CISIS12

Bei CISIS12 handelt es sich um ein Vorgehensmodell zur Einführung eines Informationssicherheitsmanagementsystems (ISMS), das sich besonders an Klein- und Mittelstandsunternehmen sowie öffentliche Einrichtungen richtet. Anwender werden dabei durch konkrete Umsetzungsmaßnahmen und Handlungsempfehlungen entlang von 12 Schritten flankiert. Dadurch wird in erster Linie die Informationssicherheit der Organisation überprüft und im Rahmen des kontinuierlichen Verbesserungsprozesses abgesichert und optimiert. Die Einführung von CISIS12 kann durch unabhängige Zertifizierungsgesellschaften auditiert und testiert werden.

Von Frank Moses, Saarbrücken, und Thomas Rehbohm, Bremen

CISIS12 ist eine Fortentwicklung von ISIS12 – „Informationssicherheit in 12 Schritten" des IT-Sicherheitsclusters e. V. Regensburg. Dabei wurde darauf Wert gelegt, besonders die ganzheitliche Betrachtung der Organisation im Sinne von Compliance, Prozessen, Personalkomponenten, Stakeholdern, Infrastruktur und Risiken zu berücksichtigen und entsprechende Handlungsempfehlungen zur Umsetzung in der Praxis aufzunehmen.

Zielgruppe und Ausrichtung

Oft überfordert die Implementierung eines ISMS auf Basis von IT-Grundschutz des BSI oder der ISO 27001 aufgrund des Umfangs einerseits oder des generischen Ansatzes andererseits die Zielgruppe von Klein- und Mittelstandsunternehmen (KMU) sowie öffentlichen Organisationen (Kommunal-, Stadt- und Landratsverwaltungen). Genau an dieser Stelle setzt CISIS12 an: Das Vorgehensmodell unterstützt den Anwender durch einen klar definierten Ablauf entlang von 12 Schritten, um ein ISMS in der Organisation aufzubauen und nachhaltig zu betreiben.

Dabei wird einerseits auf bereits etablierte Vorgehensmodelle und Werkzeuge gesetzt, die auch aus den etablierten Managementsystemen bekannt sind – andererseits wird CISIS12 an den passenden Stellen sinnvoll ergänzt, zum Beispiel durch Berücksichtigung von Compliance-Vorgaben sowie die Implementierung von IT-Servicemanagementprozessen. An anderen Stellen geht CISIS12 speziell auf die Anforderungen der Zielgruppe ein (z. B. vereinfachtes Risikomanagement), ohne dabei die Allgemeingültigkeit oder Offenheit für andere Branchen (z. B. KRITS-Betreiber oder Automobilindustrie) zu verlieren.

CISIS12 kann als eigenständiger Standard zertifiziert werden: Hier stehen als Zertifizierungsgesellschaften die Deutsche Gesellschaft zur Zertifizierung von Managementsystemen (DQS) und die datenschutz-cert GmbH zur Verfügung – weitere Partner sind geplant (z. B. TÜV-Rheinland). Das Zertifikat hat nach bestandenem Audit eine Gültigkeit von 3 Jahren, wobei der kontinuierliche Verbesserungsprozess jährlich überprüft wird und nach zwei Überwachungsaudits ein Re-Zertifizierungsaudit erfolgt. Die Umsetzung kann durch am Markt erhältliche Werkzeuge unterstützt werden – der IT-Sicherheitscluster e.V. empfiehlt dazu M24S (https://m24s.info).

Vorgehensmodell

Die Umsetzung von CISIS12 wird durch eine inhärente Norm festgeschrieben. Nach einer Einleitung und Beschreibung des Anwendungsbereichs wird das Vorgehensmodell darin auf knapp 20 Seiten detailliert beschrieben. Im Fokus stehen in erster Linie:

- Rahmenbedingungen, Organisation und Führung,
- Personal, Dokumentation und Projektmanagement,
- Betrieb,
- Risikomanagement sowie
- Leistungsbewertung, Kontrolle und Verbesserung.

Diese Inhaltskapitel werden in Bezug zum PDCA-Zyklus gesetzt und die Umsetzung von CISIS12 durch den Durchlauf der 12 Schritte und die Handlungsempfehlungen des Baustein-Maßnahmenkatalogs beschrieben (vgl. Abb. 1). Gerade dieser Kreislauf vereinfacht die Einführung des ISMS und führt Anwender Schritt für Schritt zum Erfolg. Das Vorgehensmodell fokussiert zwar grundsätzlich 12 Schritte, empfiehlt aber darüber hinaus eine Initialisierung des Projekts (Schritt 0) und ein Audit (Schritt 13).

Schritt 0: Projekt-Start-up

Zunächst sollte man die notwendigen Fundamente zur erfolgreichen Projektumsetzung legen: Hierzu gehören die Erstellung eines

Quelle: kes – Zeitschrift für Informations-Sicherheit 38. Jahrgang/Nr. 1 Februar 2022

Projekt-Auftrags und einer Projekt-Planung, beispielsweise in Gestalt eines Projekt-Strukturplans. Ferner sollte die Leitungsebene einen Projektleiter bestimmen – gegebenenfalls kann man hier auf einen vom IT-Sicherheitscluster zertifizierten externen Berater zurückgreifen. Um den Projekterfolg sicherzustellen, sind die für das anstehende Projekt notwendigen Ressourcen festzulegen und zu steuern. Neben finanziellem Aufwand sind dabei auch entsprechende personelle Ressourcen zu berücksichtigen.

Schritt 1: Leitlinie

Im Fokus des ersten Schrittes steht die Erstellung einer Leitlinie zur Informationssicherheit als eines der Referenzdokumente der CISIS12-Norm. Diese sollte folgende Mindestinhalte umfassen:

- Verantwortung der Organisationsleitung
- Festlegung des Geltungsbereichs des ISMS
- Stellenwert der Informationssicherheit
- organisationsspezifische Sicherheitsziele in Verbindung mit den Geschäftszielen
- Leitaussagen zur Durchsetzung
- Beschreibung der Organisationsstruktur zur Umsetzung des Sicherheitskonzepts
- Einbindung der Mitarbeiter und Sanktionen bei Nichteinhaltung

Schritt 2: Sensibilisierung der Beschäftigten

In vielen Projekten steht die Berücksichtigung der Beschäftigten erst am Ende des Projekts – gerade das Thema Cybersicherheit trifft aber in aller erster Linie die Beschäftigten und auch Führungskräfte. Im Rahmen des zweiten Schritts muss daher auf Basis eines entsprechenden Konzepts ein Prozess etabliert werden, der die Schulung, Sensibilisierung und Information der Beschäftigten sicherstellt. Abhängig von der Organisationsgröße können hier Präsenzveranstaltungen, E-Learning-Plattformen oder auch Kleingruppenveranstaltungen zielführend sein. Wichtig ist jedoch, nach einer erstmaligen Sensibilisierung der Beschäftigten die Nachhaltigkeit durch ein Schulungskonzept zielgruppenspezifisch sicherzustellen.

Schritt 3: Informationssicherheitsteam

Die in der Beschreibung zu Schritt 0 bereits erwähnten Rollen werden nun schriftlich fixiert – Aufgaben, Rechte und Pflichten festgelegt und ein ISMS-Team formiert.

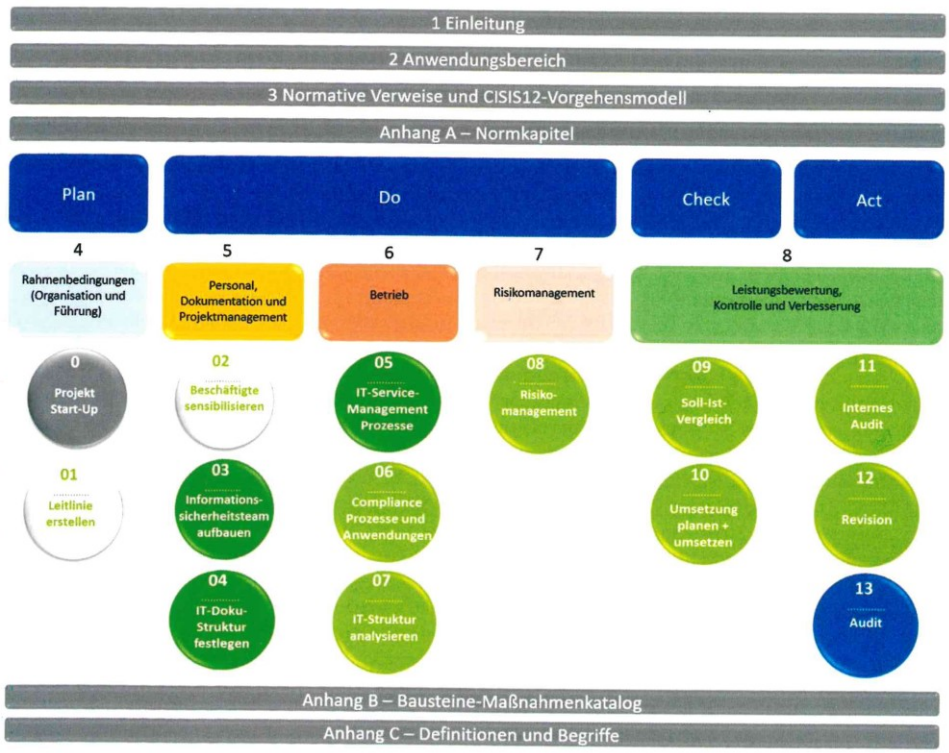

Abbildung 1: Zusammenhang der Inhaltskapitel, PDCA-Zyklus und CISIS12-Schritte

© DATAKONTEXT GmbH · 50226 Frechen · <kes> 2022*1

Quelle: kes – Zeitschrift für Informations-Sicherheit 38. Jahrgang/Nr. 1 Februar 2022

Abhängig von der Organisationsgröße ist festzulegen, mit welchen Rollen das anstehende ISMS-Projekt durchgeführt werden soll und welche Beschäftigten Rollen im Kernteam oder im erweiterten Sicherheitsteam einnehmen. Ungeachtet dieser Aufbauorganisation muss man in jedem Fall ein Mitglied der Organisationsleitung in das erweiterte Team integrieren.

Folgende Rollen bilden – neben dem Informationssicherheits- (ISB) und Datenschutzbeauftragten (DSB) – den Idealzustand ab:

- IT-Leiter
- Informationssicherheitskoordinatoren (nur bei größeren Organisationen)
- CISIS12-Berater
- Fachkraft für Arbeitssicherheit und/oder Qualitätsmanagementbeauftragter
- Gremienvertreter
- Facility-Management

Schritt 4: IT-Dokumentationsstruktur

Der in einem Managementsystem immanente PDCA-Zyklus stellt das „P für Plan" in den Vordergrund: Kein erfolgreiches Projekt, ohne guten Plan! Vor diesem Hintergrund wird im vierten Schritt des CISIS12-Vorgehensmodells die Erstellung und Fortschreibung einer für das ISMS passenden Dokumentationsstruktur fokussiert.

Dabei muss eine Dokumentation, die einerseits die Organisation beim Betrieb des ISMS unterstützen, aber andererseits auch als Nachweis für die Zertifizierung dienen soll, bestimmte Anforderungen an Strukturiertheit, Übersichtlichkeit, Vollständigkeit, Verständlichkeit, Korrektheit, Nachvollziehbarkeit, Objektivität, Integrität und Authentizität erfüllen. Durch die Erstellung einer Dokumentations-Vorlage inklusive der Definition formaler Dokumenten-Bestandteile, der Entwicklung eines Dokumenten-Lenkungsprozesses zur Erstellung und Fortschreibung sowie der Zuordnung von Verantwortlichkeiten für die Erstellung unterschiedlicher Dokumente werden diese Anforderungen erfüllt.

Die CISIS12-Norm benennt 15 Pflichtdokumente – von der Leitlinie sowie einem Schulungs- und Sensibilisierungskonzept unter anderem über Betriebshandbuch und Netzplan bis hin zu einem Managementbericht inklusive Umsetzungs- und Risikobehandlungsplan und Notfallhandbuch. Neben diesen zertifizierungsrelevanten Referenzdokumenten entstehen beim Durchlauf der 12 Schritte aber zwangsläufig weitere Dokumente – zum Beispiel Arbeitsanweisungen, Prozessbeschreibungen oder Konzepte. Nahezu alle Dokumentationen müssen den Beschäftigten bekannt gemacht und demzufolge gelenkt werden.

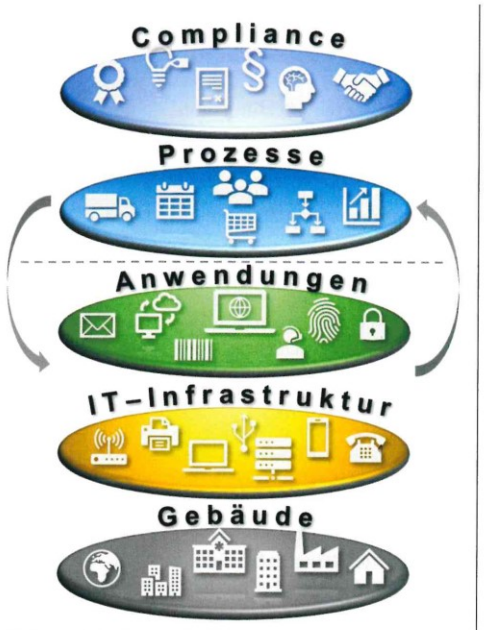

Abbildung 2: Schichtenmodell von CISIS12

Schritt 5: IT-Servicemanagement

Einer der wesentlichen Unterschiede zu anderen ISMS-Vorgehensmodellen ist die Implementierung eines IT-Servicemanagements in das CISIS12-Vorgehensmodell. Gerade die Implementierung klar definierter und beschriebener IT-Servicemanagementprozessen bildet einen wesentlichen Erfolgsfaktor für die Steigerung der Informationssicherheit und des ISMS-Reifegrads.

In Schritt 5 sind somit drei wesentliche IT-Servicemanagementprozesse organisationsspezifisch aufzubauen beziehungsweise bereits bestehende Prozesse in das ISMS zu integrieren und fortzuentwickeln:

- Wartungsprozesse (z. B. Steuerung und Durchführung von Patch- und Updateaufgaben)
- Änderungsprozesse (z. B. Etablierung eines sog. On-/Off-Boarding bei Personalwechsel)
- Störungsbeseitigungsprozesse

Das IT-Servicemanagement lässt sich in der Praxis durch weitere Werkzeuge ergänzen – zum Beispiel durch Ticketmanagementsysteme zur Erfassung und systematischen Abarbeitung von Störungs- und Wartungsarbeiten sowie Änderungsanforderungen, mit Wikis oder Dokumentenmanagementsystemen zur Unterstützung der Dokumentationsaufgaben oder CMDB-Systemen zur Unterstützung von Inventarisierungsaufgaben.

Quelle: kes – Zeitschrift für Informations-Sicherheit 38. Jahrgang/Nr. 1 Februar 2022

Schritt 6: Compliance, Prozesse und Anwendungen

Die Fortentwicklung von ISIS12 zu CISIS12 hat Anforderungen aus der Praxis aufgegriffen: nämlich sowohl gesetzliche Anforderungen und vertragliche Verpflichtungen (Compliance) als auch die Prozesssicht in das Managementsystem zu integrieren. Der Ansatz wurde dazu um zwei Schichten erweitert (Compliance- und Prozessschicht). Damit hat sich die Sichtweise gänzlich verändert und an die Sichtweise der Leitungsebene angepasst: „Welche rechtlichen Anforderungen und Compliance-Anforderungen muss ich erfüllen und wie können diese in der Praxis umgesetzt werden (Corporate Governance)?" Somit erleichtert CISIS12 der Leitungsebene das Handeln und die Delegation notwendiger Aufgaben zum Aufbau und zur Etablierung eines ISMS bei gleichzeitiger Erfüllung der gesetzlichen Vorgaben und Minimierung der Haftungsrisiken.

So werden in Schritt 6 auch die für eine Organisation wesentlichen Geschäftsprozesse identifiziert und hinsichtlich der Schutzbedarfe Vertraulichkeit, Integrität und Verfügbarkeit bewertet – sowie weitere Parameter wie die maximal tolerierbare Datenverlustzeit (MTD) und maximal tolerierbare Ausfallzeit (MTA) für die identifizierten Geschäftsprozesse ermittelt.

Diese Kriterien lassen sich toolgestützt auf Anwendungen und anschließend auf die IT-Infrastruktur und Gebäude vererben. Das bedeutet eine Erleichterung für Anwender, denn so werden nur die für die wesentlichen Geschäftsprozesse relevanten Anwendungen und die für Anwendungen wesentlichen IT-Infrastrukturelemente modelliert. Die anschließende Baustein- und Maßnahmenzuordnung erfolgt toolgestützt.

Schritt 7: IT-Infrastruktur

Die Erfassung von IT-Infrastrukturobjekten (z. B. Server, Clients, aktive Netzkomponenten, usw.) leitet sich aus den in Schritt 6 identifizierten Geschäftsprozessen und den für diese Geschäftsprozesse notwendigen Anwendungen ab. Somit tritt auch hier eine Vereinfachung für den Anwender ein – die Aufmerksamkeit lässt sich somit stärker auf die Umsetzung der Baustein- und Maßnahmenzuordnung lenken.

Schritt 8: Risikomanagement

Als eine weitere Neuerung im CISIS12-Vorgehensmodell ist das Risikomanagement zu nennen: Gerade die Ereignisse in den vergangenen Monaten haben gezeigt, dass der Aufbau eines Informationssicherheitsmanagements keinen Hygienefaktor im Sinne von „es geht auch ohne, aber etwas schlechter" mehr darstellt. Ein ISMS ist heute vielmehr ein Must-have (State of the Art) für alle Organisationen und ein darin etabliertes Risikomanagement ein wichtiges Instrument, um aus der Vergangenheit zu lernen und zukünftige Ereignisse besser einschätzen zu können. Die Risikobetrachtung kann toolgestützt über alle Schichten durchgeführt werden – und sollte auf das für den Anwender Wesentliche reduziert erfolgen. Die Risikobehandlung beziehungsweise deren Planung und Umsetzung erfolgt ebenfalls toolgestützt.

Schritt 9: Soll-Ist-Vergleich

In Schritt 9 werden auf die in den Schritten 6 und 7 erfassten Assets – Prozesse, Anwendungen, IT-Infrastrukturen und Gebäude – modellierte Maßnahmen aus dem CISIS12-Bausteinkatalog hinsichtlich ihres Umsetzungsgrad bewertet. Dieser Bewertungsprozess läuft im Rahmen eines gruppendynamischen Prozesses ab und stellt eine Selbstbewertung dar – er kann auch durch externe Dritte unterstützt werden. Die Bewertung erfolgt auch hier toolgestützt und bietet neuerdings erweiterte Auswertungsmöglichkeit in Bezug auf den Umsetzungs- und Reifegrad des ISMS auf Basis von CISIS12.

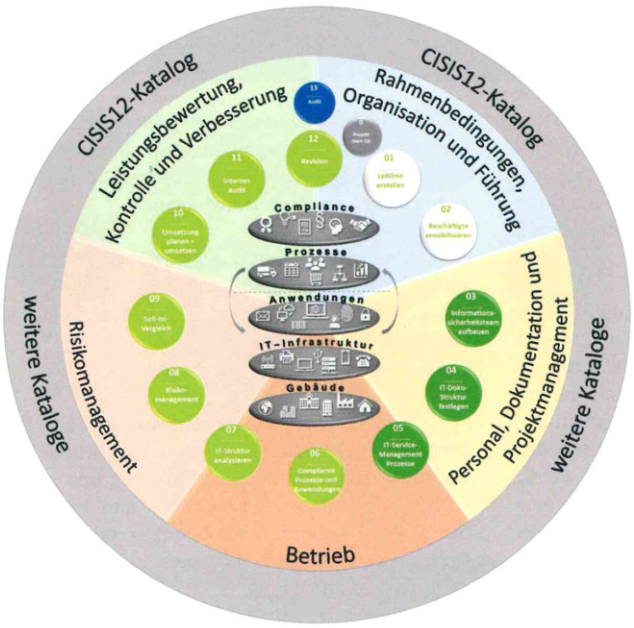

Abbildung 3: Kreislauf von CISIS12 und KVP

© DATAKONTEXT GmbH · 50226 Frechen · <kes> 2022*1

Quelle: kes – Zeitschrift für Informations-Sicherheit 38. Jahrgang/Nr. 1 Februar 2022

Schritt 10: Umsetzung

Die in Schritt 9 ermittelten Umsetzungsgrade der einzelnen Maßnahmen können in Schritt 10 toolgestützt in einen Umsetzungsplan überführt werden. Hierbei lassen sich einzelne Maßnahmen priorisieren, deren finanzieller und personeller Aufwand erfassen sowie die Rollen von Initiatoren und Umsetzern toolgestützt festlegen.

Kein System ist perfekt und „mehr" geht immer – das gilt auch für ein mit CISIS12 aufgebautes ISMS. Der Reifegrad eines Managementsystems entwickelt sich erst mit mehreren Durchläufen: Beim Erstaudit spricht man daher von einem Systemaudit, in dem bei der Zertifizierungsprüfung der Schwerpunkt auf Dokumentation und Umsetzung der Plandokumente („gelebter" Sicherheitsprozess) liegt. Im Überwachungsaudit wird dann später geprüft, wie sich das ISMS weiterentwickelt hat und wie sich diese Weiterentwicklung auf den Reifegrad auswirkt.

Schritt 11: Internes Audit

In Schritt 11 fordert CISIS12, ein Auditprogramm zu erstellen, das sowohl die jeweiligen Zertifizierungs- als auch internen Audits umfasst. Interne Audits sollen die nutzende Organisation in die Lage versetzen, ihr eigenes ISMS auf Schwachstellen hin zu untersuchen und entsprechend zu verbessern. Fehlt der Organisation die benötigte Expertise, kann dies auch durch entsprechend qualifizierte CISIS12-Berater erfolgen. Im Ergebnis muss jedenfalls ein interner Auditbericht für das Zertifizierungsaudit vorliegen.

Schritt 12: Revision

Die CISIS12-Schritte 1 bis 11 sind regelmäßig zu durchlaufen (z. B. jährlich) – Veränderungen und Ergänzungen können aber auch jederzeit in das Managementsystem eingebracht werden.

Schritt 12 fasst die Ergebnisse des letzten PDCA-Zyklus zusammen und endet mit der Erstellung eines Managementberichts. Dieser wird um Dokumente wie Umsetzungsplan und Risikobehandlungsplan ergänzt und sollte von der Leitungsebene im Rahmen einer Managementbewertung entsprechend gewürdigt werden. Gleichzeitig stellt der Managementbericht eines der zertifizierungsrelevanten Referenzdokumente dar.

Sobald die Leitungsebene den Managementbericht inklusive seiner Anlagen freigegeben hat, kann der nächste PDCA-Zyklus beginnen und der kontinuierliche Verbesserungsprozess eingeleitet werden. Der gesamte Prozess wird durch den CISIS12-Kreislauf – gegebenenfalls toolbasiert – unterstützt.

Schritt 13: Audit

Optional (empfohlen) bestätigt ein Zertifizierungsaudit die Umsetzung des ISMS. Gleichzeitig geht mit der Zertifizierung ein Nachweis für die Übernahme der Verantwortung der Leitungsebene einher und minimiert deren Haftung.

Normen im Kontext

Das Management von Informationssicherheit ist eine Führungsaufgabe – die Auswahl eines bestimmten Standards ist hingegen von mehreren Faktoren abhängig. Allem voran sind die Skalierbarkeit und die verbundenen Ressourcen in den Kontext der Organisation zu setzen: Die reine Größe der Organisation ist dabei nicht das wesentliche Element der Entscheidung – vielmehr die Fragen, wie viel Ressourcen man in die Implementierung und Aufrechterhaltung des ISMS geben muss, die Betrachtung relevanter Lieferanten in der Kette der IT-gestützten Leistungserbringung oder auch der risikobehaftete Betrieb von eigenen oder fremden Infrastrukturen.

Der Aufbau von CISIS12 macht deutlich, dass ISMS-Normen stets die gleiche Zielrichtung haben, in der Umsetzung jedoch unterschiedliche Wege vorsehen können, da unterschiedliche Schwerpunkte in der einzelnen Betrachtung bestehen (vgl. Tab. 1). Durch die offen entworfene Architektur lassen sich mit CISIS12 unterschiedliche interne und externe Interessen erfüllen: Das Vorgehensmodell ermöglicht ebenso eine native Umsetzung der CISIS12-Anforderungen wie die Umsetzung weiterer Normen – alternativ oder ergänzend. Inhaltlich verbundene Anforderungen oder Standards, wie zum Beispiel aus dem Datenschutz, können toolgestützt involviert werden.

Gleichzeitig eröffnet sich mit dem CISIS12-Vorgehensmodell die Möglichkeit, Unternehmen und Behörden ohne Größenrestriktionen zu adressieren. CISIS12 nimmt mit seinem transparenten und einfachen Vorgehensmodell und in Verbindung mit dem empfohlenen Tool M24S somit nach Meinung der Autoren einen Platz zwischen den etablierten Standards ein und schließt die Lücke zu einer prozessgesteuerten Methode und zu den Elementen des Projektmanagements.

CISIS12 zielt darauf ab die Organisationen anzusprechen, für die IT-Grundschutz oder ISO 27001 zu umfassend, zu aufwendig oder zu abstrakt sind oder die Einstiegshürde zu hoch ist. Ferner kann das Vorgehensmodell für Organisationen hilfreich sein, die branchenspezifische Sicherheitsstandards, wie den B3S „Krankenhaus", den Kommunalkatalog des BSI oder den I-KFZ-Katalog des KBA, einsetzen müssen. Darüber hinaus ist eine Ent-

© DATAKONTEXT GmbH · 50226 Frechen · <kes> 2022*1

Quelle: kes – Zeitschrift für Informations-Sicherheit 38. Jahrgang/Nr. 1 Februar 2022

wicklung des CISIS12-ISMS in erweiterten Ausrichtungen fortwährend möglich.

Forschung und Regulierung

Die Informations- und Cybersicherheit von Organisationen und Infrastrukturen in Wirtschaftsunternehmen und dem öffentlichen Dienst sind im wissenschaftlichen Diskurs durchaus relevant. Aktuelle Arbeiten adressieren dabei zum Beispiel die Versorgungssicherheit von ländlichen Regionen, das Gesundheitssystem oder auch staatliche Leistungen (wie Bildung, Bibliotheken etc.) unter dem Aspekt des demografischen Wandels – bis hin zur allgemeinen Versorgung von Gütern, Lebensmitteln, Energie, Telekommunikation, Wasser- und Abwasser-Ver- und -Entsorgung. Es handelt sich dabei nicht ausschließlich um Bevölkerungswissenschaft als solche, sondern vielmehr um Beiträge im Kontext kritischer Infrastrukturen (s. a. S. 48).

In der EU und ihren Mitgliedstaaten versucht man, mit der Richtlinie über Maßnahmen zur Gewährleistung eines hohen gemeinsamen Sicherheitsniveaus von Netz- und Informationssystemen in der Union (NIS-Richtlinie) ein vereinheitlichtes Vorgehen zu etablieren. Auch die Datenschutzgrundverordnung (DSGVO) zielt in dieselbe Richtung und verpflichtet zu einem Informationssicherheitsmanagement (Implikation) in allen Organisationen, unabhängig davon, ob man als kritische Infrastruktur eingestuft ist oder nicht.

Im Föderalstaat Deutschland werden zuvorderst gesetzliche Regelungen auf Bundesebene geschaffen, um die Informations- und Cybersicherheit stärker rechtlich zu verankern. Die IT-Sicherheitsgesetzgebung adressiert – aus Sicht des Bundes – ebenfalls vor allem kritische Infrastrukturen. Schließlich kann der Bund nicht ohne Weiteres Regelungen für die Länder treffen und regelt demnach auch die Informationssicherheit von Ländern und Kommunen nicht direkt. Gleichwohl wird mit der Portalverbundsverordnung zum Onlinezugangsgesetz dieser Vorstoß in Teilen indirekt vorgenommen.

Studien zeigen zudem, dass vor allem die kommunalen Strukturen in Deutschland oft kein- oder nur ein rudimentäres Informationssicherheitsmanagement betreiben. Gleichzeitig erweisen sich IT-Servicemanagementprozesse dort als nicht sonderlich ausgeprägt. Veröffentlichungen zu kritischen Infrastrukturen, besonders solchen, die *nicht* unter das IT-Sicherheitsgesetz fallen, liefern Hinweise auf gleichartige Herausforderungen und Defizite.

Wenige Länder bieten Wirtschaftsunternehmen und kommunalen Strukturen Kooperationsmöglichkeiten bei der Abwehr von Bedrohungen für die Informationssicherheit an. Bislang hat auch kein Land Wirtschaftsunternehmen von besonderem öffentlichem Interesse und kommunale Strukturen zur Resilienz-Erhöhung gegen Cyberbedrohungen oder zur Auskunft über den jeweiligen Zustand ihrer Informationssicherheit verpflichtet.

Tabelle 1: ISMS-Standards im Vergleich

	CISIS12	ISO 27001	Grundschutz-Kompendium	VdS 10000
Herausgeber	IT-Sicherheitscluster e.V.	International Standardization Organization – ISO	Bundesamt für Sicherheit in der Informationstechnik – BSI	VdS Schadenverhütung GmbH
Norm	ja, 30 Seiten	ja, 30 Seiten	ja, Vorgabedokumente ca. 250 Seiten	nein, lediglich Kapitel mit Anforderungen
Ausrichtung	DACH-Region	international	Deutschland	Deutschland
Zielgruppe	Organisationen jeder Größe als auch Behörden	beliebige Organisationen	Organisationen jeder Größe als auch Behörden	KMU, Public Sector, sonstige Organisationen
Komplexität	hoch	hoch	hoch	niedrig
Aufbau und Umfang des Katalogs	Norm mit Vorgehensmodell, 86 Bausteine und 1000 Maßnahmen	Maßnahmenempfehlungen entlang 114 Controls	knapp 100 Bausteine mit ca. 1100 Maßnahmen	Checklistencharakter
Risikoanalyse	ja, verpflichtend	ja, verpflichtend	ergänzend bei hohem Schutzbedarf	optional bis verpflichtend
Umsetzung	Vorgehensmodell mit konkreten Maßnahmen	kein Vorgehensmodell, allgemein formulierte Maßnahmen	abstrakt formuliertes Vorgehensmodell, Maßnahmenumsetzung auf Basis eines Maßnahmenkatalogs	Umsetzung allgemeiner Maßnahmen auf Basis einer Checkliste
Zertifizierungsmöglichkeit	ja, unabhängige akkreditierte Zertifizierungsgesellschaften	ja, unabhängige akkreditierte Zertifizierungsgesellschaften	ja, BSI-Zertifizierung	ja, VdS-Zertifizierung
Tool-Unterstützung	Ja	Ja	Ja	nein

Quelle: kes – Zeitschrift für Informations-Sicherheit 38. Jahrgang/Nr. 1 Februar 2022

Staatliche Stellen in Europa, in Deutschland und seinen Bundesländern adressieren das Thema rechtlich, soweit möglich und zielführend, im Kontext des Datenschutzes und der Daseinsvorsorge – einhergehend mit Verpflichtungen zum Betrieb eines ISMS und dem erforderlichen Austausch von Meldungen zur aktuellen Bedrohungslage. Eine Hilfestellung zur Umsetzung dieser Anforderungen existiert gleichwohl nicht – auch nicht auf wissenschaftlicher Ebene. Es wird lediglich regelmäßig auf bestehende Standards des Bundesamts für Sicherheit in der Informationstechnik (BSI) verwiesen.

Hier springt CISIS12 mit seinem Vorgehensmodell ein und möchte die Chance bieten, mit einer strukturierten und frameworkübergreifenden Architektur ein ISMS einzuführen, das konform, überprüfbar und nachhaltig aufgebaut werden kann.

Fazit

– *Vorgehensmodell:* CISIS12 bringt nicht nur einen Katalog und ein Maßnahmenbündel mit, sondern will Anwender vielmehr in die Lage versetzen, sich der Herausforderung „ISMS" professionell zu stellen – ohne spezifisches Know-how eines Projektmanagements, gegebenenfalls mithilfe einer externen Beratung durch Unternehmen oder Erfahrungen in der Umsetzung von Zertifizierungsstandards. Das schrittweise Abarbeiten aller Inhalte des Vorgehensmodells erleichtert die Erstellung notwendiger Konzepte und die Umsetzung von technischen und organisatorischen Maßnahmen.

– *Offenheit* für weitere Branchen und Standards: Auch wenn CISIS12 einen eigenen Katalog mitbringt, bedeutet die Erfüllung dieser Anforderungen nicht das Ende einer ISMS-Einführung. Moderne IT bedarf auch eines dynamischen und an den externen Kontext ausgerichteten Informationssicherheitsmanagements. Dabei sind die einschlägigen ISO-Standards oder der BSI-Grundschutz ebenso „in" CISIS12 implementierbar wie Standards des Automotive-Bereichs, aus Organisationen der kritischen Infrastrukturen (B3S) und selbstverständlich des Datenschutzes. CISIS12 wurde an den Anforderungen der Wirtschaft und des öffentlichen Dienstes ausgerichtet und weiterentwickelt.

– *Toolunterstützung:* Mit dem vom IT-Sicherheitscluster empfohlenen Tool M24S steht ein leistungsfähiges, mandantenfähiges und hochverfügbares System als Clouddienstleistung aus einem deutschen Rechenzentrum zur Verfügung. Dabei wird sichergestellt, dass das Tool zum Management der Informationssicherheit dient und nicht zwingend vertrauliche Daten in der Cloud ablegt. Durch diese Trennung verbleibt die Datensouveränität bei der nutzenden Organisation.

– Unabhängige *Zertifizierung:* Die einst lokal beschränkte Entwicklung eines Managementsystems für den öffentlichen Dienst und KMU für eine begrenzte Beschäftigtenzahl ist schon länger seinen Kinderschuhen entwachsen. Ein hohes Wachstum und eine große Nachfrage nach CISIS12 wird auch durch die mittlerweile von den zwei derzeitigen Zertifizierungsgesellschaften ausgegebenen 300 Zertifikate belegt. Weitere Anfragen von Zertifizierungsgesellschaften liegen vor.

Cyberbedrohungen werden in den nächsten Jahren weiter steigen – zusätzlich ist eine neue Qualität der Angriffe zu erwarten und die Komplexität der immer stärker vernetzten IT-Infrastrukturen steigt. Ein probates Mittel, um Risiken und im Falle eines Falles auch Schäden zu minimieren, stellt weiterhin der Aufbau und nachhaltige Betrieb eines ISMS dar. CISIS12 bildet hierzu eine gute Möglichkeit, sich dem Thema zu stellen. ■

Frank Moses war CISO des Saarlandes, Thomas Rehbohm ist CISO der Freien Hansestadt Bremen. Beide Autoren forschen zudem am Lehrstuhl für Wirtschaftsinformatik von Prof. Dr. Kurt Sandkuhl an der Universität Rostock und gehören dem sechsköpfigen Entwicklerteam von CISIS12 an.

© DATAKONTEXT GmbH · 50226 Frechen · <kes> 2022*1

Quelle: kes – Zeitschrift für Informations-Sicherheit 38. Jahrgang/Nr. 1 Februar 2022