NESEC

Gesellschaft für angewandte Netzwerksicherheit mbH

NESEC LEISTUNGEN

Externer ISB
Ganzheitliche Informations-sicherheit

Externer Informationssicherheitsbeauftragter / Einführung eines ISMS

„Die Bedrohung im Cyber-Raum ist so hoch wie nie!“

Das sagen nicht wir, das steht im Lagebericht der IT-Sicherheit in Deutschland 2022 des Bundesamt für Sicherheit in der Informationstechnik. Egal ob Sie ihre eigenen Server betreiben oder Systeme und Daten in der Cloud halten, gibt es ernstzunehmende Gefahren wie Ransomware und Phishing aber auch klassische Hacking-Angriffe.

Mögliche Risiken

Tritt ein Vorfall ein, können erhebliche Schäden entstehen.

- Ausfall wichtiger IT-Systeme
  Ein Ausfall kritischer IT-Systeme kann Ihre Produktion oder Ihre Lieferfähigkeit beeinträchtigen. Wenn Sie Termine nicht einhalten können, können Imageschäden, Vertragstrafen oder Kundenverlust die Folge sein. Zudem drohen erhebliche Kosten durch die Wiederherstellung z.B. nach einer Verschlüsselung der Daten.

- Verstoß gegen die DSGVO
  Ein Verstoß gegen die Datenschutzgrundverordnung, beispielsweise beim Verlust personenbezogener Daten kann zu Bußgeldern und Sanktionen führen. Außerdem können Haftungs- und Schadenersatzansprüche entstehen. Zusätzlich besteht eine Meldepflicht sowie gegebenenfalls eine Pflicht zur Information der betroffenen Personen.

- Verlust vertraulicher Daten
  Neben personenbezogenen Daten können auch vertrauliche Daten aus Forschung und Entwicklung gestohlen und sogar im Darknet weiterverkauft oder durch Industriespionage zu Mitbewerbern gelangen.

Neben den Schäden für das Unternehmen steht sogar die Gefahr einer Organhaftung im Raum, wenn Informationssicherheit in den Entscheidungen der Geschäftsleitung oder im Vorstand nicht angemessen berücksichtigt wurde.

Das ISMS als Lösung

Ein Informationssicherheitsmanagementsystem (ISMS) hat die Aufgabe, die Belange der Informationssicherheit angemessen und risikoorientiert in die Prozesse und Verfahren des Unternehmens einzubringen. Innerhalb des ISMS werden Regeln, Verfahren, Maßnahmen und Methoden festgelegt, mit denen sich die Informationssicherheit steuern und kontrollieren lässt. Risken werden so identifiziert und beherrschbar.

In einem ISMS werden üblicherweise in einem Top-Down-Ansatz, ausgehend von der Leitlinie, in der die Informationssicherheitspolitik definiert wird, Sicherheitsrichtlinien entwickelt und von der Geschäftsleitung in Kraft gesetzt. Die Umsetzung erfolgt durch den IT-Betrieb, wobei eine Prüfung der umgesetzten Maßnahmen gegen die Richtlinien erfolgen kann.

Ein Informationssicherheitsbeauftragter (ISB) übernimmt die Erstellung der Richtlinien und die Prüfung der Umsetzung und berät die Geschäftsleitung und den IT-Betrieb in allen Belangen der Informationssicherheit. Zusätzlich kann der ISB weitere Aufgaben im Business Continuity Management (BCM) übernehmen, beispielsweise Notfallpläne entwerfen und Übungen durchführen.

Zusammen mit der Geschäftsleitung entscheidet der ISB, welcher Standard für die Implementierung eines ISMS für das Unternehmen am besten geeignet ist. Für kleinere Unternehmen bietet sich der Standard VdS 10000 an, größere Unternehmen, die eine international anerkannte Zertifizierung anstreben, entscheiden sich oft für ein ISMS nach ISO 27001.

Zusätzlich zum ISMS können weitere Informationssicherheitsstandards und Sicherheitsanforderungen hinzukommen, z.B. PCI-DSS, TISAX oder KRITIS, die ebenfalls vom ISB betreut werden.

Diese Aufgaben hat der ISB

Der Informationssicherheitsbeauftragte soll gewährleisten, dass die Infrastruktur, die IT-Systeme und die Daten des Unternehmens jederzeit angemessen geschützt sind und das angestrebte Niveau in der Informationssicherheit erreicht und aufrechterhalten wird.

Dazu gehören insbesondere folgende Aufgaben:

- Beratung der Geschäftsleitung, der IT und der Nutzer in allen Belangen der Informationssicherheit
- Festlegung der Sicherheitsziele und der Sicherheitsstrategie zusammen mit der Geschäftsleitung
- Implementierung des Informationssicherheitsmanagementsystems
- Erstellung von Richtlinien und Prozessbeschreibungen in für das ISMS relevanten Themen
- Ermittlung von Bedrohungen und Risiken
- Prüfung vorhandener Sicherheitsmaßnahmen und ggf. Empfehlungen zur Optimierung
- Sensibilisierung von Mitarbeitern hinsichtlich Informationssicherheit

Weiterhin führt der ISB interne Audits und interne Sicherheitsprüfungen im Rahmen des ISMS durch. In Absprache mit der Geschäftsleitung kann der ISB außerdem externe Prüfungen, z.B. Penetrationstests beauftragen. Der ISB dient außerdem als Ansprechpartner für alle Belange der Informationssicherheit, sowohl für externe und interne interessierte Parteien.

Diese Anforderungen muss der ISB erfüllen

Selbstverständlich muss der Informationssicherheitsbeauftragte seine Materie kennen. Das gilt natürlich für die relevanten Normen und Standards sowie deren Anforderungen, die zur Umsetzung und einer späteren Zertifizierung erfüllt werden müssen. Das gilt aber natürlich auch für die technische Informationssicherheit und die verschiedenen IT-Security Technologien, die der ISB kennen und verstehen muss.

Der ISB sollte außerdem über gute Kommunikationsfähigkeiten verfügen, da das zu seinen Aufgaben gehört, die Informationssicherheit sowohl an Mitarbeiter als auch die Geschäftsleitung zu „verkaufen". Der ISB ist auch für regelmäßige Berichte zur Informationssicherheit an die Geschäftsleitung verantwortlich.

Das notwendige Wissen lässt sich nicht durch ein oder zwei kurze Lehrgänge gewinnen. Gleichzeitig bleibt die Nachfrage nach IT-Sicherheit hoch.

Die Rolle des externen Informationssicherheitsbeauftragten

In vielen Unternehmen gibt es keinen Informationssicherheitsbeauftragten. Und anders als im Datenschutz gibt es natürlich auch keine gesetzliche Vorschrift einen ISB zu bestellen. Gerade in kleinen Unternehmen werden einzelne Aufgaben des ISB vom Datenschutzbeauftragten (DBS) übernommen, da sich beide Aufgaben beispielsweise bei den technischen und organisatorischen Maßnahmen (TOM) überschneiden und ergänzen. In anderen Unternehmen fällt die Aufgabe dem IT-Leiter zu, der quasi nebenbei die Belange der Informationssicherheit mitbetreuen muss.

In großen Unternehmen existiert ein komplettes Informationssicherheits-Team, das den ISB unterstützt, interne Sicherheitsprüfungen durchführt und generell die Belange der IT-Sicherheit vertritt.

Für viele mittelständische Unternehmen ist jedoch beides keine geeignete Lösung. Für einen Vollzeit ISB der sich ausschließlich um die Informationssicherheit kümmern kann, sind diese Unternehmen zu klein. Die Informationssicherheit jedoch komplett der IT zu überlassen, die aufgrund von Fachkräftemangel, Cloud-Migration und vielen neuen technischen Herausforderungen oft bereits komplett ausgelastet ist, ist jedoch auch keine Lösung.

Hier kommt ein externer Informationssicherheitsbeauftragter ins Spiel.

Wir übernehmen Ihren externen ISB

Wenn Sie uns als Ihren externen Informationssicherheitsbeauftragten bestellen, erhalten Sie ein umfangreiches Leistungspaket:

✔	Sicherheitsleitlinie	Die Sicherheitsleitlinie beschreibt die Sicherheitspolitik und die Sicherheitsziele der Organisation.
✔	Richtlinie IT-Nutzung	Die Richtlinie zur IT-Nutzung legt fest, wie Ihre Mitarbeiter IT-Systeme und Anwendungen nutzen dürfen und welche Sicherheitsvorgaben dabei beachtet werden müssen.
✔	Richtlinie Mobilgeräte und Telearbeit	In der Richtlinie zu Mobilgeräten und Telearbeit werden Regeln zur Nutzung von Notebooks und Mobiltelefonen sowie Sicherheitsvorgaben zum mobilen Arbeiten festgelegt.
✔	Richtlinie Zutrittskontrolle	Die Richtlinie zur Zutrittskontrolle regelt den Schutz der Serverräume und sonstiger sensibler Bereiche im Unternehmen.
✔	Richtlinie Zugriffskontrolle	In der Richtline zur Zugriffskontrolle werden Authentifizierungsmaßnahmen und Berechtigungen festgelegt.
✔	Richtlinie Virenschutz	In der Richtline zum Virenschutz werden Sicherheitsanforderungen an den Schutz vor Schadsoftware und Ransomware festgehalten.
✔	Richtlinie Datensicherung	Die Richtlinie zur Datensicherung beschreibt die Anforderungen an Backup und Wiederherstellung von Daten.
✔	Richtlinie zur Verschlüsselung	Die Richtline zur Verschlüsselung enthält Vorgaben zu Verschlüsselungsverfahren und Algorithmen sowie zur sicheren Kommunikation.
✔	Richtlinie zum Umgang mit Sicherheitsvorfällen	In der Richtlinie zum Umgang mit Sicherheitsvorfällen wird die Meldekette bei Not- und Sicherheitsvorfällen sowie ggf. erforderliche forensische Verfahren definiert.
✔	Richtlinie Supply Chain Management	In der Richtlinie Supply Chain Management werden die Anforderungen an Lieferanten, Cloud-Provider und externe Dienstleister festgelegt.
✔	Business Continuity Konzept	Das Business Continuity Konzept enthält die Richtlinie zur Notfallvorsorge sowie die Wiederanlaufpläne.

Abhängig vom zu erreichenden Sicherheitsstandard VdS 10000, ISO 27001 oder TISAX erstellen wir selbstverständlich auch ein ISMS-Handbuch, die ISO 27001 SoA (Statement of Applicability), weitere notwendige Richtlinien und Konzepte, führen interne Audits durch und erstellen für Sie die Managementbewertung.

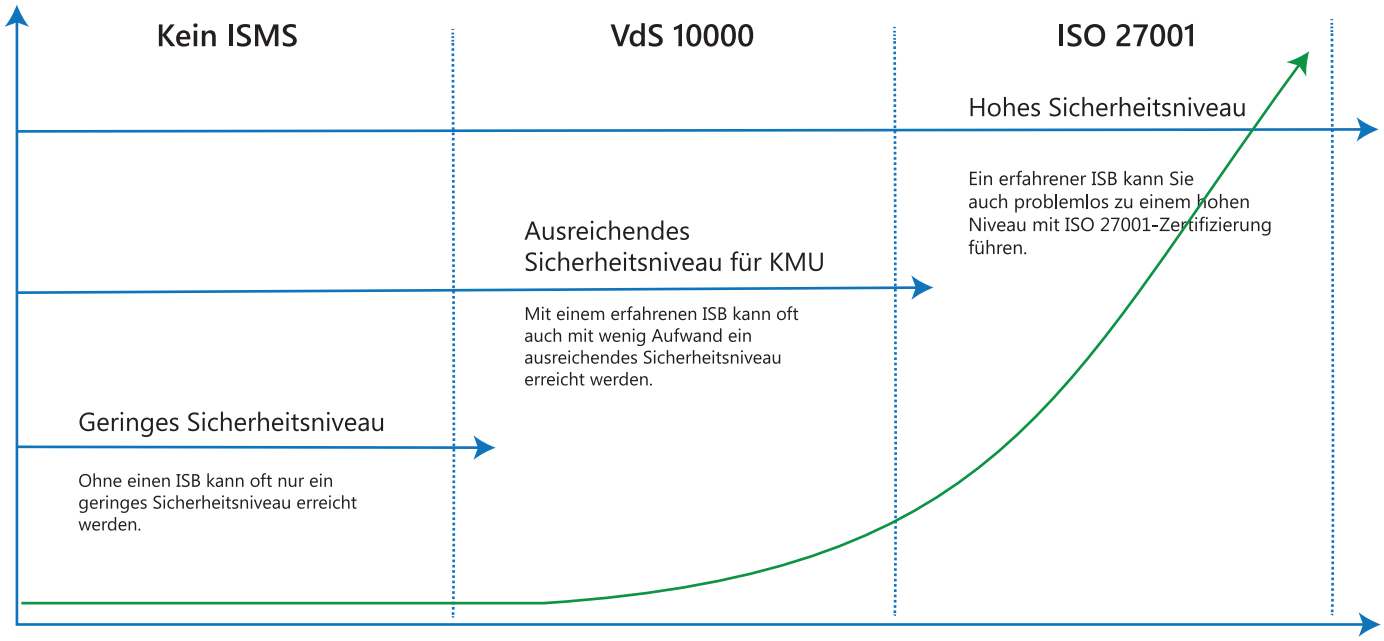
Einbindung in vorhandene Management-Systeme

Ein ISMS steht selten alleine, sondern wird üblicherweise in andere, oft bereits vorhandenen Managementsystemen integriert. Ist Ihr Unternehmen beispielsweise bereits nach ISO 9001 oder einem anderen vergleichbaren ISO-Standard zertifiziert, bietet es sich an, ein integriertes QMS/ISMS zu schaffen, da sich die Anforderungen der Managementsysteme z.B. bzgl. Verbesserungsprogrammen oder interessierter Parteien überschneiden und Arbeiten nicht doppelt gemacht werden müssen.

Wir stimmen uns deshalb eng mit Ihrem Qualitätsbeauftragten oder den Verantwortlichen sonstiger vorhandener Managementsysteme ab und integrieren das ISMS in ihr vorhandenes System.

Unser ISMS wächst mit

Niemand zwingt Sie, mit dem größten und umfangreichsten Standard zu starten. In vielen Unternehmen ist das erste Ziel, die Informationssicherheit zu verbessern und auf ein stabiles Fundament zu stellen. Dieses Fundament sind die Sicherheitsrichtlinien, aus denen sich dann die technischen IT-Sicherheitsmaßnahmen ableiten.



Falls Sie überhaupt noch keine IT-Sicherheitsrichtlinien haben, können wir gemeinsam klein anfangen:

1. Existieren noch keine Regelungen, führen wir ein Informationssicherheitsmanagement nach VdS 10000 ein, einem leichtgewichtigen Standard, der jedoch gut erweiterbar ist. Sie können natürlich selbst entscheiden, ob Sie Ihr ISMS zertifizieren lassen möchten oder nicht.

2. Kommen externe Anforderungen hinzu, weil z.B. Ihre Kunden konkret eine ISO 27001 Zertifizierung fordern, erweitern wir das VdS 10000 ISMS zu einem vollwertigen ISO 27001 ISMS mit zusätzlichen Richtlinien und Maßnahmen. Die bisher erstellten Richtlinien sind dabei nicht verloren, sondern können vollständig übernommen werden. Selbstverständlich begleiten wir Sie auch durch die ISO 27001 Zertifizierung.

3. Falls notwendig oder gewünscht, können wir Sie auf weitere branchenspezifische Audits, z.B. TISAX für Automotive oder eine Prüfung nach BSIG § 8a für KRITIS-Unternehmen vorbereiten.

Übrigens

Mit einem Cyber-Sicherheits-Check der ISACA oder einem CyberRisikoCheck nach DIN SPEC 27076 können wir vor einer eventuellen Beauftragung den Stand Ihrer Informationssicherheit feststellen. Der Cyber-Sicherheits-Check ist als risikoorientierte Prüfung gedacht. Zur Bestimmung des Risikos für die zu prüfende Organisation muss deshalb eine Risikoeinschätzung durchgeführt werden. Anhand der Risikoeinschätzung wird der zu erwartende Zeitaufwand, die Prüftiefe sowie die Wahl der Stichproben bestimmt.

Die Beurteilung durch den Cyber-Sicherheits-Check erfolgt auf der Basis eines sorgfältig durch die ISACA erstellten Rahmenwerks. In 14 Kategorien werden 55 Maßnahmenziele beurteilt. Zu jedem Maßnahmenziel gibt es Basismaßnahmen, die mindestens geprüft werden müssen. Zusätzlich verwenden wir weitere, von uns ergänzend identifizierte Maßnahmen, die abhängig von der angewandten Referenznorm, z.B. ISO 27001 oder VdS 10000 untersucht werden.

Ein CyberRisikoCheck nach DIN SPEC 27076 ist ausschließlich Interview-basiert und dauert in der Regel maximal 2-3 Stunden. Als Ergebnis des CyberRisikoChecks erhalten Sie einen Bericht, der u.a. die erreichte Punktzahl und für jede nicht erfüllte Anforderung eine Handlungsempfehlung enthält.

Darum NESEC

Wir sind spezialisiert auf kleine und mittelständische Unternehmen. Deshalb arbeiten wir mit verschiedenen Standards wie VdS 10005, VdS 10000, CISIS 12, ISO 27001 und TISAX um das passende ISMS für Ihr Unternehmen zu finden. Egal ob Ihr Unternehmen 30 oder 3000 Mitarbeiter beschäftigt schaffen wir ein effizientes und kostengünstiges Informationssicherheitsmanagement für Sie.

Außerdem wächst unser ISMS mit Ihrem Unternehmen mit. Wir können mit einem schnell umzusetzenden ISMS auf Basis der VdS 10000 starten. Stellen Ihre Kunden im Laufe der Zeit höhere Anforderungen, stellen wir das ISMS auf ISO 27001 um und führen Sie zur Zertifizierung. Wir bieten Ihnen maximale Flexibilität.

NESEC
Gesellschaft für angewandte Netzwerksicherheit mbH

Fürholzener Straße 5a
85386 Eching

Telefon: 089 - 45217100
E-Mail: welcome@nesec.de
Internet: www.nesec.de

NESEC
Gesellschaft für angewandte Netzwerksicherheit mbH