NIS2-Fragebogen für Lieferanten

Hinweis
Fragen an Lieferanten und Dienstleister zur Sicherheit der Lieferkette, eine Maßnahme nach § 30 Abs. 2 Nr. 4 BSIG (Art. 21 Abs. 2 lit. d NIS2). Fragetiefe: Grundfragen stellen Sie jedem Lieferanten, Standardfragen zusätzlich bei mittlerer Kritikalität, erweiterte Fragen bei hoher Kritikalität. Antworten: ja / teilweise / nein, bei Freitextfragen eine kurze Angabe in der Spalte Anmerkung. Der Fragebogen ist eine Arbeitshilfe; ob er Ihre Pflichten vollständig abdeckt, hängt von Ihrem Unternehmen und Ihren Lieferanten ab.

Organisation und Verantwortung

Nr.	Frage	Passender Nachweis	Antwort	Nachweis / Anmerkung
1	Ist Ihr Unternehmen selbst nach NIS2 oder BSIG als wichtige oder besonders wichtige Einrichtung eingestuft und beim BSI registriert? Art. 3 NIS2; § 28 BSIG · Grundfrage	Kein Dokument nötig. Nennen Sie die Einstufung im Antworttext; auf Wunsch genügt die Registrierungsbestätigung des BSI ohne Kennungen.		
2	Wurde Ihre Geschäftsleitung in den letzten 24 Monaten zu Cybersicherheitsrisiken geschult? Art. 20 Abs. 2 NIS2 · Erweiterte Frage	Teilnahmebestätigung oder Schulungsnachweis für die Geschäftsleitung mit Datum (höchstens 24 Monate) und Thema.		
3	Erhalten Beschäftigte mit Sicherheitsaufgaben regelmäßige Schulungen zu Cyberhygiene und aktuellen Bedrohungen? Art. 21 Abs. 2 lit. g NIS2 · Standardfrage	Schulungsnachweis mit Datum (höchstens 12 Monate), Zielgruppe und Thema.		
4	Haben Sie unsere Sicherheitsanforderungen vertraglich anerkannt (zum Beispiel als Anlage oder SLA)? Art. 21 Abs. 2 lit. d NIS2; § 30 Abs. 2 Nr. 4 BSIG · Grundfrage	Vertrags- oder Anlagenauszug mit unseren Sicherheitsanforderungen und Unterschrift oder Annahme.		
5	Räumen Sie uns oder einem beauftragten Prüfer das Recht ein, die Sicherheitsanforderungen zu prüfen? Art. 21 Abs. 2 lit. d NIS2 · Standardfrage	Vertragsklausel zum Prüfrecht.		

Risiko und Richtlinien

Nr.	Frage	Passender Nachweis	Antwort	Nachweis / Anmerkung
6	Haben Sie Maßnahmen zum Risikomanagement für Cybersicherheit umgesetzt, die Ihre Geschäftsleitung gebilligt hat? Art. 20 Abs. 1 NIS2; Art. 21 Abs. 1 NIS2 · Grundfrage	Maßnahmenübersicht oder Richtlinie mit Billigung der Geschäftsleitung und Datum (höchstens 24 Monate).		

Nr.	Frage	Passender Nachweis	Antwort	Nachweis / Anmerkung
7	Prüfen Sie mindestens jährlich, ob Ihre Sicherheitsmaßnahmen wirken (zum Beispiel internes Audit oder Kennzahlen)? Art. 21 Abs. 2 lit. f NIS2 · Standardfrage	Audit- oder Prüfbericht mit Datum (höchstens 12 Monate) und Ergebnis.		

Vorfälle und Meldungen

Nr.	Frage	Passender Nachweis	Antwort	Nachweis / Anmerkung
8	Melden Sie uns einen erheblichen Sicherheitsvorfall, der unsere Leistung betrifft, innerhalb von 24 Stunden nach Erkennen? Art. 23 Abs. 4 lit. a NIS2; § 32 BSIG · Grundfrage	Vertragsklausel oder SLA mit Meldefrist von 24 Stunden und Meldeweg.		
9	Liefern Sie uns innerhalb von 72 Stunden eine erste Bewertung (Schwere, Auswirkungen, Anzeichen eines Angriffs)? Art. 23 Abs. 4 lit. b NIS2; § 32 BSIG · Grundfrage	Vertragsklausel mit Frist von 72 Stunden und Inhalt der Erstbewertung.		
10	Erhalten wir innerhalb eines Monats einen Abschlussbericht mit Ursache und ergriffenen Maßnahmen? Art. 23 Abs. 4 lit. d NIS2; § 32 BSIG · Standardfrage	Vertragsklausel zum Abschlussbericht binnen eines Monats.		
11	Gibt es einen rund um die Uhr erreichbaren Notfallkontakt für Sicherheitsvorfälle? Art. 21 Abs. 2 lit. b NIS2 · Erweiterte Frage	Kein Dokument nötig. Nennen Sie Rufnummer oder Adresse und die Erreichbarkeit im Antworttext.		

Zugriff und Identitäten

Nr.	Frage	Passender Nachweis	Antwort	Nachweis / Anmerkung
12	Ist jeder Zugriff auf unsere Systeme mit Mehr-Faktor-Anmeldung geschützt und personalisiert? Art. 21 Abs. 2 lit. j NIS2 · Grundfrage	Screenshot der MFA-Pflicht für den Zugang zu unseren Systemen (VPN, Fernwartungswerkzeug), Datum sichtbar (höchstens 12 Monate).		
13	Erfolgt der Fernzugriff auf unsere Systeme nur nach unserer Freigabe, und können wir ihn jederzeit abschalten? Art. 21 Abs. 2 lit. i NIS2 · Standardfrage	Prozessbeschreibung zur Freigabe von Fernzugriffen mit Freigabedatum (höchstens 24 Monate).		
14	Sind Administratorzugänge auf unseren Systemen personalisiert, befristet und auf das Nötige beschränkt? Art. 21 Abs. 2 lit. i NIS2 · Standardfrage	Bericht oder Screenshot zu personalisierten, befristeten Admin-Konten mit Datum (höchstens 12 Monate).		

Nr.	Frage	Passender Nachweis	Antwort	Nachweis / Anmerkung
15	Werden Personen mit Zugang zu unseren Systemen vor dem Einsatz überprüft und beim Ausscheiden sofort abgemeldet? Art. 21 Abs. 2 lit. i NIS2 · Erweiterte Frage	Richtlinienauszug zu Überprüfung und Austritt mit Freigabedatum (höchstens 24 Monate).		

Betrieb, Patches und Schwachstellen

Nr.	Frage	Passender Nachweis	Antwort	Nachweis / Anmerkung
16	Werden Ihre Zugriffe auf unsere Systeme protokolliert, und stellen Sie uns die Protokolle auf Anfrage bereit? Art. 21 Abs. 2 lit. b NIS2 · Standardfrage	Screenshot der Protokollierung von Sitzungen mit Datum (höchstens 12 Monate).		
17	Gibt es einen Ablauf, um Meldungen zu Schwachstellen anzunehmen, zu bewerten und koordiniert zu beheben? Art. 21 Abs. 2 lit. e NIS2 · Grundfrage	Prozessbeschreibung mit Annahme, Bewertung, Fristen und Freigabedatum (höchstens 24 Monate).		
18	Werden Sicherheitsupdates nach Risiko priorisiert und zeitnah eingespielt? Art. 21 Abs. 2 lit. e NIS2 · Grundfrage	Patch-Prozess mit Fristen nach Schwere und ein Bericht zum Patch-Stand mit Datum (höchstens 12 Monate).		
19	Werden unsere Daten bei Übertragung und Speicherung nach dem Stand der Technik verschlüsselt? Art. 21 Abs. 2 lit. h NIS2 · Grundfrage	Kryptografie-Richtlinie mit Verfahren für Übertragung und Speicherung und Freigabedatum (höchstens 24 Monate).		
20	Werden die eingesetzten Systeme in einem Bestandsverzeichnis geführt und Konfigurationen kontrolliert geändert? Art. 21 Abs. 2 lit. i NIS2 · Standardfrage	Screenshot des Inventars oder des Änderungsprozesses mit Datum (höchstens 12 Monate).		
21	Setzen Sie grundlegende Cyberhygiene um (Härtung, sichere Passwörter, Schutz der Endgeräte, sichere Konfiguration)? Art. 21 Abs. 2 lit. g NIS2 · Standardfrage	Richtlinie zu Härtung, Passwörtern und Endgeräten mit Freigabedatum (höchstens 24 Monate).		
22	Verfolgen Sie Warnungen von BSI, CERTs oder Herstellern und handeln Sie danach? Art. 21 Abs. 2 lit. b NIS2 · Erweiterte Frage	Kein Dokument nötig. Nennen Sie die Quellen im Antworttext.		

Produkt- und Entwicklungssicherheit

Nr.	Frage	Passender Nachweis	Antwort	Nachweis / Anmerkung
23	Wenden Sie Grundsätze sicherer Entwicklung an, wenn Sie Software oder Systeme für uns entwickeln oder anpassen? Art. 21 Abs. 2 lit. e NIS2; Art. 21 Abs. 3 NIS2 · Standardfrage	Richtlinie für sichere Entwicklung mit Freigabedatum (höchstens 24 Monate).		

Kontinuität und Backup

Nr.	Frage	Passender Nachweis	Antwort	Nachweis / Anmerkung
24	Gibt es ein Notfall- und Wiederanlaufkonzept speziell für die Leistung an uns? Art. 21 Abs. 2 lit. c NIS2 · Grundfrage	Notfall- oder Wiederanlaufplan für die konkrete Leistung, Version und Datum (höchstens 24 Monate).		
25	Sind Verfügbarkeit, maximale Ausfallzeit und maximaler Datenverlust Ihrer Leistung vertraglich festgelegt? Art. 21 Abs. 2 lit. c NIS2 · Standardfrage	SLA-Auszug mit Verfügbarkeit, Wiederanlaufzeit und maximalem Datenverlust.		
26	Gibt es einen gesicherten Ersatzweg zur Kommunikation mit uns im Notfall (zum Beispiel wenn E-Mail ausfällt)? Art. 21 Abs. 2 lit. j NIS2 · Erweiterte Frage	Notfallkommunikationsplan mit Ersatzweg und Datum (höchstens 24 Monate).		
27	Unterstützen Sie uns beim Ausstieg (Datenübergabe in einem gängigen Format, Übergangsfrist, Hilfe beim Wechsel)? Art. 21 Abs. 2 lit. d NIS2 · Erweiterte Frage	Vertragsklausel zu Ausstieg, Datenformat und Übergangsfrist.		

Eigene Lieferkette

Nr.	Frage	Passender Nachweis	Antwort	Nachweis / Anmerkung
28	Bewerten Sie die Sicherheit Ihrer eigenen kritischen Lieferanten und Dienstleister? Art. 21 Abs. 2 lit. d NIS2; Art. 21 Abs. 3 NIS2 · Grundfrage	Bericht oder Auszug der eigenen Lieferantenbewertung mit Datum (höchstens 12 Monate).		
29	Kündigen Sie einen Wechsel wichtiger Unterauftragnehmer vorher an, mit der Möglichkeit für uns zu widersprechen? Art. 21 Abs. 2 lit. d NIS2 · Standardfrage	Vertragsklausel mit Ankündigungsfrist und Widerspruchsrecht.		
30	Achten Sie bei der Beschaffung eigener IT (Hardware, Software, Cloud) auf Sicherheitsanforderungen? Art. 21 Abs. 2 lit. e NIS2 · Erweiterte Frage	Beschaffungsrichtlinie mit Sicherheitsanforderungen und Freigabedatum (höchstens 24 Monate).		

Nr.	Frage	Passender Nachweis	Antwort	Nachweis / Anmerkung
31	Aus welchen Ländern und von welchen wesentlichen Herstellern oder Rechenzentren stammt Ihre Leistung? Art. 22 NIS2; § 41 BSIG · Erweiterte Frage	Kein Dokument nötig. Nennen Sie Länder und wesentliche Anbieter im Antworttext.		

Über diese Vorlage

Vorlagenversion 2026-11-3-b177c545
Stand der Inhalte 01.11.2026
Herausgeber Erstellt mit Complass, https://complass.eu

Rechtsgrundlage (Stand): Art. 21 Abs. 2 lit. d NIS2; § 30 Abs. 2 Nr. 4 BSIG

Diese Vorlage ist keine Rechtsberatung. Sie ersetzt nicht die Prüfung, welche Anforderungen für Ihr Unternehmen gelten, und garantiert kein Prüfungs- oder Zertifizierungsergebnis.

Lizenz: Creative Commons Namensnennung 4.0 International (CC BY 4.0). Sie dürfen die Vorlage verwenden, ändern und weitergeben, auch kommerziell, wenn Sie die Quelle nennen. Namensnennung: „Vorlage: Complass (complass.eu), CC BY 4.0“. https://creativecommons.org/licenses/by/4.0/deed.de