Mittelstand 4.0
Kompetenzzentren
Deutschlandweit

AG IT-Sicherheit

Ein Leitfaden zum Informations-sicherheitsmanagement

Mittelstand-
Digital

Gefördert durch:

Bundesministerium
für Wirtschaft
und Energie

aufgrund eines Beschlusses
des Deutschen Bundestages

Editorial

Liebe Leserinnen und Leser,

Informationssicherheit ist in aller Munde. Jeder hat davon gehört und die meisten sind sich mittlerweile einig: Digitalisierung ohne Sicherheit birgt Risiken.

Viel Unsicherheit herrscht jedoch bei der Frage, welche konkreten Risiken das im Einzelfall sind und welchen Stellenwert sie für eine Organisation haben können.

Wir denken, dass kleine und mittlere Unternehmen in die Lage versetzt werden sollten, Informationssicherheitsrisiken selbstständig zu identifizieren, ihre Eintrittswahrscheinlichkeit einzuschätzen und anschließend diesbezüglich eine strategische Entscheidung treffen zu können.

Um dies zu gewährleisten ist eine systematische Vorgehensweise notwendig, die prozessual gedacht werden muss. Ein Informationssicherheitsmanagementsystem (ISMS) beschreibt diesen Prozess und ermöglicht ein adäquates Vorgehen für jedes Unternehmen, unabhängig von der Größe und dem Wertschöpfungssegment.

In dieser Handreichung möchten wir kleinen und mittleren Unternehmen einen ersten Einblick in das Thema ermöglichen und aufzeigen, welche Absicherungswege im Einzelfall sinnvoll sind.

Wir möchten alle Interessierten dazu motivieren, sich mit dem Thema zu beschäftigen, ohne Sorge vor großen Investitionen zu haben. In vielen Fällen, ist mit vergleichsweise geringem Ressourcenaufwand der Betrieb eines ISMS sinnvoll möglich.

Dr. Frauke Goll
Leitung der
AG-IT-Sicherheit

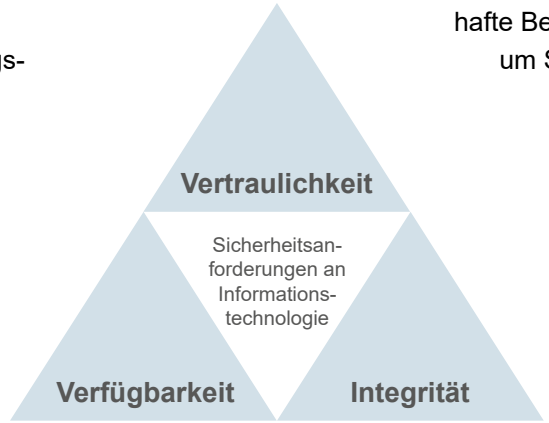
Dr. Thomas Usländer
Leitung der
AG-IT-Sicherheit

Inhalt

Einleitung

Digitalisierung ist für Unternehmen eine Chance, neue Geschäftsfelder zu entdecken, Dienste anzubieten, Kompetenzen auszubauen oder das eigene Arbeiten zu unterstützen. Dabei sollte die Digitalisierung als Werkzeug zur Unterstützung qualifizierter Arbeit verstanden werden, um die Arbeitspraxis der Mitarbeiterinnen und Mitarbeiter im Unternehmen zu unterstützen.

Mit zunehmendem Digitalisierungsgrad steigt jedoch auch die allgemeine Abhängigkeit von digitalen Geschäftsprozessen[1]. Ein Ausfall kann dann große Auswirkungen haben. Grundlegende Sicherheitsanforderungen an Informationstechnologie sind im CIA-Dreieck dargestellt. CIA steht dabei für:



Vertraulichkeit (Confidentiality) stellt die Anforderung, dass Informationen nur den Personen zur Verfügung stehen sollten, die berechtigt sind, die Information zu haben.

Integrität (Integrity) bedeutet, dass die Informationen nicht unberechtigterweise verändert werden, sondern in der Form vorliegen sollen, wie erwartet.

Verfügbarkeit (Availability) besagt, dass Informationen zur gewünschten Zeit verfügbar sein sollen.

Ist eine dieser Dimensionen verletzt, bedeutet dies ein Risiko für die datenbasierenden Geschäftsprozesse. Eine Gefährdung kann von unterschiedlichen Szenarien ausgehen: ein gezielter Angriff, der Ausfall von Hardware oder die unbeabsichtigte fehlerhafte Bedienung können Gründe sein, um Schäden zu verursachen.

Es ist also wichtig, die richtigen Maßnahmen zum Schutz der etablierten Digitalisierungs- und IT-Vorhaben zu treffen. Mit dieser Broschüre wird ein Einblick in Maßnahmen gegeben, die dazu beitragen können, das Informationssicherheitsniveau in Ihrer Organisation zu erhöhen und Risiken zu evaluieren. Es existieren unterschiedliche Vorgehensmodelle, um strategisch Maßnahmen zu planen und im Risikofall Entscheidungshilfen zu geben. Diese sollen hier kurz vorgestellt werden, um Ihnen dabei zu helfen, das passende Vorgehensmodell zu finden.

1 https://www.bitkom.org/sites/default/files/file/import/160803-Whitepaper-Digitale-Prozesse.pdf (letzter Zugriff: 03.11.2021)

Was ist Informationssicherheitsmanagement?

a) Definition

„Mit (Informations-)Sicherheitsmanagement wird die Planungs-, Lenkungs- und Kontrollaufgabe bezeichnet, die erforderlich ist, um einen durchdachten und wirksamen Prozess zur Herstellung von Informationssicherheit aufzubauen und kontinuierlich umzusetzen. Ein funktionierendes Sicherheitsmanagement muss in die existierenden Managementstrukturen jeder Institution eingebettet werden.“[2]

Bundesamt für Sicherheit in der Informationstechnik (BSI)

Ein Informationssicherheitsmanagementsystem (ISMS) beinhaltet also Regeln und Rollen, die darauf abzielen, das Informationssicherheitsniveau in einer Organisation durch Sensibilisierung und die Verteilung von Verantwortung zu erhöhen. Ein ISMS entsteht in der Regel nicht im „luftleeren Raum“. Es ist Teil der Organisationsstrategie und muss deshalb in existierende Managementsysteme eingefügt werden. Dies ist deshalb wichtig, da ein ISMS nicht für sich stehen kann, vielmehr muss es den „Risikoappetit“ der Organisation abbilden.

Im Zeitalter der Digitalisierung wird ein Großteil der Informationen, die in Organisationen existieren, auf virtuellen Systemen verarbeitet. Jedoch gibt es in den meisten Organisationen nach wie vor Informationen und Werte, die analog verarbeitet werden. Zudem gibt es Informationen, deren Status leicht von „virtuell“ zu „analog“ wechseln kann. Ein typisches Beispiel hierfür ist das Drucken von Dokumenten: Man kann ein virtuelles Dokument technisch gut absichern, sobald jedoch das Dokument auf ein Blatt Papier abgedruckt wird, ist es nicht mehr verschlüsselt und für jeden einsehbar.

Ein ISMS befasst sich deshalb mit der Absicherung aller Informationen, die in einer Organisation generiert werden und die als besonders schützenswert befunden werden – digital sowie analog.

2 https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Grundschutz/Kompendium_Einzel_PDFs_2021/01_ISMS_Sicherheitsmanagement/ISMS_1_Sicherheitsmanagement_Edition_2021.pdf?__blob=publicationFile&v=2, S. 1 (letzter Zugriff: 03.11.2021)

b) ISO27000er-Reihe

Das Themenfeld „Informationssicherheit“ wird in der ISO/IEC-27000-Reihe beschrieben. Zentral für die Implementierung eines ISMS ist die ISO/IEC 27001, da in dieser Norm die Anforderungen an ein ISMS beschrieben werden.

Begriffsnorm	**27000** Überblick und Terminologie eines ISMS		
Anforderungsnorm	**27001** Anforderung an ISMS 27701 Datenschutz	**27006** Anforderungen an die Zertifizierungsstelle	**27009** Sektorspezifische Anwendung
Leitfadennormen	**27002** Leitfaden (Code of Practice)	**27003** Einführungsleitlinie	**27004** Messungen
	27005 Risikomanagement	**27007** Leitfaden zu Audits	**TR 27008** Richtlinien für Auditoren
	27013 Einführung 27001 und 20000	**27014** Governance von IS	**TR 27016** Wirtschaftlichkeit
Sektor-spezifische Leitfadennormen	**27010** Übergreifende Kommunikation	**27011** TK-Organisation	**27017** 27002 für Cloud Dienste
	27018 Daten Public Cloud	**27019** Energieversorger	

Die Anforderungsnorm bildet die Definitionsmerkmale der entsprechenden ISO ab. Die Leitfadennorm zeigt mögliche Wege für einzelne Bereiche auf. Die Sektor-spezifische Leitfadennorm beschreibt für spezielle Sektoren die Normen genauer.

Damit die ISO/IEC 27001 für eine Vielzahl von Organisationen aus verschiedenen Bereichen (Behörden, wertschöpfende Unternehmen, NGOs, …) anwendbar ist, sind die Anforderungen generisch formuliert.

Um diese Anforderungen zu konkretisieren und Organisationen bei der Implementierung der ISO/IEC 27001 zu unterstützen, haben das Bundesamt für Sicherheit in der Informationstechnik (BSI) sowie weitere Akteure Hilfestellungen entwickelt. Diese sollen im weiteren Verlauf des Kapitels vorgestellt werden.

c) ISO/IEC 27001 „nativ“

Alle Anforderungen an ein ISMS befinden sich in der ISO/IEC 27001. Manche Informationssicherheitsmanager empfinden die Absicherungswege, die von Staat und Wirtschaft angeboten werden als zu komplex und konzentrieren sich deshalb auf die generischen Anforderungen aus dieser Norm. Die Anforderungen in der Norm beziehen sich dabei primär auf den Informationssicherheitsprozess, weniger auf die umzusetzenden Maßnahmen. Der native Absicherungsweg bedeutet, dass alle Informationen für die Absicherung aus der 27001 und 27002 herangezogen werden. Dabei konzentriert sie sich stärker auf den abstrakteren Informationssicherheitsprozess an sich. Bei dem BSI-Grundschutz wird dieser auch betrachtet. Gleichzeitig wird jedoch ein Maßnahmenorientierter Ansatz verfolgt, bei welchem auch konkrete Vorgaben gemacht werden.

Die Implementierung nach ISO/IEC 27001 „nativ“ ist in einigen Fällen sinnvoll – insbesondere, wenn das notwendige Know-how existiert, um selbst Maßnahmen zu entwickeln, die das Informationssicherheitsniveau erhöhen. Dies kann der Fall sein, wenn eine Organisation selbst im Sicherheitskontext arbeitet und Lösungen anbietet oder ein erfahrener Informationssicherheitsmanager die Implementierung des ISMS übernimmt.

Wenn dies jedoch nicht der Fall ist, dann wird die Bewertung der Bedrohungslage für diverse Objekte im Informationsverbund[3] sowie die Entwicklung von Maßnahmen schnell äußerst ressourcenintensiv.

d) IT-Grundschutz

Der IT-Grundschutz wurde durch das BSI zunächst für die Umsetzung in Behörden entwickelt. Heute wird dieser Absicherungsweg jedoch auch in Unternehmen und anderen Organisationen verwendet.

In den Varianten „Standardabsicherung“ und „Kernabsicherung“ ist der IT-Grundschutz kompatibel mit der ISO/IEC 27001 – das bedeutet, dass nach erfolgreicher Umsetzung des IT-Grundschutzes eine Zertifizierung nach dieser Norm möglich ist.

In der dritten Variante, der „Basisabsicherung“, ist der IT-Grundschutz nicht zertifizierungsfähig nach ISO/IEC 27001. Dafür gibt es in dieser Variante die

3 Objekte sind Bestandteile des Informationsverbundes, dazu zählen z. B. Server, Netzwerkstrukturen, Geschäftsprozesse etc.

Möglichkeit, ein Testat zu erhalten, das die Umsetzung der Basisabsicherung bestätigt.

Für kleine und mittlere Unternehmen (KMU) ist insbesondere die letzte Variante durchaus attraktiv, da durch einen vergleichsweise geringen Ressourcenaufwand ein adäquates Informationssicherheitsniveau geschaffen werden kann.

Der IT-Grundschutz ist in seiner Umsetzung umfangreicher als andere Absicherungswege. Dafür wird der Anwender in allen Schritten an die Hand genommen und erhält ein wertvolles Tool: Das IT-Grundschutzkompendium. In diesem Konvolut aus Bausteinen bekommt der Anwender für diverse Objekte des Informationsverbundes[4] (physische Infrastruktur, IT-Systeme, Organisation, Personal, …) Hilfestellung. Für jedes dieser Objekte beschreibt das BSI die Bedrohungslage und definiert darauf aufbauend die Anforderungen aus Informationssicherheitsperspektive.

Anforderungen an die Konfiguration eines Webservers nach der Basis-Absicherung

„Nachdem der IT-Betrieb einen Webserver installiert hat, MUSS er eine sichere Grundkonfiguration vornehmen. Dazu MUSS er insbesondere den Webserver-Prozess einem Benutzerkonto mit minimalen Rechten zuweisen. Der Webserver MUSS in einer gekapselten Umgebung ausgeführt werden, sofern dies vom Betriebssystem unterstützt wird. Ist dies nicht möglich, SOLLTE jeder Webserver auf einem eigenen physischen oder virtuellen Server ausgeführt werden. Dem Webserver-Dienst MÜSSEN alle nicht notwendige Schreibberechtigungen entzogen werden. Nicht benötigte Module und Funktionen des Webservers MÜSSEN deaktiviert werden."

Auszug aus dem IT-Grundschutz-Kompendium

Neben dem IT-Grundschutz-Kompendium hat das BSI gemeinsam mit seiner „Community"[5] verschiedene Grundschutz-Profile entwickelt. Die Grundschutzprofile sind eine Vorlage, welche nach dem IT-Grundschutz konzipiert ist. Diese Vorlage bietet Unternehmen mit ähnlichen Arbeitsgebieten, Branchen oder Sektoren die Möglichkeit ressourcenschonend ein ISMS erstellen.

Der IT-Grundschutz ist in seiner Umsetzung umfangreicher als die „native" Absicherung nach der ISO/IEC 27001 – jedoch birgt er gerade für KMU einige Vorteile:

- Durch das IT-Grundschutz-Kompendium haben auch unerfahrene Informationssicherheitsmana-

4 Der Informationsverbund beschreibt alle relevanten physischen und virtuellen Komponenten, die im Geltungsbereich des ISMS liegen.
5 Es handelt sich hierbei um Verbände und andere Akteure, die sich in einem bestimmten Wertschöpfungssegment besonders gut auskennen und somit beschreiben können, welche Herausforderungen in diesem Segment gehäuft auftreten.

ger die Möglichkeit ein adäquates Sicherheitsniveau für ihre Organisation herzustellen
- Da die verschiedenen Absicherungsvarianten (Basis-, Standard- und Kernabsicherung) konsekutiv aufgebaut sind, kann das Sicherheitsniveau schrittweise erhöht werden, je nach verfügbaren Ressourcen und „Risikoappetit“ der Organisation.

e) Trusted Information Security Assessment Exchange (TISAX)

TISAX wurde vom Verband der Automobilindustrie entwickelt und berücksichtigt die speziellen Anforderungen der Automobilwelt mit Blick auf die Informationssicherheit. Dieser Absicherungsweg leitet seine Anforderungen jedoch, ähnlich wie der IT-Grundschutz, aus der ISO/IEC 27001 ab.[6] Die Implementierung von TISAX wird immer häufiger zur Voraussetzung für die Zusammenarbeit mit der Automobilindustrie und diversen Segmenten, die mit ihr zusammenarbeiten – dies gilt insbesondere für Zulieferer und Forschungseinrichtungen.

Auch TISAX bietet eine Reihe von Hilfestellungen an, die auf der Website des Verbands der Automobilindustrie (VDA) abrufbar sind.

Die Prüfung des Zertifizierungsschemas erfolgt durch einen Prüfdienstleister der bei der ENX Association akkreditiert ist. Die ENX Association ist ein Zusammenschluss von Automobilherstellern, Zulieferern und vier nationalen Automobilverbänden, die als neutrale Instanz im Themenfeld Informationssicherheit mitwirken.

Vor dem Hintergrund der wachsenden Bedrohung durch Supply-Chain-Angriffe stellt ein generelles Zertifizierungsverfahren für Zulieferer einen bedeutenden Punkt in der IT-Sicherheitsarchitektur dar.

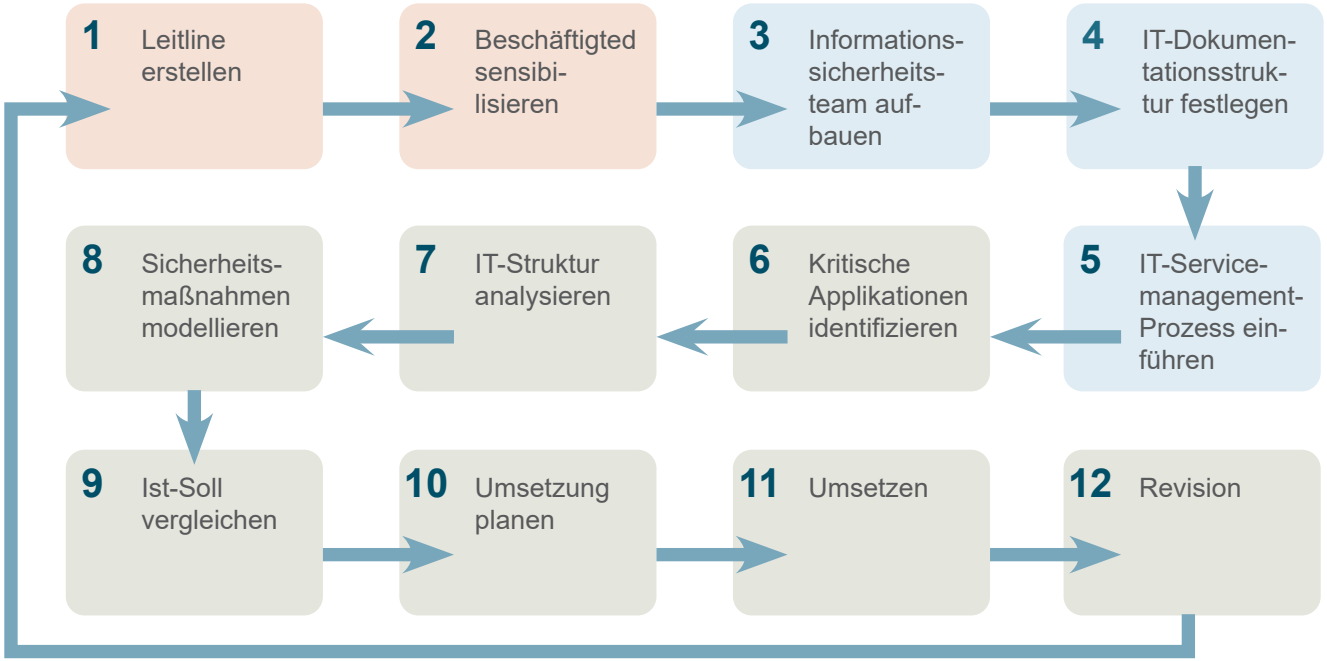
f) Weitere Absicherungswege und Frameworks

Neben den aufgeführten Absicherungswegen gibt es viele weitere Wege, die zu einer Erhöhung des Informationssicherheitsniveaus führen. Eine kleine Auswahl finden Sie hier:

- IEC 62443 „Industrial Network and System Security“ befasst sich mit ganzheitlich mit der Cybersecurity von " Industrieller Automatisierungs- und Steuerungssysteme ", d.h. die Normenreihe liefert den Ansatz zur sicheren Implementierung für Betreiber, Integratoren und Herrsteller.
- VDI 2182 „Informationssicherheit in der industriellen Automatisierung Allgemeines Vorgehensmodell“. Sie beschreibt durch konkrete Schutzmaßnahmen, wie die Informationssicherheit von Anlagen und automatisierten Maschinen gewährleistet werden kann.

6 Weitere Informationen wie die Empfehlungen zur Informationssicherheit sowie den VDA ISA Katalog in der Version 5.0 finden Sie unter: https://en.vda.de/de/themen/sicherheit-und-standards/informationssicherheit/informationssicherheit-sicherheitsanforderungen.html (letzter Zugriff: 03.11.2021)

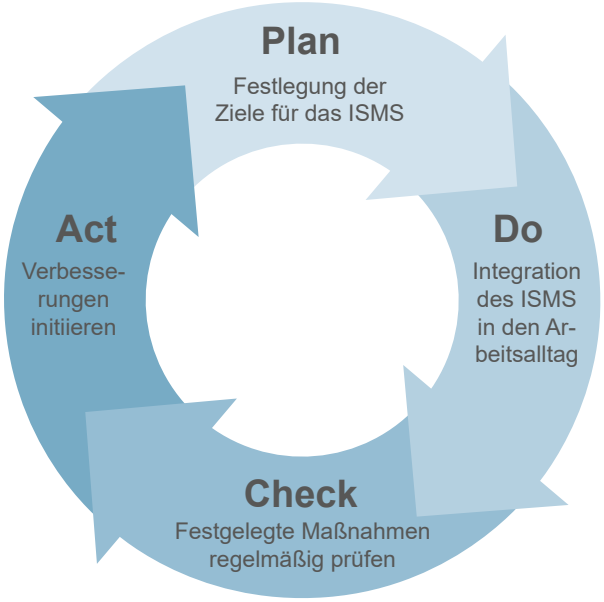
- Regelwerk VdS 10000 Informationssicherheitsmanagementsystem für KMU, welches mit wesentlich geringeren Ressourcenaufwand im Vergleich zur ISO 27001 ein angemessenes Schutzniveau schaffen kann.
- CISIS12 bietet einen einfachen Überblick und Einstieg in das Handlungsfeld der Informationssicherheit für KMU (siehe Schaubild unten).



CISIS12 Umsetzungsmodell: Initialisierungsphase: 1–2, Ablauf- und Aufbauorganisation 3–5, Entwicklung und Umsetzung 6–12

Erste Schritte bei der Implementierung

ISMS besitzen einen Aufbau, der sich an dem so genannten PDCA-(Plan-Do-Check-Act)-Zyklus orientiert. Ursprünglich wurde dieser Regelkreis für das Qualitätsmanagement in Unternehmen entwickelt, um eine stark prozessorientierte Sicht auf die Organisationen zu ermöglichen. Hieraus entstand der Anspruch, dass Prozesse sich kontinuierlich verbessern müssen.



PDCA-Zykus bei der Implementierng eines ISMS

Über die Jahrzehnte hat sich der PDCA-Zyklus für viele Managementsysteme etabliert, so dass sich auch die meisten ISMS an diesem orientieren. Für viele Unternehmen ist diese Sichtweise aufgrund der Anwendung der Qualitätsmanagementnorm DIN EN ISO 9001:2015 nicht neu, so dass sich auch die Einführung eines ISMS an diesen Punkten gestalten lässt. Ein weiterer wesentlicher Vorteil für KMU ist, dass die schrittweise Verbesserung einen einfacheren Einstieg ermöglicht und die Anforderungen an in Gänze nicht schon zu Beginn erfüllt sein müssen. Informationen, die in ersten Iterationsschritten noch nicht vorlagen oder beachtet wurden, können bei weiteren Zyklen im Sinne des kontinuierlichen Verbesserungsprozesses nachträglich ergänzt werden. Es lohnt sich also „klein“ anzufangen und das ISMS über die Zeit immer weiter zu detaillieren.

Dokumentation und Zugänglichkeit

Schon frühzeitig sollten die notwendigen und neu erstellten Informationen systematisch dokumentieren werden. Hierbei ist darauf zu achten, dass die Mitarbeiterinnen und Mitarbeiter einen guten Zugang zu diesen erhalten. Dazu sollten die Informationen auch möglichst kurz und prägnant dargestellt sowie einfach aufzurufen sein. So bietet es sich an, dass je nach Berechtigung und Organisationseinheit die jeweils relevanten Informationen zur Verfügung gestellt werden.

In vielen Fällen können strukturierte Dateiablagen auf Softwareprogramme, Intranetlösungen oder Share-

points genutzt werden, um so auch Revisionen oder Ergänzungen zeitnah an die Mitarbeiterinnen und Mitarbeiter weitergegeben zu können.

Zyklusphase – „Plan“

Generell ist es für diese und die darauffolgenden Phasen wichtig, dass das Management bzw. die Geschäftsführung komplett hinter der Implementierung eines ISMS steht. Sie muss auch dafür sorgen, dass genug Ressourcen zur Einführung und Pflege des ISMS zur Verfügung gestellt werden. IT-Sicherheit ist also Chefsache! Trotzdem sollte schon frühzeitig ein Kernteam aus den wesentlichen Expertinnen und Experten bzw. den Hauptnutzerinnen und -nutzern einzelner Unternehmensbereiche und der IT gebildet werden, damit die nachfolgenden Planungsschritte fundiert und nah an ihrem Arbeitsalltag aufgebaut werden können.

Die Phase „Plan“ stellt bei einer ersten Implementierung die größte Herausforderung dar, da zunächst die Grundinformationen zur Organisation und den Prozessen zusammengetragen werden müssen, um daran eine Entscheidung zur Festlegung der Ziele für das ISMS zu treffen. Dabei sind die Ziele als ein dynamischer Prozess zu verstehen, welche sich immer wieder an den Stand der Technik anpassen. Dementsprechend sollten sich KMU zunächst einmal eine Übersicht zum eigenen IT-Sicherheitsniveau aufbauen.

Diese Übersicht lässt sich in bestimmten Bereichen auch aus dem technischen und organisatorischen Maßnahmen (TOM) aus dem Datenschutzmanagementsystems (DSMS) übernehmen. Dabei ist zu beachten, dass in bestimmten Bereichen durch das DSMS eine Konformität zwischen DSGVO und dem ISMS hergestellt werden muss.

Nachfolgend finden Sie einen schrittweisen Ablauf, wie eine solche Zyklusphase „Plan“ geordnet ablaufen sollte, um beste Rahmenbedingungen für die weiteren Phasen zu schaffen.

a) Analyse des eigenen Sicherheitsniveaus

Je nach Komplexität der eigenen Organisation, dem bisherigen Umgang sowie den Erfahrungen mit dem Thema IT-Sicherheit bzw. Datenschutz, liegen unterschiedliche IT-Sicherheitsniveaus in den einzelnen Unternehmen vor. Daher sollten zunächst standardisierte Wege gewählt werden, um eine fundierte Abschätzung zu erzielen. In der Praxis haben sich dafür unterschiedliche Tools und Regelwerke etabliert. Ein Beispiel hierfür ist das Sicherheitstool Mittelstand www.sitom.de[7]. Hiermit lassen sich, angelehnt an Kriterien des IT-Grundschutzes des BSI und der ISO 27001, die grundlegenden Themenkomplexe der Managementsysteme auf das eigene Unternehmen projizieren und bewerten. Erste Problemstellungen, Zielkriterien und Handlungsempfehlungen können daraus für das ISMS abgeleitet werden.

7 https://www.sitom.de/home (letzter Zugriff: 03.11.2021)

b) Dokumentation von Informations- und Kommunikationstechnologien sowie Datenstrukturen

Nach einer ersten Einschätzung des Niveaus ist eine Dokumentation der eigenen IT- und Netzwerkumgebung zu empfehlen. Dies umfasst neben der Hard- und Software auch die wesentlichen Daten, mit denen im Unternehmen gearbeitet wird. Dadurch kann festgestellt werden, wer mit wem und mit welchen Inhalten kommuniziert. Folgende Datenarten können unterschiedenen werden:

- personenbezogene Daten (z. B. Kunden, Lieferanten)
- Produkt- und Materialdaten (z. B. CAD-Zeichnungen, Programmcode)
- technisch-infrastrukturelle Daten (z. B. Prozessanweisungen, Gebäudepläne)

Unternehmen haben hierbei oftmals unterschiedliche Auffassungen, welche Daten schützenswert sind. Als besonders wertvoll werden häufig die „Kronjuwelen“ des Unternehmens bezeichnet, die sich aus dem einzigartigen Geschäftszweck ergeben. Daneben könnten aber auch gesetzliche Anforderung (Datenschutz, Produkthaftung) wichtige Kriterien für diese Bewertung sein.

c) IT-Sicherheitsschutzziele definieren

In Abhängigkeit von a) und b) sind für die einzelnen analysierten Unternehmensbereiche die IT-Sicherheitsschutzziele zu definieren. Zur Aufstellung dieser Ziele haben sich die Prinzipien des CIA-Dreiecks etabliert (siehe Seite 4).

d) Leitbild, Sicherheitsrichtlinien und Sicherheitsprozesse aufstellen

In diesem Schritt sollte die Organisation eine Art Leitbild für das ISMS aufbauen. Hierzu gehört, dass die Ziele und die Gründe zur Einführung des ISMS konkret für die Mitarbeiterinnen und Mitarbeiter ausgearbeitet werden. Daraus sollten sich die ersten wichtigen Sicherheitsrichtlinien und Sicherheitsprozesse abarbeiten lassen. Dies kann ergänzend zu einem bereits bestehenden Managementsystem entstehen. Viele Unternehmen werden auch bzgl. der Sicherheitsprozesse und -richtlinien nicht bei Null anfangen, so dass häufig schon einige Anweisungen hinsichtlich des Umgangs mit mobilen Endgeräten/Datenträgern, der Datensicherung, Passwortvergabe oder dem Umgang mit Sicherheitsvorfällen existieren. Häufig wird bei diesen Prozessen auch schon auf die Verwendung und Umsetzung von Sicherheitsmaßnahmen bzw. -technologien verwiesen.

Wichtig ist, dass Unternehmen bei der Aufstellung der Richtlinien und Prozesse strukturiert vorgehen, ohne sich (insbesondere bei den ersten Iterationen) im Detail zu verlieren. Zur Strukturierung kann ein „Top-Down-Ansatz“ gewählt werden. Alternativ kann es auch hilfreich sein, dass Unternehmen in verschiedene Betriebsbereiche (Produktion, Vertrieb usw.), räumlich (Werkstatt, 1. Etage etc.) oder

themenbezogen (z. B. Datensicherung, mobile Endgeräte) eingeteilt werden. Ein nützliches Tool kann dabei der „Routenplaner: Cyber-Sicherheit für Handwerksbetriebe“ sein[8], der nicht nur für Handwerker sondern auch für viele andere kleine Unternehmen hilfreich ist.

e) Verantwortlichkeiten festlegen

Zu jedem ISMS gehören auch verantwortliche Personen im Unternehmen, die sowohl als Ansprechpartner dienen als auch die kontinuierliche Pflege übernehmen. Oftmals werden diese als „Informationssicherheitsbeauftragter“ beschrieben. Zudem ist zu empfehlen für die zuvor etablierten Sicherheitsprozesse auch „Prozessbeauftragte“ einzuführen, die sich um die Umsetzung dieser kümmern und im laufenden Betrieb die Maßnahmen koordinieren.

Zyklusphase – „Do“

Los geht es! Mit den zuvor durchgeführten Schritten kann mit der Integration des ISMS in den Arbeitsalltag im Unternehmen begonnen werden. Achten Sie dabei auf eine klare Kommunikation mit allen Mitarbeiterinnen und Mitarbeitern. Es bietet sich auch an, wesentliche Punkte in kleineren Schulungen aufzugreifen, Informationen zielgerichtet auszugeben und sie zur Mitarbeit aufzufordern. Nur so kann das ISMS in diesem Schritt auch in der Praxis getestet werden.

Es kann in ersten Iterationsphasen durchaus Sinn ergeben, nicht das komplette Unternehmen zu involvieren, sondern erst in kleineren Einheiten zu testen. So können grobe Fehler in Prozessen und Sicherheitsrichtlinien schon früh beseitigt werden. Dies befördert auch eine spätere Akzeptanz im gesamten Unternehmen.

Weiterhin können in dieser Phase weitere Maßnahmen zur Unterstützung der Sicherheitsprozesse im Rahmen der „praktischen Optimierung“ ausgearbeitet und etabliert werden.

Zyklusphase – „Check“

Regelmäßig (z. B. quartalsweise) sollten die festgelegten Maßnahmen, Richtlinien und Prozesse auf den Prüfstand gestellt werden. Diese sind anhand der festgelegten IT-Sicherheitsziele objektiv zu bewerten. Es wäre u.a. denkbar, die Wirksamkeit von Schulungs- und Sensibilisierungsmaßnahmen zu Phishing-Attacken zu prüfen, welche die Vertraulichkeit und Verfügbarkeit von Informationen negativ beeinflussen. Hierbei ist es wichtig einen Bewertungsmaßstab zu entwickeln.

Alternativ lassen sich automatisierte Tools einsetzen, welche die IT-Systeme auf Schwachstellen durchleuchten. Dies kann sowohl durch Penetrati-

8 https://www.mittelstand-digital.de/MD/Redaktion/DE/Publikationen/routenplaner-cybersicherheit.pdf (letzter Zugriff: 03.11.2021)

onstests[9], Brute-Force-Attacken[10] oder den Abgleich mit Schwachstellen-Datenbanken geschehen. Dabei sollen Unternehmen sowohl einen Schwerpunkt auf technische Angriffe legen als auch das menschliche Verhalten als Schwachstelle miteinbeziehen. Hier ist vor allem das Social Engineering[11] mittels Phishing[12] zu betonen. Aufzeigte Schwachstellen geben häufig Rückschlüsse darüber, dass Update-Prozesse nicht richtig etabliert sind, das Passwortmanagement ungenügend ist oder Schnittstellen bzw. Zugänge nicht richtig konfiguriert sind.

Alle erkannten Abweichungen sollten festgehalten werden, so dass diese in Zukunft verbessert werden können.

Zyklusphase – „Act“

Aufgrund des kontinuierlichen Verbesserungsprozesses sollten die erkannten Abweichungen behoben oder Prozesse initiiert werden, um gegenzusteuern. Hierbei kann es unter Umständen erforderlich sein, die Organisation, Verantwortlichkeiten oder auch die Ressourcen zur Unterstützung zu verändern bzw. auszubauen. Generell soll in dieser Phase das „große Ganze“ betrachtet werden, um das ISMS nachhaltig gut aufzubauen und besser zu gestalten. Eine terminliche Planung von Aufgaben z. B. in Form von Projekten ist dabei sinnvoll.

Ein wichtiger Aspekt ist, dass auch in dieser Phase eine enge Kommunikation mit den Mitarbeitern stattfindet, damit Probleme in alltäglichen Prozessen aufgedeckt werden. Die Organisation sollte aus gemachten Fehlern lernen! Dies betrifft nicht nur die Sicherheitsprozesse selbst, sondern auch die Implementierung und Umsetzung des ISMS. Daher sollten auch solche Erkenntnisse dokumentiert werden, so dass die Vermeidung dieser auch für neue Iterationsschritte des anschließenden PDCA-Zyklus genutzt werden kann.

---

9 Ein Penetrationstest ist ein gezielter, in der Regel simulierter, Angriffsversuch auf ein IT-System. Er wird als Wirksamkeitsprüfung vorhandener Sicherheitsmaßnahmen eingesetzt, Quelle: BSI-Glossar für Cyber Sicherheit: https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Informationen-und-Empfehlungen/Glossar-der-Cyber-Sicherheit/Functions/glossar.html (letzter Zugriff: 03.11.2021)

10 Wählen Nutzer ein schwaches Passwort und ist der Benutzername (z. B. die E-Mail-Adresse) bekannt, kann sich ein Angreifer unter Umständen auch durch wiederholtes Ausprobieren von Passwörtern (Brute-Force-Angriff) Zugang zu einem Benutzerkonto verschaffen. Mittels Brute-Force-Techniken kann der Angreifer auch versuchen, kryptografisch geschützte Daten, z. B. eine verschlüsselte Passwort-Datei, zu entschlüsseln, Quelle siehe Fußnote 9

11 Social Engineering ist eine Methode, um unberechtigten Zugang zu Informationen oder IT-Systemen durch soziale Handlungen zu erlangen. Beim Social Engineering werden menschliche Eigenschaften wie z. B. Hilfsbereitschaft, Vertrauen, Angst oder Respekt vor Autorität ausgenutzt. Dadurch können Personen so manipuliert werden, dass sie unzulässig handeln, Quelle siehe Fußnote 9

12 Beim Phishing wird z. B. mittels gefälschter E-Mails und/oder Webseiten versucht, Zugangsdaten für einen Dienst oder eine Webseite zu erlangen. Wird diese Manipulation vom Opfer nicht erkannt und die Authentizität einer Nachricht oder Webseite nicht hinterfragt, gibt das Opfer seine Zugangsdaten u. U. selbst unwissentlich in unberechtigte Hände. Bekannte Beispiele sind Phishing-Angriffe gegen Bankkunden, die in einer E-Mail aufgefordert werden, ihre Zugangsdaten auf der Webseite der Bank einzugeben und validieren zu lassen, Quelle siehe Fußnote 9

Somit kann die Act-Phase auch als Vorbereitung der nächsten Plan-Phase gesehen werden und hierfür wichtige Handlungsfelder aufzeigen.

Anlaufstellen und kostenlose Unterstützung

Das Mittelstand-Digital-Netzwerk bietet mit den Mittelstand-Digital Zentren und der Initiative IT-Sicherheit in der Wirtschaft kostenfreie und umfassende Unterstützung im Themenschwerpunkt Informationssicherheit. Die folgenden Angebote geben einen kurzen Überblick über Anlaufstellen und Unterstützungsangebote innerhalb des Netzwerks. Neben diesen Zentren bieten vor allem Ministerien und Behörden wie das BSI kostenfreie Angebote[13] im Bereich der Informationssicherheit an. Aufbauend auf dem kostenfreien Angebot des BSI gibt es auch kostenpflichtige Schulungsangebote von privaten Anbietern[14]. Aber auch Verbraucherzentralen oder Projekte wie die Transferstelle IT-Sicherheit im Mittelstand (TISiM) unterstützen beim Themenschwerpunkt Informationssicherheit.

Aktive Unterstützungsangebote

Hierbei handelt es sich um kostenfrei nutzbare Unterstützungsangebote, die in Form personenbezogener Dienstleistungen durch die Zentren im Netzwerk Mittelstand-Digital erbracht werden. Diese erfolgen entweder im Gruppenverband (z. B. Veranstaltungen) oder individuell wie beispielsweise in einzelbetrieblichen Unternehmensgesprächen.

Passive Unterstützungsangebote

Bei passiven Unterstützungsangeboten handelt es sich um kostenfrei nutzbare Unterstützungsleistungen, deren Mehrwert in Form von Arbeits- und Lernmaterial im „Selbststudium“ bezogen werden kann. KMU können neben Leitfäden auch interaktive Werkzeuge oder Checklisten zur Selbsteinschätzung nutzen.

13 Kostenlose Schulungsangebot des BSI https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Standards-und-Zertifizierung/IT-Grundschutz/Zertifizierte-Informationssicherheit/IT-Grundschutzschulung/it-grundschutzschulung_node.html (letzter Zugriff: 03.11.2021)

14 Kostenpflichtige Schulungsangebote des BSI https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Standards-und-Zertifizierung/IT-Grundschutz/Zertifizierte-Informationssicherheit/Personenzertifizierung-IT-Grundschutzberater/Schulungen-zum-IT-Grundschutz-Praktiker-und-IT-Grundschutzberater/schulungen-zum-it-grundschutz-praktiker-und-it-grundschutzberater.html (letzter Zugriff: 03.11.2021)

	Gegen Cyberattacken gewappnet – Sechs Einfallstore für Cyberangriffe bei kleineren und mittleren Unternehmen	Selbstcheck IT-Sicherheit: Wie sicher ist meine IT?	Sicherheitstool Mittelstand
Herausgeber	Mittelstand 4.0-Kompetenzzentren Deutschlandweit	Mittelstand 4.0-Kompetenzzentrum Chemnitz	Mittelstand-Digital Zentrum Chemnitz
Format	PDF-Broschüre (digital)	Online-Fragebogen	Online-Fragebogen
Methode	Selbststudium (Textform)	Frage/Antwort	Frage/Antwort
Kurzbeschreibung	Es werden sechs verschiedene Angriffsszenarien vorgestellt, um den Lesern das Thema IT-Sicherheit greifbarer zu machen.	Interaktiver Fragebogen zur Risikoabschätzung im eigenen Unternehmen mit anschließender Auswertung. Gibt im Anschluss Tipps, an welchen Stellen Handlungsbedarf besteht.	Interaktiver Fragebogen zur Risikoabschätzung im eigenen Unternehmen mit anschließender Auswertung. Gibt im Anschluss Tipps, an welchen Stellen Handlungsbedarf besteht.
Voraussetzungen/Vorkenntnisse	keine	Fachübergreifende Kenntnisse der eigenen Unternehmensprozesslandschaft sowie Kenntnisse über den Status quo der IT-Landschaft	Fachübergreifende Kenntnisse der eigenen Unternehmensprozesslandschaft sowie Kenntnisse über den Status Quo der IT-Landschaft
Link	https://www.mittelstand-digital.de/MD/Redaktion/DE/Publikationen/it-sicherheitsrisiko-gegen-cyberatacken.pdf?__blob=publicationFile&v=3 (letzter Zugriff: 03.11.2021)	https://betrieb-machen.de/selbstcheck/ (letzter Zugriff: 03.11.2021)	https://www.sitom.de/home (letzter Zugriff: 03.11.2021)

Die AG IT-Sicherheit

Die Arbeitsgruppe IT-Sicherheit vernetzt die Zentren des Förderschwerpunkts „Mittelstand-Digital“. Geleitet wird die Arbeitsgruppe durch Dr. Frauke Goll und Dr. Thomas Usländer.

Das wichtigste Ziel der Arbeitsgruppe ist die Aufnahme von sicherheitsrelevanten Problem- und Fragestellungen aus den verschiedenen Wertschöpfungssegmenten sowie deren mittelstandsgerechte Aufarbeitung.

Zentrale Themen, die aktuell von der Arbeitsgruppe bearbeitet werden, sind „Sensibilisierung“ sowie „Risikoeinschätzung“. IT-Sicherheit ist jedoch ein „Moving Target“ – deshalb werden die Themen regelmäßig dem Bedarf der Kompetenzzentren und ihrem Anwenderkreis angepasst.

David Ruge
Koordinator der
AG IT-Sicherheit

Neben der internen Vernetzung der Kompetenzzentren steht die Arbeitsgruppe in ständigem Austausch mit anderen Arbeitsgruppen des Forschungskonsortiums „Mittelstand-Digital“ sowie diversen Projekten der Initiative „IT-Sicherheit in der Wirtschaft“.

Auf der Webseite der AG IT-Sicherheit finden sich weitere Produkte und Hilfestellungen für KMU, beispielsweise eine Online-Entscheidungshilfe zum Thema „ISMS-Absicherungswege“. Diese Hilfe gibt eine erste Übersicht zu ISMS-Absicherungswegen für unterschiedliche Branchen und Sektoren, wobei sie auch auf konkrete Zertifizierungen verweist. Alle Informationen und Kontaktdaten unter: https://ag-it-sicherheit.de.

Das Mittelstand-Digital Netzwerk

Das Mittelstand-Digital Netzwerk bietet mit den *Mittelstand-Digital Zentren*, der Initiative *IT-Sicherheit in der Wirtschaft* und *Digital Jetzt* umfassende Unterstützung bei der Digitalisierung. Kleine und mittlere Unternehmen profitieren von konkreten Praxisbeispielen und passgenauen, anbieterneutralen Angeboten zur Qualifikation und IT-Sicherheit. Das Bundesministerium für Wirtschaft und Energie ermöglicht die kostenfreie Nutzung und stellt finanzielle Zuschüsse bereit. Weitere Informationen finden Sie unter www.mittelstand-digital.de.

Bildnachweis

Titel: FZI Forschungszentrum Informatik
Grafiken Innenteil: FZI Forschungszentrum Informatik

Impressum

Herausgeber
Mittelstand 4.0-Kompetenzzentrum Stuttgart
c/o FZI Forschungszentrum Informatik
Haid-und-Neu-Straße 10-14
76131 Karlsruhe

Rechtsform
Das FZI Forschungszentrum Informatik ist eine Stiftung des bürgerlichen Rechts.

Stand
Oktober 2021

Druck
Fraunhofer Verlag
Mediendienstleistungen
Nobelstraße 12
70569 Stuttgart

Auflage
300