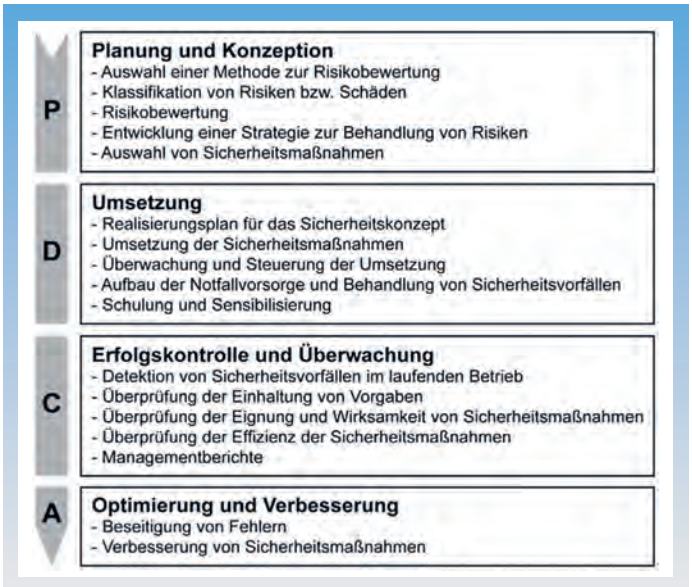
Umsetzung eines ISMS

In den vergangenen Folgen haben wir sehr viel über die Anforderungen an ein Informationssicherheitsmanagementsystems (kurz ISMS) kennengelernt. Wie die Umsetzung aussieht, wie man idealerweise vorgeht, fehlt aber komplett. Hier können die Standards 200-x des deutschen Bundesamts für Sicherheit in der Informationstechnik (BSI) helfen.



Lebenszyklus, BSI 200-1, Seite 33.

Das BSI hatte bereits im Dezember 2005 die kostenlosen Standards 100-1 und 100-2 veröffentlicht. Im 100-1 wird Schritt für Schritt beschrieben, was ein erfolgreiches Informationssicherheitsmanagement ausmacht und welche Aufgaben der Leitungsebene und Unternehmen zukommt. Der Standard 100-2 beschreibt jede Phase ausführlich, wie der IT-Grundschutz umgesetzt werden kann. Beide Standards stiessen auf grosses Interesse, standen aber in der Kritik, vor allem auf Behörden einzugehen. Nach einer kompletten Überarbeitung wurden die beiden Standards im Oktober 2017 durch die Nachfolger 200-1 und 200-2 abgelöst. Sie sind damit 100 Prozent kompatibel zur ISO 27001:2013.

ZUM AUTOR

Andreas Wisler, Dipl. Ing FH
goSecurity AG
Schulstrasse 11
CH-8542 Wiesendangen

T +41 (0)52 511 37 37
www.goSecurity.ch
wisler@gosecurity.ch

Hinweis: Nicht weiter erläutert werden die Standards 200-3 (Risikoanalyse auf der Basis von IT-Grundschutz) und 200-4 (Business Continuity Management, Community Draft).

Standard 200-1

Dieser Standard ist in Deutsch und Englisch verfügbar. Während ISO 27001 die Anforderungen definiert, beantwortet der BSI-Standard folgende Fragen:

- Was sind die Erfolgsfaktoren beim Management von Informationssicherheit?
- Wie kann der Sicherheitsprozess vom verantwortlichen Management gesteuert und überwacht werden?
- Wie werden Sicherheitsziele und eine angemessene Sicherheitsstrategie entwickelt?
- Wie werden Sicherheitsmassnahmen ausgewählt und Sicherheitskonzepte erstellt?
- Wie kann ein einmal erreichtes Sicherheitsniveau dauerhaft erhalten und verbessert werden?

Das Kapitel 3 geht auf die Kern-Komponenten eines Managementsystems ein. Es sind dies:

- der Sicherheitsprozess, welcher eine Leitlinie, ein Konzept und die Organisation umfasst;
- die notwendigen Ressourcen;
- die Mitarbeiter, inkl. deren Aufgaben und Verantwortlichkeiten; sowie
- die Management-Prinzipien.

Den zuletzt genannten Management-Prinzipien wird ein ganzes Kapitel gewidmet. Bereits die ISO 27001 verlangt im Kapitel 5 «Führung» verschiedene Punkte von der obersten Leitung. Im 200-1 werden diese weiter ausgeführt. Es handelt sich um die folgenden sechs Punkte:

- Übernahme der Gesamtverantwortung für Informationssicherheit
- Informationssicherheit initiieren, steuern und kontrollieren
- Informationssicherheit integrieren
- Erreichbare Ziele setzen
- Sicherheitskosten gegen Nutzen abwägen
- Vorbildfunktion

Weitere Punkte im Kapitel 4 sind die Kommunikation und Wissen (4.2), die Erfolgskontrolle im Sicherheitsprozess (4.3) sowie die kontinuierliche Verbesserung des Sicherheitsprozesses (4.4).

Gerade die Kommunikation stellt einen Erfolgsfaktor für die Informationssicherheit dar. Dies beinhaltet unter anderem die Berichte an die Leitungsebene.

Dies beinhaltet Probleme, Ergebnisse von Audits und Überprüfungen, neue Entwicklungen, Veränderungen, aber auch Verbesserungsmöglichkeiten. Auch muss der Informationsfluss im gesamten Unternehmen sichergestellt sein.

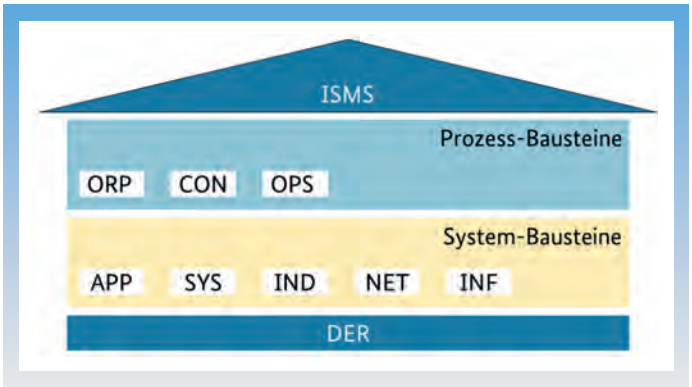
Werden neue Richtlinien oder Weisungen verabschiedet, müssen diese allen involvierten Personen zugestellt werden. Es muss unter allen Umständen verhindert werden, dass jemand sagt «davon habe ich nichts gewusst».

Bei der Erfolgskontrolle geht es um die Überprüfung des aktuellen Standes. In der ISO-Norm wird dies die Management-Bewertung genannt (ISO 27001, Kapitel 9.3). Ist das Unternehmen noch auf dem richtigen Kurs? Haben sich Anforderungen geändert? Gibt es Rückmeldungen von interessierten Parteien, aber auch Resultate von Audits?

Sind die Informationssicherheitsziele noch passend? Abweichungen und Veränderungen werden schriftlich erfasst und Massnahmen geplant, umgesetzt, kontrolliert und wieder zurückgemeldet. Mit diesen Schritten kann sich ein Unternehmen kontinuierlich weiter verbessern und die Informationssicherheit damit erhöhen.

In kurzen Kapiteln werden die notwendigen Ressourcen (5) und die Einbindung der Mitarbeiter in den Sicherheitsprozess (6) beschrieben.

Ausführlich beschrieben ist der Sicherheitsprozess in Kapitel 7. Unterteilt ist das Kapitel in die Planung (Ermittlung von Rahmenbedingungen, Definition von Sicherheitsziele, Ermitteln eines angemessenen Sicherheitsniveaus), den Aufbau der Sicherheitsorganisation, die Umsetzung, die Aufrechterhaltung und die kontinuierliche Verbesserung. Details zu diesen Themen sind im BSI-Standard 200-2 mit konkreten Beispielen enthalten.



Bausteine IT-Grundschutz-Kompendium, Seite 23.

Ebenfalls ausführlich beschrieben wird das Sicherheitskonzept in Kapitel 8. Es ist nach dem PDCA-Ablauf (Plan, Do, Check, Act) aufgebaut. Es umfasst den folgenden Lebenszyklus:

Das Kapitel 9 beschreibt den Weg zu einer erfolgreichen Zertifizierung des ISMS. Details dazu finden Sie in der Ausgabe «Maschinenbau 2022/5: ISO 27001: Der Weg zur Zertifizierung».

Das Kapitel 10 geht auf die IT-Grundschutz-Methodik und verbindet das ISMS mit dem IT-Grundschutz-Kompendium. Dieses bereits 1000 Seiten umfassende Werk inkl. weiterführenden Informationen ist kostenlos im Internet aufrufbar. Das Kompendium ist in zehn Bausteine unterteilt und bietet damit eine ganzheitliche Betrachtung der Informationssicherheitsthemen:

Die Abkürzungen stehen dabei für:

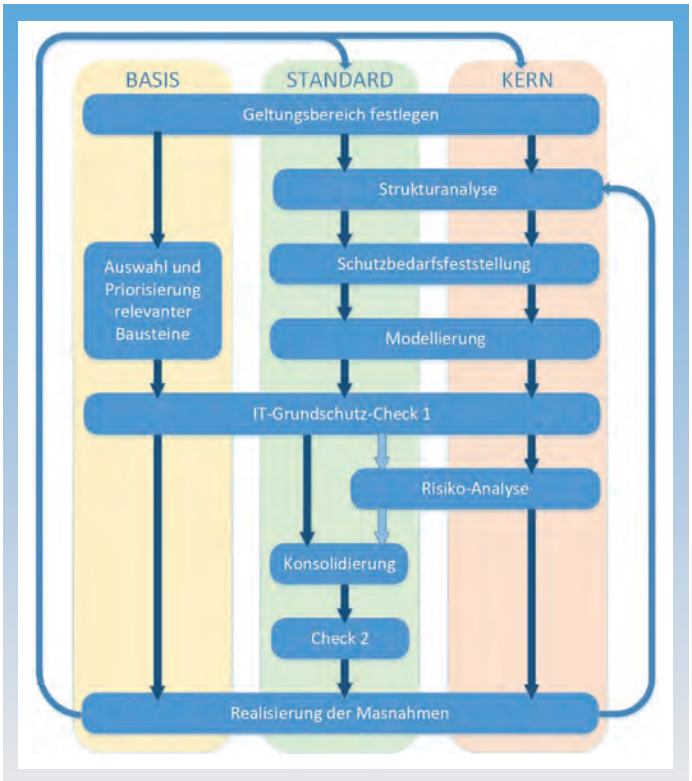
- ISMS: Informationssicherheitsmanagementsystem
- ORP: organisatorische und personelle Sicherheitsaspekte
- CON: Konzepte und Vorgehensweise
- OPS: Sicherheitsaspekte betrieblicher Art
- APP: Absicherung von Anwendungen und Diensten
- SYS: IT-Systeme
- IND: Sicherheitsaspekte industrieller IT
- NET: Vernetzungsaspekte
- INF: infrastrukturelle Sicherheit
- DER: Detektion und Reaktion von Sicherheitsvorfällen

In jedem dieser Bausteine werden Gefährdungen und konkrete Massnahmen beschrieben, inklusive den verantwortlichen Personen und Kontrollfragen.

Standard 200-2

Der ebenfalls kostenlos verfügbare Standard mit dem Titel «IT-Grundschutz-Methodik kann in Deutsch auf der Homepage des BSI heruntergeladen werden.

Diese Methodik beschreibt, wie ein ISMS in der Praxis aufgebaut und betrieben werden kann. Die Aufgaben des Informationssicherheitsmanagements und der Aufbau einer Organisationsstruktur sind dabei wichtige Elemente. Es orientiert sich an den drei Vorgehensweisen Basis-, Kern- und Standard-Absicherung.



Vergleich Basis-, Kern- und Standard-Absicherung.

Basis-Absicherung

Die Basis-Absicherung ermöglicht einen Einstieg in die Thematik. Es ist eine breit angelegte Erst-Absicherung. Die Massnahmen werden nicht bis ins letzte Detail umgesetzt verlangt.

Kern-Absicherung

Die Kern-Absicherung ermöglicht den Sicherheitsprozess auf besonders gefährdete Geschäftsprozesse oder Werte (im Standard Kronjuwelen genannt) zu legen. Nachteilig ist, dass allenfalls ebenfalls wichtige Geschäftsprozesse nicht betrachtet werden.

Standard-Absicherung

Die Standard-Absicherung ermöglicht den im Standard 200-1 beschriebenen Ansatz vollständig umzusetzen. Als Endergebnis kann eine Zertifizierung nach ISO 27001 durchgeführt werden.

Wie das Bild zeigt, steigt der Aufwand an die Umsetzung. Wie von ISO 27001 her schon bekannt, wird im ersten Schritt der Anwendungsbereich definiert. Es ist möglich, auch Teilbereiche eines Unternehmens durch den Prozess zu führen und nicht das gesamte. Dies macht beispielsweise Sinn, wenn ein kritischer Bereich vorhanden ist, zum Beispiel der Betrieb eines Rechenzentrums. Eine Unterteilung muss jedoch gut überlegt werden, steigt damit doch der Aufwand zur genauen Definition der Schnittstellen. Bei kleineren Unternehmen macht dies oft keinen Sinn, da dadurch der Aufwand sogar steigen kann.

Im Kapitel 4 wird die Organisation des Sicherheitsprozesses aufgezeigt. Der Kapitel-Aufbau entspricht dem Standard 200-1, zeigt aber konkrete Beispiele für grosse, mittelgrosse und kleine Institutionen. Weiter werden Rollen wie der Informationssicherheitsbeauftragte, das IS-Management-Team, die Bereichs- und Projekt-Sicherheitsbeauftragte, der ICS-Informationssicherheitsbeauftragte, den IS-Koordinierungsausschuss, die Datenschutzbeauftragte inkl. deren Aufgaben sowie das Zusammenspiel mit anderen Einheiten oder dem Bezug von externen Spezialisten sehr detailliert aufgezeigt.

Das Kapitel 5 geht auf die Dokumentation im Sicherheitsprozess ein. Ein wichtiger Aspekt ist die Klassifikation von Informationen und der Informationsfluss. Die Kapitel 6 bis 8 beschreiben im Detail die Vorgehensweise der Basis-, Kern- und Standardabsicherung. In der Strukturanalyse wird erfasst, welche Mittel vorhanden sind. Dies umfasst die Erfassung der Prozesse, der Anwendungen, den Systemen, Netzwerkkomponenten, Räumen, Menschen und Kommunikationsverbindungen. Danach wird der Schutzbedarf festgelegt. Dieser geht von den Prozessen aus und vererbt sich auf die Anwendungen, von dort auf die Systeme usw. Details zu diesem Vorgehen sind im Beitrag im «maschinenbau 2020/12: Genügend vorbereitet auf einen Notfall» zu finden. Wenn diese Tätigkeit abgeschlossen ist, werden die genutzten Bausteine aus dem Kompendium bestimmt und einem Soll-Ist-Vergleich unterzogen. In jedem Baustein sind mehrere Massnahmen beschrieben und es gilt nun die Frage zu beantworten, ob diese im eigenen Unternehmen umgesetzt sind (Ja, Teilweise, Nein). Alles, was einen erhöhten Schutzbedarf hat, der nicht mit dem Grundschutz-Kompendium abgedeckt werden kann, muss zusätzlich einer Risiko-Analyse unterzogen werden. Alle Resultate werden anschliessend konsolidiert und nochmals kurz auf Vollständigkeit überprüft, bevor es dann an die Umsetzung der offenen Massnahmen geht.

Die Kapitel 9 bis 11 gehen noch auf die Umsetzung, die Aufrechterhaltung und kontinuierlichen Verbesserung sowie der Zertifizierung nach ISO 27001 ein.

Mit den beiden Standards BSI 200-1 und -2 stehen ausführliche Leitfäden zum Aufbau eines ISMS zur Verfügung. Alle notwendigen Elemente werden sehr detailliert beschrieben. Die Absicherung in drei Stufen ermöglicht einen pragmatischen Weg zur Umsetzung der Informationssicherheit im eigenen Unternehmen. Im ersten Moment sieht dies zwar nach einem grossen Aufwand aus, die gut strukturierte Vorgehensweise führt aber zielsicher zum gewünschten Ergebnis, der erfolgreichen Zertifizierung des eigenen ISMS.