Alles für Ihre Informationssicherheit ›

Kompetente und praxisgerechte Unterstützung.

Mit dem Full Kritis Service der EnBW AG erhalten Sie einen zuverlässigen und erfahrenen Partner für Informationssicherheit.

EnBW

Inhalt

1. Einleitung und Grundlagen

„Informationssicherheit ist doch das gleiche wie IT-Sicherheit“.
Diesen oder ähnliche Sätze haben Berater schon öfter während den ersten Kundenterminen gehört. Informationssicherheit ist jedoch weit mehr als nur IT-Sicherheit.

IT-Sicherheit fokussiert sich auf den Schutz der informationstechnischen Systeme (Server, Clients, Netzwerk, TK-Anlage, ...) und den darin befindlichen Informationen wie z. B.:

- Elektronische Gehaltsabrechnungen
- Kundeninformationen
- Forschungs- und Entwicklungsdaten
- Firewall-Konfigurationen
- Datensicherungen

Ziel ist es, zumindest die drei grundlegenden Schutzziele Verfügbarkeit, Vertraulichkeit und Integrität zu gewährleisten.

Informationssicherheit beinhaltet die IT-Sicherheit und erweitert den Fokus auch auf die nicht-digitale Welt. Daher werden hier auch Themen wie zum Beispiel papiergebundene Informationen, (Geschäfts-) Prozesse und die Gebäudesicherheit berücksichtigt, da diese ebenfalls die Schutzziele beeinflussen. Darüber hinaus werden einige Aspekte des Datenschutzes adressiert.

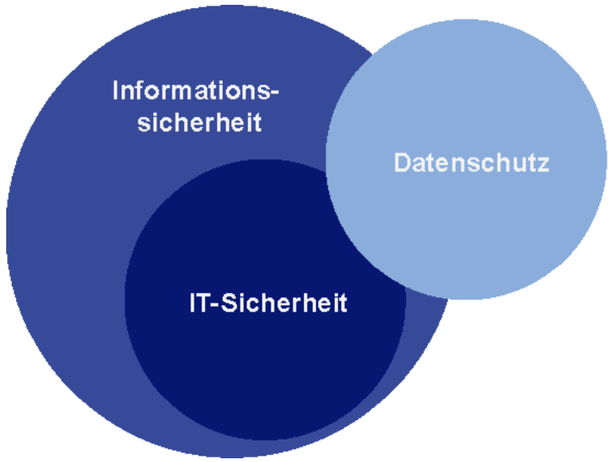
Für die Umsetzung der Informationssicherheit wird fast immer auf den Begriff „Stand der Technik“ verwiesen, und dieser wird auch in gesetzlichen Vorgaben als notwendiges Niveau aufgeführt. Der Stand der Technik ist jedoch nirgends klar durch vorgegebene Anforderungen definiert. Dies erfolgt durch die gängigen Standards, Normen sowie technischen Richtlinien wie zum Beispiel:

- ISO 27001
- IT-Grundschutz
- Branchenspezifische Standards
  - o B3S Gesundheit
  - o B3S Wasser/Abwasser
- IT-Sicherheitskatalog

Gesetzliche Forderungen mit Bezug zur Informationssicherheit finden sich unter anderem in folgenden Gesetzen:

- IT-Sicherheitsgesetz
- Energiewirtschaftsgesetz
- Patientendaten Schutzgesetz
- Europäische Datenschutzgrundverordnung

Die Umsetzung des Stands der Technik der Informationssicherheit erfolgt durch den Aufbau und Betrieb eines Informationssicherheitsmanagementsystems (ISMS). In diesem werden verschiedene technische und organisatorische Maßnahmen zur Sicherstellung der Informationssicherheit und zur Erfüllung der Schutzziele umgesetzt.



1.1. Warum ein ISMS für Sie und Ihre Kunden wichtig ist

Der Grund, weswegen Sie ein ISMS betreiben oder aufbauen, kann vielfältig sein: gesetzliche Vorgaben, Anforderung Ihrer Kunden, Eigenschutz oder die Tatsache, dass Sie bereits Opfer eines Angriffs wurden. Unabhängig davon, was genau Sie zum Aufbau und Betrieb Ihres ISMS bewegt, bietet Ihnen ein ISMS mehrere Vorteile, um Ihr Unternehmen und Ihre Geschäftsprozesse abzusichern.

- Schutz Ihrer Unternehmenswerte (Daten, Informationen, Prozesse)
- Informationssicherheitsrisiken kennen, beherrschen und reduzieren
- Regelmäßige Kontrolle der Informationssicheheitsstandards Ihres Unternehmens
- Sicherstellung der Verfügbarkeit Ihrer IT-Landschaft und Prozesse
- Awareness Ihrer Mitarbeiter für IT- & Informationssicherheit sowie Datenschutz

Darüber hinaus kann ein ISMS auch zum Erfüllen von Compliance-Anforderungen Ihrer Geschäftspartner und Kunden notwendig sein.

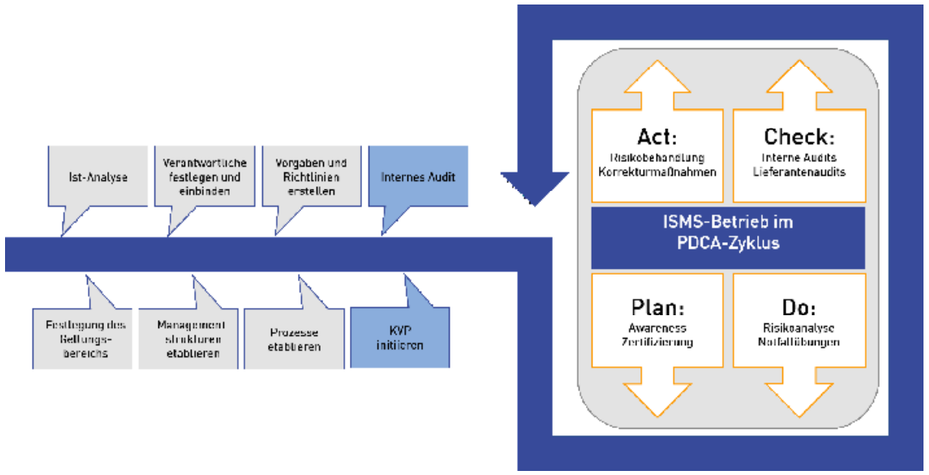
- Sicherstellung der Verfügbarkeit Ihrer erbrachten Services durch ein Business Continuity Management
- Sicherstellung der Vertraulichkeit verarbeiteter Kundendaten durch geeignete IT-Sicherheitsmaßnahmen
- Steigerung des Vertrauens in Ihr Unternehmen, insbesondere in Ihre IT-Sicherheit und die Reduzierung potenzieller Gefährdungen, die durch Ihre Services auf Ihre Kunden wirken können

Kurz zusammengefasst reduziert ein wirksames ISMS Ihre Geschäftsrisiken aus den Bereichen IT-Sicherheit, Informationssicherheit und Datenschutz und weist nach, dass Sie den Stand der Technik der Informationssicherheit in Ihrem Unternehmen umsetzen.

1.2. Wobei wir Sie unterstützen können

Wir unterstützen Sie gerne dabei Ihr ISMS aufzubauen und lassen Sie natürlich nicht im Regen stehen, sollten Sie beim Betrieb Ihres ISMS (ob mit oder ohne unserer Unterstützung aufgebaut) Hilfe benötigen. Die folgende Skizze zeigt die häufigsten Themen, bei welchen wir unsere Kunden im Aufbau und Betrieb unterstützen.

Der Schlüssel zu Ihrer Informationssicherheit ›



2. Aufbau eines ISMS

Während des Projektes müssen intensive Gespräche mit den jeweiligen Verantwortlichen geführt werden. Hierbei stößt das ISMS-Team immer wieder auf Verbesserungspotentiale, z. B. in Prozessabläufen oder der IT-Sicherheit, welche sonst vielleicht unentdeckt oder ungenutzt geblieben wären.

Der Aufbau eines ISMS ist ein umfangreiches Projekt und der zeitliche Aufwand hängt dabei stark von den bereits vorhandenen Vorgaben, Strukturen und Prozessen in Ihrem Unternehmen ab. Für Ihr ISMS müssen die zugrundeliegende Managementstruktur aufgebaut und Vorgaben in Richtlinien definiert und dokumentiert werden. Um diese Richtlinien mit „Leben" zu füllen sind Verfahrensanweisungen, Konzepte und Prozesse zu erstellen und bei Ihnen zu etablieren. Die Zielsetzung ist, Ihr ISMS konform zu den für sie geltende Anforderungen (z. B. ISO 27001, IT-Grundschutz, TISAX, B3S) aufzubauen und einen effektiven Betrieb des ISMS sicherzustellen.
Der Aufbau Ihres ISMS erfolgt in diesen vier grundlegenden Schritten:

- Ist-Analyse und Geltungsbereich definieren
- Aufbau der Managementstruktur
- Erstellen der Richtlinien und Vorgaben
- Prozesse etablieren

Dieser Ablauf muss nicht strikt eingehalten werden. Wir berücksichtigen während des Projekts auch die personellen Verfügbarkeiten und können einzelne Aspekte auf Ihren Wunsch hin oder aufgrund interner/externer Erfordernisse höher priorisieren.
Nach dem Abschluss des ISMS-Aufbaus (Plan) wird der Betrieb (Do) aufgenommen, das erste interne Audit durchgeführt (Check), daraus resultierende Korrekturmaßnahmen ermittelt (Act) und der Managementbericht erstellt. Diese Phase stellt den ersten von vielen PDCA-Zyklen dar (Plan-Do-Check-Act), dessen Durchführung auch eine Grundvoraussetzung für ein Zertifizierungsvorhaben ist.

2.1. Ist-Analyse

Für den Aufbau des ISMS ist es wichtig, die Werte und Geschäftsprozesse sowie die Rahmenbedingungen zu kennen, welche für Ihr Unternehmen von Bedeutung sind. Dies beinhaltet auch interessierte Parteien an Ihrem Unternehmen. Beispiele hierfür sind z. B. Behörden wie das BSI oder die BNetzA, Ihre Kunden sowie ggf. Ihr Mutterkonzern oder Teilhaber.
Die Ist-Analyse führen wir üblicherweise in einem Workshop mittels Interviews sowie einem Einblick in die vorhandene Dokumentation durch. Bei Bedarf ergänzen wir dies durch eine kurze Vor-Ort Begehung ihrer wichtigsten Räumlichkeiten. Während des Workshops lernen wir auf diese Weise Ihr Unternehmen kennen und verschaffen uns einen ersten Überblick darüber, welche Aspekte eines ISMS in welchen Ausprägungen bei Ihnen bereits umgesetzt bzw. gelebt werden. Immer wieder stellen wir bei unseren Neukunden fest, dass einige der geforderten Prozesse eines ISMS bereits intuitiv gelebt werden, diese jedoch in den seltensten Fällen durch dokumentierte Vorgaben definiert wurden. Dies erleichtert und reduziert den Aufwand des darauffolgenden ISMS-Aufbaus.
Die Ergebnisse der Ist-Analyse werden wir für Sie in einem Bericht festhalten. Dieser zeigt die Lücken zwischen dem aktuellen Ist-Stand und der geforderten Umsetzung auf und wird als Grundlage für den ISMS-Aufbau genutzt.
Auf Wunsch können wir mit Ihnen bereits während der Ist-Analyse den geeigneten Geltungsbereich für Ihr ISMS erarbeiten. Dies kann ein „full scope" sein, welcher Ihr gesamtes Unternehmen umfasst oder auch ein Teilbereich, den wir individuell für Ihr Unternehmen definieren.

Daten und Fakten

- 87 Prozent aller Unternehmen, die von einer Cyber attacke betroffen waren, hatten in der Folge der Attacke eine Betriebsstörung oder einen Ausfall.
- 53 Prozent befragter Unternehmen verfügten 2018 über kein ISMS.

Quelle: BSI 2019: Cyber-Sicherheits-Umfrage 2018

2.2. Managementstruktur etablieren

Für den Aufbau eines ISMS und auch für jedes andere Managementsystem müssen die Rahmenbedingungen und die Grundstruktur definiert werden, anhand derer das Managementsystem etabliert und mit Leben gefüllt wird. Einer der wichtigsten Schritte in diesem frühen Stadium ist die Zuweisung von Verantwortlichkeiten. Diese hängt stark von den Strukturen Ihres Unternehmens und auch dem festgelegten Geltungsbereich des ISMS ab. Je umfangreicher der Geltungsbereich und je größer Ihr Unternehmen ist, desto feingranularer wird auch die Rollenzuweisung innerhalb des ISMS benötigt

Wir werden gemeinsam mit Ihnen festlegen, welche Aufgaben und Verantwortlichkeiten welchen Rollen zugewiesen werden müssen bzw. können. Dabei berücksichtigen wir Ihre aktuelle Personalsituation, da die Übernahme der Aufgaben und Verantwortlichkeiten Zeit und Fachwissen benötigt, die ggf. nicht immer „on top" durch Mitarbeiter wahrgenommen werden können.

Mehr im Internet unter
www.enbw.com/kritis

Rollen, die in Ihrem ISMS unbedingt zu besetzen sind:

- Informationssicherheitsbeauftragte(r)
- RisikomanagerIn
- NotfallmanagerIn
- IncidentmanagerIn

Je nach Größe des Geltungsbereichs und Ihres Unternehmens können diese Rollen auf wenigen Mitarbeitern gebündelt werden.
Kleinere Unternehmen besetzen meist die Rolle des ISB und weisen diesem auch die Verantwortung als Risikomanager, Notfallmanager und Incidentmanager zu. Darüber hinaus werden bereits bestehende Rollen einzelne Aufgaben aus dem ISMS übernehmen. Dies betrifft z. B. die Leitung bzw. Verantwortliche für folgende Bereiche:

- IT-Abteilung
- Personalabteilung
- Qualitätsmanagement
- Datenschutz
- Einkauf & Beschaffung

Nach der Festlegung der Rollen und Verantwortlichkeiten im ISMS wird die Dokumentenlenkung definiert.

Diese ist aus vielerlei Gründen für jedes ISMS wichtig. Der Hauptgrund für die frühe Umsetzung ist jedoch die Zeitersparnis. Während dem ISMS-Aufbau werden Richtlinien und andere Vorgabedokumente erstellt und im späteren Verlauf Arbeitsanweisungen und Vorlagen für den ISMS-Betrieb vorbereitet. All diese müssen entsprechend ihrer Inhalte klassifiziert und in einer einheitlichen Struktur erstellt werden. Die Vorgabe dazu liefert die Dokumentenlenkung und erspart Ihnen (und uns) das spätere Anpassen der bereits erstellten Dokumente.

Wir empfehlen, einen weiteren wichtigen Aspekt Ihres ISMS bereits während dieser frühen Phase aufzubauen:

- Risikomanagement

Sobald die Vorgaben des Risikomanagements durch das Top Management freigegeben sind, können bereits erste Risikoerfassungen eingeleitet werden. Je nach Verfügbarkeit Ihrer Mitarbeiter (zugewiesene Risikoverantwortliche) können wir erste Erfassungen durchführen. Urlaubszeiten und Nicht-Verfügbarkeiten wichtiger Ansprechpartner können so in den nächsten Phasen des ISMS-Aufbaus sinnvoll genutzt werden.

2.3. Vorgaben und Richtlinien definieren

Durch den Aufbau der Managementstruktur können wir nun zielgerichtet und mit den jeweiligen Verantwortlichen gemeinsam die umzusetzenden Vorgaben für Ihr ISMS entwickeln. Hierbei stellen wir sicher, dass diese den Anforderungen der, für Ihr ISMS gewählten, Normen und Standards genügen.
In einem ersten Schritt wird die Leitlinie für Ihr ISMS erstellt, welche durch Ihr Top Management freigegeben wird. In dieser werden zum Beispiel die Ziele des ISMS vorgegeben und die Unterstützung durch das Top Management schriftlich bestätigt.
Daraufhin werden für folgende Kernthemen Richtlinien entwickelt:

- Risikomanagement
- Assetmanagement
- Incidentmanagement
- Notfallmanagement
- Betriebssicherheit

Auf deren Grundlage folgen weitere Richtlinien sowie das Erstellen von Vorlagen und Verfahrensanweisungen, welche im Regelbetrieb Ihres ISMS benötigt werden. Je nach Fortschritt der Richtlinienentwicklung können wir bereits die ersten Prozessabläufe des ISMS gemeinsam initiieren.

2.4. Prozesse etablieren

Für den Nachweis der Wirksamkeit eines ISMS muss dieses in einen Regelbetrieb übergehen, welcher durch die erstellten Richtlinien und Verfahrensanweisungen beschrieben wird. Zum Nachweis dienen auch die erstellten Vorlagen, anhand derer die durchzuführenden Tätigkeiten dokumentiert werden. Diese umfassen zum Beispiel:

- Risikoerfassungen
- KVP & Managementbericht
- Daten-Recovery testen
- Standortbegehungen
- Notfälle üben

Während dieser Phase der Inbetriebnahme Ihres ISMS unterstützen wir Ihre Mitarbeiter tatkräftig und mit Augenmaß. Eines unserer Ziele ist es, Ihre Mitarbeiter so anzuleiten, dass diese die Tätigkeiten in Zukunft ohne unsere Unterstützung durchführen können.
Sobald die Inbetriebnahme Ihres ISMS einen bestimmten Umsetzungsgrad erreicht hat, kann das interne Audit durchgeführt werden. Darauf aufbauend folgt der Abschluss des ersten PDCA-Zyklus. Es werden anhand der Feststellungen des internen Audits Maßnahmen identifiziert und deren Umsetzung eingeleitet. Die Ergebnisse des ersten PDCA-Zyklus werden im Managementbericht dokumentiert, welcher durch Ihr Top Management freigegeben wird.

3. Unterstützung des ISMS-Betriebs

Ein ISMS einfach mal so „nebenbei“ zu betreiben, ist kaum möglich. Hierzu benötigt es kommunikativ starke und fachlich erfahrene Verantwortliche für die Kernelemente sowie ein Top Management, welches diesen Umstand versteht und die notwendigen Ressourcen zur Verfügung stellt.

Der Betrieb eines ISMS umfasst verschiedenste Aufgaben, die regelmäßig durchgeführt werden müssen. Die bedeutendsten und zeitintensivsten Aufgaben sind hierbei:

- Jährlich zu aktualisierende Risikobewertungen
- Schulungs- und Awareness-Kampagnen
- Regelmäßige Notfallübungen
- Jährliche Reviews der Richtlinien und Vorgabedokumente
- Jährlich durchzuführende Audits
- Kennzahlenerfassung und Managementberichte
- Steuerung und Kontrolle der Maßnahmenbehandlungen
- Notfallübungen durchführen

Diese und die vielen anderen Aufgaben lassen sich verschiedenen Rollen (z. B. ISB, Notfallmanager, Risikomanager) zuordnen. Sollten Sie oder Ihre Mitarbeiter Unterstützung bei einigen der im ISMS-Betrieb anfallenden Aufgaben benötigen, helfen wir Ihnen gerne.

Nachfolgend stellen wir Ihnen eine Auswahl unserer Unterstützungsleistungen vor, welche von unseren Kunden am häufigsten in Anspruch genommen werden.

3.1. Informationssicherheitsbeauftragter

Die Aufgaben eines ISB sind vielfältig und ergeben sich aus dem Informationssicherheitsmanagementsystem, welches von Ihnen betrieben wird. Für folgende Kernaufgaben ist Ihr ISB verantwortlich:

- Risiken identifizieren, behandeln und verwalten
- Für eine angemessene Schulung und Awareness der Mitarbeiter sorgen
- Die Einhaltung der Informationssicherheitsvorgaben sicherstellen
- Dienstleister und Lieferanten in die Informationssicherheit einbinden
- Regelmäßige Überprüfungen des ISMS vornehmen

Außerdem muss Ihr ISB ggf. das ISMS oder Teile Ihres ISMS erst implementieren, bevor es in den aktiven Betrieb übergehen kann. Einige dieser Aufgaben kann der ISB an andere Personen bzw. Rollen wie zum Beispiel den Notfallmanager oder Risikomanager übergeben, sofern diese in Ihrem Unternehmen besetzt sind. Viele Aufgaben müssen jedoch durch den ISB durchgeführt werden.

Einen geeigneten Informationssicherheitsbeauftragten für das eigene Unternehmen zu finden, stellt sich manchmal als schwierig dar. Entweder mangelt es an Bewerbungen für die Stelle oder Sie haben vor, einen Ihrer eigenen Mitarbeiter als ISB auszubilden. Sollten Sie die Rolle des ISB nicht unmittelbar besetzen können, unterstützen wir Sie gerne beim Aufbau eines Mitarbeiters durch unsere Berater sowie bei der Übernahme der ISB-Rolle durch unsere Interims-ISBs, bis Sie einen geeigneten Kandidaten gefunden oder aufgebaut haben.Darüber hinaus stehen unsere Berater gerne für Sie zur Verfügung, sollten sich während dem ISMS-Alltag Fragestellungen ergeben, bei denen wir Sie unterstützen können.

3.2. Interne Audits

Interne Audits müssen bei einem zertifizierten Unternehmen jährlich durchgeführt werden und gelten als Nachweis für die Funktionsfähigkeit des ISMS. Die Berichte der internen Audits werden bei Zertifizierungsaudits durch die Auditoren überprüft.

Ein internes Audit läuft nach demselben Prinzip wie ein Zertifizierungsaudit ab. Im Vorfeld wird ein Auditplan erstellt und mit dem ISB abgestimmt. Je nach Größe Ihres Unternehmens läuft dieses üblicherweise zwischen zwei bis sechs Audittage. Bei internen Audits können auch nur Teile des ISMS auditiert werden, solange sichergestellt ist, dass alle Aspekte des ISMS in einem 3-Jahreszyklus geprüft wurden.

Bestandteil jedes Audits, somit auch der internen Audits, ist das Erstellen eines Berichts sowie einer Liste der identifizierten Feststellungen. Diese bilden die Grundlage für Verbesserungen des ISMS und werden in einen Maßnahmen- und Behandlungsplan des Unternehmens übernommen.

Wir unterstützen oder übernehmen für Sie gerne die Planung und Durchführung der internen Audits sowie die spätere Nachbereitung und stellen sicher, dass diese in Inhalt und Ergebnis den Ansprüchen externer Auditoren genügen.

3.3. Lieferantenaudits

Lieferantenaudits dienen dem Zweck, Lieferanten oder Dienstleister bzgl. der Einhaltung der Verträge, insbesondere in Bezug auf die Einhaltung der vertraglich geforderten Informationssicherheitsstandards zu überprüfen.

Sofern Dienstleister oder Lieferanten über ein gültiges und geeignetes Zertifikat verfügen, reicht dieser Nachweis meist aus. Gibt es keine gültige Zertifizierung, so kann ein Lieferantenaudit durchgeführt werden. In einigen Fällen fordern die Auditoren Ihres ISMS, dass Sie Lieferantenaudits bei Ihren, als kritisch bzw. besonders relevant eingestuften, Lieferanten oder Dienstleistern durchführen. Hierbei übernehmen Sie die Rolle des Auditors.

Wie auch bei internen Audits können wir Sie bei der Planung und Durchführung der Lieferantenaudits unterstützen.

3.4. Awareness-Kampagnen

Während redundant ausgelegte Systeme, verschlüsselte Kommunikation und regelmäßige Datensicherungen die technische Seite der Informationssicherheit adressieren, sind es auch die organisatorischen Aspekte, die Sie nicht vernachlässigen dürfen. Hierzu zählt auch, dass Ihre Mitarbeiter wissen, wie man reagieren soll, wenn ungewöhnliche bzw. unerwartete Reaktionen der Systeme erfolgen oder simple Dinge wie ein offenstehendes Fenster im Erdgeschoss bemerkt werden.

Die Sensibilisierung und Awareness der Mitarbeiter hat einen hohen Stellenwert in der Informationssicherheit, da es häufig Ihre Mitarbeiter sind, die in Entstehung befindliche Gefahren oder ungewöhnliches (System-) Verhalten melden können - oder eben nicht. Um das Interesse nachhaltig zu gestalten, sollte eine gute Awareness-Kampagne nicht nur den geschäftlichen Arbeitsalltag Ihrer Mitarbeiter adressieren. Auch für das private Umfeld Ihrer Mitarbeiter sollte eine Awareness-Kampagne wichtige Hinweise und Empfehlungen bieten, um sich vor potenziellen Gefahren zu schützen.

Wir können Sie bei der Ausarbeitung von Awareness-Kampagnen unterstützen, welche Ihre Mitarbeiter darin sensibilisieren, auf ungewöhnliche bzw. gefährliche Situationen richtig zu reagieren. Dies umfasst auch Newsletter oder Meldungen im Intranet, welche auf aktuelle Gefährdungen hinweisen.

3.5. Notfallübungen

Der Aufbau eines unternehmensumfassenden Notfallmanagements ist eine komplexe Aufgabe. Insbesondere für die Ausarbeitung von geeigneten Notfallplänen müssen verschiedenste Rollen in Ihrem Unternehmen involviert werden.

Damit aus den erstellten Notfallplänen keine rein theoretischen Abfolgen und Handlungsanweisungen entstehen, müssen diese anhand von Notfallübungen hin und wieder aktiv geübt werden. Dies ermöglicht zu überprüfen, ob die am Schreibtisch entwickelten Pläne der Realität Stand halten können.

Die Planung solcher Notfallübungen ist aufwändig, da viele Bereiche in Ihrem Unternehmen entweder direkt oder indirekt durch die Notfallübung beeinflusst werden. Dabei muss darauf geachtet werden, dass der Regelbetrieb nicht oder nur marginal gestört wird. Bei Trockenübungen am Schreibtisch ist dies meist einfacher sicherzustellen als bei einer, unter realistischen Bedingungen angesetzten, Übung.

Wir unterstützen Sie bei der Planung und Übung Ihrer Notfallpläne und helfen, angepasste Drehbücher für die Notfallsituationen zu erstellen. Selbstverständlich unterstützen wie Sie auch, anhand der Erkenntnisse aus den Notfallübungen Verbesserungen für Ihre Notfallpläne abzuleiten.

3.6. Risikoanalysen und Korrekturmaßnahmen

Risikoanalysen sind aufwändig und müssen zumindest jährlich oder nach externen Ereignissen erneut aktualisiert werden. Die Risikoverantwortlichen müssen dabei die aktuelle Situation Ihres Unternehmens kennen, um Gefährdungen und deren potenzielle Auswirkungen richtig einschätzen zu können. Dies erfordert sowohl das technische Verständnis bereits vorhandener Schutzmaßnahmen als auch die richtige Einschätzung der Eintrittswahrscheinlichkeit und der potenziellen Schadenshöhe von Gefährdungen.

Während dem Aufbau Ihres ISMS werden bereits erste Risikoanalysen durchgeführt und einigen Risikoverantwortlichen fehlt ggf. die Routine, um die Analysen mit vertretbarem Aufwand durchzuführen. Wir unterstützen Sie gerne bei der Durchführung der ersten Risikoanalysen oder helfen denjenigen Mitarbeitern, welche die Rolle des Risikoverantwortlichen neu übernommen haben. Unser Fokus liegt hierbei nicht nur auf der fachlich korrekten Durchführung der Analysen. Wir binden Ihre Risikoverantwortliche aktiv mit ein und helfen, dass diese die zukünftigen Analysen auch ohne Unterstützung durchführen können.

Auf Grundlage der Risikoanalysen müssen geeignete Maßnahmen identifiziert werden, welche die Eintrittswahrscheinlichkeit oder die Schadenshöhe von potenziellen Gefährdungen auf ein akzeptables Maß reduzieren sollen.
Bei der Auswahl und Planung geeigneter Korrekturmaßnahmen zur Risikobehandlung können wir Sie ebenfalls unterstützen. Hierbei ist es uns besonders wichtig, dass der (Kosten-)Aufwand einer Maßnahme immer in einem akzeptablen Verhältnis zum zugrundeliegenden Risiko und dem erzielten Effekt der Risikoreduktion steht.

Unterstützende Dienstleistungen im ISMS-Umfeld

› EnBW FKS CyberRating

Ad-Hoc-Bewertung von IT-Sicherheitsvorkehrungen eines Unternehmens durch frei verfügbare Informationen sowie anschließende Erstellung von Lösungsansätzen auf Basis von Expert*innen-Know-how von EnBW.

› EnBW FKS Penetrationstest

Simulierter Angriff auf IT-Systeme, um mittels Penetrationstest Schwachstellen und Sicherheitslücken zu identifizieren und Handlungsbedarf zu verdeutlichen, u.a. bei Applikationen, Server, Clients, Mobile Devices, Netzwerkkomponenten und ganzen Systemen.

› Cyber Defense Center

Mit dem Cyber Defense Center des EnBW Full Kritis Service steht Ihnen ein umfassendes und facettenreiches Lösungs-Portfolio für die Absicherung Ihrer IT- und OT-Systeme, Netze und Geschäftsabläufe zur Verfügung. Hier werden perfekt aufeinander abgestimmte Komponenten dynamisch zur wirksamen und effizienten Erfüllung der individuellen Anforderungen orchestriert. Durch die Erschließung von Synergien profitieren Sie von einem spürbaren Mehrwert und Praxisnutzen.

› IT-Sicherheitsberatung

Regelungen und Vorgaben für den Datenschutz und die Informationssicherheit haben Sie etabliert und diese erfordern zur Wirksamkeit eine solide Umsetzung der IT-Sicherheit. Wir bieten Ihnen unsere IT-Sicherheitsexperten für die Umsetzung von Sicherheitskonzepten, einer Netzsegmentierung, Fernzugänge sowie weiterer Themen für die Stärkung Ihrer IT-Sicherheit an und können Sie auch bei der Umsetzung von Bausteinen aus dem IT-Grundschutz-Kompendium unterstützen. Feststellungen aus Penetrationstests, unserem EnBW FKS CyberRating oder weiterer, technischer Prüfungen erfordern das Lösen der identifizierten Probleme. Auch hier können Sie auf unsere Experten zurückgreifen.

› Datenschutz

Wir unterstützen Sie beim Aufbau und Betrieb Ihres Datenschutzmanagementsystems zur Einhaltung der EU-DSGVO und unterstützen Sie mit einem unseren externen Datenschutzbeauftragten zur Erfüllung Ihrer Benennungspflicht eines DSB. Mit unserem EU-DSGVO-Check bewerten wir, wie Ihre Organisation die EU-DSGVO lebt und die technischen und organisatorischen Maßnahmen (TOM) umgesetzt hat. Sollten wir Abweichungen feststellen, so helfen Ihnen unsere Experten auch gerne bei der Maßnahmenbehandlung.

4. Prüfung und Zertifizierung eines ISMS

Manchmal wollen es Behörden, Kunden oder das Top Management ganz genau wissen und fordern einen unabhängigen Nachweis, dass Ihr ISMS dem Stand der Technik entspricht.

Der kontinuierliche Verbesserungsprozess ist für die Wirksamkeit und Funktionsfähigkeit des ISMS ein bedeutender Faktor. Die Überprüfung und Überwachung des ISMS ist somit eine Kernaufgabe, um hieraus Input für den kontinuierlichen Verbesserungsprozess zu erhalten und umfasst unter anderem:

- Kennzahlen erfassen
- Regelmäßige Jour Fixe des ISMS-Teams
- Managementbericht
- Interne Audits

Um gegenüber interessierten Dritten (z. B. Kunden, Behörden) und auch gegenüber Ihrem Top Management die Wirksamkeit und Funktionsfähigkeit eines ISMS glaubhaft nachweisen zu können, eignen sich Überprüfungen durch unabhängige Stellen. Sofern ein Zertifikat (ISO 27001, IT-Grundschutz, ...) angestrebt bzw. aufrechterhalten werden soll, sind diese Überprüfungen Pflicht. Dasselbe gilt für Prüfungen und Zertifizierungen, wenn diese aufgrund einer gesetzlichen Anforderung, beispielsweise dem IT-Sicherheitsgesetz (§ 8a), dem Energiewirtschaftsgesetz (§ 11) oder dem Messstellenbetriebsgesetz (§ 25) gefordert werden.

Wir können bei der Auswahl einer für Sie geeigneten Prüf- und Zertifizierungsstelle helfen und Sie sowohl bei der Auditvorbereitung als auch durch eine Auditbegleitung unterstützen. In den meisten Audits werden Auditoren Abweichungen oder Empfehlungen feststellen. Für eine Behandlung dieser Feststellungen stehen wir Ihnen gerne mit unserer Expertise zur Verfügung.

4.1. Audit-Vorbereitung und -Begleitung

Ein Audit durch externe Prüfer muss gut vorbereitet werden. Dies umfasst:

- das Briefing der geplanten Interviewpartner
- die Vorbereitung der Räume
- die Planung ggf. notwendiger Standortbegehungen
- die schnelle Bereitstellung geforderter Dokumente während der Auditsessions
- die Bereitstellung der notwendigen Interviewpartner (Session-Planung)

Ein reibungsloser Auditablauf, gut vorbereitete Interviewpartner und zeitnah zur Verfügung gestellte Dokumente können einen positiven Einfluss auf das Gesamterscheinungsbild Ihres ISMS sowie den zugehörigen Prozessabläufen haben. Unsicherheiten der Interviewpartner sollten möglichst vermieden werden. Hierbei stellen gegenläufige Aussagen in unterschiedlichen, teils parallel ablaufenden, Auditsessions eine besondere Gefahr dar. Darüber hinaus gibt es noch weitere Dinge, welche vorbereitet werden können, um ein Audit reibungslos und zur Zufriedenheit der Auditoren ablaufen lassen.

Unsere auditerfahrenen Berater können Sie bei der Auditvorbereitung unterstützen und die Interviewpartner in den einzelnen Auditsessions begleiten. Hierbei gelten jedoch einige Spielregeln für unsere Berater, denn diese können und dürfen nicht die Aufgabe des Interviewpartners übernehmen:

- Berater sollten möglichst nicht oder nur bei offenen Diskussionen aktiv teilnehmen
- Berater sind nur ein Backup, falls Unsicherheiten der Interviewpartner auftreten
- Fachliche Unterstützung bei Diskussionen um Norm-Auslegungen

Durch die Teilnahme bei Auditsessions können wir noch während des Audits helfen, durch die Auditoren geforderte Nachweise oder Informationen zu liefern, die ad hoc in einer Session nicht zugreifbar waren. Die Auditbegleitung bietet außerdem Vorteile für die spätere Behebung von Feststellungen. Unsere Beratung zur Maßnahmenbehandlung beruht in diesem Fall nicht nur auf dem Beschreibungstext einer

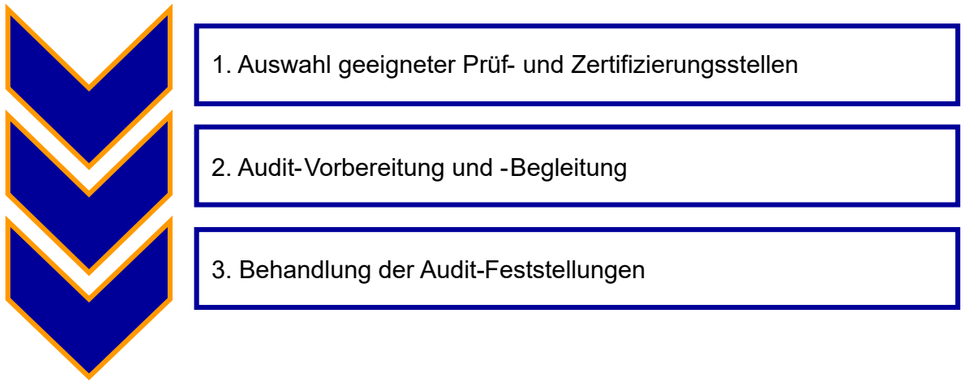
Feststellung, sondern auch auf den Erkenntnissen, Diskussionen und Argumentationsketten aus dem Audit, welche zu einer Feststellung führten. Dies ermöglicht eine effizientere und meist schnellere Identifizierung geeigneter Maßnahmen.

4.2. Behandlung der Audit-Feststellungen

In Audits kommt es selten vor, dass durch die Auditoren keine Feststellungen identifiziert werden. Diese reichen von Empfehlungen bzw. Verbesserungspotentialen über geringfügige Abweichungen bis hin zu schwerwiegenden und sogar zertifikatsverhindernden Abweichungen.

Spätestens mit der Übergabe des Auditberichts, meist jedoch mit Ende des Audits, beginnen Fristen für die Behandlung der identifizierten Feststellungen.

Bei aktiven Zertifizierungen oder bei Nachweispflichten unterstützen wir Sie dabei, einen geeigneten Maßnahmenplan zur Behandlung der identifizierten Feststellungen zu erstellen und diesen bei der Prüf- bzw. Zertifizierungsstelle oder dem BSI einzureichen. Durch unser fachlich breit aufgestelltes Team können wir Sie sowohl bei der Detailplanung der Behandlung einzelner Feststellungen als auch aktiv bei der Umsetzung der Korrekturmaßnahmen unterstützen.



5. Weiterführende Informationen

Wir stellen Ihnen gerne weiterführende Informationen auf Anfrage zur Verfügung:

- Beispielprojektplan mit Meilensteinen
- Übersicht zu erstellender Richtlinien
- Auszug aus der Richtlinie zur Dokumentenlenkung

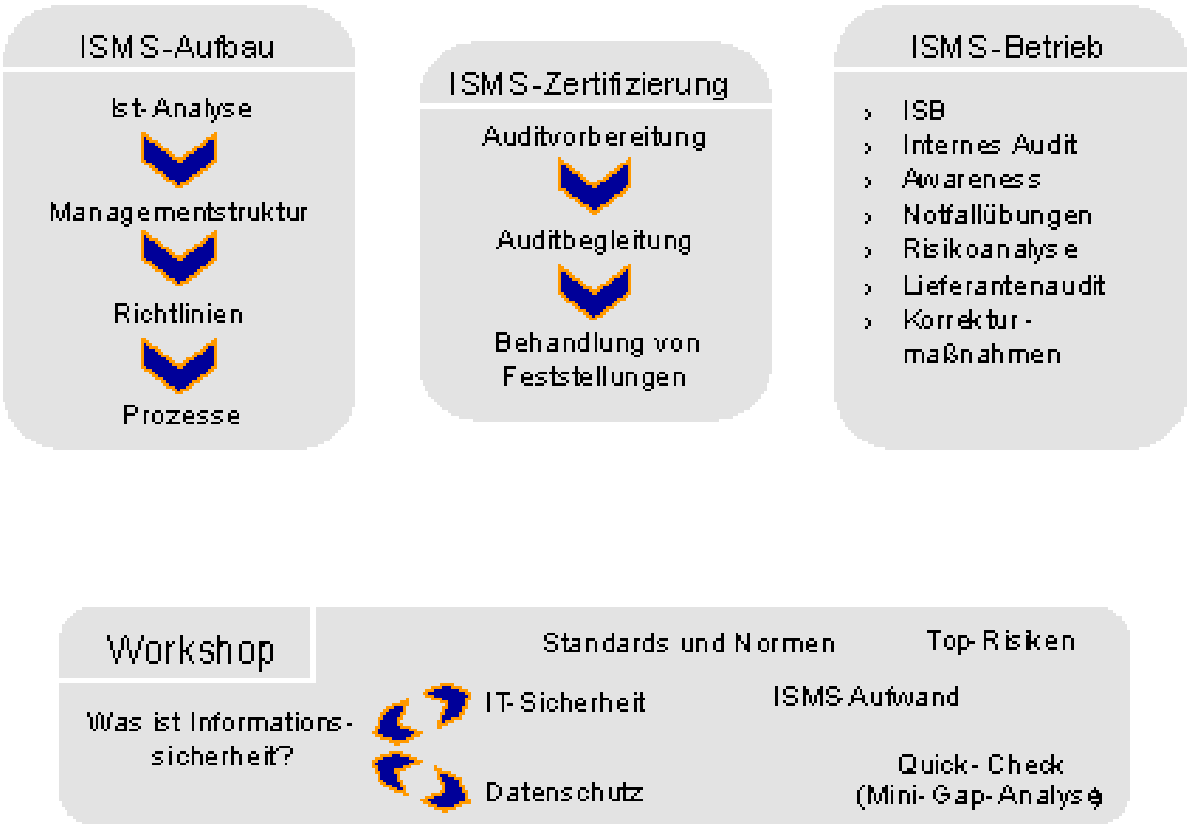
6. Ihr Kontakt zu uns

Interessiert an mehr? Weiterführende und aktuelle Informationen rund um den EnBW Full Kritis Service und unser Leistungsangebot erhalten Sie jederzeit über unsere Homepage, die Produktflyer sowie durch persönliche Gespräche mit uns.

Unsere aktuelle Homepage mit vielen interessanten Informationen rund um die Themen Informationssicherheit, Datenschutz, IT- und OT-Sicherheit sowie zu unserem Cyber Sicherheits Center erreichen Sie über www.enbw.com/kritis oder den untenstehenden QR-Code.

Nehmen Sie gerne direkt Kontakt zu uns auf.
Wir stehen Ihnen gerne beratend zur Seite!

0800 0 KRITIS
kritis@enbw.com
www.enbw.com/kritis



EnBW Energie Baden-Württemberg AG
Full Kritis Service
Durlacher Allee 93
76131 Karlsruhe
Telefon 0800 0 KRITIS
www.enbw.com/kritis
kritis@enbw.com