MUSTERBERICHT, GEKÜRZT

NIS2-Architektur-Check

Bericht zur vernetzten Architektur des Maschinenportals der Beispielwerk Maschinenbau GmbH

Auftraggeber	Beispielwerk Maschinenbau GmbH (fiktiv), Verpackungsmaschinen, rund 180 Mitarbeiter
Geprüfte Architektur	Maschinenportal als IoT-Plattform auf AWS (Produktion und Test), Fernwartung über ein Gateway je Maschine, Anbindung an das ERP (fiktiv)
Gebaut und betrieben von	Externer Dienstleister seit 2022 (fiktiv)
Stufe	NIS2-Architektur-Check, drei Wochen
Prüfer	Mark Joachim, tarienna GmbH
Stand	Oktober 2026, Gesetzesstand Oktober 2026

Dieser Bericht ist ein gekürztes Muster.

Auftraggeber, Architektur, Dienstleister und alle Feststellungen sind frei erfunden. Ähnlichkeiten mit bestehenden Unternehmen oder Systemen sind nicht beabsichtigt.

Der Bericht zeigt den Aufbau eines Berichts des NIS2-Architektur-Checks in Auszügen. Ein Bericht aus einem beauftragten Check enthält zu allen sieben Prüfpunkten sämtliche Feststellungen, die vollständige Gegenüberstellung und Maßnahmenliste, die Zusammenfassung der Befunde für Kundenfragebögen und alle offenen Fragen.

tarienna GmbH, Fallenbrunnen 14, 88045 Friedrichshafen
www.tarienna.eu/nis2-architektur-check/, Impressum unter www.tarienna.eu/impressum/

1 Gesamteinschätzung

Bewertung **Rot** Die Plattform läuft, aber Zugänge und Erkennung tragen nicht

Sektor und Größe sprechen für eine mögliche Einstufung als wichtige Einrichtung. Diese Plausibilisierung ersetzt keine rechtliche Einstufung, die Rechtsberatung klärt sie (Abschnitt 6). Das Maschinenportal selbst ist ordentlich gebaut. Die Gateways haben eigene Zertifikate, Updates sind signiert, und die Maschinen produzieren weiter, wenn die Cloud ausfällt.

Zwei Punkte tragen in der vorliegenden Form nicht. Der Dienstleister hält dauerhaft Administratorrechte ohne zweiten Faktor, alle Techniker teilen sich ein Fernwartungskonto, und die Schlüssel der Gateways liegen im Quellcode-Repository. Ein Angriff würde heute nicht erkannt, und niemand wüsste, wen er innerhalb von 24 Stunden zu informieren hätte. Beides ist in wenigen Tagen behoben (Abschnitt 5).

2 Ampelübersicht

Nr.	Prüfpunkt	Ampel	Kernaussage
1	Betroffenheit und Geltungsbereich	Gelb	Teilsektor Maschinenbau (Anlage 2 BSIG), Mitarbeiterzahl über der Schwelle. Tochtergesellschaft und Abgrenzung der Systeme sind offen.
2	Risiko und Übersicht	Gelb	Systemübersicht vorhanden, Datenflüsse der Fernwartung und zum ERP fehlen darin. Keine dokumentierte Risikoanalyse.
3	Identitäten und Zugänge	Rot	Administratorrechte ohne zweiten Faktor, geteiltes Fernwartungskonto, Schlüssel im Quellcode-Repository.
4	Erkennung und Meldefähigkeit	Rot	Protokolle ohne Alarm. Außerhalb der Arbeitszeit ist niemand zuständig, ein Meldeweg ist nicht festgelegt.
5	Betriebskontinuität	Gelb	Maschinen laufen ohne Cloud weiter. Backups täglich, Wiederherstellung nie geprobt.
6	Lieferkette und Dienstleister	Gelb	Vertrag ohne technische Sicherheitszusagen, Drittkomponente im Gateway seit zwei Jahren ohne Update, Kundenfragebogen unbeantwortet.
7	Vernetzte Produkte und Schnittstellen	Grün	Eigenes Zertifikat je Maschine, signierte und gestaffelte Updates, verschlüsselte Schnittstellen.

So ist die Ampel zu lesen

Grün	Kein wesentliches Risiko erkennbar.
Gelb	Es besteht ein Risiko, das sich mit überschaubarem Aufwand beheben lässt. Die Maßnahme steht in der Maßnahmenliste.
Rot	Es besteht ein wesentliches Risiko für den Betrieb oder die Meldefähigkeit. In der vorliegenden Form trägt dieser Punkt nicht.

So sind die Feststellungen gekennzeichnet

G	Geprüft. Ich habe die Aussage über den lesenden Zugang, mit einem Werkzeug von AWS, in einem Konfigurationsexport oder in den Unterlagen nachvollzogen.
A	Angabe. Die Aussage beruht auf dem Gespräch mit dem Auftraggeber oder dem Dienstleister und wurde nicht überprüft.

3 Die Prüfpunkte im Einzelnen (Auszug)

Dieser Musterbericht zeigt drei der sieben Prüfpunkte mit einer Auswahl der Feststellungen. Ein Bericht aus einem beauftragten Check enthält zu jedem Prüfpunkt alle Feststellungen, die Einordnung und die zugehörigen Maßnahmen. Die Prüfpunkte folgen den Maßnahmenbereichen des §30 BSIG, gelesen aus Sicht eines Architekten.

3.1 Betroffenheit und Geltungsbereich

Ist der Auftraggeber eine Einrichtung im Sinne des Gesetzes, und welche Systeme fallen darunter?

Bewertung Gelb

Feststellungen (Auszug)

- G Der Auftraggeber stellt Verpackungsmaschinen her und gehört damit zum verarbeitenden Gewerbe, Teilsektor Maschinenbau (Anlage 2 BSIG) (Handelsregisterauszug, Anlage 2 BSIG, Stand Oktober 2026).
- G Rund 180 Mitarbeiter und ein Jahresumsatz über 10 Millionen Euro liegen über den Schwellenwerten des §28 BSIG für wichtige Einrichtungen (Jahresabschluss 2025, Personalübersicht).
- A Eine Tochtergesellschaft in Österreich mit zwölf Mitarbeitern übernimmt den Service vor Ort und arbeitet im Maschinenportal. Ob sie bei der Einstufung mitzählt, ist nicht geklärt.

… Weitere Feststellungen sind im Musterbericht gekürzt.

Bedeutung für die Entscheidung

Sektor und Größe sprechen für eine mögliche Einstufung als wichtige Einrichtung. Die Einstufung ist eine technisch-organisatorische Plausibilisierung. Die verbindliche Einstufung und die Registrierung beim BSI nach §33 BSIG klärt der Auftraggeber mit seiner Rechtsberatung. Für den Check habe ich das Maschinenportal, die Gateways, die Fernwartung und die Schnittstelle zum ERP als betroffene Systeme abgegrenzt, weil sie den Service der Maschinen im Feld tragen. Die Büro-IT und das ERP selbst liegen außerhalb. Auch diese Abgrenzung gehört zur Rechtsberatung.

3.2 Risiko und Übersicht

Weiß der Auftraggeber, welche Systeme, Geräte und Datenflüsse es gibt, und welche davon geschäftskritisch sind?

Bewertung **Gelb**

… Feststellungen und Einordnung sind im Musterbericht gekürzt.

3.3 Identitäten und Zugänge

Wer kommt an die Plattform, die Maschinen und die Fernwartung heran, und würde es jemand merken?

Bewertung **Rot**

Feststellungen (Auszug)

- **G** Der Dienstleister nutzt im Produktions-Account dauerhaft eine Rolle mit Administratorrechten, ohne erzwungene Mehrfaktor-Anmeldung. Beim Auftraggeber gibt es keinen Nutzer mit diesen Rechten (Rechteübersicht, IAM Access Analyzer, Anmeldeeinstellungen).
- **G** Alle Servicetechniker nutzen für die Fernwartung dasselbe Konto mit einem gemeinsamen Passwort. Welche Person wann auf welche Maschine zugegriffen hat, lässt sich nicht nachvollziehen (Konfiguration des Fernwartungsdienstes, Zugriffsprotokolle).
- **G** Der Schlüssel, mit dem sich neue Gateways an der Plattform anmelden, und ein Zugangsschlüssel für den Datenspeicher liegen im Klartext in einer Konfigurationsdatei im Quellcode-Repository der Gateway-Software (Konfigurationsdateien im Repository).

… Weitere Feststellungen sind im Musterbericht gekürzt.

Bedeutung für die Entscheidung

Hier liegt das größte Risiko. Ein abgefangenes Passwort beim Dienstleister genügt, um die Plattform zu übernehmen, und der Auftraggeber könnte nicht selbst eingreifen, weil er kei-

ne eigenen Administratorrechte hat. Ein Techniker, der das Unternehmen verlässt, kennt das Fernwartungspasswort weiter, und niemand könnte seinen Zugriff von dem seiner Kollegen unterscheiden. Mit den Schlüsseln aus dem Repository ließe sich ein fremdes Gerät als Maschine des Auftraggebers anmelden. Alle drei Punkte sind in wenigen Tagen behoben. Der Dienstleister bleibt an Bord, nur nicht mehr als einziger Schlüsselhalter.

3.4 Erkennung und Meldefähigkeit

Würde der Auftraggeber einen Vorfall innerhalb von 24 Stunden erkennen und nach §32 BSIG melden können?

Bewertung **Rot**

... Feststellungen und Einordnung sind im Musterbericht gekürzt.

3.5 Betriebskontinuität

Läuft die Produktion weiter, wenn die Plattform ausfällt, und wie schnell ist sie wieder da?

Bewertung **Gelb**

... Feststellungen und Einordnung sind im Musterbericht gekürzt.

3.6 Lieferkette und Dienstleister

Welche Sicherheit sichern Dienstleister und Komponentenlieferanten technisch zu, und was davon lässt sich belegen?

Bewertung **Gelb**

Feststellungen (Auszug)

- **G** Der Vertrag mit dem Dienstleister regelt Verfügbarkeit und Reaktionszeiten. Technische Sicherheitszusagen zu Mehrfaktor-Anmeldung, Protokollierung, Updates oder der Meldung von Vorfällen enthält er nicht (Vertrag, nur auf technische Zusagen gelesen).
- **G** Die Fernwartungskomponente im Gateway stammt von einem Drittanbieter und läuft seit zwei Jahren in derselben Version, obwohl der Anbieter seitdem Sicherheitskorrekturen veröffentlicht hat. Einen Prozess, der solche Updates auf die Gateways bringt, gibt es nicht (Softwarestand im Portal, Veröffentlichungen des Anbieters).
- **A** Ein Kunde aus der Automobilzulieferung hat im Sommer 2026 einen Sicherheitsfragebogen mit rund 60 Fragen geschickt. Er ist unbeantwortet, weil niemand weiß, wer die Fragen zu Zugängen, Backup und Vorfallmeldung beantworten kann.

... Weitere Feststellungen sind im Musterbericht gekürzt.

Bedeutung für die Entscheidung

Der Auftraggeber ist selbst Teil der Lieferkette seiner Kunden. Der offene Fragebogen zeigt, dass er seine Sicherheit heute nicht belegen kann, obwohl ein Teil der Antworten nach diesem Check vorliegt. Die Zusammenfassung der Befunde im vollständigen Bericht ist dafür gedacht. Gegenüber dem Dienstleister fehlt die Grundlage, um Mehrfaktor-Anmeldung, Protokollierung oder Updates einzufordern. Welche Zusagen nachzuziehen sind, klärt der Auftraggeber mit seiner Rechtsberatung. Die veraltete Komponente im Gateway ist der dringendste technische Punkt, weil sie auf jeder Maschine im Feld läuft.

3.7 Vernetzte Produkte und Schnittstellen

Sind die vernetzten Maschinen im Feld sicher zu betreiben und zu aktualisieren?

Bewertung Grün

… Feststellungen und Einordnung sind im Musterbericht gekürzt.

4 Gegenüberstellung der Maßnahmenbereiche (Auszug)

Die Gegenüberstellung ordnet den technischen Befund den Maßnahmenbereichen des §30 BSIG zu. Ob ein Befund rechtlich eine Lücke ist, entscheidet die Rechtsberatung des Auftraggebers.

Maßnahmenbereich des §30 BSIG	Technischer Befund	Ampel
Zugriffskontrolle und Mehrfaktor-Anmeldung	Administratorrechte liegen dauerhaft beim Dienstleister ohne zweiten Faktor. Die Fernwartung läuft über ein geteiltes Konto, Zugriffe sind keiner Person zuzuordnen.	Rot
Sicherheit der Lieferkette	Der Vertrag mit dem Dienstleister enthält keine technischen Sicherheitszusagen. Eine Drittkomponente im Gateway erhält seit zwei Jahren keine Updates.	Gelb
Bewältigung von Sicherheitsvorfällen	Protokolle bestehen, werden aber von keinem Alarm ausgewertet. Zuständigkeiten außerhalb der Arbeitszeit und ein Meldeweg nach §32 BSIG sind nicht festgelegt.	Rot

… Weitere Maßnahmenbereiche sind im Musterbericht gekürzt.

5 Maßnahmenliste (Auszug)

Die Maßnahmen sind nach Dringlichkeit sortiert. Aufwand und Nutzen sind Schätzungen für die Umsetzung durch das Team des Auftraggebers oder seinen Dienstleister.

Nr.	Maßnahme	Priorität	Aufwand	Nutzen	Zuständigkeit
1	Mehrfaktor-Anmeldung für Administratorrechte erzwingen, eigene Administratorrolle beim Auftraggeber	Hoch	1 Tag	Ein Passwort genügt nicht mehr, Auftraggeber handlungsfähig	IT-Leitung, Dienstleister
2	Persönliche Fernwartungskonten mit zweitem Faktor statt des geteilten Kontos	Hoch	2 Tage	Jeder Zugriff ist einer Person zuzuordnen	Serviceleitung, Dienstleister
3	Schlüssel aus dem Repository in einen Dienst für Secrets verschieben und erneuern	Hoch	2 Tage	Fremde Geräte können sich nicht anmelden	Dienstleister
4	Alarme, Rufbereitschaft und Meldeweg nach §32 BSIG festlegen	Mittel	3 Tage	Ein Vorfall wird in 24 Stunden erkannt und gemeldet	Geschäftsführung, IT-Leitung

… Weitere Maßnahmen sind im Musterbericht gekürzt.

6 Offene Fragen (Auszug)

Diese Fragen gehören zu Rechtsberatung, Datenschutzbeauftragtem oder ISMS-Berater.

1. Ist der Auftraggeber eine wichtige Einrichtung nach §28 BSIG und nach §33 BSIG beim BSI zu registrieren? (Rechtsberatung)
2. Zählt die Tochtergesellschaft in Österreich bei der Einstufung mit, und welches Recht gilt für sie? (Rechtsberatung)
3. Welche Daten der Techniker fallen mit persönlichen Fernwartungskonten an, und wie lange dürfen die Protokolle aufbewahrt werden? (Datenschutzbeauftragter)
4. Welche Richtlinien zu Zugängen, Vorfällen und Lieferanten braucht das Unternehmen, damit die Maßnahmen dauerhaft gelten? (ISMS-Berater)

… Weitere offene Fragen sind im Musterbericht gekürzt.

7 Grundlagen und Grenzen des Checks

Grundlagen

- Rein lesender Zugang zu beiden AWS-Accounts über eine eigene Rolle, danach entfernt
- Fragebogen zur Betroffenheit, Architekturunterlagen, Dienstleistervertrag, Konfigurationsexport der Gateways, Kundenfragebogen
- Zwei Stunden Gespräch mit Geschäftsführung, IT, Service und Dienstleister

Grenzen

- Der Check ist keine Rechtsberatung. Die Einstufung ist eine technisch-organisatorische Plausibilisierung. Die verbindliche Einstufung und die Registrierung beim BSI klärt der Auftraggeber mit seiner Rechtsberatung, ebenso die Vertragsgestaltung.
- Der Check ist keine Zertifizierung und kein Nachweis gegenüber dem BSI. Der Bericht liefert Befunde und Maßnahmen, aus denen Nachweise entstehen.
- Der Check baut kein Managementsystem auf, Richtlinien gehören zum ISMS-Berater.
- Der Check ist kein Penetrationstest, keine Quellcode- oder Firmware-Analyse und kein Test am Gerät. Er beruht auf lesendem Zugang, Unterlagen und Gesprächen.
- Der Check ist keine Vertragsprüfung, der Vertrag wurde nur auf technische Zusagen gelesen.
- tarienna hat nichts geändert, alle Befunde sind reproduzierbar dokumentiert.

Unabhängigkeit

- Die Vergütung hängt nie vom Ergebnis ab, auch nicht von der Betroffenheit.
- tarienna erhält keine Provisionen von Cloud-Anbietern, Dienstleistern oder Werkzeuganbietern.
- Der Bericht empfiehlt keine Umbauten, die tarienna selbst verkaufen will.
- Geschäftsbeziehungen zum Dienstleister legt tarienna vor der Beauftragung offen.
- Architekturen, die tarienna selbst gebaut oder mitgebaut hat, prüft tarienna nicht.

Dieser Bericht ist ein gekürztes Muster mit frei erfundenem Inhalt. Informationen zum NIS2-Architektur-Check stehen unter www.tarienna.eu/nis2-architektur-check/.