Mittelstand-Digital
Zentrum
Chemnitz

NACHGELESEN

IT-Sicherheit strukturiert aufbauen – 10 Goldene Regeln

ANDREAS NEUENFELS

Mittelstand-Digital

Gefördert durch:

Bundesministerium
für Wirtschaft
und Klimaschutz

aufgrund eines Beschlusses
des Deutschen Bundestages

Auf der Basis jahrelanger Erfahrungen und in enger Zusammenarbeit mit Unternehmen haben wir zehn goldene Regeln identifiziert, wie Sie zum strukturierten Aufbau Ihrer IT-Sicherheit ein **„Informationssicherheitsmanagementsystem“ (ISMS)** anwenden können. Die Tipps stammen aus der betrieblichen Praxis kleiner und mittlerer Unternehmen (KMU) sowie dem Handwerk.

In diesem *Nachgelesen* erfahren Sie,

- wozu ein Informationssicherheitsmanagementsystem (ISMS) dient,
- welche Chancen und Hürden ein ISMS mit sich bringt,
- welche Schritte bei einer Einführung eines ISMS zu beachten sind,
- welche Planungen stattfinden müssen,
- wie ein ISMS umgesetzt wird und
- wie ein ISMS nachhaltig geführt werden kann.

Impressum

HERAUSGEBER
Mittelstand-Digital Zentrum Chemnitz
c/o TU Chemnitz
Erfenschlager Str. 73, 09125 Chemnitz
Tel: 0371 531 19935 Fax: 0371 531 819935
info@digitalzentrum-chemnitz.de
www.digitalzentrum-chemnitz.de

REDAKTION Diana Falke

GESTALTUNG
PUNKT191 – Marketing und Design
www.punkt191.de

BILDNACHWEIS TITEL
Freepik.com

VERÖFFENTLICHUNG Juni 2023

©funtap - Freepik.com

Was ist ein ISMS und wozu dient das System?

In KMU ist der Einsatz von Informations- und Kommunikationstechnik nicht mehr weg zu denken. Die dabei genutzten, vielfältigen Anwendungen verarbeiten wichtige personenbezogene sowie Unternehmens- und Produktdaten. Um den geforderten Schutzbedarf zu erreichen, müssen deshalb verschiedene Maßnahmen ergriffen und Prozesse ausgerichtet werden.

Die Anforderungen können durch die Kunden und Partner des Unternehmens sowie auf Grundlage verschiedener Gesetze und Regularien entstehen. Häufig ist dafür ein geordnetes Herangehen oder ein Nachweis, dass der Stand der Technik erreicht wird, erforderlich. Dies stellt viele Unternehmen vor große Herausforderungen. Standards, Normen und Branchenrichtlinien können helfen, die unternehmensspezifischen IT-Sicherheitsprozesse und -maßnahmen strukturiert anzugehen. Teilweise sind sogar Zertifizierungen möglich bzw. geeignet.

Gemäß der Definition des Bundesamtes für Sicherheit in der Informationstechnik[1] soll ein ISMS ein organisatorisches Unternehmenswerkzeug sein, mit dem eine strukturierte Vorgehensweise zur Erhöhung der Informationssicherheit ermöglicht wird.

DEFINITION ISMS

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.[1]

Hierbei wird auf Regelungen, Rollen- und Verantwortlichkeiten sowie Verfahrens- bzw. Prozessanweisungen Wert gelegt. Gleichzeitig soll sich ein ISMS in die Strategie des Unternehmens und in andere Managementsysteme nahtlos einfügen.

Chancen und Hürden bei der ISMS-Einführung

Die zentrale Chance, die sich mit einer ISMS-Einführung ergibt, ist der konsequente und strukturierte Aufbau eines Informationssicherheitsprozesses. Da dem Unternehmen für die Festlegung von Regeln und Zuständigkeiten zunächst Mehraufwände entstehen, sollte die Einführung eines bestimmten ISMS kein Selbstzweck sein, sondern der eigenen Risikoabschätzung folgen. Zahlreiche Vorteile rechtfertigen jedoch den Aufwand.

Innerbetrieblich können im Falle von ISMS wesentliche IT-Prozesse verbessert werden, was sich mittel- und langfristig positiv auf Mitarbeiter, Produkte und Kunden auswirkt. Dies wird durch eine konsequente und strukturierte Herangehensweise zur Definition und Erreichung der eigenen IT-Sicherheitsschutzziele erreicht (siehe Exkurs). Somit können die IT-Systeme, Informationen und Daten im Unternehmen geschützt und systematisch sowie methodisch gestützt werden.

Darüber hinaus wird dem Unternehmen eine eigene Risikobewertung ermöglicht, die im Rahmen des allgemeinen Risikomanagements Anwendung finden kann. Zusätzlich können Entscheidungen für oder gegen die Einführung von IT-Systemen oder der Implementierung bestimmter Maßnahmen durch die Risikobewertung getroffen werden.

Auch die Wirkung nach außen ist ein nicht unerheblicher Grund für die Einführung eines Standards. So verlangen immer mehr Geschäftspartner eine Zertifizierung als Nachweis, dass IT-Sicherheitsrisiken minimiert werden und somit die

Zusammenarbeit nicht gefährdet ist. Weiterhin kann solch ein Nachweis die Kapitalbeschaffung bei Banken unterstützen oder zu geringeren Beiträgen für Cyber-Versicherungen führen. Neben der bereits gesetzlich festgelegten Pflicht zur Zertifizierung von Unternehmen im Bereich Kritische Infrastrukturen (KRITIS) kann ein derartiges Zertifikat auch gegenüber dem Gesetzgeber verwendet werden. Es zeigt auf, dass der Stand der Technik gewahrt wird und wirkt somit möglichen negativen Folgen von Gesetzen aus dem Bereich der Datenübertragung oder des Datenschutzes entgegen.

EXKURS SCHUTZZIELE DER INFORMATIONSSICHERHEIT

Je nach Literaturquelle[2],[3] werden generelle Schutzziele für die Informationssicherheit definiert. Häufig wird dabei vom VIVA- oder englisch CIA-Prinzip gesprochen. VIVA (CIA) steht für Vertraulichkeit (Confidentiality), Integrität (Integrity), Verfügbarkeit (Availability) und Authentizität. Eine Organisation sollte Informationen, Daten und verarbeitende Systeme nach diesen Kriterien bewerten und deren entsprechenden Schutzbedarf als Ziel formulieren.

Welche Schritte sind bei einer ISMS-Einführung zu beachten?

REGEL 1: ÜBERBLICK ZUM THEMA ISMS VERSCHAFFEN

Glückwunsch, Sie befolgen mit der Sichtung des *Nachgelesens* bereits die erste Regel! Zunächst ist es wichtig, sich als Unternehmen mit dem Thema ISMS vertraut zu machen. In der Praxis zeigt sich häufig, dass Ziele und Möglichkeiten eines ISMS missverstanden, Aufwände nicht richtig eingeschätzt oder nicht passende ISMS eingeführt werden. Machen Sie sich auch bewusst, was Sie mit der Einführung eines ISMS erreichen wollen, etwa. einen Reputationsgewinn, die Verbesserung von Prozessen oder das Vorweisen eines Zertifikats. Sie können hier auch auf Unterstützungsangebote zurückgreifen, wie dem ISMS-Coaching der Mittelstand-Digital Zentren.

REGEL 2: IT-SICHERHEIT ANALYSIEREN

Als nächstes sollten Sie feststellen, auf welchem IT-Sicherheitsniveau sich Ihr Unternehmen befindet. Hierfür steht Ihnen mit der neuen DIN SPEC 27076[4],[5] ein Beratungsstandard zur Verfügung, der insbesondere für kleinere Unternehmen konzipiert wurde, um ein grundlegendes Verständnis zu bekommen, wie es um Ihre IT-Sicherheit steht, insofern Sie sich bisher noch nicht mit dem Thema auseinandergesetzt haben. Am Markt stehen Ihnen zur Durchführung dieser Analyse externe Dienstleister sowie auch Experten vom Mittelstand-Digital Netzwerk zur Verfügung. Nutzen Sie auch weitere Angebote von Mittelstand-Digital, wie das Sicherheitstool SiToM mit dem Unternehmen das vorhandene IT-Sicherheitsniveau sowie Risiken und Schwachstellen ermitteln (www.sitom.de).

REGEL 3: IT DOKUMENTIEREN

Neben der grundlegenden Analyse sollten Sie unbedingt Ihre gesamte IT vollständig dokumentiert haben. Dabei sollten Sie sich am besten vom „Groben“ in das „Feine“ vorarbeiten. Es bietet sich meistens an, zunächst die Unternehmensinfrastruktur zu beachten und dabei sowohl Organisationseinheiten, Standorte, räumliche bzw. strukturelle Trennungen sowie die Verbindungen zueinander zu betrachten. Analysieren Sie alle Geräte, die dazugehörenden Adressen bzw. Protokolle und dokumentieren Sie sämtliche Abzweigungen sowie Verbindungen. Elementar sind hier Informationen über einzelne Server (inklusive Services) und Clients. Dazu gehören auch eingesetzte Software, Lizenzen, Konfigurationen, Firmware-Versionen etc

REGEL 4: PASSENDES ISMS WÄHLEN

Am Markt und in der Literatur stehen umfangreiche Informationen zu ISMS – zum Beispiel in Form von Normen und Standards – zur Verfügung. Die bekanntesten Vertreter sind die DIN ISO 27001[6], der BSI-Grundschutz[7] und die VDS 10000[8]. Generell haben alle Systeme zum Ziel, die Informationssicherheit in Ihrem Unternehmen zu fördern, indem Prozesse, Produkte und Maßnahmen verbessert werden. Bezüglich des Aufwands, der Inhalte (bzw. Spezialisierung) und den Zielgruppen gibt es jedoch erhebliche Unterschiede. Ein wichtiger Aspekt ist dabei eine mögliche Integration in bestehende Managementsysteme. Nutzen Sie zur Unterstützung Ihrer Entscheidungsfindung die Hilfestellung aus dem Mittelstand-Digital Netzwerk. Die unter dem Dach der Initiative agierenden Zentren verstärken ihre Angebote hinsichtlich ISMS und führen Miniprojekte standardisiert durch. Eine Übersicht zu den Projekten und den Coaches ist derzeit in Vorbereitung.

Welche Planungen müssen stattfinden?

REGEL 5: RISIKEN UND SCHUTZBEDARFE BESTIMMEN

Gemäß den Regularien des gewählten ISMS sollten im nächsten Schritt die Schutzbedarfe der IT-Systeme sowie die genutzten Informationen und Daten in den Fokus rücken[9],[10]. Insofern hohe und sehr hohe Schutzbedarfe festgestellt werden, sollten etwaige Risiken analysiert werden[11]. Damit diese vollständig sind, sollten die folgenden Arbeitsschritte

eingehalten werden: Gefährdungsübersicht erstellen, Risiken bewerten und Risiken behandeln (Sicherheitsmaßnahmen).

REGEL 6: ZIELE UND LEITLINIEN FESTLEGEN

Damit ein Sicherheitsmanagement gelingt, muss die Unternehmensleitung vollständig hinter der Einführung des ISMS stehen. Dies schließt ein, selbst Verantwortung zu übernehmen, Ressourcen zu steuern und freizugeben sowie eine Strategie für den Sicherheitsprozess festzulegen. Zur Strategie gehört, dass die wesentlichen Sicherheitsziele für die Organisation definiert werden und diese in Bezug zu den Geschäftszielen stehen. Sinnvoll ist es, den Sicherheitszielen konkrete Kennzahlen[12] zuzuordnen, da so Entscheidungen und Steuerungen anhand von messbaren Kriterien getroffen werden können.

REGEL 7: VERANTWORTLICHKEITEN BESTIMMEN UND SCHULUNGSMASSNAHMEN INITIIEREN

Zu den notwendigen Ressourcen gehört die Vergabe von Verantwortlichkeiten im Sinne des ISMS. Häufig wird hierbei mindestens ein/e Informationssicherheitsbeauftragte/r bestimmt und mit angemessenen Ressourcen ausgestattet. Essentiell ist, dass die Person ausreichend qualifiziert ist und sich zukünftig weiterbilden kann, da sich die Informationssicherheit ständig mit neuen Gefährdungslagen verändern kann. Weiterhin sollten auch alle weiteren Personen, die für sicherheitsrelevante Prozesse verantwortlich sind, in Abstimmungen einbezogen werden. Generell ist die gesamte Belegschaft in den Einführungsprozess zu integrieren, damit etwaige Vorbehalte ausgeräumt und Fehler in Prozessen direkt gelöst werden können. Hierfür ist es erforderlich, dass alle Mitarbeitenden regelmäßig zu Gefährdungslagen sensibilisiert und bezüglich der Sicherheitsrichtlinien aufgeklärt werden[13].

Wie wird das ISMS umgesetzt?

REGEL 8: RICHTLINIEN, PROZESSE UND ANWEISUNGEN DEFINIEREN

Nach den einführenden Schritten zur Planung sollten Sie die gewonnenen Erkenntnisse dafür nutzen, geeignete Prozesse aufzustellen[14]. Dazu kann beispielsweise gehören, wie ein Prozess zur Datensicherung geführt wird, bei dem unter anderem Verantwortlichkeiten sowie wesentliche Schritte und Schnittstellen definiert werden. Die Prozesse ordnen sich dabei in den Richtlinien ein, die einem übergeordneten Ziel dienen (etwa der Herstellung der Verfügbarkeit von Daten) und häufig mit speziellen Anweisungen gegenüber den Mitarbeitenden verbunden sind.

REGEL 9: PLAN-DO-CHECK-ACT-ZYKLUS (PDCA) BEACHTEN

Sowohl das ISMS selbst als auch die definierten Prozesse sollten der Methodik des PDCA-Zyklus (Plan-Do-Check-Act) unterliegen[15]. Das heißt, dass anhand der festgestellten Schutzbedarfe und Risiken eine Behandlung geplant wird. Dies geht häufig einher mit der Einführung von Sicherheitsmaßnahmen (Plan). Diese sollten beim Umsetzen in einen Realisierungsplan integriert und in die Sicherheitsprozesse überführt werden (Do). Wichtig ist hierbei, dass diese Sicherheitsprozesse überwacht und deren Wirksamkeit geprüft wird. Dafür bietet sich unter anderem die Belegung durch geeignete Kennzahlen an (Check). Nach der Prüfung werden mögliche Fehler beseitigt bzw. Maßnahmen zur Sicherheitsverbesserung initiiert, wodurch der Zyklus neugestartet wird (Act).

Wie kann ein ISMS nachhaltig geführt werden?

REGEL 10: SICHERHEITSPROZESS DOKUMENTIEREN UND KONTINUIERLICH VERBESSERN

Achten Sie darauf, dass Ihr ISMS über eine standardisierte Dokumentation verfügt und Informationen (z. B. Risikobewertungen, durchgeführte Maßnahmen, Auswertungen von Fehlern) nachvollziehbar abgelegt werden. Dies erleichtert eine Nachverfolgung und die Aufrechterhaltung des PDCA-Zyklus enorm. Befragen Sie zudem Ihre Mitarbeiter regelmäßig zur Durchführbarkeit sowie Akzeptanz von definierten Sicherheitsprozessen und Anweisungen. Lassen Sie dieses Feedback in den Verbesserungsprozess einfließen, da nichtgelebte oder komplizierte Prozesse einer erfolgreichen Weiterführung des ISMS im Wege stehen.

Quellen

1 https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Grundschutz/Kompendium_Einzel_PDFs_2021/01_ISMS_Sicherheitsmanagement/ISMS_1_Sicherheitsmanagement_Edition_2021.html [15.03.2023]

2 https://www.kryptowissen.de/schutzziele.php [15.03.2023]

3 https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Standards-und-Zertifizierung/IT-Grundschutz/Zertifizierte-Informationssicherheit/IT-Grundschutzschulung/Online-Kurs-IT-Grundschutz/Lektion_4_Schutzbedarfsfeststellung/4_01_Definitionen.html [15.03.2023]

4 https://mit-standard-sicher.de/ [15.03.2023]

5 https://www.din.de/de/forschung-und-innovation/din-spec/alle-geschaeftsplaene/wdc-beuth:din21:354867484 [15.03.2023]

6 https://www.din.de/de/mitwirken/normenausschuesse/nia/entwuerfe/wdc-beuth:din21:365634117 [15.03.2023]

7 https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Standards-und-Zertifizierung/IT-Grundschutz/it-grundschutz_node.html [15.03.2023]

8 https://vds.de/kompetenzen/cyber-security/vds-richtlinien/anforderungsrichtlinien-/-leitfaeden/vds-10000-informations-sicherheit-fuer-kmu [15.03.2023]

9 https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Grundschutz/BSI_Standards/standard_200_2.pdf Vgl. S. 104ff. [15.03.2023]

10 https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Standards-und-Zertifizierung/IT-Grundschutz/Zertifizierte-Informationssicherheit/IT-Grundschutzschulung/Online-Kurs-IT-Grundschutz/online-kurs-it-grundschutz_node.html [15.03.2023]

11 https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Standards-und-Zertifizierung/IT-Grundschutz/Zertifizierte-Informationssicherheit/IT-Grundschutzschulung/Online-Kurs-IT-Grundschutz/Lektion_7_Risikoanalyse/Lektion_7_node.html [15.03.2023]

12 https://www.isaca.de/sites/default/files/attachements/isaca_germany_-_kpi_leitfaden.pdf [15.03.2023]

13 https://digitalzentrum-chemnitz.de/wissen/schutzschild-mensch/ [15.03.2023]

14 https://www.hs-augsburg.de/Binaries/Binary33218/Prozesse-zum-Betrieb-eines-ISMS.pdf [15.03.2023]

15 https://www.mittelstand-digital.de/MD/Redaktion/DE/Publikationen/it-sicherheit-leitfaden-Informationssicherheits-managememt.html [15.03.2023]

Autor

ANDREAS NEUENFELS ist Projektmanager bei der tti Technologietransfer und Innovationsförderung Magdeburg GmbH. Im Mittelstand-Digital Zentrum Chemnitz ist er ials Mitarbeiter im Bereich IT-Sicherheit tätig.
andreas.neuenfels@digitalzentrum-chemnitz.de

Weitere Informationen

Das Mittelstand-Digital Zentrum Chemnitz gehört zu Mittelstand-Digital. Mit dem Mittelstand-Digital Netzwerk unterstützt das Bundesministerium für Wirtschaft und Klimaschutz die Digitalisierung in kleinen und mittleren Unternehmen und dem Handwerk.

WAS IST MITTELSTAND-DIGITAL?

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 Klimaschutz ermöglicht die kostenfreie Nutzung und stellt finanzielle Zuschüsse bereit. Weitere Informationen finden Sie unter www.mittelstand-digital.de.

Mittelstand-Digital
Zentrum
Chemnitz

Mittelstand-
Digital

Gefördert durch:

Bundesministerium
für Wirtschaft
und Klimaschutz

aufgrund eines Beschlusses
des Deutschen Bundestages