

Sind wir alle von NIS2 betroffen?

Lieferketten im Fokus

...und betrifft mich NIS2 jetzt?

...und betrifft mich NIS2 jetzt?

Ja, wenn...

...Sie für ein Unternehmen arbeiten, das direkt von NIS2 als „wesentliche“ oder „wichtige“ Einrichtung eingestuft wird.

- Das wird in Österreich 4.000-9.000 meist mittlere und große Organisationen betreffen.
- Diese Unternehmen müssen neben der eigenen Cybersicherheit auch jene ihrer Lieferanten sicherstellen
- Sie benötigen – unter anderem - ein „Third Party Cyber Risk Management“

...und betrifft mich NIS2 jetzt?

Ja, wenn...

...Sie für ein Unternehmen arbeiten, das direkt von NIS2 als „wesentliche“ oder „wichtige“ Einrichtung eingestuft wird.

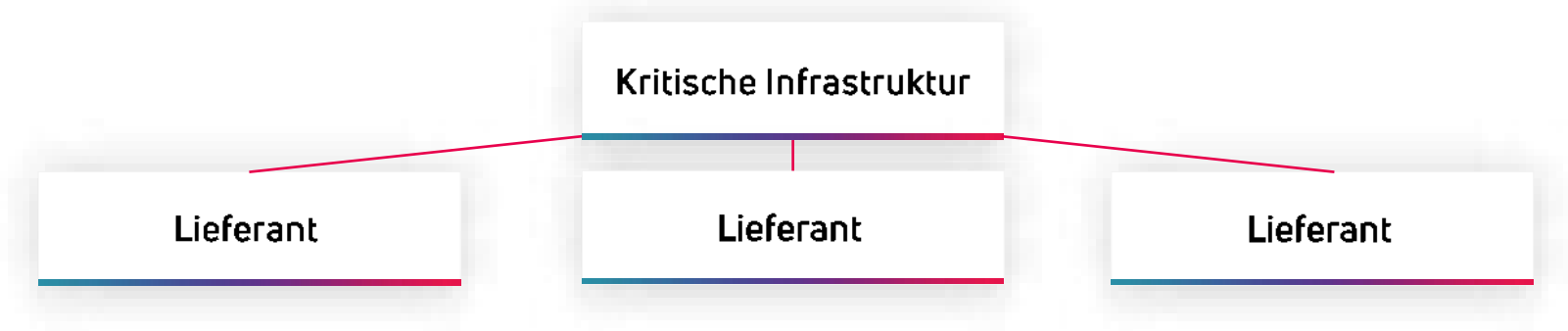
- Das wird in Österreich 4.000-9.000 meist mittlere und große Organisationen betreffen.
- Diese Unternehmen müssen neben der eigenen Cybersicherheit auch jene ihrer Lieferanten sicherstellen
- Sie benötigen – unter anderem - ein „Third Party Cyber Risk Management“

...eine dieser 4.000 bis 9.000 Organisationen Ihr Kunde ist.

- Das wird 65.000-100.000 österreichische Lieferanten betreffen.
- Ihre Kunden werden NIS2 Pflichten schlicht an Sie - ihren Lieferanten – vertraglich übertragen.
- Ihre Kunden werden aus Haftungsgründen einen Nachweis für Cybersicherheit von Ihnen - ihrem Lieferanten - verlangen.

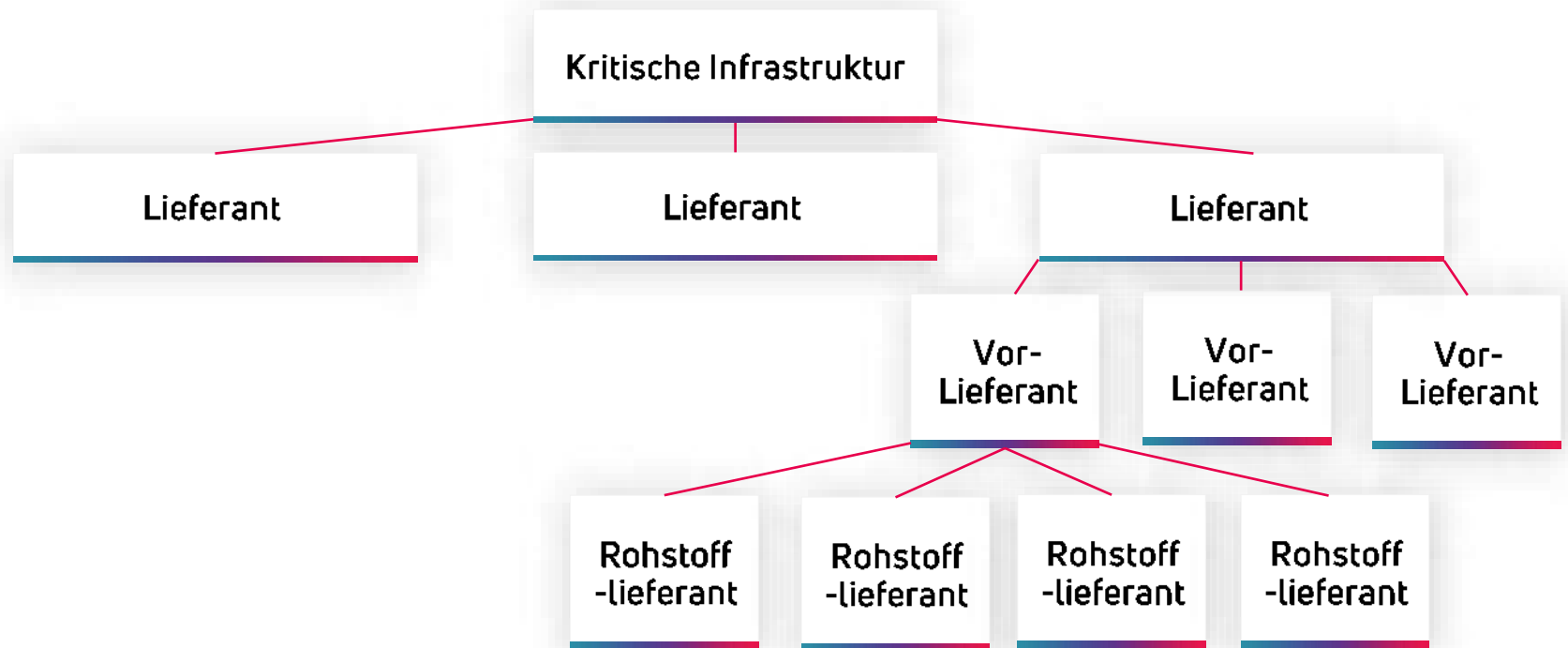
Lieferketten-Baum

Eines der über 4.000 NIS2 Unternehmen ist Ihr Kunde.



Lieferketten-Baum

Eines der über 4.000 NIS2 Unternehmen ist Ihr Kunde.



NIS2 betrifft alle Unternehmen.

Eines der über 4.000 NIS2 Unternehmen ist Ihr Kunde.

1.200

Großunternehmen

5.900

Mittlere Unternehmen

360.000

Kleinst- und
Kleinunternehmen

NIS2 betrifft alle Unternehmen.

Eines der über 4.000 NIS2 Unternehmen ist ihr Kunde.

Das bedeutet:

Mehr als die Hälfte (~56%) der Groß- und Mittelunternehmen wird direkt von NIS2 erfasst werden.

(Annahme: 4.000 von 7.100)

Aber auch:

360.000 Klein- und Kleinstunternehmen liefern oft an größere Unternehmen und haben meist kein:

- Cybersicherheitspersonal
- Cybersicherheitsbudget
- Cybersicherheitszertifikat
- passendes Angebot an finanzierbaren Produkten und Services, um Cybersicherheit zu erhöhen

Folgen bei Nicht-Einhaltung

Bei Nicht-Einhaltung drohen Folgen.

**Bis zu 10
Mio.**

Euro Bußgelder

**Persönliche
Haftung**

Leitender Angestellter

Verlust

von Aufträgen

Zwischenfrage:

Fallen Sie unter NIS2?

- Ja, NIS2 betrifft mich direkt.
- Ja, ich bin Lieferant.
- Nein.
- Keine Angabe.

Noch unsicher?

<https://ratgeber.wko.at/nis2/>

Was benötigen Sie von Ihren
Lieferanten?

Cybersicherheitsnachweis

Von den über 4.000 österreichischen NIS Unternehmen wird ein professionelles Cyberrisiko Management für Dienstleister, Lieferanten und Dritte gefordert.

Das bedeutet:

- Die NIS-Verordnungen machen es notwendig, die Cybersicherheit Ihrer Lieferanten gegenüber Ihrem Unternehmen mithilfe eines Nachweises zu belegen.
- Umgekehrt müssen NIS Unternehmen alle Sicherheitsnachweise ihrer Lieferanten dokumentieren.
- Liegt kein Sicherheitsnachweis vor, sollte dieser beim Lieferanten aufgefordert oder für den Lieferanten beauftragt werden.

CyberRisk Manager

Der CyberRisk Manager

Die Plattform für ein effizientes Cyberrisiko-Management von Lieferanten nach NIS

Kostenlose Basisversion:

1. Abdeckung aller Lieferanten mit dem WebRisk-Score

The screenshot displays the 'CyberRisk Ratings Ihrer Lieferanten' interface. On the left is a dark sidebar with navigation options: Dashboard, VALIDIERUNG, Validierung, CYBERRISK RATING, Assessment, **CyberRisk Ratings**, Datenschutzmodul, RISIKOMINIMIERUNG, Aufgaben, Risikomatrix, Maßnahmen, DATEN VERWALTEN, and Accountdetails. The main content area shows a table of suppliers with columns for Risiko, Unternehmen, WebRisk, B-Rating, A-Rating, verfügbar bis, DSGVO, and Aktionen. A red box highlights the WebRisk scores for all five suppliers.

Risiko	Unternehmen	WebRisk	B-Rating	A-Rating	verfügbar bis	DSGVO	Aktionen
▲	Lieferant 1	120			-	DSGVO	☰
▲	Lieferant 2	213	100 B	125 A+	20. Januar 2024	DSGVO	☰
▲	Lieferant 3	175	128 B	116 A+	08. Juni 2024	DSGVO	☰
▲	Lieferant 4	112			-	DSGVO	☰
▲	Lieferant 5	127	100 B		01. April 2024	DSGVO	☰

Der CyberRisk Manager

Die Plattform für ein effizientes Cyberrisiko-Management von Lieferanten nach NIS

Kostenlose Basisversion:

1. Abdeckung aller Lieferanten mit dem WebRisk-Score
2. Anzeige von vorhandenen Gütesiegeln und Zertifizierungen

The screenshot displays the 'CyberRisk Ratings Ihrer Lieferanten' interface. On the left is a dark sidebar with navigation options: Dashboard, VALIDIERUNG, Validierung, CYBERRISK RATING, Assessment, **CyberRisk Ratings** (highlighted), Datenschutzmodul, RISIKOMINIMIERUNG, Aufgaben, Risikomatrix, Maßnahmen, DATEN VERWALTEN, and Accountdetails. The main content area shows a table of suppliers with columns for Risiko, Unternehmen, WebRisk, B-Rating, A-Rating, verfügbar bis, DSGVO, and Aktionen. The 'Lieferant 3' row is highlighted with a red border. The interface includes a search bar, filters for A-Rating and B-Rating, and a 'DATEN EXPORTIEREN' button.

Risiko	Unternehmen	WebRisk	B-Rating	A-Rating	verfügbar bis	DSGVO	Aktionen
▲	Lieferant 1	120			-	DSGVO	☰
▲	Lieferant 2	213	100 B	125 A+	20. Januar 2024	DSGVO	☰
▲	Lieferant 3	175	128 B	116 A+	08. Juni 2024	DSGVO	☰
▲	Lieferant 4	112			-	DSGVO	☰
▲	Lieferant 5	127	100 B		01. April 2024	DSGVO	☰

Der CyberRisk Manager

Die Plattform für ein effizientes Cyberrisiko-Management von Lieferanten nach NIS

Kostenlose Basisversion:

1. Abdeckung aller Lieferanten mit dem WebRisk-Score
2. Anzeige von vorhandenen Gütesiegeln und Zertifizierungen
3. Anzeige von ISO27001 Nachweisen, die von Lieferanten hinterlegt wurden

The screenshot displays the 'CyberRisk Ratings Ihrer Lieferanten' interface. On the left is a dark sidebar with navigation options: Dashboard, VALIDIERUNG, Validierung, CYBERRISK RATING, Assessment, CyberRisk Ratings (highlighted), Datenschutzmodul, RISIKOMINIMIERUNG, Aufgaben, Risikomatrix, Maßnahmen, DATEN VERWALTEN, and Accountdetails. The main content area shows a table of suppliers with columns for Risiko, Unternehmen, WebRisk, B-Rating, A-Rating, verfügbar bis, DSGVO, and Aktionen. Supplier 1 is highlighted with a red box. Supplier 2 has a B-Rating of 100 B and an A-Rating of 125 A+. Supplier 3 has a B-Rating of 128 B and an A-Rating of 116 A+. Supplier 4 has a B-Rating of 112. Supplier 5 has a B-Rating of 127. A 'RATING ANFORDERN' button is visible for Supplier 1 and Supplier 4.

Risiko	Unternehmen	WebRisk	B-Rating	A-Rating	verfügbar bis	DSGVO	Aktionen
▲	Lieferant 1	120			-	DSGVO	☰
▲	Lieferant 2	213	100 B	125 A+	20. Januar 2024	DSGVO	☰
▲	Lieferant 3	175	128 B	116 A+	08. Juni 2024	DSGVO	☰
▲	Lieferant 4	112			-	DSGVO	☰
▲	Lieferant 5	127	100 B		01. April 2024	DSGVO	☰

Der CyberRisk Manager

Die Plattform für ein effizientes Cyberrisiko-Management von Lieferanten nach NIS

Kostenlose Basisversion:

1. Abdeckung aller Lieferanten mit dem WebRisk-Score
2. Anzeige von vorhandenen Gütesiegeln und Zertifizierungen
3. Anzeige von ISO27001 Nachweisen, die von Lieferanten hinterlegt wurden
4. Eintragung der eigenen Risikoeinschätzung

The screenshot displays the 'CyberRisk Ratings Ihrer Lieferanten' dashboard. On the left is a dark sidebar with navigation options: Dashboard, VALIDIERUNG, Validierung, CYBERRISK RATING, Assessment, CyberRisk Ratings (highlighted), Datenschutzmodul, RISIKOMINIMIERUNG, Aufgaben, Risikomatrix, Maßnahmen, DATEN VERWALTEN, and Accountdetails. The main content area shows a table of suppliers with columns for Unternehmen, WebRisk, B-Rating, A-Rating, verfügbar bis, DSGVO, and Aktionen. A vertical red box highlights the 'Risiko' column, which contains colored triangles indicating risk levels: red for Lieferant 1, orange for Lieferant 2, yellow for Lieferant 3, yellow for Lieferant 4, and green for Lieferant 5. The table data is as follows:

Unternehmen	WebRisk	B-Rating	A-Rating	verfügbar bis	DSGVO	Aktionen
Lieferant 1	120			-		
Lieferant 2	213	100 B	125 A+	20. Januar 2024		
Lieferant 3	175	128 B	116 A+	08. Juni 2024		
Lieferant 4	112			-		
Lieferant 5	127	100 B		01. April 2024		

Der CyberRisk Manager

Die Plattform für ein effizientes Cyberrisiko-Management von Lieferanten nach NIS

Kostenlose Basisversion:

1. Abdeckung aller Lieferanten mit dem WebRisk-Score
2. Anzeige von vorhandenen Gütesiegeln und Zertifizierungen
3. Anzeige von ISO27001 Nachweisen, die von Lieferanten hinterlegt wurden
4. Eintragung der eigenen Risikoeinschätzung
5. Hinterlegung einer Maßnahmenmatrix

The screenshot displays the CyberRisk Manager interface. On the left is a dark sidebar with navigation options: Dashboard, VALIDIERUNG, Validierung, CYBERRISK RATING, Assessment, CyberRisk Ratings (highlighted), Datenschutzmodul, Aufgaben, Risikomatrix (highlighted), Maßnahmen, DATEN VERWALTEN, and Accountdetails. The main area is titled 'CyberRisk Ratings Ihrer Lieferanten' and features a search bar, filters for 'A-Rating' and 'B-Rating', and a 'DATEN EXPORTIEREN' button. Below is a table of supplier ratings with columns for Risiko, Unternehmen, WebRisk, B-Rating, A-Rating, verfügbar bis, DSGVO, and Aktionen. The table lists five suppliers with their respective risk levels and ratings.

Risiko	Unternehmen	WebRisk	B-Rating	A-Rating	verfügbar bis	DSGVO	Aktionen
▲	Lieferant 1	120	RATING ANFORDERN	-	-	DSGVO	☰
▲	Lieferant 2	213	100 B	125 A+	20. Januar 2024	DSGVO	☰
▲	Lieferant 3	175	128 B	116 A+	08. Juni 2024	DSGVO	☰
▲	Lieferant 4	112	RATING ANFORDERN	-	-	DSGVO	☰
▲	Lieferant 5	127	100 B	-	01. April 2024	DSGVO	☰

Der CyberRisk Manager

Die Plattform für ein effizientes Cyberrisiko-Management von Lieferanten nach NIS

Kostenlose Basisversion:

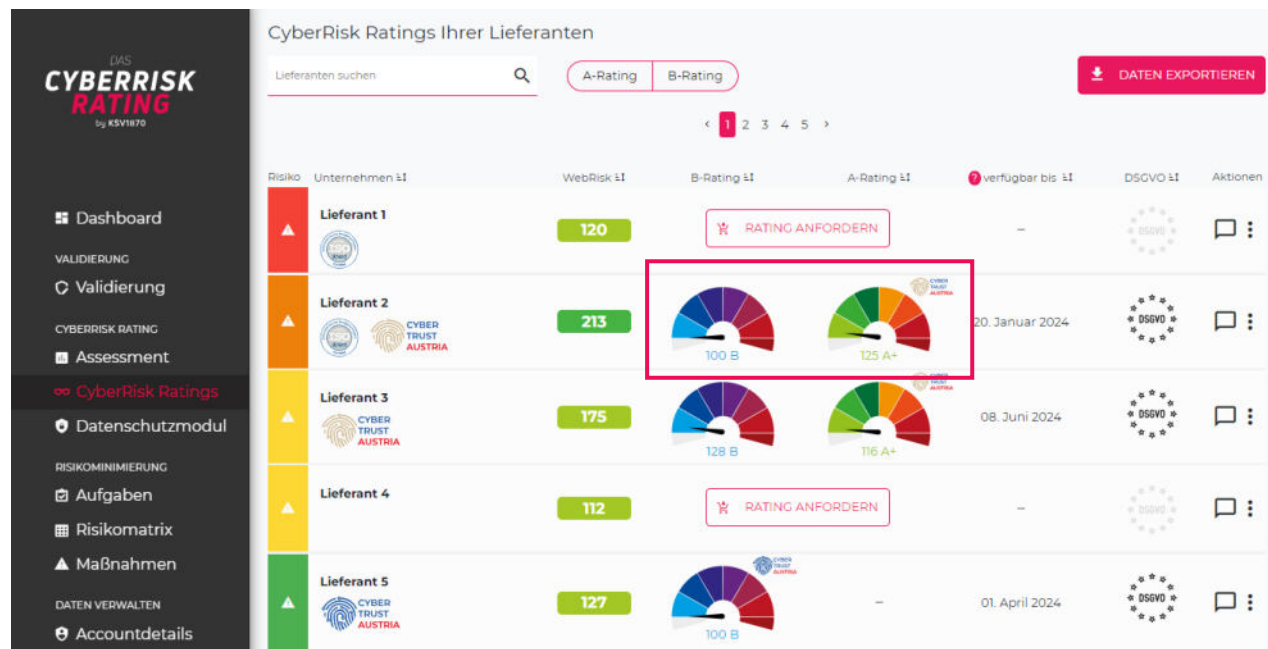
1. Abdeckung aller Lieferanten mit dem WebRisk-Score
2. Anzeige von vorhandenen Gütesiegeln und Zertifizierungen
3. Anzeige von ISO27001 Nachweisen, die von Lieferanten hinterlegt wurden
4. Eintragung der eigenen Risikoeinschätzung
5. Hinterlegung einer Maßnahmenmatrix
6. DSGVO Modul

The screenshot displays the 'CyberRisk Ratings Ihrer Lieferanten' (CyberRisk Ratings of your Suppliers) interface. On the left is a dark sidebar with navigation options: Dashboard, VALIDIERUNG, Validierung, CYBERRISK RATING, Assessment, CyberRisk Ratings (selected), Datenschutzmodul, RISIKOMINIMIERUNG, Aufgaben, Risikomatrix, Maßnahmen, DATEN VERWALTEN, and Accountdetails. The main content area shows a table of suppliers with columns for Risiko, Unternehmen, WebRisk, B-Rating, A-Rating, verfügbar bis, DSGVO, and Aktionen. The table lists five suppliers (Lieferant 1 to 5) with their respective risk levels (indicated by colored triangles), WebRisk scores (e.g., 120, 213, 175, 112, 127), and B-Rating/A-Rating scores (e.g., 100 B, 125 A+, 128 B, 116 A+, 100 B). The DSGVO column shows compliance status with a 'DSGVO' icon, and the 'Aktionen' column includes a 'RATING ANFORDERN' button for some suppliers. A red box highlights the 'DSGVO' icon for Lieferant 2.

Risiko	Unternehmen	WebRisk	B-Rating	A-Rating	verfügbar bis	DSGVO	Aktionen
▲	Lieferant 1	120	100 B	-	-	DSGVO	⋮
▲	Lieferant 2	213	100 B	125 A+	20. Januar 2024	DSGVO	⋮
▲	Lieferant 3	175	128 B	116 A+	08. Juni 2024	DSGVO	⋮
▲	Lieferant 4	112	-	-	-	DSGVO	⋮
▲	Lieferant 5	127	100 B	-	01. April 2024	DSGVO	⋮

Der CyberRisk Manager

Die Plattform für ein effizientes Cyberrisiko-Management von Lieferanten nach NIS



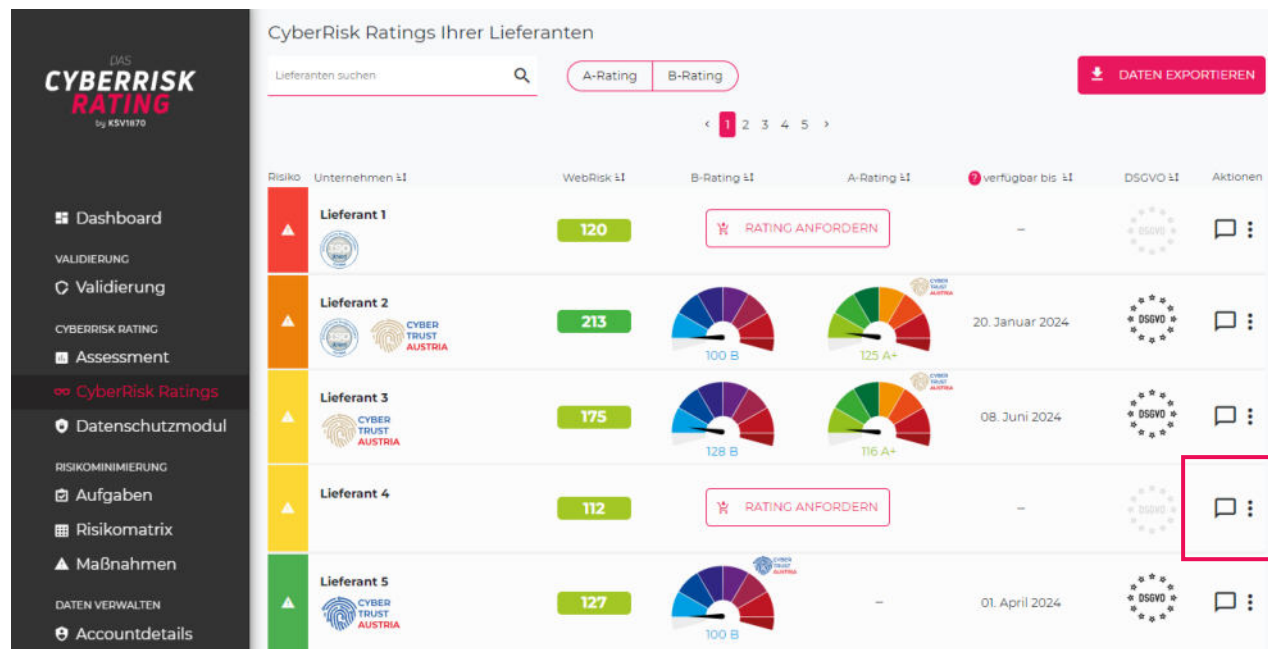
Bezahlte Zusatzservices:

7. Erstellung von Einzel-Ratings für beliebige Lieferanten

- „Basis“ B-Ratings für KMU
 - „Advanced“ A-Ratings für Hochrisiko-Lieferanten
- Right to Audit für Ratingangaben
 - API-Integration und Prozessautomatisierung in bestehende Lieferantenverwaltung

Der CyberRisk Manager

Die Plattform für ein effizientes Cyberrisiko-Management von Lieferanten nach NIS



Bezahlte Zusatzservices:

7. Erstellung von Einzel-Ratings für beliebige Lieferanten

- „Basis“ B-Ratings für KMU
- „Advanced“ A-Ratings für Hochrisiko-Lieferanten

- Right to Audit für Ratingangaben
- API-Integration und Prozessautomatisierung in bestehende Lieferantenverwaltung
- Direkte Kontaktierung des IT-Sicherheitsansprechpartners beim Lieferanten
- Eigene Zusatzmodule möglich
- Quartalsweiser Review

Wie kann ich die NIS2-
Konformität als Lieferant
nachweisen?

Das CyberRisk Rating Ökosystem



NIS2 - konkrete Hilfestellungen

Um die Anforderungen von NIS2 für Lieferantenmanagement zu erfüllen, gibt es mehrere Möglichkeiten.

Von NIS-Behörden empfohlene Standards:

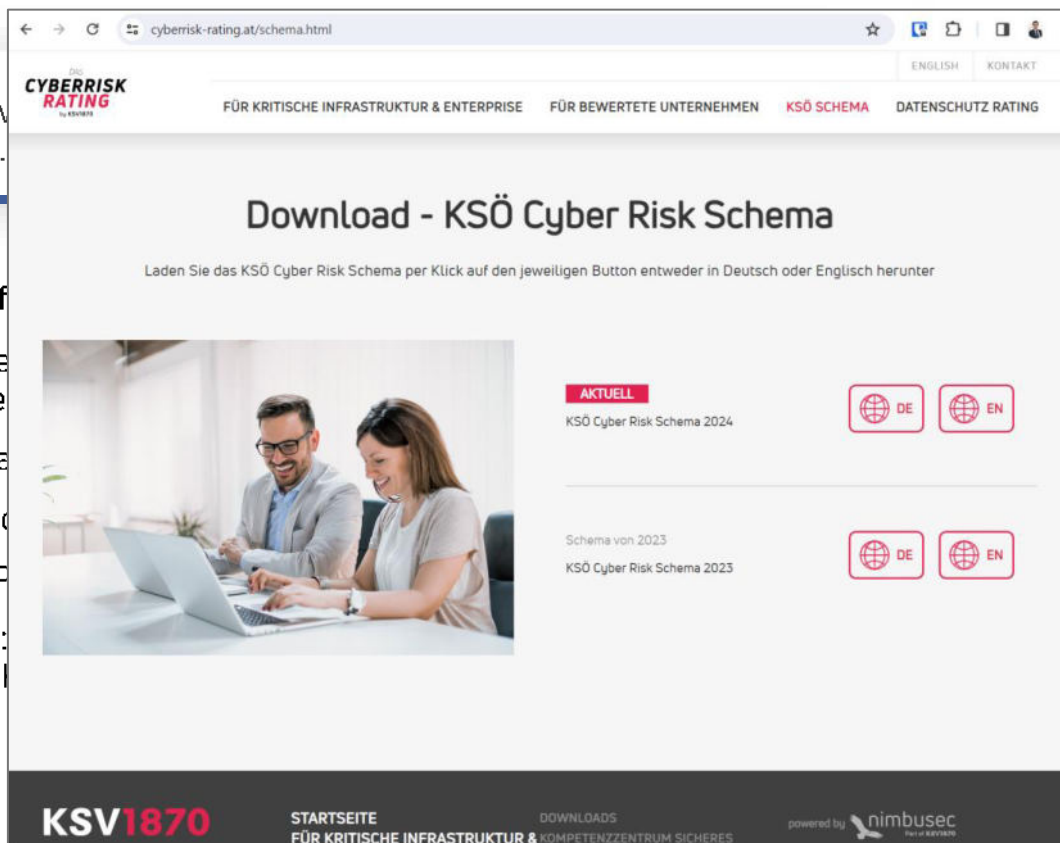
- ÖISHB: Zusammenarbeit mit Externen, Evaluierung von Zertifizierungen, Lieferantenbeziehungen
- ISO/IEC 27001: Information security in supplier relationships
- IEC 62443 2-1: Supply chain security
- CIS CSC v8.0: Service Provider Management
- KSÖ Cyber Risk Rating: Einheitliche, kostenlose Mindeststandards des KSÖ -> Basis für das CyberRisk Rating

NIS2 - konkrete Hilfestellungen

Um die Anforderungen von NIS2 zu erfüllen, gibt es mehrere Möglichkeiten.

Von NIS-Behörden empfohlen:

- ÖISHB: Zusammenarbeit mit Lieferantenbeziehungen
- ISO/IEC 27001: Informationssicherheitsmanagement
- IEC 62443 2-1: Supply Chain Security
- CIS CSC v8.0: Service Provider Security
- KSÖ Cyber Risk Rating: Mindeststandards des Bundes



The screenshot shows a web browser at the URL `cyberrisk-rating.at/schema.html`. The page header includes the logo for "THE CYBERRISK RATING by REVIEWS" and navigation links for "ENGLISH" and "KONTAKT". Below the header, there are three main categories: "FÜR KRITISCHE INFRASTRUKTUR & ENTERPRISE", "FÜR BEWERTETE UNTERNEHMEN", and "KSÖ SCHEMA" (which is highlighted). The main heading is "Download - KSÖ Cyber Risk Schema". Below this, a text instruction reads: "Laden Sie das KSÖ Cyber Risk Schema per Klick auf den jeweiligen Button entweder in Deutsch oder Englisch herunter". There are two sections of download buttons. The first section is labeled "AKTUELL" and "KSÖ Cyber Risk Schema 2024", with buttons for "DE" and "EN". The second section is labeled "Schema von 2023" and "KSÖ Cyber Risk Schema 2023", also with buttons for "DE" and "EN". On the left side of the page, there is an image of a man and a woman working together at a laptop. The footer contains the logo "KSV1870", the text "STARTSEITE FÜR KRITISCHE INFRASTRUKTUR & KOMPETENZZENTRUM SICHERES", the word "DOWNLOADS", and the logo "powered by nimbusec".

NIS2 -

Um die Anforderung
mehrere Mögli

Von NIS-Behörde

- ÖISHB: Zusammenarbeiten mit Lieferantenbetreibern
- ISO/IEC 27001
- IEC 62443 2-1
- CIS CSC v8.0: Cyber Security Checklist
- KSÖ Cyber Risikoanalyse: Mindeststandard

The screenshot shows a web browser displaying a page from WKO (Wirtschaftskammer Österreich) titled "Basismaßnahmen für Informationssicherheit im Unternehmen". The page content includes a sub-header "Informationssicherheit ist die Voraussetzung für eine erfolgreiche Digitalisierung und nachhaltigen Erfolg im Unternehmen.", a reading time of "1 Minute", and a date of "26.02.2024". The main text discusses challenges for small and medium enterprises in cybersecurity, such as low awareness and high costs, and offers a baseline security checklist. A list of four measures for compliance is provided at the bottom. On the right, there is a "Kontakt" section for "Innovationsmanagement" with contact details for Linz, Austria, and a "Links" section. A social media sharing bar is visible below the article text.

WKO

Kontakt Anmelden

Transforma... Digitalisierung Startups Innovation Oberösterreich

Basismaßnahmen für Informationssicherheit im Unternehmen

Informationssicherheit ist die Voraussetzung für eine erfolgreiche Digitalisierung und nachhaltigen Erfolg im Unternehmen.

Lesedauer: 1 Minute

26.02.2024

Viele kleine und mittlere Unternehmen stehen vor besonderen Herausforderungen im Bereich der Cybersicherheit, wie z. B. geringes Bewusstsein für Gefahren und wenig Fachkompetenz im Betrieb im Bereich Cybersicherheit, hohe Kosten für Cybersicherheitslösungen und ein hohes Maß an Bedrohungen, wie z. B. Ransomware.

Die meisten Angriffe können jedoch mit grundlegenden Maßnahmen erfolgreich abgewehrt werden. Die Baseline Security stellt Tools zur Verfügung um diese Mindestmaßnahmen auch in kleinen und mittleren Unternehmen mit einfachen Schritten implementieren zu können.

Ein Unternehmen, das die Basissicherheitsmaßnahmen erfüllt,

1. hat sich mit Informationssicherheit beschäftigt und eine Richtlinie für das eigene Unternehmen erlassen ([Muster: Sicherheitsrichtlinie](#))
2. schult seine Mitarbeiter regelmäßig in Informationssicherheit ([Muster: MA-Schulung](#))
3. hat einen oder mehrere zuständige Ansprechpartner für Informationssicherheit ([Liste Ausbildungen/Personenzertifizierungen](#));
4. hat ein aktuelles Verzeichnis seiner Geräte und Anwendungen

Kontakt

Innovationsmanagement

Hessenplatz 3
4020 Linz, Österreich

+43 5 90909
innovation@wkoee.at

Detaillierte Kontaktseite >

Links

CyberRisk Rating

Das CyberRisk Rating

Der Cybersicherheitsnachweis für Lieferanten der mehr als 4000 NIS2 Unternehmen in Österreich

B1

CYBERRISK RATING | GOVERNANCE & ÖKOLOGISCHES SICHERHEITSRICHTLINIE

Haben Sie eine aktuelle Informationssicherheitsrichtlinie (bzw. IT-Sicherheitsrichtlinie), die für Ihr Unternehmen gültig ist?

Anforderungskriterien

Die Informationssicherheitsrichtlinie muss die wesentlichen Anforderungen an Informationssicherheit abdecken (alle Kernthemen müssen - sofern sie anwendbar sind - in dieser Richtlinie beschrieben werden) und sollte auf ein bestehendes Regelwerk aufbauen (zB. ISO 27001/27002, NIST 800, IT Grundschutz, IT-Sicherheitshandbuch der WKÖ, u.ä.). Die Richtlinie muss von der Geschäftsführung freigegeben und für alle Mitarbeiter verfügbar sein.

Evidenzen

- Dokument muss vorhanden sein und die letzte Überprüfung darf nicht länger als zwei Jahre zurückliegen.

Schemaänderungen anzeigen

Wie setzen Sie diese Maßnahme in Ihrer Organisation um?

B / Antwortlänge 0 von 3000

Unternehmen in Österreich

Basismaßnahmen für Informationssicherheit im Unternehmen



Informationssicherheit ist die Voraussetzung für eine erfolgreiche Digitalisierung und nachhaltigen Erfolg im Unternehmen.

Lesedauer: 1 Minute

26.02.2024



Viele kleine und mittlere Unternehmen stehen vor besonderen Herausforderungen im Bereich der Cybersicherheit, wie z. B. geringes Bewusstsein für Gefahren und wenig Fachkompetenz im Betrieb im Bereich Cybersicherheit, hohe Kosten für Cybersicherheitslösungen und ein hohes Maß an Bedrohungen, wie z. B. Ransomware.

Die meisten Angriffe können jedoch mit grundlegenden Maßnahmen erfolgreich abgewehrt werden. Die Baseline Security stellt Tools zur Verfügung um diese Mindestmaßnahmen auch in kleinen und mittleren Unternehmen mit einfachen Schritten implementieren zu können.

Ein Unternehmen, das die Basissicherheitsmaßnahmen erfüllt,

1. hat sich mit Informationssicherheit beschäftigt und eine Richtlinie für das eigene Unternehmen erlassen ([Muster-Sicherheitsrichtlinie](#))
2. schult seine Mitarbeiter regelmäßig in Informationssicherheit ([Muster-MA-Schulung](#))
3. hat einen oder mehrere zuständige Ansprechpartner für Informationssicherheit ([Liste Ausbildungen/Personenzertifizierungen](#)):
4. hat ein aktuelles Verzeichnis seiner Geräte und Anwendungen

Kontakt

Innovationsmanagement

Hessenplatz 3
4020 Linz, Österreich

+43 5 90909

innovation@wkoee.at

[Detaillierte Kontaktseite](#)

Links





Basissmaßnahmen Informationssicherheit Unternehmen

Informationssicherheit erfolgreiche Digitalisierung Unternehmen.

Lesedauer: 1 Minute

26.02.2024

Viele kleine und mittlere Unternehmen stehen vor B. geringes Bewusstsein für Gefahren und wenig Cybersecuritylösungen und ein hohes Maß an

Die meisten Angriffe können jedoch mit grundlegende stellt Tools zur Verfügung um diese Mindestmaßnahmen implementieren zu können.

Ein Unternehmen, das die Basissicherheitsmaßnahmen

1. hat sich mit Informationssicherheit beschäftigt [Sicherheitsrichtlinie](#)
2. schult seine Mitarbeiter regelmäßig in Inform
3. hat einen oder mehrere zuständige Ansprech [Ausbildungen/Personenzertifizierungen](#):
4. hat ein aktuelles Verzeichnis seiner Geräte u



eCall Projektverwaltung

Förderungen suchen.

- Thema -

- Zielgruppe -

- nationale Förderung
- internationale Förderung

Aktuelle Ausschreibungen

Förderungen und Services

Cyber Security Checks 2023



Ausschreibung offen von 16.10.2023 12:00 bis 15.04.2024 12:00

Programmeigentümer/Geldgeber



Cyber Security Checks unterstützen österreichische KMU, die zur Anwendung der Cybersicherheits-Richtlinie NIS2 verpflichtet sind, bei der Umsetzung von Cyber Security Maßnahmen zu NIS2 und sind eine Maßnahme des Nationalen Koordinierungszentrums für Cybersicherheit (NCC-AT), das das BKA in Kooperation mit der FFG leitet.

Die Ausschreibung wurde **bis 15.04.2024 (12:00 Uhr) verlängert**. Details entnehmen Sie dem Ausschreibungsleitfaden.



Basissmaßnahmen Informationssicherheit Unternehmen

Informationssicherheit erfolgreiche Digitalisierung Unternehmen.

Lesedauer: 1 Minute

26.02.2024

Viele kleine und mittlere Unternehmen stehen vor B. geringes Bewusstsein für Gefahren und wenig f Cybersicherheitslösungen und ein hohes Maß an B

Die meisten Angriffe können jedoch mit grundlegende stellt Tools zur Verfügung um diese Mindestmaßna Schritte implementieren zu können.

Ein Unternehmen, das die Basissicherheitsmaßna

1. hat sich mit Informationssicherheit beschäftige [Sicherheitsrichtlinie](#)
2. schult seine Mitarbeiter regelmäßig in Inform
3. hat einen oder mehrere zuständige Ansprech [Ausbildungen/Personenzertifizierungen](#));
4. hat ein aktuelles Verzeichnis seiner Geräte un

ffg.at/ausschreibung/CyberSecurityChecks2023

FFG Forschung.wirkt

Förderungen suchen

- Thema -

Cyber Security

Ausschreibung offen von

Programmeigentümer/

FFG Forschung.wirkt

NCC-AT Nationales Koordinier Cybericherheit

Info Kontakt Lin

Cyber Security Sch verpflichtet sind, b Koordinierungsz

Die Ausschre Sie dem Auss

kmudigital.at

KMU.DIGITAL

Beratungsförderung Umsetzungsförderung Services Infos für Berater:innen Über KMU.DIGITAL

Schützen Sie Ihr Unternehmen vor Hacker-Angriffen und Datenverlust!

KMU.DIGITAL fördert die individuelle Beratung österreichischer Klein- und Mittelbetriebe (KMU) durch zertifizierte Expert:innen zu den Themen Geschäftsmodelle und Prozesse (inkl. Ressourcenoptimierung), E-Commerce und Online-Marketing, IT- und Cybersecurity sowie Digitale Verwaltung. Gefördert wird anschließend auch die Umsetzung Ihrer Digitalisierungsprojekte mit Hilfe von Neuinvestitionen.

Die Digitalisierungsoffensive KMU.DIGITAL ist eine Initiative des Bundesministeriums für Arbeit und Wirtschaft (BMAW) in Kooperation mit der Wirtschaftskammer Österreich (WKÖ) und wird durch die Europäische Union refinanziert.

Derzeit können keine Anträge mehr für das KMU.DIGITAL Förderprogramm gestellt werden. An einer Neuauflage der Förderung ab 2024 wird gearbeitet. Bitte tragen Sie sich bei unserem [Infoservice](#) ein, um rechtzeitig über den Neustart der Antragsmöglichkeit benachrichtigt zu werden.

Das CyberRisk Rating DEMO

Der Cybersicherheitsnachweis für Lieferanten der mehr als 4000 NIS2 Unternehmen in Österreich

The screenshot shows a web browser at the URL `demo.cyberrisk-rating.at`. The page header includes the logo "DAS CYBERRISK RATING by KSV1970" and the text "Demo Assessment ohne Datenspeicherung und ohne Validierung". A red circle with "B1" is visible. The main heading reads "CYBERRISK RATING B1 - GOVERNANCE & ÖKOSYSTEM - SICHERHEITSRICHTLINIE". The central question is "Haben Sie eine aktuelle Informationssicherheitsrichtlinie (bzw. IT-Sicherheitsrichtlinie), die für Ihr Unternehmen gültig ist?". Below this are two red circular icons: one with a checkmark and one with an 'X'. The "Anforderungskriterien" section states that the policy must cover essential requirements and be based on standards like ISO 27001/27002, NIST 800, etc. The "Evidenzen" section lists that the document must be current and available to all employees. At the bottom, there are "ZURÜCK" and "WEITER" buttons.

Assessment Zusammenfassung

B **Basis Sicherheit**

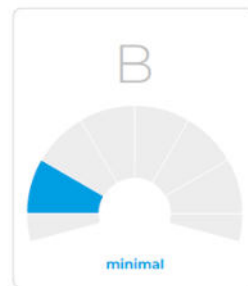
Das B-Rating definiert Anforderungen um ein grundlegendes Schutzniveau gegen Cyber Risiken gewährleisten zu können, welches für jede Organisation erreichbar sein sollte.

Grundlage für dieses Rating ist eine Selbstdeklaration der Organisation.

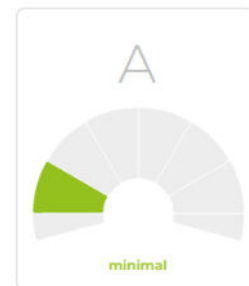
A **Erhöhte Sicherheit**

Das A-Rating definiert Anforderungen um ein erhöhtes Schutzniveau gegen Cyber Risiken gewährleisten zu können. Es richtet sich an Organisationen, an die, aufgrund ihres Tätigkeitsfeldes, erhöhte Sicherheitsstandards gestellt werden.

Grundlage für dieses Rating ist eine Selbstdeklaration der Organisation.



CYBERRISK RATING B



CYBERRISK RATING A

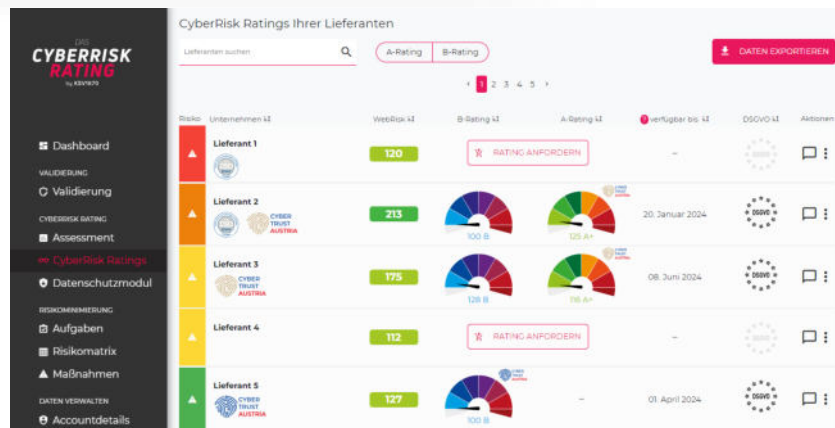


Nützliche Links

Demo durchführen: demo.cyberrisk-rating.at oder hier auf der Veranstaltung!

CyberRisk Rating bestellen: ksv.at/crr

Info-Paket & CyberRisk Manager anfordern: ksv.at/infopaket-cyberrisk-rating



Vielen Dank!

Alexander Mitter

Geschäftsführer KSV1870 Nimbusec GmbH

KSV1870 Nimbusec GmbH

Kaisergasse 16b

4020 Linz

T: +43 732 860 626

Mail: info@cyberrisk-rating.at

www.ksv.at/cyberrisk-rating