Leitfaden für die individuelle NIS2 Umsetzung

Inhalt

Einleitung

Der vorliegende Leitfaden beschreibt die Umsetzung der NIS2 Anforderungen für wesentlichen und wichtigen Einrichtungen. Wesentlichen Einrichtungen empfehlen wir die frühzeitige Kontaktaufnahme mit NIS2 Prüfdienstleistern in Österreich auch Unabhängige Stellen genannt, da sich wesentliche Einrichtungen einem NIS2 Audit unterziehen müssen.

Dokumentierte Informationen

Für die NIS2 Umsetzung empfehlen wir die Erstellung der folgenden Dokumente:

Bereich	Eigentümer	Vorlage	Typ
Leitdokument	GF	InfoSec Politik	W
Definition ISMS	GF	ISMS Handbuch	W
	GF	Bestellung ISB	W
	GF	Dokumentenlenkungs-Richtlinie	W
	GF	Liste der interessierten Parteien	X
	GF	Chancen- und Risikomanagement Methodik	W*
ISMS operativ	ISB	InfoSec Richtlinie + Begriffsbestimmungen	W
	ISB	BenutzerInnen-Richtlinie	W
	ISB	Liste der ISMS Chancen & Risiken	X
	ISB	Methodik Business Impact Analyse	W
	ISB	BIA Erhebung, BIA Berichte	X W
	ISB + IT	IT-Risiko-Assessment	X
	ISB	Liste von ISMS Maßnahmen	X
	ISB	Prozessbeschreibung Sicherheitsvorfälle	P W
	ISB	Liste von Sicherheitsvorfällen	X
	ISB	Liste von Informationswerten	X
	ISB	Freigabeprotokolle für Cloud-Dienste	W
	ISB	Auditprogramm/Kalender	X
	ISB	NIS2 Auditprogramm	W
	ISB + TL	Erhebung der KPIs	X
	ISB	ISMS/NIS2 Management-Bewertung + Protokolle	P W
Maßnahmen	Alle TLs	Liste von Projekten	X
	TL Einkauf	InfoSec Bewertung der Lieferanten	X
	TL Facility	Physische Zonenpläne	P
	TL HR	Security Awareness Schulungskonzept	P
	TL HR	Checklisten Personaleintritt und -austritt	W
	TL HR	Verschwiegenheitsvereinbarung MitarbeiterInnen	W
	TL Legal	NDA für Firmen	W
	TL Legal	NDA für externe Personen	W
	TL IT	Change-Management Verfahren	P W
	TL IT	IT-Notfallhandbuch, BCM-Dokumentation	W
	TL IT	Liste der Sekundärassets	X
	TL IT	Liste der Cloud Freigaben	X
	TL IT	Dokumentierte Kapazitätsplanung	X
	TL IT	Dokumentierter Kryptographieeinsatz	X
	TL IT	IT-Betriebsabläufe	W
	TL Entwicklung	Secure Coding Manual	W

Empfohlener Dokumenttyp: ***W***... Word Dokument, ***X***... Excel Dokument, ***P***... PowerPoint
TL... Team-Leads / Abteilungsleiter

Klärung der Betroffenheit

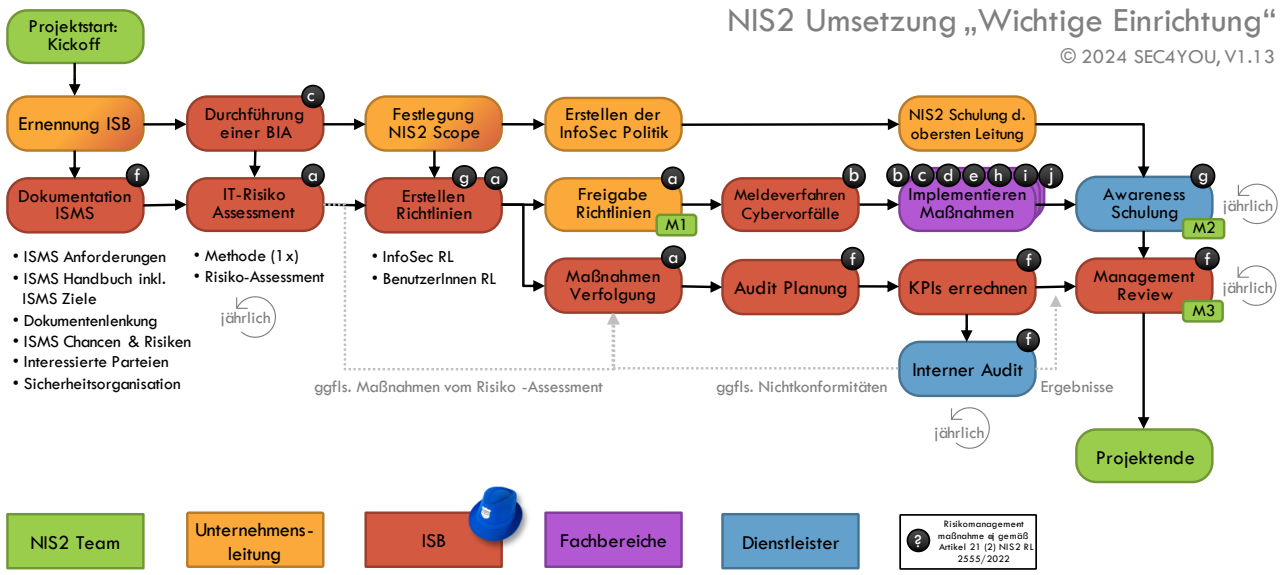
Vor der Umsetzung prüfen Sie bitte über den NIS2 Online Ratgeber der WKO, ob Sie als „Wesentliche Einrichtung“ oder „Wichtige Einrichtung“ gelten: https://ratgeber.wko.at/NIS2/

Einen vereinfachten Entscheidungsbaum zur NIS2 Betroffenheit haben wir unter dem folgenden Link veröffentlicht: https://www.sec4you.com/nis2-entscheidungsbaum/

Auch nicht direkt von NIS2 betroffene Unternehmen können eine NIS2 Umsetzung anstreben, wenn sie über die Lieferkette zur Einhaltung der Anforderungen verpflichtet werden.

Umsetzung

Starten Sie Ihr NIS2 Projekt gemäß dem folgenden Umsetzungsablauf. Die Schritte vom Projektstart/Kickoff bis hin zum Projektende werden in dem vorliegenden Leitfaden erklärt.



Projektstart: Kickoff

Definieren Sie zuerst Ihr ISMS-Team bestehend aus zumindest folgenden Mitgliedern:

- Zumindest einen **Vertreter der Geschäftsführung**, da viele der Maßnahmen die IT betreffen, ggfs. den für IT übergeordneten Geschäftsführer.
- Die Person, die **Verantwortung für die Informationssicherheit** trägt, oder diese Rolle übernehmen wird
- Die **IT-Leitung**
- Sofern verfügbar: den **Datenschutzkoordinator oder Datenschutzbeauftragten**

In einem rd. 2-stündigen Kickoff-Meeting sollen folgende Punkte besprochen werden:

- Die Betroffenheit des Unternehmens als „wesentliche Einrichtung“ oder „wichtige Einrichtung“
- Generelles Verständnis der NIS-2-Richtlinie (EU) 2022/2555: https://eur-lex.europa.eu/legal-content/DE/TXT/?uri=CELEX%3A32022L2555

- Generelles Verständnis des nationalen Umsetzungsgesetzes, in Österreich das NISG 2024 und in Deutschland das NIS-2-Umsetzungs- und Cybersicherheitsstärkungsgesetz. (jeweils geltende Fassung oder Entwurfsfassung beachten)
- Die Rollen lt. dem SEC4YOU Umsetzungsablauf und deren personelle Besetzung im Unternehmen. Sollte die Rolle des ISB vakant sein, kann diese Position auch extern, z.B. durch einen externen ISB/CISO oder ein CISO-as-a-Service Angebot besetzt werden.
- Der generelle Ablauf des NIS2 Projektes gemäß dem SEC4YOU Umsetzungsablauf
- Wo sind Dokumente für das zu schaffende Informationssicherheits-Managementsystem (ISMS) abzulegen und wer hat darauf Zugriff.
- Die Fristen für die Umsetzung

Ergebnisse:

- Das Commitment des ISMS-Teams für die fristgerechte Umsetzung.
- Ein definierter Speicherort für ISMS Dokumente.

Nachweise:

- Ein Meetingprotokoll mit den wesentlichen Punkten, inkl. der Aufteilung der Verantwortlichkeiten. Das Protokoll ist an die Teilnehmer des Kickoff -Meetings zu verteilen.

Ernennung eines Informationssicherheitsbeauftragten (ISB)

Der Informationssicherheitsbeauftragte (ISB) wird in größeren Unternehmen auch Chief Information Security Officer (CISO). Die Aufgaben und Verantwortlichkeiten sind ident, im Folgenden wird die Rolle ISB genannt.

Definieren Sie die Verantwortlichkeit für Informationssicherheit in einer Bestellungsurkunde mit dem ISB und übertragen Sie die operative Verantwortung für die Informationssicherheit an den ISB. Alternativ kann die Verantwortung auch per Stellenbeschreibung des ISBs übertragen werden.

Nachweise:

- Von der Unternehmensleitung und dem ISB unterschriebene Bestellung oder Stellenbeschreibung. Ablage als PDF am ISMS Speicherort.

Dokumentation des Informationssicherheits-Managementsystems (ISMS)

Der ISB ist verantwortlich für den Aufbau, Betrieb und die Weiterentwicklung des Informationssicherheits-Managementsystems (ISMS) und in dieser Funktion direkt der Unternehmensleitung unterstellt und an diese berichtspflichtig.

Für die Durchführung dieses komplexen Ablaufes muss die Arbeitsweise des ISB definiert werden:

- Erstellung eines ISMS-Handbuches, das die Aufgaben des ISB beschreibt
- Einführung einer Dokumentenlenkung als Teil des ISMS Handbuchs oder als eigene Dokumentenlenkungs-Richtlinie
- Erstellung einer Methodik für das Chancen- und Risikomanagement
- Erhebung der Chancen & Risiken für das ISMS selbst

Nachweise:

- von der Unternehmensleitung freigegebenes ISMS Handbuch
- nur bei größeren Unternehmen: von der Unternehmensleitung freigegebene Dokumentenlenkungs-Richtlinie
- von der Unternehmensleitung freigegebene Chancen- und Risikomanagement Methodik
- eine fertige ISMS Chancen & Risiken Bewertung

Durchführung einer Business Impact Analyse (BIA)

Im Zuge der Business-Impact-Analyse (BIA) erfolgt die Identifikation und Bewertung kritischer Geschäftsprozesse, die im Fall eines Notfalls priorisiert behandelt werden müssen. Im Vorfeld zur BIA müssen alle wertschöpfenden Prozesse (Kernprozesse) des Unternehmens bekannt sein. Im Zuge der BIA Bewertung werden folgende zwei zentralen Kennzahlen pro Kernprozess bestimmt:

- die Wiederherstellungszeit (RTO)
- den Wiederherstellungszeitpunkt (RPO)

Vor der Bewertung muss eine Methode für die Durchführung einer Business-Impact-Analyse erstellt und von der Unternehmensleitung freigegeben werden:

- Erstellung einer Methodik Business-Impact-Analyse
- Erstellung einer Kalkulationsvorlage für die Durchführung einer Business-Impact-Analyse je Kernprozess

Die Durchführung der BIA auf Basis der Kalkulationsvorlage:

- BIA Erhebung

Nachweise:

- von der Unternehmensleitung freigegebene Methodik Business-Impact-Analyse
- BIA Erhebung je Kernprozess, Ablage als PDF am ISMS Speicherort.

IT-Risko Assessment

Das IT-Risiko Management umfasst zum einen die Definition einer Methodik für die Risiko-Bewertung und zum anderen die regelmäßige und anlassbezogene Bewertung von Gefährdungen im Zuge eines IT-Risiko-Assessments.

Für die Methode muss eine Risiko-Management-Methode erstellt und von der Unternehmensleitung freigegeben werden:

- Erstellung einer Chancen- und Risikomanagement-Methodik, Verfahrensbeschreibung zur Beurteilung und Behandlung von Chancen und Risiken

Die Durchführung der Bewertung erfolgt in folgenden Arbeitsblättern:

- Erhebung der IKT-Risiken in der Liste IT-Risiko-Assessment
- Erfassung von organisatorischen und technischen Maßnahmen die im Zuge der Risikobewertung identifiziert wurden in der Liste von ISMS Maßnahmen

Nachweise:

- von der Unternehmensleitung freigegebene Verfahrensbeschreibung Chancen- und Risikomanagement-Methodik
- Vollständig ausgefülltes IT-Risiko-Assessment, Export als PDF Dokument am ISMS Speicherort

- Im Zuge des Risiko-Assessment identifiziere Risiko-mitigierende Maßnahmen sind in der Liste von ISMS Maßnahmen erfasst

Festlegung NIS2 Scope

In diesem Schritt müssen die Prozesse identifiziert werden, die von der EU-NIS2-Richtlinie 2555/2022 betroffen sind und für die verpflichtende Maßnahmen umzusetzen sind. Genau diese Prozesse müssen im Fokus der Business-Continuity-Planung und der Meldepflichten gegenüber der NIS Behörde liegen.

Zur Reduzierung des NIS2 Projektaufwandes sollten NIS2-unrelevante Kern- und Unterstützungsprozesse und dahinterliegende IT-Systeme zwar im Risiko-Assessment berücksichtigt sein, jedoch für diese müssen keine vollständigen Richtlinien und Maßnahmen erstellt und durch Audits überprüft werden, sofern nicht andere Compliance-Anforderungen dies fordern.

Unklarheiten zum NIS2 Scope können mit der WKO oder in späterer Folge mit der NIS Behörde geklärt werden.

Nachweise:

- Prozesslandkarte des Unternehmens mit Kennzeichnung der NIS2-relevanten Prozessen

Erstellen der InfoSec Politik

Erstellen Sie eine oberste Leitlinie – eine InfoSec Politik - für Ihr Unternehmen, welche die Informationssicherheit in den wesentlichen Geschäftsbereichen berücksichtigt. In der InfoSec Politik ist die Verpflichtung ein ISMS einzuführen und die Besetzung des ISB obligatorisch.

Sollte es bereits eine Unternehmenspolitik oder eine Qualitätsmanagement-Politik geben empfehlen wir diese Dokumente, um die Inhalte der InfoSec Politik zu erweitern.

Nachweise:

- von der Unternehmensleitung freigegebene InfoSec Politik

Erstellung Richtlinien

Durch die Anpassung und Freigabe von Richtlinien zur Informationssicherheit regelt das Unternehmen in den Kernbereichen operative Sicherheit, physische Sicherheit, personelle Sicherheit und technische Sicherheit alle wesentlichen Maßnahmen zur Einhaltung der Informationssicherheit. Die Richtlinien umfassen sowohl präventive Maßnahmen als auch aufdeckende und korrigierende Maßnahmen.

Folgende Vorlagen sind an das Unternehmen anzupassen, von der Unternehmensleitung freizugeben und an die Zielgruppe zu veröffentlichen:

- Informationssicherheits-Richtlinie
- BenutzerInnen-Richtlinie

Die Informationssicherheitsrichtlinie kann thematisch in kleinere Richtlinien geteilt werden, z.B. organisatorische Sicherheitsrichtlinien, physische Sicherheitsrichtlinien, personelle Sicherheitsrichtlinien, IT-Sicherheitsrichtlinien und Sicherheitsrichtlinien für die SoftwareentwicklerInnen. Generell empfiehlt es sich in kleineren Unternehmen eher wenige Richtlinien, dafür in möglichst kompakter Form zu erstellen.

Die BenutzerInnen-Richtlinie richtet sich an alle BenutzerInnen von IT-Endgeräten mit IT-Zugang. In dieser Richtlinie sollen nur Maßnahmen beschrieben werden, die unter direktem Einfluss der BenutzerInnen stehen. Technische Maßnahmen, die durch zentrale Konfigurationen definiert sind und von den BenutzerInnen nicht beeinflusst werden, z.B. Malwareschutz am Endgerät, URL-Filter, BitLocker-Verschlüsselung der Endgeräte, erfordern keine Aktion der BenutzerInnen und sind stattdessen in der Informationssicherheitsrichtlinie als Vorgabe für die IT Abteilung zu formulieren.

Nachweise:

- Eine zwischen IT und dem ISB abgestimmte BenutzerInnen-Richtlinie
- Eine zwischen den Fachbereichen und dem ISB abgestimmte Informationssicherheits-Richtlinie

Freigabe Richtlinien

Sobald die BenutzerInnen-Richtlinie und die Informationssicherheits-Richtlinie abgestimmt sind, sind diese von der Unternehmensleitung freizugeben und an die interessierten Parteien (i.d.R. die internen und externen Mitarbeiter) zu veröffentlichen.

Ein manuelles Unterschreiben der Richtlinien ist nicht erforderlich, es genügen dokumentierte Nachweise eine Freigabe, z.B. auch die E-Mail des Geschäftsführers, dass die jeweilige Richtlinie freigegeben ist. Auf eingescannte Unterschriften ist aus Sicherheitsgründen zu verzichten.

Nachweise:

- Freigabeprotokolle für die Richtlinien
- Veröffentlichte BenutzerInnen-Richtlinie
- Veröffentlichte Informationssicherheits-Richtlinie

Maßnahmen Verfolgung

Ein wesentliches Element eines kontinuierlichen Verbesserungsprozesses (KVP) ist ein korrekter Umgang mit identifizierten Verbesserungsmaßnahmen. Hierbei handelt es sich nicht um kleinteilige Verbesserungen wie Konfigurationsänderungen an IT-Systemen, oder die Bereinigung von Schwachstellen, sondern um ISMS Maßnahmen zur strategischen Stärkung der Informationssicherheit, wie:

- die Einführung eines verbesserten Malwareschutzes,
- die Einführung eines SIEM Systems,
- die Durchführung zusätzlicher IT-Audits, oder
- die Etablierung eines Schulungssystems für Security Awareness Trainings.

ISMS Maßnahmen können bei verschiedenen Anlässen durch den ISB oder durch Dritte identifiziert werden, z.B.:

- beim Risiko-Assessment
- durch Sicherheitsvorfälle
- durch technische Überprüfungen
- durch Beobachtungen des ISB
- Nichtkonformitäten bei internen Audits
- Nichtkonformitäten bei Zertifizierungsaudits, wie einer ISO 27001 Prüfung

Bei Identifizierung einer ISMS Maßnahme müssen diese in der Liste von ISMS Maßnahmen erfasst und gemäß den Vorgaben des ISMS Handbuchs behandelt werden.

Nachweise:

- Eine aktuell gepflegte Liste von ISMS Maßnahmen

Meldeverfahren Cybervorfälle

Die EU-NIS2-Richtlinie 2555/2022 sieht kurze Meldefristen an die nationalen NIS Behörden vor. Alle Sicherheitsvorfälle und nicht nur Cyberattacken, die zu einer Betriebsunterbrechung führen sind gemäß der nationalen Gesetzgebung i.d.R. innerhalb von 24h zu melden.

Details zu Meldepflichten finden Sie in den nationalen NIS2 Umsetzungsgesetzen.

Passen Sie die folgende Vorlage an:

- Prozessbeschreibung Sicherheitsvorfälle

Nachweise:

- Freigegebene Prozessbeschreibung Sicherheitsvorfälle

Implementierung Maßnahmen

Die vom ISB in den unterschiedlichen Richtlinien und weiteren Vorgaben festgelegten Maßnahmen müssen nun von den Fachbereichen umgesetzt und dokumentiert werden.

Erstellen Sie entsprechende Vorgaben die von den Team-Leads (Abteilungsleitern) der jeweiligen Fachbereiche an das Unternehmen anzupassen und inhaltlich zu ergänzen sind. Sollte es einzelne Abteilungen in Ihrem Unternehmen nicht geben, müssen die Vorgaben in dem Bereich angepasst werden, der die Tätigkeit tatsächlich durchführt.

Maßnahmen in allen Abteilungen:

- Pflege der Liste der Projekte, inkl. Reporting von Projekten lt. Informationssicherheits-Richtlinie an den ISB, damit diese Projekte bezüglich der Informationssicherheit bewertet werden

Maßnahmen im Bereich Einkauf:

- Erhebung der InfoSec Bewertungen der Lieferanten, die Umsetzung kann z.B. nach der SEC4YOU Veröffentlichung https://www.sec4you.com/lieferantenbewertung-iso-27001-2022/ erfolgen.

Maßnahmen im Bereich Facility:

- Dokumentation der physischer Zonenpläne des Unternehmens gemäß der Informationssicherheits-Richtlinie

Maßnahmen im Bereich Human Resources:

- Erstellung eines Security Awareness Schulungskonzept
- Erstellung einer Checkliste für den Personaleintritt
- Erstellung einer Checkliste für den Personalaustritt
- Erstellung einer Verschwiegenheitsvereinbarung für MitarbeiterInnen, die WKO hat hierzu ein Vertragsmuster veröffentlicht, siehe https://www.wko.at/oe/erklaerung-zum-datengeheimnis.docx

Maßnahmen im Bereich Legal:

- Erstellung eines NDA für Firmen
- Erstellung eines NDA für externe Personen

Maßnahmen im Bereich IT:

- Erstellung einer Change-Management Verfahrensbeschreibung
- Erstellung eines IT-Notfallhandbuch bzw. einer BCM-Dokumentation
- Erstellung und Pflege einer Liste der Sekundärassets
- Nutzung des Freigabeprotokolls für Cloud-Dienste pro Cloud-Dienst der im Unternehmen eingesetzt wird
- Pflege einer Liste der Cloud Freigaben
- Dokumentation der Kapazitätsplanung
- Dokumentation des Kryptographieeinsatzes
- Dokumentation der IT-Betriebsabläufe, beginnen Sie mit:
    - Installations- und Konfigurationsanweisungen für Endgeräte,
    - Installations- und Konfigurationsanweisungen für IT-Infrastruktur,
    - Backupanweisungen,
    - Usermanagement-Prozess,
    - Berechtigungsvergabe,
    - Projektmanagementanweisungen,
    - Supportanweisungen inklusive Ansprechpartner und Eskalationsmethodik,
    - Anweisungen für den IT-Neustart nach einem Systemausfall,
    - Protokollierungsanweisungen,
    - Überwachungsanweisungen (Alarmierungen aufgrund von Ereignissen oder Protokollen) und
    - erfassen Sie weitere relevante IT-Betriebsabläufe

Sofern es eine Softwareentwicklung gibt, definieren Sie Maßnahmen im Bereich Entwicklung:

- Erstellen Sie Vorgaben für die sichere Softwareentwicklung, ein sogenanntes Secure Coding Manual

Nachweise:

- Alle o.a. Vorlagen bzw. Dokumentationen sind gepflegt und gemäß der Dokumentenlenkung freigegeben und veröffentlicht.

NIS2 Schulung der obersten Leitung

Die NIS2 Richtlinie fordert in Artikel 20 Governance, dass die Mitglieder der Leitungsorgane wesentlicher und wichtiger Einrichtungen an Schulungen teilnehmen müssen. Gleichzeitig fordert sie wesentliche und wichtige Einrichtungen auf, allen Mitarbeitern regelmäßig entsprechende Schulungen anzubieten, um ausreichende Kenntnisse und Fähigkeiten zur Erkennung und Bewertung von Risiken sowie Managementpraktiken im Bereich der Cybersicherheit und deren Auswirkungen auf die von der Einrichtung erbrachten Dienste zu erwerben. (Publications Office of the European Union, 2022)

Aufgaben:

- Zur Erfüllung der Anforderung empfehlen wir, dass alle Leitungsorgane[1] eine NIS2 Schulung absolvieren und sich so nachweislich mit den NIS2 Pflichten und die Verantwortung aus der EU Richtlinie und des nationalen Umsetzungsgesetzes beschäftigen.
- Team-Leads, die eine Verantwortung im Bereich der Informationssicherheit tragen müssen in das Risikomanagement des Unternehmens eingebunden werden und diesbezüglich geschult werden.
- Die MitarbeiterInnen von Fachbereichen mit besonderen Informationssicherheits-anforderungen wie Entwicklung, IT, Einkauf, etc. müssen in Ihrem Fachbereich hinsichtlich spezifischer Informationssicherheitsrisiken geschult werden.
- Alle MitarbeiterInnen müssen in Bezug auf Security Awareness geschult werden, siehe Abschnitt „Awareness Schulung".

Nachweise:

- Schulungsbestätigung für die Leitungsorgane
- Teilnahmebestätigung der Team-Leads an einer Risikomanagement Einweisung
- Teilnahmebestätigung von MitarbeiterInnen ausgewählter Fachbereiche an speziellen InfoSec Schulungen

Awareness Schulung

Die MitarbeiterInnen, davon speziell jene mit Zugang zu IT-Systemen, benötigen eine Security Awareness Schulung. Auch wenn die NIS2 Richtlinie dies nicht explizit vorschreibt, empfehlen wir die Durchführung von jährlichen Security Awareness Schulungen. Die Awareness der MitarbeiterInnen kann zusätzlich durch ergänzende Maßnahmen wie Security Newsletter und Phishing Tests verbessert werden. In größeren Unternehmen empfiehlt sich der Einsatz einer Schulungsplattform.

Aufgaben:

- Erstellen Sie ein Security Awareness Schulungskonzept für Ihr Unternehmen, das auch die Schulung der veröffentlichten Richtlinien beinhaltet.
- Erstellen Sie einen Schulungsplan in einer Kalenderform der abbildet, wann welche MitarbeiterInnen-Gruppen zum Thema Security Awareness in Ihren Fachbereichen geschult werden. Generelle Security Awareness Schulungen für alle MitarbeiterInnen sollten jährlich geplant werden.
- Berücksichtigen Sie Neueintritte im HR Prozess und sorgen Sie dafür, dass neue Mitarbeiter zeitnahe zum Eintritt eine Security Awareness Schulung inklusive der Vorgaben aus Richtlinien erhalten.
- Dokumentieren Sie die Teilnahme der MitarbeiterInnen an Awareness Schulungen.

Nachweise:

- Eine zwischen ISB und HR abgestimmte Security Awareness Schulung.
- Einen zwischen ISB und HR abgestimmten Schulungsplan für Informationssicherheit.
- Awareness Schulungsnachweise (Teilnehmerlisten) für alle MitarbeiterInnen mit IT-Zugang.

[1] Leitungsorgane sind mit der Geschäftsführung betraute Organe, wie etwa Geschäftsführer, Vorstand oder Stiftungsvorstand.

Audit Planung

Eine Kernaufgabe des ISB ist die Einhaltung der Vorgaben in Bezug auf die Informationssicherheit im Unternehmen zu prüfen. Hierzu muss ein Auditplan erstellt werden, der sowohl die Führung des ISMS prüft, als auch die Maßnahmen der Fachbereiche berücksichtigt. Auch technische Prüfungen wie Penetrationstests sind in der Auditplanung zu berücksichtigen.

Erstellen Sie folgende Dokumentation:

- Auditprogramm/Kalender für das ISMS und alle definierten Maßnahmen über einen Zeitraum von 3 Jahren

Die Audits können je nach Themenbereich von einem dafür qualifizierten ISB durchgeführt werden, oder von einem externen Dienstleister erbracht werden.

KPI errechnen

Für die Umsetzung der Anforderung f) der NIS2 Artikel 21 (2) Konzepte und Verfahren zur Bewertung der Wirksamkeit von Risikomanagementmaßnahmen im Bereich der Cybersicherheit (Publications Office of the European Union, 2022), sind Key Performance Indicators (KPIs) zu definieren und regelmäßig zu erheben. Wir empfehlen zu Beginn der NIS2 Umsetzung mit wenigen KPIs zu starten und diese in den Folgejahren sinnvoll zu erweitern.

Zu den wichtigsten KPIs zählen:

- Abdeckungsgrad der Security Awareness Maßnahmen
- Abdeckung des Endgeräteschutzes (Malware-Protection, Endgeräteverschlüsselung)
- Abdeckung des Patch-Management
- Fristeinhaltung bei den ISMS Maßnahmen

Erstellen Sie eine Berechnungsmethode sowie einen KPI Report. Zur Durchführung aktualisieren Sie die Messwerte zumindest quartalsweise:

- Erhebung der KPIs in einem KPI Report
- Reporten Sie die KPIs quartalsweise an die oberste Leitung

Nachweise:

- Quartalsweise Meldung der KPIs an die oberste Leitung.
- Berücksichtigung der KPIs in dem jährlichen Management Review.

Interner Audit

Die im Punkt Audit Planung geplanten Audithandlungen müssen fristgerecht durchgeführt und dokumentiert werden. Dokumentieren Sie die Audits sorgfältig in einem Auditprogramm. Alle Anforderungen der NIS2 müssen abdeckt werden und die Wirksamkeit der Umsetzung muss geprüft und dokumentiert werden:

- Erstellung eines NIS2 Auditprogramms
- Durchführung von NIS2 Audits gemäß dem Auditprogramm

Nachweise:

- Einzelprotokolle der internen Audits
- Meldung von Nicht-Konformitäten an die Fachbereiche mit Fristen für die Umsetzung und Nachverfolgung der Umsetzung durch den ISB

Management Review

Zur Bewertung der Wirksamkeit von Risikomanagementmaßnahmen durch die oberste Leitung ist es erforderlich, dass der ISB jährlich einen sogenannten Management-Review plant und durchführt. In diesem Management Review wird der Reifegrad des ISMS, Analysen von Sicherheitsvorfällen und die Umsetzung von Maßnahmen vorgebracht. Die oberste Leitung kann auf dieser Basis entscheiden, ob das implementierte ISMS im Unternehmen wirksam ist und weitere Projekte oder Maßnahmen beschließen.

Erstellen Sie dazu folgende Vorlagen:

- Managementbewertung-ISMS Präsentation
- Managementbewertung-ISMS Meetingprotokoll

Nachweise:

- Jährliche Managementbewertung-ISMS Präsentation
- Protokoll des Meetings mit Beschluss über die Wirksamkeit des ISMS und Entscheidungen der obersten Leitung über neue Projekte/Maßnahmen

Betrieb und Aufrechterhaltung der NIS2 Anforderungen

Um die NIS2 Umsetzung nach der initialen Errichtung in ein laufendes Managementsystem zu wandeln, müssen einige Aufgaben regelmäßig durchgeführt werden. Hierzu zählen unter anderem:

- Jährliche Kontrolle und Pflege der Dokumentationen (Politik, Richtlinien, Methoden, Vorlagen, etc.)
- Jährliche und anlassbezogene Aktualisierung des IT-Risiko-Assessments
- Jährliche Security Awareness Schulungen
- Regelmäßige Durchführung von internen Audits gemäß Auditprogramm und Erneuerung des Auditprogrammes nach 3 Jahren
- Jährlicher Management-Review

Beim Betrieb eines ISMS können Sie sich an den bewährten und gut dokumentierten Methoden der ISO 27001 orientieren.

Tipps zur Umsetzung

Passende Vorlagen für die o.a. Dokumentationen finden Sie im Online-Shop der SEC4YOU unter https://www.sec4you.com/shop/

Beratungsleistungen zur Unterstützung bei der Implementierung bietet SEC4YOU gerne an, vereinbaren Sie einen unverbindlichen Kennenlerntermin mit unserem Online Kalender Tool: https://www.sec4you.com/termin-buchen-andreas-schuster/

Ein NIS2 Richtlinien- und Coaching Paket für KMU finden Sie unter folgendem Link: https://www.sec4you.com/kategorie/isms-richtlinien-und-vorlagen/

Ein NIS2 Richtlinien- und Coaching Paket für Enterprise Unternehmen finden Sie unter folgendem Link: https://www.sec4you.com/produkt/nis2-richtlinienpaket-enterprise/

Literaturverzeichnis

Publications Office of the European Union. (27. 12 2022). *RICHTLINIE (EU) 2022/2555 DES EUROPÄISCHEN PARLAMENTS UND DES RATES vom 14. Dezember 2022*. Von EUR-Lex: https://eur-lex.europa.eu/legal-content/DE/TXT/HTML/?uri=CELEX:32022L2555#d1e3318-80-1 abgerufen