsgesetz (ZAG) angeführt. Die drei Paragraphen

- 53 „Beherrschung operationeller und sicherheitsrelevanter Risiken“
- 54 „Meldung schwerwiegender Betriebs- oder Sicherheitsvorfälle“
- 55 „Starke Kundenauthentifizierung“

stellen verschiedene Anforderungen an die technisch-organisatorische Umsetzung wie beispielsweise „Risikominderungsmaßnahmen und Kontrollmechanismen zur Beherrschung der operationellen und der sicherheitsrelevanten Risiken“, „wirksame Verfahren für die Behandlung von Störungen im Betriebsablauf“ und „Verfügen über angemessene Sicherheitsvorkehrungen,

um die Vertraulichkeit und die Integrität der personalisierten Sicherheitsmerkmale der Zahlungsdienstnutzer zu schützen“. Bereits an diesen Beispielen lässt sich die Vorteilhaftigkeit eines funktionierenden und umfassenden ISMS für ZAG-Anwendungsfälle belegen.

Zertifizierung nach ISO 27001 sollte angestrebt werden – How to

Der Aufbau eines ISMS ist für jedes Unternehmen ein großer Erfolg, jedoch muss dieses auch aktuell gehalten werden, soll der ständige Veränderungsdruck aus Änderungen der Infrastruktur, neuen Angriffen und neuen Schwachstellen mitigiert werden. Diese Verbindlichkeit des ISMS wird am besten über eine ISO 27001-Zertifizierung erreicht, die zur Erhaltung des Zertifikats jährlich neu erlangt werden muss – im ersten Jahr das Erstaudit mit den Teilprüfungen Stage 1 (Feststellung der Zertifizierungsfähigkeit) und Stage 2 (Erlangung des Zertifikats im Erfolgsfall), dann in den zwei nachfolgenden Jahren je ein Überwachungsaudit, nach 3 Jahren erneuter Start der Sequenz mit einem vollumfänglichen Erstaudit. Mit dem Zertifikat wird die Funktionsfähigeit des ISMS in Policies und Prozessen gegenüber internen und externen Stakeholdern nachgewiesen; beispielsweise muss die Sicherheit nicht bei jeder Verhandlung mit Kunden umständlich bewiesen werden. In der Regel reicht ein Nachweis des gültigen Zertifikats. Durch die Vorbereitung auf das Audit werden das Sicherheitsbewusstsein der relevanten Akteure in der Organisation geschärft und die IT-Infrastruktur gehärtet.

„Doch wie geht man konkret vor?“, ist die oft gehörte Frage. Unserer Erfahrung nach bedarf es Dreierlei:

1. Unterstützung des Managements
2. Umsetzung der Zwei-Pizza-Regel
3. Eine leere SOA (Settlement of Applicability)

Ohne das Bekenntnis des Managements die eigene Informationssicherheit durch ein zertifiziertes ISMS zu belegen kann das Vorhaben nicht gelingen. Es geht vor allem um die Zurverfügungstellung der benötigten personellen und finanziellen Ressourcen. Die personellen Ressourcen sollten dabei nicht zu üppig ausfallen, es dürfen nur so viele Teilnehmer im Team sein wie von zwei Pizzen satt werden. Diese Jeff Bezos zugeschriebene Regelbildung beschränkt das Team somit auf maximal acht Personen.

Das Team kann ausschließlich aus internen KollegInnen bestehen oder auch mit externer Unterstützung arbeiten. Wichtig ist, dass eine Person den Hut aufhaben muss und dabei mit gutem Beispiel vorangeht, d.h. nicht nur delegiert, sondern konkret mitarbeitet und das Team in der Selbstorganisation unterstützt. Das Team benötigt Expertise zur eigenen IT-Infrastruktur sowie zu ISMS/ISO 27001. Die letzt genannte Expertise kann von extern beigemischt werden. In diesem Falle arbeiten Interne und Externe Hand in Hand am Aufbau des ISMS, d.h. der Entwicklung der Policies und der Implementierung der Prozesse in die Organisation hinein. Letzteres kann zum Beispiel in Form von Schulungen mit den Leads stattfinden. Die Leads führen dann die Prozesse in ihre Organisationseinheiten ein. Ein guter Übergabepunkt der externen Unterstützung an die internen Kollegen stellt der Abschluss der Stage 2-Prüfung dar.

Den Start bildet eine leere „Erklärung der Anwendbarkeit“ (SOA). Dieses Dokument erklärt zum HLS und zu jedem security control die Maßnahme zu dessen Erfüllung und wird bei Erlangung

als einziges Dokument im Zertifikat genannt. Diese Maßnahmen kann die Nennung einer Policy, eines Prozesses oder die Beschreibung einer konkreten Maßnahme selbst sein. Hierbei sollte sinnvoll priosiert werden, sodass wichtige oder leicht umzusetzende Sicherheitsziele vor solchen angegangen werden, die als zweitrangig oder für den Beginn als sehr aufwendig angesehen werden. Mit diesem Vorgehen werden schnell erste und zugleich wichtige Erfolge erzielt. Ein möglicher Einstieg in das ISMS könnte wie folgt aussehen:

1. HLS Nr. 6 und Nr. 8: Risikomanagement
2. A.8: Wertemanagement (inkl. Informationsklassifizierung)
3. A.9: Zugangsmanagement (Zutritt, Zugang inkl. IAM[5], Zugriff)
4. A.16: Management von Sicherheitsvorfällen
5. A.17: Notfallmanagement inkl. BCM

Mit diesem strukturierten Vorgehen werden sukzessiv sämtliche Inhalte des ISO 27001-Standards bearbeitet.

Aus der Erfahrung der Autoren sind (teil-)automatisierte Tools keine sinnvolle Alternative zu einem eingespielten Team mit Fokus auf die pragmatische und strukturierte Abarbeitung der SOA. Werkzeuge beziehen Ihre Grundlagen aus detaillierten Informationen zu Daten, der IT-Infrastruktur und zu Informationsflüssen. Eine solche Modellierung als Grundlage des eigentlichen Prozesses zur Maßnahmenentwicklung scheitert erfahrungsgemäß an der Informationserlangung, dem Verlieren in Details oder einer unzureichenden Nachvollziehbarkeit berechneter Maßnahmen. Software bindet die Mitarbeiter nicht ein, sondern setzt sie vor vollendete Tatsachen, woraus in der Regel Akzeptanzprobleme resultieren.

Durch das beschriebene manuelle Vorgehen aus der Zwei-Pizza-Regel und als Beginn mit den ersten fünf besonders wichtigen und/oder für den Anfang leichteren Sicherheitszielen wird schnell ein stabiler und reifer Stand beim Aufbau des ISMS erreicht, der auch früh Erfolge der Erhöhung des Sicherheitsniveaus zeitigt. Danach werden alle weiteren Sicherheitsziele bearbeitet. Den Abschluss bilden die finale Aktualisierung der SOA und die Erstellung der Dokumentenlenkung – diese beschreibt den Aufbau des ISMS und die Abbildung von Maßnahmen auf HLS und security controls (Sicherheitsziele).

Fazit

Es ist eine Binse, aber Informationen sind die Ressource der Gegenwart, und sie werden es in der Zukunft noch mehr sein. Somit werden auch Angriffe weiter zunehmen, um Informationen zu stehlen, zu manipulieren oder unbrauchbar zu machen, denn mit Informationen wird legal wie illegal viel Geld verdient. Ohne entsprechend aufwachsende Abwehrmaßnahmen werden immer mehr Informationen der Unternehmen bei kriminellen Strukturen landen. Zusätzlich zum operativen Schaden können ein Reputationsschaden und ein Schaden aus Compliance-Verstößen entstehen, denkt man nur an Verletzung der DSGVO durch Verlust personenbezogener Daten. Dadurch steigt gleichermaßen der Bedarf nach Schutz der Informationen. Das Mittel der Wahl ist ein Informationssicherheits-Managementsystem. Ein ISMS

[5] Identity Access Management (Rollen & Rechte Management)

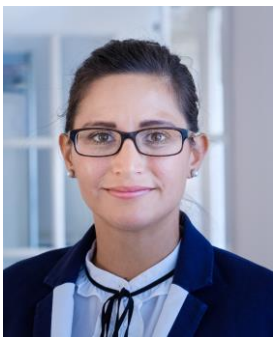
stellt die Baseline für ein reifes Sicherheitsniveau der Organisation dar, zertifitiert nach ISO 27001 mit Nachweis der professionellen Implementierung. Additiv ermöglicht ein ISMS die bessere Erfüllung von Compliance-Anforderungen wie aus Datenschutz und dem Schutz von Geschäftsgeheimnissen.

Die Erlangung des Zertfikats ist kein Hexenwerk, sondern die kontinuierliche, konzentrierte, klare und konsequente (4k's) Arbeit eines kleinen Teams von motivierten Personen, die das Ziel vereint, das Schutzniveau der Informationen des eigenen Unternehmens signifikant zu erhöhen und die erreichte Reife der Sicherheitsorganisation auch zu halten. Ausgehend von der Prämisse des „Drang zu Daten", d.h. dass immer mehr Wirtschaftsweisen zunehmend datengetrieben in das Internet überführt werden, muss man kein Prophet im eigenen Land sein, um feststellen zu müssen, dass Sicherheit in der Zukunft noch wichtiger sein wird und deshalb jetzt mit dem Aufbau eines ISMS begonenn werden sollte.

Quellen

1. **Angriffsziel deutsche Wirtschaft: mehr als 100 Milliarden Euro Schaden pro Jahr**
   https://www.bitkom.org/Presse/Presseinformation/Angriffsziel-deutsche-Wirtschaft-mehr-100-Milliarden-Euro-Schaden-pro-Jahr

Autoren



Nadine Hofmann ist Transformation Associate bei CORE. Ihr technischer Hintergrund liegt als Luft- und Raumfahrtingenieurin in der Konstruktion von Entwicklungsprozessen, sowie in der Produktion und Automatisierung. Bei CORE nutzt Nadine diese Erfahrung insbesondere für die Entwicklung zukunftsweisender Konzepte und Lösungen in der Informationssicherheit und unterstützt Kunden bei ihrer strategischen Geschäftsausrichtung durch den Einsatz innovativer Technologien.

Mail: nadine.hofmann@core.se

Dr. Waldemar Grudzien ist Expert Director und Datenschutzbeauftragter sowie Informationssicherheitsbeauftragter bei CORE und beschäftigt sich mit den Sicherheitsvorschriften der Finanzindustrie und deren technologischen Auswirkungen auf IT-Infrastrukturen. Während seiner Tätigkeit bei einem nationalen Verband der Finanzindustrie war er Spezialist für Retailbanking und Bankentechnologien. Er hat Elektrotechnik und VWL studiert.

Mail: waldemar.grudzien@core.se

Daniel Augustin ist Managing Director bei der SSE GmbH und ist für Strategie, Geschäftsentwicklung und Software-Engineering verantwortlich. Daniel ist ein Informatiker, der sich auf Software-Engineering und IT-Sicherheit spezialisiert hat. Als Gründungsmitglied und Geschäftsführer bringt er seine langjährige Erfahrung als IT-Sicherheitsberater, Entwickler, Architekt und Projektleiter für hochkritische Anwendungen ein.

Mail: daniel.augustin@securesystems.de

CORE SE
Am Sandwerder 21-23
14109 Berlin | Germany
https://core.se/
Phone: +49 30 263 440 20
office@core.se

COREtransform GmbH
Am Sandwerder 21-23
14109 Berlin | Germany
https://core.se/
Phone: +49 30 263 440 20
office@core.se

COREtransform GmbH
Limmatquai 1
8001 Zürich | Helvetia
https://core.se/
Phone: +41 44 261 0143
office@core.se

COREtransform Ltd.
Canary Wharf, One Canada Square
London E14 5DY | Great Britain
https://core.se/
Phone: +44 20 328 563 61
office@core.se

COREtransform Consulting MEA Ltd.
DIFC – 105, Currency
House, Tower 1
P.O. Box 506656
Dubai I UAE Emirates
https://core.se/
Phone: +97 14 323 0633
office@core.se