

• CYBERSICHERHEIT FÜR BETROFFENE UNTERNEHMEN UND ZULIEFERER

NIS2: DIE 10 MASSNAHMENBEREICHE ALS CHECKLISTE

Die NIS2-Richtlinie verpflichtet betroffene Unternehmen zu Risikomanagementmaßnahmen. Artikel 21 nennt dafür zehn Bereiche, die das deutsche Umsetzungsgesetz übernimmt. Das Gesetz schreibt Maßnahmen vor, aber keine Produkte – für ein KMU heißt das: Die meisten Punkte sind mit soliden IT-Grundlagen erfüllbar, wenn sie dokumentiert sind. Diese Liste stellt je Bereich die Fragen, die bei einer Gap-Analyse zuerst kommen.

So nutzt du die Liste

- Hake eine Frage nur ab, wenn die Maßnahme umgesetzt *und* nachweisbar ist. „Machen wir, steht aber nirgends“ zählt als offen.
- Die rechte Spalte „Nachweis“ nennt, was bei einer Prüfung oder einem Kundenfragebogen typischerweise vorgelegt wird.
- Geh die Liste zu zweit durch: jemand aus der Geschäftsführung und jemand, der die IT betreut. NIS2 nimmt die Leitung ausdrücklich in die Verantwortung.
- Offene Punkte in den Bereichen 2, 3 und 10 haben in der Praxis meist Vorrang.

Keine Rechtsberatung

Diese Liste ist eine technische Orientierung, keine rechtliche Bewertung. Ob dein Unternehmen unter NIS2 fällt, in welche Kategorie es gehört und welche Fristen laufen, klärst du mit einer Kanzlei oder der IHK. Wir setzen die Maßnahmen um und machen sie nachweisbar – die Einstufung übernehmen wir nicht.

Erste Einordnung in zwei Minuten, Auswertung im Browser ohne Datenübertragung:
art-kon-tor-digital.de/it/cyber-security/nis2-check/

1 RISIKOANALYSE UND SICHERHEITSKONZEPTE

Art. 21 Abs. 2 lit. a

FRAGE	NACHWEIS
☐ Gibt es ein aktuelles Verzeichnis aller Systeme, Anwendungen, Datenbestände und ihrer Verantwortlichen?	Asset-Verzeichnis mit Datum, Verantwortlichen und Kritikalität
☐ Ist für die wichtigen Systeme dokumentiert, welche Risiken bestehen, wie sie bewertet wurden und welche Maßnahme dagegen wirkt?	Risikoanalyse (System, Risiko, Bewertung, Maßnahme, Restrisiko)
☐ Gibt es eine von der Geschäftsführung freigegebene Sicherheitsleitlinie mit Zielen, Zuständigkeiten und Geltungsbereich?	Leitlinie mit Freigabedatum und Unterschrift der Leitung
☐ Wird die Risikoanalyse mindestens jährlich und bei größeren Änderungen (neues System, neuer Standort, Vorfall) aktualisiert?	Änderungshistorie, Datum der letzten Überprüfung

2 BEWÄLTIGUNG VON SICHERHEITSVORFÄLLEN

Art. 21 Abs. 2 lit. b

☐ Ist festgelegt, was als Sicherheitsvorfall gilt, wer ihn intern meldet und wer entscheidet, was als Nächstes passiert?	Vorfallprozess mit Rollen und Meldekette
☐ Gibt es einen Notfallplan mit Erreichbarkeiten, Reihenfolge der Schritte und Vorlagen – auch ausgedruckt, falls die IT selbst betroffen ist?	Notfallhandbuch, Kontaktliste offline verfügbar
☐ Ist der Meldeweg zum BSI vorbereitet: benannte Person, Zugang zum Meldeverfahren, Vorlage für die Erstmeldung innerhalb von 24 Stunden?	Meldevorlage, Registrierungsnachweis, benannte Kontaktstelle
☐ Werden Vorfälle protokolliert und nachbereitet – was ist passiert, was wurde geändert, damit es nicht wieder passiert?	Vorfallregister, Nachbereitungsprotokolle

3 BETRIEBSKONTINUITÄT: BACKUP, WIEDERHERSTELLUNG, KRISENMANAGEMENT Art. 21 Abs. 2 lit. c

☐	Werden Backups nach dem 3-2-1-Prinzip angelegt, mit mindestens einer Kopie, die vom Netz getrennt oder unveränderbar ist?	Backup-Konzept, Konfiguration, Speicherorte
☐	Wurde die Wiederherstellung in den letzten zwölf Monaten tatsächlich getestet – nicht nur geprüft, ob das Backup durchgelaufen ist?	Restore-Testprotokoll mit Datum, Umfang und Dauer
☐	Sind für die wichtigen Systeme festgelegt, wie lange ein Ausfall höchstens dauern darf und wie viel Datenverlust tragbar ist?	Tabelle je System mit Wiederanlaufzeit und Datenverlust-Toleranz
☐	Gibt es einen Plan, wie das Unternehmen weiterarbeitet, wenn IT, Standort oder ein zentraler Dienstleister ausfällt – inklusive Krisenstab und Kommunikation?	Notfall- und Wiederanlaufplan, Übungsprotokoll

4 SICHERHEIT DER LIEFERKETTE Art. 21 Abs. 2 lit. d

☐	Ist bekannt, welche Dienstleister und Lieferanten Zugriff auf Systeme oder Daten haben – inklusive Fernwartung, Hosting und Software-as-a-Service?	Dienstleisterverzeichnis mit Zugriffsart und Datenkategorien
☐	Sind Sicherheitsanforderungen mit diesen Dienstleistern vertraglich vereinbart – Auftragsverarbeitung, Meldepflichten bei Vorfällen, Mindeststandards?	Verträge, AV-Verträge, Sicherheitsanhänge
☐	Sind Fernzugänge von Dienstleistern personengebunden, mit zweitem Faktor gesichert, protokolliert und nur bei Bedarf freigeschaltet?	Zugangsliste, Protokolle der Fernzugriffe
☐	Wurde für die kritischen Lieferanten (IT-Betrieb, Hosting, Fachsoftware) bewertet, was ihr Ausfall bedeutet und wie er überbrückt wird?	Lieferantenbewertung mit Ersatzstrategie

5 BESCHAFFUNG, ENTWICKLUNG, WARTUNG UND SCHWACHSTELLEN Art. 21 Abs. 2 lit. e

☐	Gibt es ein Patch-Management mit Fristen – kritische Sicherheitsupdates kurzfristig, alles andere in festen Wartungsfenstern?	Patch-Richtlinie, Update-Berichte, Übersicht des Patch-Stands
☐	Sind Systeme ohne Herstellersupport erfasst und entweder abgelöst oder vom übrigen Netz getrennt?	Liste der Altsysteme mit Maßnahme und Termin
☐	Wird bei der Beschaffung von Hardware, Software und Cloud-Diensten geprüft, ob Updates, Verschlüsselung, Protokollierung und Datenstandort passen?	Beschaffungs-Checkliste, Prüfvermerke
☐	Werden Schwachstellen aktiv gesucht und behandelt – durch Scans, Herstellerwarnungen und Meldungen der CERTs?	Scan-Berichte, Schwachstellenliste mit Status

6 BEWERTUNG DER WIRKSAMKEIT Art. 21 Abs. 2 lit. f

☐	Wird regelmäßig geprüft, ob die Maßnahmen tatsächlich wirken – etwa durch einen jährlichen Sicherheitscheck, internes Audit oder Penetrationstest?	Prüfplan, Prüfberichte mit Datum
☐	Bekommt die Geschäftsführung Kennzahlen, die sie ohne Technikstudium versteht – offene Patches, Backup-Erfolg, MFA-Abdeckung, Anzahl der Vorfälle?	Regelmäßiger Sicherheitsbericht an die Leitung
☐	Werden festgestellte Abweichungen mit Verantwortlichem und Frist nachverfolgt, bis sie geschlossen sind?	Maßnahmenliste mit Status und Erledigungsdatum

7 CYBERHYGIENE UND SCHULUNG Art. 21 Abs. 2 lit. g

☐	Gelten für alle Beschäftigten Grundregeln – Passwort-Manager, Bildschirmsperre, Umgang mit Anhängen, Links und USB-Sticks, Meldung von Verdachtsfällen?	Nutzungsrichtlinie mit Kenntnisnahme
--------------------------	---	--------------------------------------

☐	Werden alle Beschäftigten mindestens einmal im Jahr geschult, neue beim Einstieg – ergänzt um Phishing-Übungen mit Auswertung?	Teilnehmerlisten, Schulungsinhalte, Übungsergebnisse
☐	Hat die Geschäftsführung selbst an einer Schulung teilgenommen? NIS2 verlangt das ausdrücklich von der Leitung.	Teilnahmenachweis der Geschäftsführung
☐	Sind Grundkonfigurationen abgesichert – keine Standardpasswörter, unnötige Dienste abgeschaltet, Admin-Rechte vom Alltagskonto getrennt?	Härtungs-Checkliste je Systemtyp

8 KRYPTOGRAPHIE UND VERSCHLÜSSELUNG

Art. 21 Abs. 2 lit. h

☐	Sind Notebooks, Smartphones und mobile Datenträger vollständig verschlüsselt, und lässt sich das zentral nachvollziehen?	Geräteverwaltung, Stichprobenprotokoll
☐	Sind alle Verbindungen verschlüsselt – Websites und E-Mail per TLS, Fernzugriff per VPN, WLAN mit aktuellem Standard und Zertifikaten?	Konfigurationsnachweise, Zertifikatsübersicht
☐	Ist festgelegt, wo Schlüssel und Zertifikate liegen, wer sie verwaltet und wann sie ablaufen – mit Erinnerung vor dem Ablauf?	Schlüssel- und Zertifikatsverzeichnis
☐	Sind Backups und Archive verschlüsselt und die zugehörigen Schlüssel getrennt vom Backup gesichert?	Backup-Konzept, Ablage des Wiederherstellungsschlüssels

9 PERSONAL, ZUGRIFFSKONTROLLE UND ANLAGENVERWALTUNG

Art. 21 Abs. 2 lit. i

☐	Bekommt jede Person nur die Rechte, die ihre Aufgabe braucht, und werden Rechte bei Wechsel oder Austritt am selben Tag angepasst?	Berechtigungskonzept, Ein- und Austrittscheckliste
☐	Sind Administrator-Konten personengebunden und vom normalen Arbeitskonto getrennt – keine geteilten Zugänge, kein „admin“ für alle?	Kontenübersicht mit Zuordnung
☐	Werden Berechtigungen regelmäßig überprüft: Wer hat noch Zugriff worauf, und braucht er ihn noch?	Protokoll der letzten Berechtigungsprüfung
☐	Sind alle Geräte inventarisiert und einer Person zugeordnet – inklusive privater Geräte, falls deren Nutzung erlaubt ist?	Geräteinventar, Regelung zu privaten Geräten

10 MEHRFAKTOR-AUTHENTIFIZIERUNG UND GESICHERTE KOMMUNIKATION

Art. 21 Abs. 2 lit. j

☐	Ist ein zweiter Faktor für alle Fernzugänge, E-Mail-Konten, Cloud-Dienste und Administrator-Zugänge aktiv – ohne Ausnahmen für die Geschäftsführung?	MFA-Abdeckung je Dienst, Ausnahmenliste mit Begründung
☐	Sind Sprach-, Video- und Textkommunikation abgesichert – freigegebene, verschlüsselte Dienste statt privater Messenger für Firmendaten?	Liste freigegebener Werkzeuge, Kommunikationsrichtlinie
☐	Gibt es einen abgestimmten Weg, im Notfall zu kommunizieren, wenn E-Mail, Telefonanlage oder Firmennetz ausgefallen sind?	Notfall-Kommunikationsplan mit alternativen Kanälen

AUSWERTUNG

Alles abgehakt: Dann fehlt meist nur noch, die Nachweise an einem Ort zu sammeln und jährlich zu aktualisieren. Einige Punkte offen: Beginne mit den Sofortmaßnahmen – zweiter Faktor, getrennte Backup-Kopie, Protokollierung, Notfallplan –, dann Dokumentation, dann Prozesse. Viele Punkte offen: Eine Gap-Analyse bringt Reihenfolge und Aufwand auf den Tisch, bevor Geld ausgegeben wird.

Wer nicht unter NIS2 fällt, verliert mit denselben Maßnahmen nichts: Sie senken das Risiko, egal ob ein Gesetz sie verlangt – und sie beantworten die Fragebögen, die betroffene Kunden zunehmend an ihre Zulieferer schicken.

Du willst die offenen Punkte schließen?

Wir vergleichen den Stand deiner IT mit den NIS2-Anforderungen, setzen die technischen und organisatorischen Maßnahmen um und machen sie nachweisbar – für Unternehmen und Zulieferer in Jena und Thüringen.

art-kon-tor-digital.de/it/cyber-security/nis2/
kontakt@akt-digital.de · 03641 5598209