

Informationssicherheit und Datenschutz einfach&effektiv

Integriertes Managementinstrumentarium systematisch
aufbauen und verankern

» Hier geht's
direkt
zum Buch

DIE LESEPROBE

1

Herausforderungen in Informationssicherheit und Datenschutz

Man wächst mit der Herausforderung.

Quelle: Unbekannt

Die Informations- und Kommunikationstechnik hat alle Lebensbereiche durchdrungen. Die Geschäftsprozesse von Unternehmen kommen kaum mehr ohne IT-Unterstützung aus. Die horizontale und vertikale Vernetzung von Partnern bis zu Maschinen nimmt immer weiter zu. Nur so kann schnell auf Kundenanfragen und sich ändernde Kundenbedürfnisse reagiert werden. Die hohe Durchdringung mit Informations- und Kommunikationstechnik erhöht jedoch gleichzeitig die Abhängigkeit und die Anfälligkeit für die kontinuierlich zunehmenden Sicherheitsbedrohungen, zum Beispiel im Kontext von Cyber-Security.

Sicherheits- und Datenpannen, wie Massen-E-Mails mit Viren, Veröffentlichung von vertraulichen Daten oder manipulierte, missbräuchlich verwendete, mutwillig zerstörte oder kompromittierte Daten, können für die Unternehmen zu ernsthaften rechtlichen oder wirtschaftlichen Konsequenzen führen. Insbesondere aber auch die Nichtverfügbarkeit von Systemen hat erhebliche wirtschaftliche Auswirkungen. Ein Beispiel hierzu ist die Unterbrechung einer Lieferkette in einer Just-in-time-Fertigung (JIT-Fertigung) aufgrund eines Systemabsturzes, der zu einem Produktionsstillstand führt, da wesentliche Rohstoffe oder Teile nicht angefordert werden und somit fehlen.

Externe Vorgaben wie Gesetze, Regulatoren und Normen sowie Anforderungen interessierter Parteien (z. B. BDSG, UWG, TMG, Regierungsbehörden) und Verträge erfordern ein angemessenes Sicherheitsniveau und die Einhaltung von Formalien. Vorstände und Geschäftsführer haften persönlich für viele Versäumnisse und mangelnde Risikoversorge. Ein Beispiel sind die hohen Bußgelder bei Datenpannen im Kontext der EU-DSGVO (europäische Datenschutzgrundverordnung) oder aber der NIS-2-Richtlinie. Imageschäden und Folgekosten erhöhen die Schadensauswirkungen noch erheblich. Die Gewährleistung der Persönlichkeitsrechte Betroffener und die Sicherstellung

der Rechenschaftspflicht sind daher Grundanforderungen an ein Datenschutz-Managementsystem.

Informationssicherheit und Datenschutz sind unerlässlich, um sowohl personenbezogene Daten als auch Geschäfts- und Unternehmensgeheimnisse zu schützen und einen zuverlässigen Geschäftsbetrieb und die kontinuierliche Weiterentwicklung des Geschäftsmodells zu gewährleisten. Es geht letztendlich darum, mit Informations-sicherheitsmanagement und Datenschutz den Erfolg des Unternehmens abzusichern (siehe Bild 1.1). Gerade im Zeitalter der digitalen Transformation sind „sichere“ Daten- und Integrationsplattformen mit vielen Automatismen als integraler Bestandteil des Managementsystems unerlässlich. Nur so kann der Mehrwert aus Daten gehoben und Big Data, Business-Analytics rechtssicher und berechtigt genutzt werden.

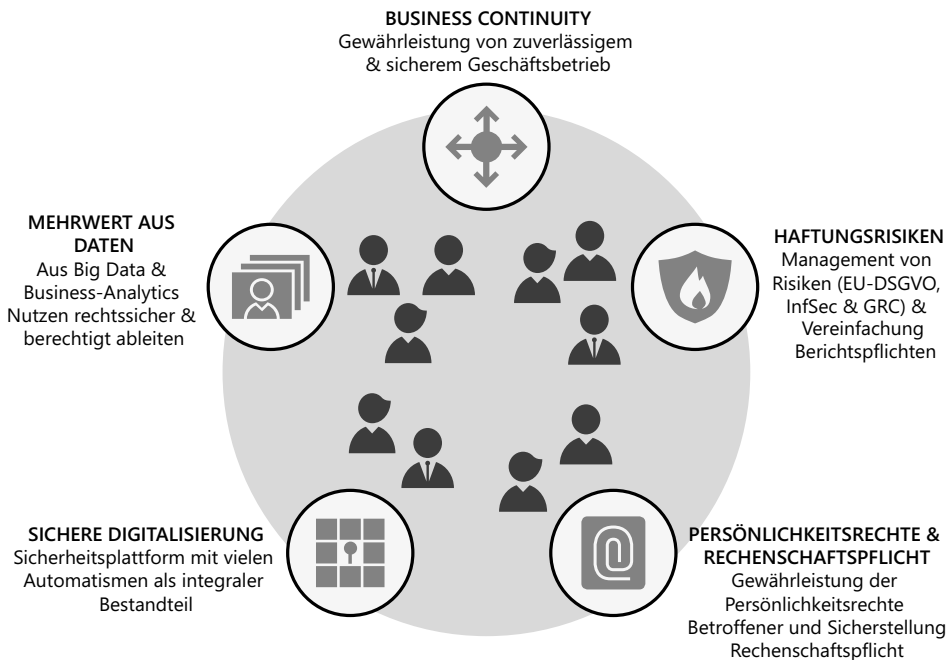


Bild 1.1 Nutzenorientiertes Management von Datenschutz und Informationssicherheit

Die Informationssicherheit und der Datenschutz eines Unternehmens müssen einen Handlungsrahmen und Hilfestellungen liefern, um den kontinuierlichen Geschäftsbetrieb und auch die Geschäftsmodellweiterentwicklung hinreichend sicher zu ermöglichen.

Die Herausforderungen in Informationssicherheit und Datenschutz nehmen immer weiter zu und sind eng auch mit der Umsetzung weiterer Compliance-Anforderungen

verbunden. Nach einer Einordnung von Informationssicherheit und Datenschutz schauen wir uns die Anforderungen etwas näher an.



In diesem Kapitel finden Sie die Antworten auf folgende Fragen

- Warum sind Informationssicherheit und Datenschutz wichtig?
- Was ist Informationssicherheit?
- Was ist Datenschutz?
- Welche Anforderungen leiten sich aus Gesetzen und Normen ab?

1.1 Einordnung von Informationssicherheit und Datenschutz

Wie bereits ausgeführt, sind Informationssicherheitsmanagement und Datenschutz essenziell, um den Erfolg des Unternehmens abzusichern. Was versteht man aber unter Informationssicherheit und Datenschutz?



Die **Informationssicherheit** zielt auf den angemessenen Schutz von Informationen und IT-Systemen in Bezug auf alle festgelegten Schutzziele, wie Vertraulichkeit, Integrität und Verfügbarkeit, ab. Ein unbefugter Zugriff oder die Manipulation von Daten soll verhindert und soweit möglich vorgebeugt werden, um daraus resultierende wirtschaftliche Schäden zu verhindern. Bei den Daten ist es unerheblich, ob diese einen Personenbezug haben oder nicht. Informationen können sowohl auf Papier als auch in IT-Systemen vorliegen.

IT-Sicherheit adressiert als Teilbereich der Informationssicherheit den Schutz elektronisch gespeicherter Informationen und deren Verarbeitung inklusive Funktionssicherheit, also das fehlerfreie Funktionieren und die Zuverlässigkeit der IT-Systeme. Hier müssen auch Systeme einbezogen werden, die häufig nicht unmittelbar als IT-Systeme wahrgenommen werden, wie Steuerungs- (ICS) oder IoT-Systeme. Die IT-Sicherheit ist also Bestandteil der Informationssicherheit. Das Aktionsfeld der klassischen IT-Sicherheit wird bei der Cyber-Sicherheit auf den gesamten Cyber-Raum ausgeweitet.

Unter **Datenschutz** wird primär der Schutz personenbezogener Daten vor missbräuchlicher Verwendung und Datenverarbeitung verstanden, um das Recht des Einzelnen auf informationelle Selbstbestimmung zu stärken.

Es stellt sich hierbei nicht die Frage, ob man Informationssicherheit und Datenschutz adressiert, sondern nur wann und in welchem Umfang. Die Kernfrage lautet: „Wann ist man hinreichend sicher?“

- *Welche Richtlinien, Verfahrensanweisungen und Arbeitsanweisungen sind erforderlich?*

Mögliche Antwort: verpflichtende und empfohlene Dokumente aus Informationssicherheit und Datenschutz (u. a. ISO 2700X, BSI IT-Grundschutz, NIS-2-Richtlinie und EU-DSGVO)

- *Wie kann man die IT-Systeme hinreichend „technisch“ absichern?*

Hierauf gibt es eine einfache Antwort: „Systeme sind hinreichend sicher, wenn der Aufwand eines Angreifers dessen Nutzen erheblich übersteigt.“

Widerstandsfähige Systeme überstehen absichtliche Angriffe ohne inakzeptablen Schaden für das Unternehmen. Für viele Systeme mit normalem Schutzbedarf reicht eine Absicherung nach dem „Stand der Technik“ aus (siehe Abschnitt 1.2.4).



Hinweis

Der Begriff „Stand der Technik“ im Kontext des IT-Grundschutzes beschreibt Maßnahmen, Technologien und Verfahren, die aktuell als geeignet und effektiv angesehen werden, um Sicherheitsziele zu erreichen (siehe [BSI23-1]).

- *Wann ist die Absicherung hinreichend?*

Wie viel Schutz ist notwendig, um einen kontinuierlichen Geschäftsbetrieb sicherzustellen, die sichere Geschäftsmodellweiterentwicklung zu ermöglichen und Imageschäden und Reputationsverlust zu vermeiden?

So dürfen z. B. Hackerangriffe nicht zum Ausfall von Kernsystemen führen.



Schutz ist kein Selbstzweck. Es ist so viel Schutz notwendig, um einen kontinuierlichen Geschäftsbetrieb, keinen Reputationsverlust, die Kundenbindung und allgemein die Voraussetzungen für das Erreichen der Unternehmensziele zu gewährleisten.

Hinreichend ist hierbei das Schlüsselwort. Denn eine hundertprozentige Sicherheit ist auch mit noch so hohem Aufwand nicht zu erreichen. Eine extrem hohe Absicherung ist unverhältnismäßig teuer oder geschäftsverhindernd. Ein Beispiel sind nicht vernetzte Systeme. Diese sind natürlich einfacher abzusichern. Jedoch erfordern die meisten Geschäftsabläufe gerade im Zeitalter der Digitalisierung vernetzte Systeme. Ein Kappen der Vernetzung verhindert oder erschwert den Geschäftsbetrieb so stark, dass wahrscheinlich auf Dauer nicht wirtschaftlich gearbeitet werden kann. Der konkrete Schutzbedarf hängt stark vom unternehmensindividuell eingeschätzten Schutzbedarf der jeweiligen Unternehmenswerte, wie z. B. die Kritikalität von Informationen oder Systemen, ab.

Ein hinreichender Informationsschutz ist für die meisten Werte mit normalem Schutzbedarf schon mit einer Standardabsicherung (siehe Abschnitt 1.2.4) der IT mit ver-

hältnismäßig geringen Mitteln zu erreichen. In Bild 1.2 finden Sie eine Prinzip-Darstellung für die Festlegung des optimalen Sicherheitsniveaus. In der Abbildung werden die Maßnahmenkosten und das Sicherheitsbedürfnis gemessen über das Schadensausmaß in Abhängigkeit vom Restrisiko dargestellt. Zudem finden Sie eine grobe Zuordnung zu Fehlerklassen nach dem CRISAM®-Modell (siehe [Hen13]) dargestellt.

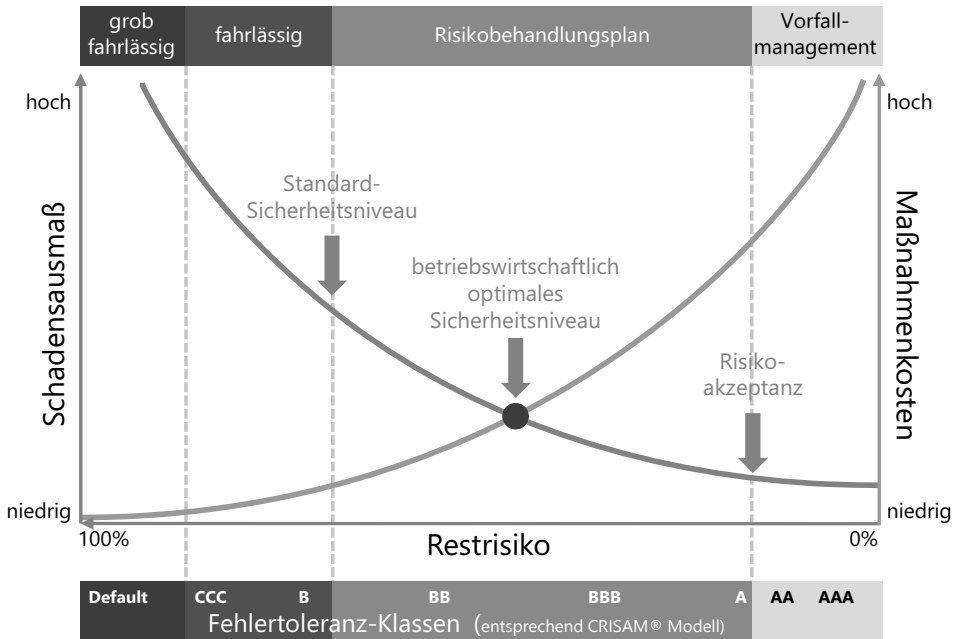


Bild 1.2 Optimales Sicherheitsniveau

Ohne Sicherheitsmaßnahmen und damit ohne Maßnahmenkosten wird ein extrem niedriges Schutzniveau erreicht und bestehende gesetzliche Anforderungen, wie z. B. aus der EU-DSGVO (siehe Abschnitt 1.2.5), werden nicht eingehalten. Die Organisation ist anfällig für Sicherheitsbedrohungen wie z. B. Kompromittierung von Webseiten, da entsprechende Vorkehrungen fehlen. Die Leitungsebene handelt grob fahrlässig und ist auch persönlich haftbar.

Das andere Extrem ist das Ziel, das Restrisiko von Sicherheitspannen weitestgehend auszuschließen. Jedoch ist der Versuch, alle möglichen Sicherheitsvorfälle vorherzusehen, sehr teuer; sowohl einmalig in der Erstellung als auch im kontinuierlichen Betrieb des Datenschutz- und Informationssicherheitsinstrumentariums. Für alle möglichen Konstellationen müssen organisatorische Maßnahmen, wie z. B. Richtlinien und Verfahrensanweisungen, oder technische Maßnahmen, wie z. B. automatisierte Forcierung der Einhaltung der Passwortrichtlinie, vorgesehen werden.

Jedes Unternehmen muss sein vorhandenes Sicherheitsniveau ermitteln und sein angestrebtes Sicherheitsniveau, den „Risikoappetit“, festlegen. Durch eine GAP-Analyse (siehe Abschnitt 3.1) können entsprechende Maßnahmen zur Schließung der Lücke ermittelt werden.

Das angestrebte Sicherheitsniveau sollte sich idealerweise nahe an dem in Bild 1.2 dargestellten betriebswirtschaftlich optimalen Sicherheitsniveau befinden. Über Standard-Absicherungsmaßnahmen z. B. aus dem IT-Grundschutz (siehe Abschnitt 1.2.4) kann für die Werte mit normalem Schutzbedarf ein Standard-Sicherheitsniveau auf dem „Stand der Technik“ erreicht werden. Für die darüberhinausgehenden Risiken, insbesondere für die Werte mit erhöhtem Schutzbedarf, sollte ein Risikobehandlungsplan erstellt und umgesetzt werden. Jedoch sollte hierbei eine Abwägung zwischen Schadensausmaß und Maßnahmenkosten durchgeführt werden. Wenn die Maßnahmenkosten in keinem Verhältnis zum Schadensausmaß stehen, dann muss die oberste Leitungsebene über die Risikoübernahme entscheiden. Akzeptierte Risiken müssen bei ihrem Auftreten schnell erkannt und über eine Vorfal- und Notfallmanagement-Organisation gemanagt werden. So können auch bei akzeptierten Risiken die Schadensauswirkungen reduziert werden.

Beispiele für akzeptierte Risiken aus der Praxis sind:

■ **IT-System-bedingte Einschränkungen**

Die Umsetzung von Sicherheitsanforderungen bedarf einer erheblichen Veränderung von IT-Systemen, die nur mit großem Aufwand mittelfristig umgesetzt werden können.

Beispiel: „unverzichtbare“ Standardlösungen, die auf veralteten Patch-Level aufsetzen.

■ **„Daten“ sind wesentlich für den Geschäftserfolg**

Beispiel: (Personenbezogene) Daten, wie z. B. Kundeninteressen oder -vorlieben werden für Marketing- und Vertriebsaktionen benötigt. Hier werden diese Daten zum „berechtigten“ Interesse erklärt und nur auf Einzelaufforderung hin gelöscht oder anonymisiert.

Ein Hilfsmittel für die Abwägung zwischen Schadensausmaß und Maßnahmenkosten sowie die Risikoübernahme sind Risikoportfolios mit den Dimensionen Schadensauswirkung und Eintrittswahrscheinlichkeit. Den Bereichen im Portfolio kann eine entsprechende Risikobehandlungsstrategie, wie z. B. Risikoübernahme, zugeordnet werden. In Abschnitt 4.2 finden Sie Best-Practices zum Risikomanagement.



Die Abwägung zwischen Schadensausmaß und Maßnahmenkosten sowie der Risikoappetit müssen unternehmensindividuell festgelegt werden.

Normen, wie z. B. die ISO-2700X-Familie (siehe [Bre24]), geben sowohl Anforderungen als auch Empfehlungen für die umzusetzenden Sicherheitsmaßnahmen vor. Insbe-

sondere der BSI-IT-Grundschutz (siehe Abschnitt 1.2.4) gibt zudem Umsetzungshinweise und Maßnahmenempfehlungen. Rund 80 % der bekannten Angriffe lassen sich mit den Standard-Schutzmaßnahmen des IT-Grundschutzes abwehren. Über technische und organisatorische Maßnahmen (TOMs) müssen sowohl die Sicherheit der für das Unternehmen schützenswerten Assets als auch insbesondere die personenbezogenen Daten abgedeckt werden. Die richtige Auswahl der Sicherheitsmaßnahmen für die hinreichende Absicherung und deren handhabbare Operationalisierung ist erfolgsentscheidend.

Die Sicherheitsmaßnahmen zur Erreichung und Aufrechterhaltung einer störungsfreien Informationsverarbeitung müssen einerseits wirksam (effektiv) sein, um ein erforderliches Schutzniveau zu erreichen. Das Schutzniveau wird maßgeblich von der Kritikalität der zu schützenden Assets, wie z. B. Kundendaten, sowie von geltenden Gesetzen und Regularien bestimmt, die eingehalten werden müssen.

Andererseits müssen die Schutzmaßnahmen auch wirtschaftlich angemessen (effizient) sein und dürfen die Organisation nicht überfordern, d. h., die Möglichkeiten der Aufbau- und Ablauforganisation sowie weiterer Randbedingungen müssen berücksichtigt werden. Ein handhabbares und integriertes Instrumentarium ist notwendig, um sowohl die EU-Datenschutz-Grundverordnung (EU-DSGVO) als auch die Anforderungen der Informationssicherheit (u. a. BSI und ISO 27001) nachhaltig zu erfüllen.

Im Folgenden werden sowohl die Anforderungen der EU-Datenschutz-Grundverordnung als auch des Informationssicherheitsmanagements eingeführt.

1.2 Anforderungen an Informationssicherheit und Datenschutz

Zunehmende Cyber-Angriffe sowie stärkere Regulierung und Compliance-Anforderungen, wie die EU-DSGVO, die NIS-2-Richtlinie oder das Lieferkettengesetz, erfordern eine deutlich höhere Aufmerksamkeit in den Unternehmen für Informationssicherheits- und Datenschutzfragestellungen. Für die Festlegung eines integrierten Managementsystems für Informationssicherheit und Datenschutz müssen die Anforderungen verstanden und im Kontext des Unternehmens bewertet werden.

Die immer weiter zunehmende Durchdringung von Informationstechnik in den Geschäftsprozessen, die steigende Bedrohungslage sowie gesetzliche und Compliance-Anforderungen führen zu Gefahren, wie

- Missbrauch oder Verlust von schützenswerten Daten,
- Verstöße gegen gesetzliche Bestimmungen oder unternehmensspezifische Richtlinien und Regeln mit zum Teil persönlicher Haftung und
- Behinderung oder sogar Unterbrechung der Geschäftstätigkeit durch z. B. nicht verfügbare Systeme.

Diese Bedrohungslage nimmt immer weiter zu. Gründe sind hierfür u. a.:

- KI-gestützte Angriffe: Die Nutzung von KI durch Hacker wächst. So können Phishing-Mails einfacher und überzeugender generiert und andere Sicherheitsmaßnahmen umgangen werden.
- Technologische Entwicklungen: Quanten-Computing wird zur potenziellen Bedrohung für bestehende Verschlüsselungsstandards.
- Steigender Vernetzungsgrad: Menschen und IT-Systeme arbeiten zunehmend vernetzt (horizontal und vertikal siehe [Han24]) auch über Unternehmensgrenzen hinweg. Eine Sicherheitslücke kann nicht isoliert, sondern muss mit ihren Abhängigkeiten betrachtet werden. Gerade auch mit dem neuen Lieferkettengesetz muss die Sicherheit in der gesamten Lieferkette gestärkt werden. Angreifer nutzen gezielt Schwachstellen bei Drittanbietern oder in der Lieferkette aus.
- IT-Verbreitung und Durchdringung: Immer mehr Bereiche werden von der Informationstechnik durchdrungen. Beispiele sind Smart Home oder RFIDs zur Steuerung von Besucher- oder Warenströmen oder IT-gestützte Sensorik in Autos, um automatisch auf veränderte Umgebungsverhältnisse reagieren zu können. Die verschiedenen IT-Komponenten kommunizieren miteinander zunehmend drahtlos und sind über das Internet lokalisierbar und steuerbar.
- Zunehmende und schnellere Ausnutzung von Schwachstellen: Die Zeitspanne zwischen dem Bekanntwerden einer Sicherheitslücke und den ersten gezielten Massenangriffen (z. B. Computerviren, Trojanische Pferde oder andere Angriffe) sinkt immer weiter. So muss zunehmend schneller die Information über Sicherheitslücken und deren Beseitigung, z. B. durch Einspielen von Patches und Updates, bekannt sein. Ein gut aufgestelltes Informationssicherheitsmanagement mit Warnsystem ist extrem wichtig, um schnell die richtigen Maßnahmen zu ergreifen.

Neben den zunehmenden Bedrohungen der Cyber-Security sind die steigenden Anforderungen aus Datenschutz und Informationssicherheit aufgrund der EU-Datenschutz-Grundverordnung (siehe [SDM18] und [Voi24]) und in der Informationssicherheit entsprechend der individuellen Anforderungen oder gesetzlichen Vorgaben sowie der Compliance-Anforderungen zu bewältigen.

1.2.1 Wesentliche Normen und gesetzliche Vorschriften

ISO/IEC 2700X

ISO/IEC 2700X ist die internationale De-facto-Normenreihe für die Informationssicherheit. Sie legt die Anforderungen für den Aufbau, die Implementierung, den Betrieb, die Überwachung, die Wartung und die kontinuierliche Verbesserung eines Informationssicherheitsmanagementsystems (ISMS) fest.

**Definition**

Ein Informationssicherheitssystem (ISMS) ist ein umfassendes Managementsystem mit definierten Richtlinien, Regeln und Prozessen zur Planung, Durchführung, Steuerung und fortlaufenden Optimierung der Informationssicherheit im Unternehmen. Es ist ein strukturierter Ansatz, um die Vertraulichkeit, Integrität und Verfügbarkeit von Informationen zu gewährleisten.

Ziel ist es, Organisationen darin zu unterstützen, Informationen systematisch zu schützen und Sicherheitsrisiken effektiv zu managen. Die Sicherheitsstandards der ISO/IEC-2700X-Normenreihe zielen darauf ab, das Sicherheitsniveau in Unternehmen zu verbessern. Die ISO/IEC 2700X enthält Anforderungen und Maßnahmen für den Aufbau, Betrieb und die kontinuierliche Verbesserung eines Informationssicherheitsmanagementsystems (ISMS). Die Anforderungen der Norm sind durch die Implementierung von für das Unternehmen passenden Sicherheitsmechanismen zu erfüllen.

Die Zertifizierung nach ISO 27001 bestätigt, dass ein Unternehmen angemessene Prozesse und Maßnahmen implementiert hat, um die Vertraulichkeit, Integrität und Verfügbarkeit von Informationen zu schützen.

Weitere Informationen zur ISO 27001 finden Sie in Abschnitt 1.2.3.

TISAX

TISAX (Trusted Information Security Assessment Exchange) ist eine branchenspezifische Adaption der ISO 27001 für die Automobilindustrie. Es handelt sich um einen branchenspezifischen Standard, der von der ENX Association in Zusammenarbeit mit der deutschen Automobilindustrie entwickelt wurde. TISAX baut auf den Prinzipien der ISO/IEC 27001 auf und fügt spezifische Anforderungen hinzu, die für die Automobilbranche relevant sind, wie etwa den Umgang mit Prototypenschutz und Anforderungen an den Datenschutz gemäß EU-DSGVO. TISAX ist ein Austauschsystem, bei dem Assessment-Ergebnisse über die TISAX-Plattform zwischen teilnehmenden Unternehmen ausgetauscht werden können. TISAX-Audits werden von speziell autorisierten Prüfdienstleistern durchgeführt, die von der ENX (European Network Exchange) Association akkreditiert sind. Die Zertifizierung erfolgt aber über ISO 27001.

**Hinweis**

ENX ist eine von europäischen Automobilherstellern, Zulieferern und Verbänden gegründete Organisation, um sichere Datenaustauschplattformen und Standards für die Branche zu entwickeln und zu fördern. Aufgaben von ENX im TISAX-Kontext sind:

- **Betrieb und Verwaltung von TISAX**
Bereitstellung einer Austausch-Plattform für den sicheren Austausch der Ergebnisse von TISAX-Assessments.

- **Akkreditierung von Prüfdienstleistern**
Autorisierung und Überwachung der unabhängigen Prüfdienstleister für TISAX-Assessments.
- **Etablierung von TISAX als einheitlichen Standard**
ENX sorgt dafür, dass TISAX als einheitlicher Standard für Informationssicherheit in der Automobilbranche etabliert ist und von allen relevanten teilnehmenden Akteuren anerkannt wird.

Weitere Informationen zur ISO 27001 und TISAX finden Sie in Abschnitt 1.2.3.

IT-Grundschutz (IT-GS)

Der IT-Grundschutz ist ein von der Bundesrepublik Deutschland entwickeltes Konzept für einen praktikablen und aufwandsarmen sowie angemessenen Schutz von Informationen und die strukturierte und umfassende Absicherung von IT-Systemen und Prozessen, um das Informationssicherheitsniveau in Unternehmen zu erhöhen. Er liefert einen De-facto-Standard für IT-Sicherheit und liefert die methodische Grundlage, um ein Informationssicherheitsmanagementsystem (ISMS) aufzubauen und Sicherheitsmaßnahmen in einer Organisation umzusetzen. Er wird vom Bundesamt für Sicherheit in der Informationstechnik (kurz BSI) herausgegeben. Er wird in regelmäßigen Abständen weiterentwickelt und hierbei immer mit den relevanten internationalen Normen wie ISO/IEC 27001 abgeglichen.

Der IT-Grundschutz ist ein universell anwendbares Sicherheitsframework und eignet sich für alle Organisationen, die Informationssicherheit auf eine strukturierte und nachvollziehbare Weise umsetzen wollen. Besonders relevant ist er für öffentliche Einrichtungen und Unternehmen im Bereich KRITIS.

Der IT-Grundschutz basiert auf BSI-Standards, die detaillierte Anforderungen an Informationssicherheit und Vorgehensweisen beschreiben (z. B. BSI-Standard 200-1 bis 200-3). Ein wichtiger Bestandteil war das IT-Grundschutz-Kompendium (siehe [BSI23-1]), das konkrete Maßnahmenkataloge enthält. Dieses wurde jährlich aktualisiert.

Ab 2024 wird es kein neues IT-Grundschutz-Kompendium geben, da das Bundesamt für Sicherheit in der Informationstechnik (BSI) die Strategie für die Weiterentwicklung des IT-Grundschutzes angepasst hat. Statt eines jährlich überarbeiteten Kompendiums legt das BSI verstärkt Wert auf kontinuierliche und gezielte Updates einzelner IT-Grundschutz-Bausteine. Diese Anpassung ermöglicht eine flexiblere Reaktion auf technologische Entwicklungen und Nutzerfeedback, statt die gesamten Inhalte jährlich zu überarbeiten. Siehe hierzu www.bsi.bund.de.

Siehe www.bsi.bund.de: Der neue IT-Grundschutz wird vollständig prozessorientiert aufgebaut und basiert auf einem digitalen Regelwerk in Form einer JSON-Datei. Jede Anforderung an die Cybersicherheit wird als Regel in einem standardisierten Format erfasst, sodass diese Regeln auch durch Computerprogramme interpretiert und ausgewertet werden können. Das digitale Regelwerk löst das IT-Grundschutz-Kompen-

dium ab, welches Anforderungen an Cybersicherheit in Textform (u. a. als PDF und als gedruckte Version) für menschliche Adressaten beschreibt. Der Wechsel auf ein digitales Regelwerk ermöglicht eine Automatisierung von Sicherheitsprozessen, sodass Anforderungen an die Cybersicherheit nicht nur von Personen, sondern auch über ein Managementsystem für Informationssicherheit (ISMS) modelliert werden können und die Einhaltung der Anforderungen überwacht werden kann. Um die Anwendbarkeit weiter zu erleichtern, werden die Absicherungsstufen Basis, Standard und erhöhter Schutzbedarf durch flexible Leistungszahlen in Verbindung mit dynamischen Schwellwerten ersetzt.

Weitere Informationen zum IT-Grundschutz finden Sie in Abschnitt 1.2.4.

IT-Sicherheitsgesetz (IT-SIG)

Das IT-SIG zielt darauf ab, die Sicherheit informationstechnischer Systeme zu erhöhen, um den Gefahren beim Ausfall von kritischen Infrastrukturen zu begegnen. Das IT-SIG schafft bereits seit Juli 2015 einen einheitlichen Rechtsrahmen für die Zusammenarbeit von Staat und Unternehmen für mehr Cybersicherheit bei KRITIS. Im Vordergrund stehen Betreiber sogenannter „kritischer Infrastrukturen“.



Definition KRITIS

Kritische Infrastrukturen (KRITIS) sind Organisationen oder Einrichtungen mit hoher Bedeutung für das staatliche Gemeinwesen, bei deren Ausfall oder Beeinträchtigung nachhaltig wirkende Versorgungsengpässe, erhebliche Störungen der öffentlichen Sicherheit oder andere dramatische Folgen auftreten würden.

Am 3. Mai 2016 ist der erste Teil der BSI-KRITIS-Verordnung (§ 10 BSI-Gesetz) in Kraft getreten. Hier werden neben dem BSI-Gesetz auch das **Energiewirtschaftsgesetz (EnWG)**, das Telemediengesetz, das Telekommunikationsgesetz und weitere Gesetze geändert und ergänzt.

Die KRITIS-Betreiber müssen sich beim BSI registrieren und ihre IT-Sicherheit nach dem „Stand der Technik“ umsetzen. Sie müssen innerhalb von vorgegebenen Fristen (zwei Jahre) Mindeststandards für IT-Sicherheitsmaßnahmen in den kritischen Branchen wie Energie oder Gesundheit entwickeln und nachweislich umsetzen. Zudem bestehen bei Ausfällen oder IT-Sicherheitsvorfällen Meldepflicht gegenüber dem BSI sowie Informationspflichten gegenüber betroffenen Nutzern.

Um die Betreiber kritischer Infrastrukturen noch wirksamer zu unterstützen, hat das BSI das *Mobile Incident Response Teams (MIRT)* eingerichtet. Diese Spezial-Task-Forces bestehen aus Cybersicherheitsexpertinnen und -experten des BSI, die auf Wunsch der KRITIS-Betreiber besonders schwerwiegende Cyberangriffe vor Ort untersuchen und bei deren Bewältigung helfen.

Die NIS-2-Richtlinie erweitert die Befugnisse des BSI und stärkt gleichzeitig die Kooperation von Staat und Wirtschaft. Die NIS-2-Richtlinie ergänzt und erweitert das

IT-Sicherheitsgesetz (IT-SiG) in Deutschland. Das IT-SiG wurde zum IT-SiG 2.0 angepasst, um u. a. die Vorgaben der NIS-2-Richtlinie zu erfüllen. Das IT-SiG 2.0 wurde am 23. April 2021 im Bundestag verabschiedet (siehe www.bsi.bund.de).



Hinweis

Auch das Gesetz über das Bundesamt für Sicherheit in der Informationstechnik (BSI-Gesetz – BSIG) musste entsprechend der NIS-2-Richtlinie angepasst werden. Das BSIG wurde zuletzt durch Artikel 12 des Gesetzes vom 23. Juni 2021 geändert.

Im IT-SiG 2.0 wurde neben der Integration der NIS-2-Vorgaben der Anwendungsbereich erweitert. Mittelgroße Unternehmen in bestimmten kritischen Sektoren, die bisher nicht im Fokus des IT-Sicherheitsgesetzes standen, sind jetzt auch mit einbezogen. Während das IT-Sicherheitsgesetz eine nationale Regelung ist, harmonisiert die NIS-2-Richtlinie die Cybersicherheitsregelungen in der gesamten EU.

NIS-2-Richtlinie (Netz- und Informationssicherheitsrichtlinie 2)

Die NIS-2-Richtlinie ist eine EU-weite Gesetzgebung, die darauf abzielt, die Cybersicherheit innerhalb der Europäischen Union zu verbessern. Sie setzt neue, strengere Standards für die Sicherheit von Netz- und Informationssystemen und erweitert den Geltungsbereich auf mehr Branchen und Unternehmen.

Die NIS-2-Richtlinie ist die EU-Richtlinie 2022/2555 des Europäischen Parlaments und des Rates vom 14. Dezember 2022 über Maßnahmen für ein hohes gemeinsames Cybersicherheitsniveau in der Union. Sie soll das Niveau der Cyberresilienz in der Union stärken.

Die europäische Sicherheitsrichtlinie NIS-2 (Netzwerk- und Informationssicherheit) ersetzt die ursprüngliche Richtlinie NIS aus dem Jahr 2016 und erweitert diese um strengere Sicherheitsanforderungen, zusätzliche Branchen bzw. Sektoren und eine höhere Zahl betroffener Betriebe (siehe wikipedia.com).

Die betroffenen Unternehmen müssen sich nach NIS-2 als Teil internationaler Lieferketten bis Ende 2024 besser gegen IT-Angriffe schützen: Bereits bis zum 17. Oktober 2024 musste die NIS2-Richtlinie von den einzelnen EU-Mitgliedstaaten in nationales Recht umgewandelt werden. Ab dem 18. Oktober 2024 sind betroffene Betriebe sofort verpflichtet, sich bei der zuständigen nationalen Behörde zu registrieren, Vorfälle zu melden und die Einhaltung der Sicherheitsanforderungen zu gewährleisten.

Der Nachweis der Compliance muss regelmäßig erbracht werden. Anderenfalls drohen empfindliche Strafen von bis zu zehn Millionen Euro oder zwei Prozent des weltweiten Umsatzes – je nach Einstufung und Kritikalität der Unternehmen.



Hinweis

Betroffene Branchen bei NIS-1 waren bereits Energie, Finanzmarktinfrastrukturen, Trinkwasser, Digitale Infrastruktur/Netze, Anbieter digitaler Dienste, Gesundheit, Verkehr und Ernährung. Bei NIS-2 kommt noch Forschung, Bankwesen, Weltraum, öffentliche Verwaltung, Abfall, Post- und Kurierdienste, Abwasser, Verwalter von IKT-Diensten, Chemie und die industrielle Produktion hinzu. Dies gilt für Großunternehmen ab 250 Mitarbeiter und mehr als 50 Mio. Euro Umsatz und/oder mehr als 43 Mio. Euro Bilanzsumme. Bei NIS-2 sind auch mittelständische Unternehmen betroffen mit 50–249 Mitarbeiter.

Das NIS2UmsuCG – das deutsche NIS2-Umsetzungsgesetz – ist derzeit allerdings noch in Arbeit. Geplant ist das Inkrafttreten ab März 2025. Neben NIS2 wird das KRITIS-Dachgesetz kritische Betreiber mit Resilienz und BCM regulieren. Das OpenKRITIS-Mapping von NIS2 auf ISO 27001 und KRITIS erleichtert die Umsetzung.

Wichtig ist hier insbesondere, die **Resilienz** des Unternehmens zu stärken und zugleich Kosten zu senken. Geschäftsmodelle, Prozesse, Applikationen und Infrastrukturen müssen widerstandsfähig gegen die unterschiedlichsten externen Einflüsse sein und gleichzeitig schnell auf Entwicklungen reagieren können. Die digitale Resilienz ist zu einem der wichtigsten Leistungsindikatoren (KPI) für die digitale Transformation geworden.



Resilienz ist die Flexibilität von Maschinen, Systemen und Organisationen bei sich verändernden Situationen mithilfe digitaler Technologien optimal zu reagieren. Sie müssen widerstandsfähig gegen die unterschiedlichsten externen Einflüsse sein und gleichzeitig schnell auf Entwicklungen reagieren können. Es gilt, das Gleichgewicht zwischen Innovation und Wirtschaftlichkeit zu finden.

Die NIS-2-Richtlinie stellt hohe Anforderungen in Bezug auf Cybersicherheit. Ziel ist es, die Widerstandsfähigkeit (Resilienz) gegen Cyberangriffe zu stärken. Hier sind die zentralen Sicherheitsmaßnahmen für die Umsetzung von NIS-2:

- **Kontext Organisation und Governance**
 - **Risikomanagement:** Entwicklung und Implementierung eines systematischen Ansatzes zur Bewertung und Minimierung von Cybersicherheitsrisiken. Hinweis: Dies schließt das IT-Risikomanagement mit ein.
 - **Verantwortlichkeiten:** Benennung einer für die Cybersicherheit zuständigen Führungskraft (z. B. Chief Information Security Officer, CISO)
 - **Schulungs- und Awareness-Maßnahmen:** Aufsetzen von vollständigen und wirksamen Schulungs- und Awareness-Maßnahmen sowie regelmäßige Schulungen und Sensibilisierungsmaßnahmen für Mitarbeitende
 - **Policies und Richtlinien:** Informationssicherheitsrichtlinie, Risikomanagement und für alle Prozesse und Themenbereiche, wie hier aufgeführt