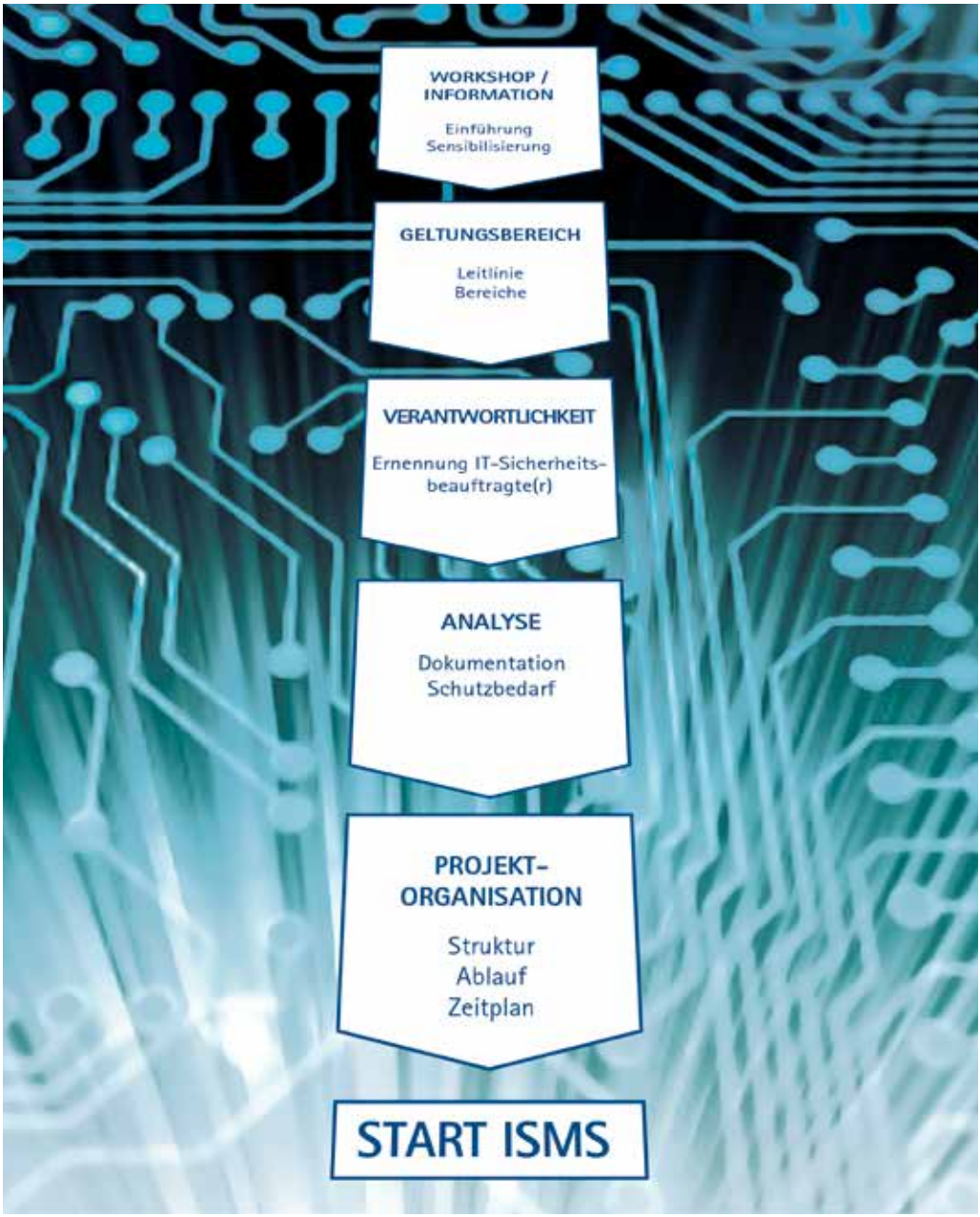
Management von Informationssicherheit

Leitfaden für Unternehmen

IHK Schwaben

aitiRaum
Bestens vernetzt.

TECHNISCHE UND ORGANISATORISCHE STANDORTBESTIMMUNG VOR DER EINFÜHRUNG EINES INFORMATIONSSICHERHEITSMANAGEMENTSYSTEMS (ISMS)



INHALT

GRUSSWORT

Dr. Andreas Kopton,
Präsident der
IHK Schwaben

Jörn Steinhauer,
Vorsitzender des
aitiRaum e. V.

»Mit dem Leitfaden „Management von Informationssicherheit" möchten wir den Unternehmen eine Hilfestellung an die Hand geben, in der kurz und bündig erklärt wird, was Informationssicherheitsmanagement bedeutet, wie erste wirkungsvolle Schritte eingeleitet werden können und welche Punkte dabei zu beachten sind.«

Im globalen Wettbewerb um innovative Produkte und Dienstleistungen kommt es in einer zunehmend vernetzten Arbeitswelt immer mehr auf den Schutz und die vertrauliche Übermittlung von Unternehmensdaten an. Jedes zweite Unternehmen in Deutschland wurde in den vergangenen Jahren bereits Opfer von Wirtschaftskriminalität. Insbesondere kleine und mittelständische Unternehmen sind von dieser Bedrohungslage betroffen. Dies erfordert ein klares Bewusstsein für die Abhängigkeit des Unternehmens von der Sicherheit moderner Informations- und Kommunikationslösungen.

Für die IHK Schwaben und den aitiRaum e. V. hat die IT-Sicherheit der schwäbischen Unternehmen eine zentrale Bedeutung. Dies zeigt unsere Kooperation zur IT-Sicherheit, in der wir Ihnen mit Leitfäden und Veranstaltungen Expertenwissen und Hintergründe zu aktuellen Fragestellungen der IT-Sicherheit anbieten. Der vorliegende Leitfaden bildet den Auftakt zu einer Reihe von Orientierungshilfen. Er richtet sich an Geschäftsführer und das Management von Unternehmen, denen Fachwissen und Hintergründe zur Etablierung eines geordneten IT-Sicherheitsprozesses im Unternehmen gegeben werden. Denn nicht nur die technische Umsetzung von Sicherheitsmaßnahmen ist essenziell; vielmehr spielt auch der Faktor Mensch eine zentrale Rolle. Im Leitfaden finden Sie deshalb entsprechende Handlungsempfehlungen zur Mitarbeitersensibilisierung.

DIE AUTOREN

Kent Andersson, Geschäftsführer der ausecus GmbH

KENT ANDERSSON

leitet seit 2012 als geschäftsführender Gesellschafter und Firmengründer die ausecus GmbH. Er bringt 15 Jahre Managementerfahrung aus der Automatisierungstechnik und IT-Sicherheit in Pharma und Biotechnologie, in der Lebensmittelindustrie und im Energieversorgungsbereich im In- und Ausland mit. Davor war er zehn Jahre bei dem führenden skandinavischen Automatisierungsunternehmen SattControl (heute ABB) international in Service und Inbetriebnahme, in der Projektierung und in der Projektleitung tätig.

Klaus Wagner, Geschäftsleitung der DEXevo GmbH

KLAUS WAGNER

hat an der Technischen Universität München im Jahr 1998 seinen Abschluss als Diplom-Informatiker (Univ.) gemacht. Von 1998 bis 2000 war er als Softwareentwickler und Projektleiter bei einem Softwareunternehmen im Bereich Bankensoftware tätig. Seit 2000 ist er selbstständig als Berater und Softwareentwickler aktiv. Er ist Mitgründer und Gesellschafter der DEXevo GmbH mit den Schwerpunkten IT-Sicherheit, Softwareentwicklung, Prozessoptimierung und IT-Projektmanagement.

WAS BEDEUTET INFORMATIONSSICHERHEITSMANAGEMENT?

INTERVIEW MIT KENT ANDERSSON UND KLAUS WAGNER

Immer häufiger wird die Meinung vertreten, dass Unternehmenssicherheit nur in Verbindung mit einem Informationssicherheitsmanagement umgesetzt werden kann. Weshalb reicht die Installation einer Antivirensoftware und einer Firewall heute nicht mehr aus?

Kent Andersson: *Vorausgeschickt sei gesagt, dass technische Maßnahmen wie Firewall, Virenwächter, Verschlüsselung, Einschränkung von Benutzerrechten und Zugriffen sowie die Netzwerksegmentierung schon sehr gute und bewährte Ansätze sind, um die IT-Sicherheit zu erhöhen. Allerdings gilt es, vertrauliche und sensible Informationen zu schützen. Dies geht über den Schutz rein personenbezogener und technischer Daten hinaus und beinhaltet auch das Know-how der Mitarbeiter. Man spricht hier auch vom Schutz der „Kronjuwelen eines Unternehmens". Das beinhaltet u. a. Informationen über Forschungs- und Entwicklungsergebnisse, Fertigungsprozesse, Produktions-, Prozess- und Fertigungsprotokolle bis hin zu Auswertungen von Produktions-, Lager- und Logistikbeständen.*

Diese Informationssicherheit muss nicht nur organisiert, sondern auch verwaltet werden. Das lässt sich in der Praxis am effektivsten mit einem Managementsystem machen.

Herr Wagner, was gilt es bei diesem Managementsystem zu beachten?

Klaus Wagner: *Es wäre fatal zu glauben, man könne einfach ein Softwareprodukt kaufen. Vielmehr muss ein eigenes Informationssicherheitsmanagementsystem (ISMS) aufgebaut werden. Das erfordert Zeit und Detailwissen. Beispielsweise gibt es Normen und Standards, die dieses Vorhaben unterstützen, wie die ISO 27001 oder ISIS12. Ein ISMS muss nicht im ganzen Unternehmen eingeführt werden. Sie können den Geltungsbereich auf die wichtigsten Kernprozesse festlegen.*

Das größte Sicherheitsrisiko ist jedoch der Mensch. Die Informationssicherheit eines Unternehmens hängt stark von der Akzeptanz und der Motivation aller Mitarbeiter ab. Daher ist es am wichtigsten, die Mitarbeiter zu sensibilisieren und zu schulen. Schließlich sollen diese die Sicherheitsleitlinie verstehen und beachten.

Dann muss man also mehr als nur die PCs und Server im Geltungsbereich des Unternehmens betrachten?

Klaus Wagner: *Das ist so korrekt. Viele bekannt gewordene IT-Angriffe der letzten Jahre basierten auf sogenanntem Social Engineering. Ein Angreifer versucht dabei, das Vertrauen zu einem Mitarbeiter zu gewinnen, beispielsweise am Telefon oder per E-Mail. Dieses nutzt er dann aus, um über den Mitarbeiter Schadsoftware zum Beispiel per E-Mail in das Unternehmen zu schleusen oder die Betroffenen zur Herausgabe von Passwörtern zu bewegen.*

Die Bedrohungen für Unternehmen sind ja vielfältig. Wie kann man dem am besten begegnen und welche Ziele sollte man am dringlichsten verfolgen?

Kent Andersson*: Es gibt eigentlich nur drei sogenannte Schutzziele, die Sie mit Ihrem Unternehmen verfolgen können. Dies sind Vertraulichkeit, Integrität und Verfügbarkeit der Informationen. Jedes Unternehmen muss dabei für sich entscheiden, wie diese drei Schutzziele priorisiert werden.*

Ein Energieversorger wird beispielsweise die Verfügbarkeit der Informationen an die oberste Stelle setzen. Ein Strom-, Gas- und Wassernetz lässt sich nur sicher führen, wenn die Informationen aus den Außenstationen und dezentralen Anlagen jederzeit verfügbar sind. Ein Dienstleister hingegen stellt die Vertraulichkeit von Informationen an oberste Stelle. Schließlich muss er Kundendaten datenschutzkonform unter Verschluss halten.

Grundsätzlich ist es wichtig, dass Unternehmen Informationssicherheit ganzheitlich betrachten. Technische und organisatorische Maßnahmen sowie die damit verbundene Dokumentation müssen strukturiert und kontinuierlich bewertet und überwacht werden.

Vielen Dank für das Gespräch und für die Informationen!

In der Praxis hat sich vor Einführung eines Informationsmanagementsystems (ISMS) die technische und organisatorische Standortbestimmung bewährt (siehe hierzu die Grafik auf Seite 2).

DER MENSCH ALS ANGRIFFSZIEL

Angriffe auf Unternehmen beginnen sehr oft beim schwächsten Glied in der Verteidigungskette – beim Mitarbeiter. Anstatt technische Hürden zu überwinden, versuchen Angreifer, Mitarbeiter eines Unternehmens dazu zu bewegen, bestimmte Aktionen auszuführen. Am einfachsten gelingt dies über Social-Engineering-Praktiken wie z. B. über Phishing-E-Mails. Auf diese Weise wurde z. B. der Bundestag gehackt.

Im Rahmen der Einführung eines Managementsystems für Informationssicherheit ist es daher besonders wichtig, von Anfang an den Faktor Mensch einzubeziehen. Durch die Verabschiedung und Bekanntgabe einer Unternehmensleitlinie für Informationssicherheit durch die Geschäftsführung wird der Stellenwert von Informationssicherheit für das Unternehmen allen Mitarbeitern deutlich gemacht. Damit alle Mitarbeiter ein Bewusstsein für Informationssicherheit entwickeln, muss ein nachhaltiger Lernprozess angestoßen werden.

LEITLINIE FÜR INFORMATIONSSICHERHEIT

Eine Leitlinie für Informationssicherheit sollte folgende wesentliche Punkte abdecken:

Verantwortung der Unternehmensleitung

Durch das Bekenntnis der Unternehmensleitung zur Übernahme der Gesamtverantwortung für die Informationssicherheit wird der hohe Stellenwert verdeutlicht und die zukünftige Arbeit eines Beauftragten für Informationssicherheit ermöglicht und verbindlich geregelt.

Geltungsbereich der Leitlinie

In nahezu allen Bereichen werden in den Unternehmen Daten und Informationen verarbeitet oder übermittelt. Die Leitlinie gilt daher in der Regel in allen Abteilungen der Organisation. Dies kann an dieser Stelle so explizit allen Mitarbeitern bekannt gegeben werden.

Stellenwert der Informationssicherheit

Unternehmenserfolg ist direkt oder indirekt vom schnellen, sicheren und aktuellen Zugriff auf Informationen abhängig, da in nahezu allen Bereichen schützenswerte Daten und Informationen verarbeitet werden. In diesem Abschnitt der Leitlinie wird dies durch anschauliche Beispiele verdeutlicht, wie z. B. bei der Verarbeitung von Personaldaten, dem Umgang mit vertraulichen Informationen aus Kunden- und Lieferantenbeziehungen und der Verdeutlichung von Geheimhaltungsanforderungen bei firmeneigenen Ideen und Technologien oder Entwicklungs- und Investitionsvorhaben.

Sicherheitsziele und Sicherheitsstrategie

Hier werden besonders wichtige Ziele und strategische Vorgaben des Unternehmens

dargestellt. Diese Vorgaben werden später im Rahmen eines Sicherheitskonzeptes konkretisiert.

Durchsetzung und Erfolgskontrolle

In der Leitlinie wird bekannt gegeben, dass für die Durchsetzung dieser Ziele und Leitaussagen eine Position geschaffen wird, die direkt der Unternehmensleitung unterstellt ist – die Position des Beauftragten für Informationssicherheit.
Von allen Mitarbeitern wird eingefordert, sich an die Vorgaben der Leitlinie zu halten. Für Verstöße werden entsprechende Konsequenzen angedroht.

Training und Sensibilisierung der Mitarbeiter

Aus der Leitlinie für Informationssicherheit ergeben sich die verschiedensten Anforderungen an die Mitarbeiter. Damit diese den Anforderungen gerecht werden können, müssen sie das nötige Rüstzeug erhalten. Wichtig ist vor allem, die Mitarbeiter von Anfang an mit ins Boot zu holen und für das Thema Informationssicherheit regelmäßig zu sensibilisieren, aber auch entsprechend zu schulen.
Im Rahmen von Sensibilisierungsmaßnahmen kann dem Mitarbeiter der Stellenwert der Informationssicherheit für das Unternehmen deutlich gemacht werden. Hier kann beispielsweise dargestellt werden, welche Schäden andere Unternehmen bei „Datenpannen" erlitten hatten.
Im Rahmen von „Anti-Phishing-Trainings" werden Mitarbeiter mit den Tricks von Spammern und Phishern vertraut gemacht. Sie werden geschult, Phishing-Mails effektiv zu erkennen, und lernen die Gefahren kennen, die von diesen Mails ausgehen.
Mitarbeiter müssen auch Verhaltensregeln und Meldewege bei Sicherheitsvorfällen erlernen und im Ernstfall umsetzen.

PROZESSE FÜR DIE INFORMATIONSSICHERHEIT

INFORMATIONSSICHERHEITS-BEAUFTRAGTE IM UNTERNEHMEN

Ein wesentlicher Erfolgsfaktor für die Anhebung des Sicherheitsniveaus in einem Unternehmen ist die Bestellung eines qualifizierten Beauftragten für Informationssicherheit (ISB). Mit der Leitlinie als Arbeitsauftrag ist er im Team mit der Geschäftsführung und der IT-Leitung für deren Umsetzung verantwortlich.

Idealerweise verfügt der ISB über Wissen in den Bereichen IT und Informationssicherheit und hat Erfahrung im Bereich Projektmanagement. Keinesfalls sollte der IT-Leiter diese Position übernehmen, da hier die Interessenkonflikte zu groß sind.
Zu den Aufgaben des ISB gehören der Aufbau und die Aufrechterhaltung des Informationssicherheitsprozesses. Er ist die zentrale Anlaufstelle für Informationssicherheit.

Dies sind die Hauptaufgaben des Informationssicherheitsbeauftragten:

- Erstellung von Richtlinien, Regelungen und Konzepten
- Mitarbeiterschulung und Awareness
- Untersuchung sicherheitsrelevanter Zwischenfälle

IT-SERVICE-MANAGEMENT

Solide und strukturierte Dokumentation ist eine Grundvoraussetzung für das Management von Informationssicherheit. Dazu gehört die Dokumentation aller IT-Systeme und Verfahren aus der IT-Organisation. Die Einführung eines Managementsystems von Informationssicherheit stellt hier hohe Anforderungen. Deren Erfüllung wird durch die Einführung eines IT-Service-Managements sichergestellt.
In dessen Rahmen werden Serviceprozesse definiert, über die Änderungen, Wartungen und Störfallbeseitigung gelenkt werden. Diese Prozesse stellen sicher, dass die Dokumentation der Systeme stets auf dem aktuellen Stand ist.
Aufbauend auf diesem Informationspool kann der ISB Sicherheitskonzepte erstellen, Schwachstellen analysieren etc.
Für den normalen Anwender werden diese Veränderungen bei der Einführung oft in Form eines Ticketsystems sichtbar. Damit kann der Anwender Anfragen oder Störungen in geführter und damit qualitativ hochwertiger Form an die IT-Abteilung melden und wird über das Ticketsystem gleichzeitig über den Status seiner Anfrage auf dem Laufenden gehalten.

KONTINUIERLICHER VERBESSERUNGSPROZESS

Letztendlich schließt sich hier der Kreis. Durch die Anforderungen eines Managementsystems für Informationssicherheit werden auch hohe Anforderungen an die IT-Prozesse gestellt. Diese werden dadurch transparenter und effizienter, was wiederum die Erstellung eines IT-Betriebshandbuches und darauf aufbauend die Erstellung eines IT-Notfallhandbuches ermöglicht und erleichtert. Das Informationssicherheitskonzept wird ständig verfeinert und der Reifegrad der Informationssicherheit steigt stetig an. Der kontinuierliche Verbesserungsprozess ist somit angestoßen.

SCHUTZBEDARF UND RISIKOMANAGEMENT

Jedes Unternehmen ist Informationssicherheitsrisiken ausgesetzt. Die Art und der Umfang dieser Risiken sind aber so individuell, wie Unternehmen unterschiedlich sind. Aus diesem Grund muss für jedes Unternehmen ein eigenes Risikomanagement aufgebaut werden.

Um Risiken zu identifizieren, hat sich in der Praxis eine Schutzbedarfsfeststellung bewährt. Das ist eine standardisierte und strukturierte Analyse, um die Informationswerte in einem Unternehmen zu identifizieren und nach ihrem Schutzbedarf zu bewerten. Auch hier ist der Geltungsbereich zu beachten.

TIPP!

Halten Sie für den ersten Schritt den Geltungsbereich so gering wie möglich und erweitern Sie ihn erst später bei Bedarf. Dies erleichtert Ihnen den Einstieg in die Thematik.

TECHNISCHE MASSNAHMEN

TIPP!

Erfinden Sie das Rad nicht neu. In der ISO 27002 und dem im BSI-Grundschutz sind bereits Best-Practice-Beispiele abgebildet. Diese sollten, wann immer möglich, angewandt werden.

Die Einführung von technischen Sicherheitsmaßnahmen ist zeitaufwendig und teuer. Der Aufwand für eine Maßnahme und das dazugehörige Risiko sollten sich die Waage halten. Daher ist es sinnvoll, Maßnahmen nur dann einzuführen, wenn ein entsprechend hohes Risiko identifiziert wurde. Bei niedrigen Risiken sollte nur bei einem adäquaten Kosten-Nutzen-Verhältnis eine Maßnahme eingeführt werden.

TIPP!

Setzen Sie zuerst die Maßnahmen um, die gleichzeitig mehrere Risiken minimieren. Dies schafft in kurzer Zeit ein gutes Plus an Informationssicherheit.

Der BSI-Grundschutzkatalog und die ISO 27002 eignen sich als Richtlinien zur Einführung von Maßnahmen. Beide enthalten den gleichen Maßnahmenkatalog, allerdings in unterschiedlicher Detailtiefe, und beschreiben, wie die Maßnahmen nach guter fachlicher Praxis („Best Practice“) umgesetzt werden sollen.

CHECKLISTEN

STRUKTURANALYSE UND SCHUTZBEDARFSFESTSTELLUNG

- ☐ Identifikation aller Anwendungen
- ☐ Identifikation aller Clients und Server sowie der Netzwerkgeräte
- ☐ Identifikation aller relevanten Räumlichkeiten
- ☐ Zuordnung der Anwendungen zu den Clients und Servern
- ☐ Zuordnung der Kommunikationsflüsse zwischen Clients und Servern
- ☐ Zuordnung der Systeme zu den identifizierten Räumlichkeiten
- ☐ Analyse der Verbindungen und Bewertung nach deren Kritikalität
- ☐ Bewertung des Bedarfs an Vertraulichkeit, Integrität und Verfügbarkeit für:
  Anwendungen | Systeme
  Netzwerkverbindungen | Räume
- ☐ Festlegung des Schutzbedarfs für Anwendungen, Systeme, Netzwerkverbindungen und Räume in den Kategorien: normal, hoch und sehr hoch

RISIKOANALYSE

- ☐ Identifikation der Informationssicherheitsrisiken und der damit verbundenen Geschäftsrisiken für:
  Anwendungen | Systeme
  Netzwerkverbindungen | Räume
- ☐ Bewertung der Risiken nach der Formel:
  Risiko = Schadenswahrscheinlichkeit × Schadenshöhe
- ☐ Risiken in einen Behandlungsplan überführen: Entscheidung, ob ein Risiko getragen, minimiert oder verlagert (z. B. versichert) wird

TIPP!

Verfahren Sie nach dem Prinzip „Sicherheit = Technische Maßnahme + Sensibilisierung". Ohne Sensibilisierung und Schulung der Mitarbeiter verpuffen technische Maßnahmen.

Dabei sollten Sie sich möglichst dicht an die gewählte Richtlinie halten. In begründeten Fällen kann jedoch davon abgewichen werden. Es gilt auch hier der Merksatz: „Die Norm passt sich an das Unternehmen an, nicht das Unternehmen an die Norm."

RECHTLICHE UND VERTRAGLICHE RAHMENBEDINGUNGEN

Unternehmen agieren heute in einem Umfeld, in dem zahlreiche gesetzliche Regelungen gelten, welche die Informationstechnologie betreffen. Zusätzlich existieren oft weitere vertragliche Rahmenbedingungen. Das Management der Informationssicherheit muss immer in diesem rechtlichen und vertraglichen Kontext gesehen werden. Hier gibt es eine Reihe von Gesetzen und Richtlinien, die zu beachten sind.

Bundesdatenschutzgesetz (BDSG)
Telekommunikationsgesetz (TKG)

IT-SICHERHEITSGESETZ

Für bestimmte Branchen gelten darüber hinaus weiter gehende Anforderungen. Im Rahmen des Informationssicherheitsmanagements verschafft sich das Unternehmen einen Überblick über die vertraglichen und gesetzlichen Anforderungen, die sich aus der Informationsverarbeitung ergeben.

DATENSCHUTZGESETZ

Nahezu jedes Unternehmen ist vom BDSG betroffen. Datenschutz und Informationssicherheit überschneiden sich in sehr vielen Aspekten und sind eng miteinander verzahnt.

Auf der Seite des Datenschutzes wird ausschließlich der Umgang mit personenbezogenen Daten betrachtet.
Im Rahmen des Managements für Informationssicherheit werden dagegen alle unternehmenskritischen Informationen betrachtet. Ebenso wie beim Datenschutz beschränkt sich diese Betrachtung aber nicht nur auf Daten, die in elektronischer Form vorliegen, sondern auch auf Informationen, die z. B. in gedruckter Form in den Archiven lagern oder auf den Schreibtischen der Mitarbeiter abgelegt sind.
Beim Datenschutz werden vom Gesetzgeber strenge technische und organisatorische Maßnahmen für die Einhaltung gefordert.
Das Managen der Informationssicherheit im Unternehmen folgt an sich den gleichen Prinzipien. Auch hier sind entsprechende vom Gesetzgeber festgelegte Anforderungen an technische und organisatorische Maßnahmen einzuhalten.

VERTRAGSGESTALTUNG MIT DRITTEN

Mitarbeiter

Die private Nutzung von E-Mail und Internet im Unternehmen sowie die Verwendung von privaten Arbeitsgeräten wie Smartphones oder Notebooks sollten immer klar geregelt sein. Gerade hier lauern oft rechtliche Fallstricke, die sich aus den Anforderungen des Datenschutzgesetzes oder aus den Vorgaben des Telekommunikationsgesetzes ergeben.
Zum Beispiel bei der forensischen Aufklärung von Sicherheitsvorfällen müssen oft jede

Menge Daten analysiert und in einen zeitlichen Zusammenhang gebracht werden.

Diese Analyse kann oft nur dann erfolgreich durchgeführt werden, wenn Protokolldateien zur Verfügung stehen oder der Zugriff auf E-Mail-Konten und E-Mail-Archive erfolgen kann. Abhängig von der Regelung zur Privatnutzung können derartige Zugriffe jedoch gegen geltende gesetzliche Regelungen z. B. aus dem Datenschutzgesetz oder dem Telekommunikationsgesetz verstoßen.

Geschäftspartner und Dienstleister

Eine Auslagerung von Daten oder Informationsprozessen an externe Geschäftspartner kann Auswirkungen auf Sicherheitskonzepte und Schutzvorgaben haben und muss immer im rechtlichen Kontext geprüft werden. Auch hier muss im Rahmen des Informationssicherheitsmanagements eine Erhebung stattfinden, welche Daten und Prozesse ausgelagert sind und welche Auswirkungen und Anforderungen sich daraus ergeben. Eine frühzeitige Einbindung des Beauftragten für Informationssicherheit sowie des Datenschutzbeauftragten ist in solchen Fällen notwendig.

Werden personenbezogene Daten bzw. Informationen mit externen Dienstleistern ausgetauscht und/oder bei externen Dienstleistern verarbeitet?

Wenn ja, sind die Anforderungen des Datenschutzgesetzes einzuhalten. So sind dann z. B. Verpflichtungserklärungen zum Einhalten der geltenden Datenschutzbestimmungen oder aber auch Verträge zur Auftragsdatenverarbeitung zwischen den Vertragspartnern abzuschließen. Die notwendigen Prüfungen werden vom Datenschutzbeauftragten durchgeführt. Die sich daraus ergebenden notwendigen technischen und organisatorischen Maßnahmen werden im Zuge des ISMS durchgeführt.

Werden wichtige Geschäftsprozesse in die Cloud ausgelagert?

Bei der Auslagerung von Geschäftsprozessen dürfen die Kosten, die sich aus den Anforderungen der Informationssicherheit ergeben, nicht vernachlässigt werden. Hier werden oft Anforderungen an die Verfügbarkeit nicht ausreichend berücksichtigt. Speziell die Rückmigration von Daten und Informationen bei Beendigung eines Vertragsverhältnisses mit einem Cloud-Dienstleister sollte schon beim Vertragsabschluss geregelt werden.

IT-SICHERHEITSGESETZ

Deutschland hat zum Juli 2015 ein neues IT-Sicherheitsgesetz (ITSiG) erlassen. Es handelt sich dabei jedoch um kein grundsätzlich neues Gesetz. Lediglich bereits bestehende Gesetze wurden erneuert, um den gestiegenen Anforderungen in der IT-Sicherheit an sogenannte kritische Infrastrukturen in der Bundesrepublik gerecht zu werden. Damit sind alle Infrastrukturen und Organisationen gemeint, auf die wir in unserer Gesellschaft für das tägliche Leben angewiesen sind. Dazu zählen explizit folgende Sektoren:

- Strom- und Gasnetzbetreiber
- Energie (Erzeugung und Verteilung)
- Informationstechnologie
- Telekommunikation
- Transport und Verkehr
- Gesundheit
- Wasser
- Ernährung
- Finanz- und Versicherungswesen

Firmen und Organisationen – insbesondere die Dach- und Branchenverbände – sind aufgefordert, Anforderungen an die IT-Sicherheit in den jeweiligen Sektoren zu definieren und einzureichen. Das Innenministerium (BMI) wird hierzu im Einvernehmen mit dem Bundesamt für Sicherheit in der Informationstechnik (BSI) und in Absprache mit den Fachverbänden voraussichtlich im ersten Quartal 2016 mehrere sektorspezifische Rechtsverordnungen erlassen.

Hierin werden die konkreten Anforderungen an die Informations- und IT-Sicherheit in den jeweiligen Sektoren festgelegt und gesetzlich verpflichtend gemacht. Nach Inkrafttreten der Rechtsverordnungen für den jeweiligen Sektor sind alle Firmen und Organisationen, die hierin tätig sind, verpflichtet, alle zwei Jahre einen geeigneten Nachweis über die Umsetzung von erforderlichen Sicherheitsmaßnahmen zu erbringen.

Kleinstunternehmen mit weniger als zehn Mitarbeitern und unter 2 Mio. Euro Umsatz sind mit einer De-minimis-Regelung vom ITSiG ausgenommen.

Bei nicht vollständiger, fehlerhafter oder unterlassener Umsetzung kann das BSI Geldstrafen zwischen 50.000 und 100.000 Euro verhängen.

Zudem ist es gesetzlich verpflichtend, wesentliche IT-Sicherheitsvorfälle anonymisiert an das BSI zu melden. Hierzu ist die Einführung eines geeigneten Systems zur kontinuierlichen Erkennung, Behandlung und Meldung von Sicherheitsvorfällen dringend anzuraten. Das lässt sich am leichtesten und effektivsten im Rahmen eines Informationssicherheitsmanagementsystems (ISMS) umsetzen.

Für alle Strom- und Gasnetzbetreiber in Deutschland hat die Bundesnetzagentur (BNetzA) bereits die Anforderung an die IT-Sicherheit aller Systeme, die der mittelbaren Netzführung und dem sicheren Netzbetrieb dienen, verpflichtend gestellt.

Hier gilt übrigens die De-minimis-Regelung

nicht - die BNetzA hat bereits im regulierten Umfeld für alle Strom- und Gasnetzbetreiber am 12.08.2015 einen IT-Sicherheitskatalog erlassen.
Dort wird die verpflichtende Einführung und Zertifizierung eines ISMS nach DIN ISO/IEC 27001 unter Berücksichtigung der ISO 27002 und 27019 gefordert. Dies ist durch die Einreichung einer Kopie eines gültigen Zertifikats bis zum **31.01.2018** an die BNetzA nachzuweisen. Die Betreiber von Strom- und Gasnetzen müssen außerdem bis zum **30.11.2015** einen Ansprechpartner/eine Ansprechpartnerin IT-Sicherheit an die BNetzA schriftlich melden.

TIPP!

Vom IT-Sicherheitsgesetz sind nur Unternehmen und Organisationen direkt berührt, die in einem der genannten Sektoren tätig sind. Die jeweiligen Rechtsverordnungen werden im ersten Quartal 2016 erwartet. Darin werden die Anforderungen konkretisiert und gesetzlich verankert.

Die nachfolgende Grafik gibt einen Überblick über das IT-Sicherheitsgesetz und den IT-Sicherheitskatalog:

BNetzA
IT-Sicherheits-katalog

IT-Sicherheitskatalog der BNetzA
- Betrifft alle Strom- und Gasnetzbetreiber in Deutschland
- ISMS nach ISO 27000 ff. einführen und zertifizieren
- Ansprechpartner(in) IT-Sicherheit an BNetzA bis 30.11.2015 melden
- Erstellung eines aktuellen Netzstrukturplans
- Seit 12. August 2015 verbindlich gültig
- Vorlage einer Kopie des Zertifikats an BNetzA bis 31.01.2018

Bund
IT-Sicherheits-gesetz

IT-Sicherheitsgesetz der Bundesregierung
- Erhöhte Anforderungen an die IT-Sicherheit für kritische Infrastrukturen seitens des Bundesministeriums des Innern (BMI)
- Sektoren: Energie, Informationstechnologie, Telekommunikation, Transport und Verkehr, Gesundheit, Wasser, Ernährung sowie Finanz- und Versicherungswesen
- Meldepflicht an das BSI (Bundesamt für Sicherheit in der Informationstechnik)
- Am 25. Juli 2015 als Gesetz in Kraft getreten
- BNetzA-IT-Sicherheitskatalog für Kraftwerke sowie sektorspezifische Rechtsverordnungen werden im ersten Quartal 2016 erwartet

BESTEHENDE STANDARDS UND VORGEHENSMODELLE

BSI IT-GRUNDSCHUTZ

Das Bundesamt für Sicherheit in der Informationstechnik (BSI) hat den IT-Grundschutz entwickelt. Dazu gehören vier Standards (BSI 100-1, BSI 100-2, BSI 100-3, BSI 100-4), die den Aufbau eines Informationssicherheitsmanagementsystems (ISMS) beschreiben, die Vorgehensweise erläutern, die Erstellung einer Risikoanalyse beschreiben und das Notfallmanagement betrachten. Zusätzlich werden die IT-Grundschutz-Kataloge veröffentlicht, in denen Gefährdungen und Maßnahmen beschrieben werden.
Den Kern des fast 5000-seitigen Grundschutzkataloges bilden die Bausteine. In den Bausteinen werden Handlungsempfehlungen in Form von Maßnahmen und Gefährdungen jeweils für einen Objekttyp beschrieben. Es gibt Bausteine für übergreifende Aspekte, Infrastruktur, IT-Systeme und Netze sowie für Anwendungen.

ISO-27000-REIHE

Die ISO/IEC-27000-Reihe enthält über 20 Normen und Standards zur IT-Sicherheit. Sie wird von der International Organization for Standardization (ISO) und der International Electronical Commission (IEC) herausgegeben. So werden z. B. in der ISO/IEC 27001 die Anforderungen an ein Managementsystem für Informationssicherheit beschrieben und in der ISO/IEC 27002 Empfehlungen für Kontrollmechanismen gegeben. In weiteren Teilen wird z. B. das Risikomanagement betrachtet und fachspezifische Ausarbeitungen für Sparten erstellt.

ISIS12

ISIS12 ist ein ganzheitliches Vorgehensmodell zur Einführung eines Informationssicherheitsmanagementsystems (ISMS) in mittelständischen Unternehmen und Kommunen. Das Vorgehensmmodell basiert auf dem BSI-IT-Grundschutz und ISO 27001, ist aber den Anforderungen von kleinen und mittleren Unternehmen angepasst. Das ISMS wird auf der Basis eines zwölf Schritte umfassenden Workflows mit einem angepassten Maßnahmenkatalog eingeführt. ISIS12 wurde am Bayerischen IT-Sicherheitscluster vom Netzwerk für Informationssicherheit entwickelt.

ANLAUFSTELLEN

aitiRaum e. V.
Werner-von-Siemens-Str. 6
86159 Augsburg
E-Mail: info@aitiRaum.de
Web: www.aitiRaum.de

Allianz für Cybersicherheit
Bundesamt für Sicherheit in der Informationstechnik (BSI)
Godesberger Allee 185-189
53175 Bonn
E-Mail: bsi@bsi.bund.de
Web: www.bsi.bund.de

Bayerisches IT-Sicherheitscluster e. V.
Geschäftsstelle im aiti-Park Augsburg
Werner-von-Siemens-Str. 6
86159 Augsburg
E-Mail: itsecurity@aitiRaum.de
Web: www.it-sicherheit-bayern.de

Bayerisches Landesamt für Datenschutzaufsicht
Promenade 27
91522 Ansbach
E-Mail: poststelle@lda.bayern.de
Web: www.lda.bayern.de

Bayerisches Landesamt für Verfassungsschutz
Bereich Spionageabwehr/ Wirtschaftsschutz
Postfach 450145
80901 München
E-Mail: wirtschaftsschutz@lfv.bayern.de
Web: www.lfv.bayern.de

Bayerisches Landeskriminalamt
SG 541 Zentrale Ansprechstelle Cybercrime – ZAC
Mailingerstraße 15
80636 München
E-Mail: zac@polizei.bayern.de
Web: www.polizei.bayern.de

WEITERE NÜTZLICHE LINKS:

BITKOM e. V.:
BITKOM ist der Digitalverband Deutschlands
Web: www.bitkom.org

Mittelstand-Digital:
Das Bundesministerium für Wirtschaft und Energie (BMWi) unterstützt mit dem Förderschwerpunkt Mittelstand-Digital den effizienten Einsatz von IKT-Anwendungen
Web: www.mittelstand-digital.de

Ihre Ansprechpartner:

Dr. Kristin Joel
IHK Schwaben
Geschäftsfeld Innovation und Umwelt
Telefon: 0821 31621-406
E-Mail: kristin.joel@schwaben.ihk.de

Stefan Schimpfle
aitiRaum e. V.
Geschäftsführer
Telefon: 0821 450433-111
E-Mail: s.schimpfle@aitiRaum.de

Diese Publikation kann unter www.schwaben.ihk.de, Dok.-Nr. 2706258 heruntergeladen werden.

Weitere Informationen zu IT-Recht und Sicherheit finden Sie unter www.schwaben.ihk.de Dok.-Nr. 75069

IHK Schwaben

Impressum:

Herausgeber
Industrie- und Handelskammer Schwaben

Diese Publikation ist in Kooperation mit aitiRaum e. V. im November 2015 entstanden.

Redaktion
IHK Schwaben: Claudia Rall, Ercin Özlü (Leitung)
aitiRaum e. V.: Stefan Schimpfle, Beate Sailer

Gesamtgestaltung
Grow communications, Augsburg
Bilder: 123RF und fotolia

IHK Schwaben
Stettenstraße 1+3 | 86150 Augsburg
Telefon: 0821 3162-0 | Fax: 0821 3162-323
info@schwaben.ihk.de | www.schwaben.ihk.de