NIS2 Assessment

NIS2 – Das ist jetzt zu tun?

Informieren Sie sich zum Anwendungsbereich, den Anforderungen und welche Maßnahmen wir zur Umsetzung von NIS2 empfehlen.

Softline GmbH

Gutenberg-Galerie | Gutenbergplatz 1
04103 Leipzig
+49 341 24051-0
info@softline.de

Inhalte

Über die Softline GmbH

Die Softline ist ein ganzheitlicher IT-Service-Provider und vertrauenswürdiger Partner für Unternehmen aller Branchen und Größenordnungen. Mit innovativen und individuellen Lösungen in den Bereichen Security, Cloud und IT Asset Management begleiten wir unsere Kunden weltweit bei der Optimierung Ihrer IT. Unsere Services decken dabei den gesamten IT-Lebenszyklus ab und umfassen die Beratung, Konzeptionierung, Implementierung und den Betrieb Ihrer IT-Infrastruktur mit hochwertigen Managed Services – unabhängig davon, ob Sie sich in der Cloud, On-Premise oder in einer hybriden Umgebung bewegen.

Bei allem, was wir tun, liegt unser Fokus darauf, Ihre individuellen Anforderungen zu verstehen und als Ihr enger Partner die Effizienz IT-gestützter Prozesse, die Sicherheit Ihrer Daten sowie Informationen und letztlich Ihre Wettbewerbsfähigkeit zu steigern – immer mit einem wachsamen Auge auf Ihre Ausgaben.

Die Softline GmbH mit Standorten in Leipzig und Aschheim/München ist Teil der Noventiq Holding PLC Unternehmensgruppe, einem weltweit führenden Anbieter von Lösungen und Services in den Bereichen Digital Transformation und Cyber Security mit Hauptsitz und Börsennotierung in London. Das Unternehmen realisiert, erleichtert und beschleunigt die digitale Transformation seiner Kunden, indem es neben seinen eigenen Services und Lösungen mehr als 80.000 Organisationen aus allen Branchen mit Hunderten von erstklassigen IT-Anbietern verbindet. Die 6.400 Mitarbeiterinnen und Mitarbeiter von Noventiq arbeiten in fast 60 Ländern in Asien, Lateinamerika, Europa und Afrika, Märkte mit großem Wachstumspotenzial.

1. MANAGEMENT SUMMARY

Durch unsere Expertise im Bereich ISMS (Informationssicherheitsmanagement System) nach ISO 27001 haben wir bereits viel Erfahrung auf diesem Gebiet sammeln und in erfolgreichen Projekten mit unseren Kunden umsetzen können. Die Softline verfügt nicht nur über ausgeprägte Kompetenzen im Informationssicherheitsbereich, sondern ist durch langjähriges technisches KnowHow auch auf der betrieblichen Ebene ein zuverlässiger Partner.

Dies hat für Sie vor allem bei der Beseitigung von eventuellen Schwachstellen in der IT Security viele Vorteile:

1. Softline Reifegradermittlungen für die Themen Informationssicherheit (nach ISO 27001 und ISO 27002) und IT-Security
2. GAP-Analyse erstellen
3. Handlungsempfehlungen

Nachfolgend sind die Leistungen aufgeführt, die im Service enthalten sind.

2. Consultingleistungen

Softline unterstützt mit hochqualifizierten Consulting-Leistungen, die neben der Ausführung am Standort des Auftraggebers eine entsprechende Vor- und Nachbereitung durch die Mitarbeiter umfassen. Es wird darauf hingewiesen, dass die Dienstleistungsaufwände Schätzwerte basierend auf Erfahrungen und vorliegenden Informationen sind. Änderungen der Mengen während des Projekts sind möglich.

2.1. Dienstleistungen durch Consultants

Durchführung einer Reifegradanalyse in den Bereichen Informationssicherheit und IT-Security mit einem geschätzten Gesamtaufwand ab 8 Personentagen, je nach Unternehmensgröße.

NIS2 (Network and Information Security) regelt die Cyber- und Informationssicherheit von Unternehmen und Institutionen. Die Richtlinie ist eine Verschärfung und Erweiterung der bisherigen Richtlinie NIS von 2016. Aus diesem Grund enthält NIS2 strengere Sicherheitsanforderungen, Meldepflichten und Durchsetzungsvorschriften für einen breiteren Kreis von Organisationen. Die Wahl des Sicherheitsgrades entscheiden die Unternehmen selbst, je nach Ausmaß der Risikoexposition, der Einrichtungsgröße sowie der Wahrscheinlichkeit von Sicherheitsvorfällen und deren Schweregrad:

- Erstellung von Konzepten in Bezug auf die Risikoanalyse und für die Sicherheit der Informationssysteme
- Incident-Response-Maßnahmen (Erkennung, Analyse, Eindämmung und Reaktion auf Vorfälle)
- Sichere Sprach-, Video- und Text-Kommunikation sowie gesicherte Notfallkommunikation
- Aufrechterhaltung des Betriebes (inkl. Backup-Management und Wiederherstellung nach Vorfall)
- Grundlegende Schulungen (Awareness) in der Cybersicherheit sowie Cyberhygiene
- Sicherheitsmaßnahmen bei Erwerb, Entwicklung und Wartung von Netz- und IT-Systemen
- Konzepte und Bewertung der Wirksamkeit von Risikomanagementmaßnahmen (Krisensimulation)
- Konzepte und Verfahren für den Einsatz von Kryptografie (ggf. Verschlüsselung)
- Sicherheit des Personals, Zugriffskontrolle und Assetmanagement
- Sicherheit in der Lieferkette

Neu bei NIS2 sind auch die erheblich verschärften Bußgelder. Die Aufsichtsbehörden werden wohl erstmals im April 2025 und dann alle zwei Jahre die regulierten Unternehmen melden müssen. Das Bußgeld wird abhängig vom weltweiten Jahresumsatz festgelegt werden. **Der Geschäftsführung wird die Verantwortung für die Umsetzung der Richtlinien übertragen**. Sie muss die Umsetzung der Maßnahmen überwachen und haftet bei Nichteinhaltung persönlich. Die Meldepflicht wird ebenfalls verschärft. Binnen 24 Stunden muss eine vorläufige Meldung erfolgen; spätestens nach 72 Stunden muss eine qualifizierte Meldung über einen Vorfall vorliegen. Einen Monat nach dem Vorfall muss ein Fortschritts-/Abschlussbericht vorliegen.

2.2. Reifegradanalyse Informationssicherheit

Die Evaluierung basiert auf der Vorgehensweise gemäß ISO 27001, um den Reifegrad im Prozess-reifegradmodell zwischen 0 bis 5 zu bestimmen. Es werden sowohl organisatorische als auch technische Aspekte des Unternehmens auditiert, um den aktuellen Reifegrad bezüglich IT- und Informationssicherheit festzustellen und ein Maßnahmenpaket zur Erhöhung vorzustellen.

Folgende Dienstleistungen durch Consultants werden von Softline erbracht.

Step 1: Auftakt Workshop

- gemeinsames Kennenlernen
- festlegen der Ziele und der Ergebnisform
- Vorstellung des Vorgehensmodell
- Identifikation des Scopes (Umfang)
- Bestimmung der Stakeholder und Fachansprech-partner
- gemeinsame Terminplanung
- Zusammenfassung

Step 2: Analyse vorhandener Maßnahmen zu IT-Sicherheit und Datenschutz

Technischer Art

- Welche Lösungen in Bezug auf die Absicherung der IT-Infrastruktur sind im Einsatz?
- Gibt es Regelungen zum Einsatz von Kryptographie bzw. welche?
- Wie sind AV-System / Mail-Filter/ Firewalls etc. konfiguriert?

In Betrachtung der gesetzlichen Bestimmungen (gemäß §9 BDSG / BSI IT-SIG 2.0)

- Wie ist das IT-Sicherheitsmanagement konzipiert?
- Welche Sicherheitsleitlinien und IT-Prozesse sind vorhanden? (Verschlüsselungs-, Lösch-Konzepte, Change Management u.a.)
- Wie sieht die aktuelle Backup- und Restore-Strategie aus?
- Wie steht es um die personelle Sicherheit?
- Wie wird mit Kundendaten bzw. personenbezogenen Daten verfahren? (Verschlüsselung, Sperrung, Zugriffsberechtigungen nach §9 BDSG Anlage 1)
- Wer hat über welchen Weg Zugriff auf Kundendaten?
- Gibt es generelle Zugangs- und Zugriffskontrollen und wofür?
- Welche Regelungen und Verfahren gibt es zur Kommunikationssicherheit?
- Schutz der Kommunikationsverbindungen, wie z.B. E-Mail, Netzwerk, Mobile Kommunikation, Zwischen zwei oder mehreren Partnern
- Wie können Vorfälle im Bereich der Informationssicherheit erkannt werden und wie wird damit umgegangen? (Risikomanagement, Frühwarnsystem)
- Ist ein Business Continuity Management (BCM) etabliert?
- Wie und inwieweit werden gesetzliche und anderweitige Verpflichtungen eingehalten?
- Wie geht man mit Lieferanten Risiken um?
- Gibt es einen incident response Plan?

Step 3: Auswertung und Dokumentation

- Auswertung der gewonnen Informationen des IST-Zustandes
- Beurteilung und Einordnung des aktuellen Reifegrades in den einzelnen Facetten
- Abgleich mit Anforderungen aus der ISO 27001 und ISO 27002 und Dokumentation notwendiger Umsetzungsmaßnahmen

2.3. Reifegradanalyse IT Security

Die Dienstleistungen umfassen die Analyse und Bewertung der IT-Sicherheitsmaßnahmen in verschiedenen Bereichen, gefolgt von einer Auswertung, Dokumentation und der Festlegung von Umsetzungsmaßnahmen.

Step 1: Auftakt Workshop Analyse vorhandener Maßnahmen zu IT-Sicherheit,

Beleuchtet werden folgende Bereiche:

- Server Administration
- Firewall
- Netzwerk
- Endpoint Protection
- VPN
- Monitoring
- Email
- Secure Browsing
- Client Administration
- Patch-Management
- Zertifikate und PKI
- Backup
- Privilege Access Management (PAM)
- Schwachstellen-Management

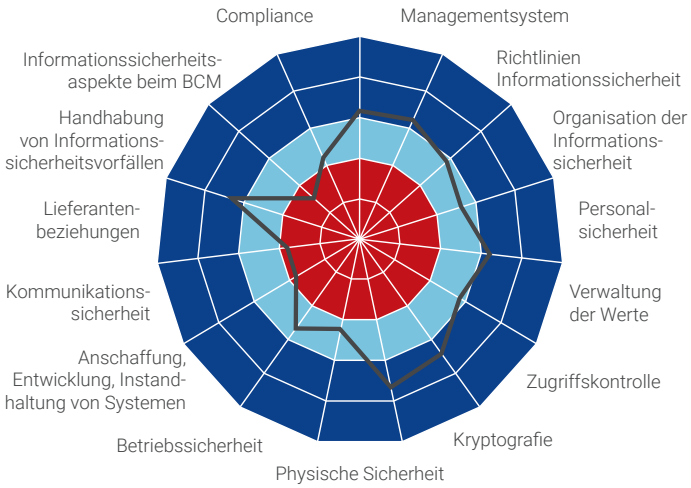
Step 2: Auswertung und Dokumentation

- Auswertung der gewonnen Informationen des IST-Zustandes
- Beurteilung und Einordnung des aktuellen Reifegrades in den einzelnen Facetten
- Festlegung der einzelnen Umsetzungsmaßnahmen nach Priorität
- Handlungsempfehlung

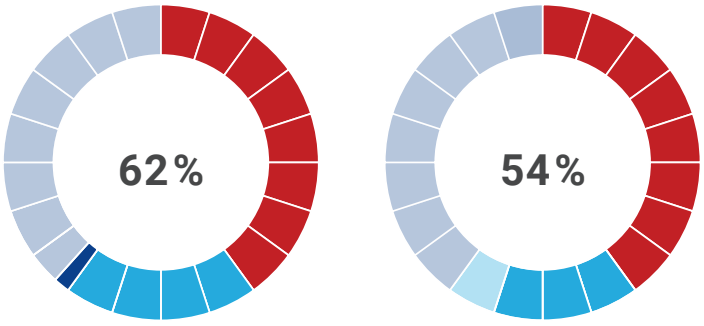
Die Ergebnisse der Reifegradanalyse

Die Ergebnisse werden von uns dokumentiert und ausgewertet. Sie erhalten einen Auditbericht, in dem wir Ihnen eine Übersicht der bewerteten Teilbereiche sowie priorisierte Handlungsempfehlungen für konkrete Umsetzungsmaßnahmen vorschlagen. Am Ende steht somit Ihr Reifegrad für ein zertifizierbares ISMS nach ISO 27001 fest. Hier sehen Sie eine beispielhafte Einschätzung der Analyse:

Reifegrad der Umsetzung



Erfüllung der Anforderungen



Haben Sie noch Fragen?

Rufen Sie uns an oder schreiben Sie uns eine E-Mail. Wir freuen uns darauf, Ihre offenen Fragen zu beantworten und stehen Ihnen sehr gern bei Ihren IT-Projekten zur Seite.

Melden Sie sich unter info@softline.de oder +49 341 24051-0.