KRITIS-Dachgesetz und NIS2 im Agrarhandel

Warum sollten sich Agrarhändler mit diesen Themen beschäftigen?

In den vergangenen Jahren hat der Gesetzgeber neue Vorgaben geschaffen, um Unternehmen besser gegen Sabotage, Naturkatastrophen, technische Ausfälle und Cyberangriffe zu schützen. Dabei sind zwei Regelwerke besonders relevant:

I. **KRITIS-Dachgesetz**: Schutz kritischer Infrastruktur vor physischen Gefahren.

II. **NIS2-Richtlinie / BSI-Gesetz**: Schutz der IT-Systeme und digitalen Prozesse vor Cyberangriffen.

Obwohl beide Regelwerke ähnliche Ziele verfolgen, betreffen sie teilweise unterschiedliche Unternehmen. KRITIS-Betreiber (ca. 1.800 Unternehmen) sind eine Teilmenge der NIS2-Betroffenen (ca. 30.000 Einrichtungen).

KRITIS-Betreiber tragen doppelte Pflichten: NIS2-Anforderungen plus Systeme zur Angriffserkennung, Nachweispflicht alle 3 Jahre und Registrierung bei BSI und BBK.

Für die meisten klassischen Agrarhändler dürfte künftig die ***Frage der NIS2-Betroffenheit wichtiger*** sein als die Einordnung als KRITIS-Betreiber. Das KRITIS-Dachgesetz richtet sich primär an Betreiber besonders versorgungsrelevanter Anlagen. Ein reines Handelsunternehmen mit Büroorganisation, aber ohne eigene Lager-, Umschlag- oder Verarbeitungsinfrastruktur wird demgegenüber häufig nicht in den unmittelbaren Anwendungsbereich des KRITIS-Dachgesetzes fallen.

WICHTIG: Aktuell noch keine Handlungspflicht nach KRITIS

Aktuell müssen Sie als ein Betreiber einer sog. kritischen Anlage (s. u.) noch nicht tätig werden. Sobald die Rechtsverordnung zur Bestimmung kritischer Anlagen gem. § 4 Abs. 3 und § 5 Abs. 1 KRITISDachG in Kraft getreten ist, sind Betreiber verpflichtet, ihre kritischen Anlagen zu registrieren. An die Registrierung sind weitere Anforderungen an die Betreiber kritischer Anlagen geknüpft. Das BBK (als zuständige Behörde) empfiehlt jedoch, sich jetzt schon mit der Steigerung der Resilienz auseinanderzusetzen, um Vorfälle im eigenen Interesse der Betreiber und im Interesse der Allgemeinheit zu verhindern.

ABER: Anforderungen nach NIS2 müssen bereits erfüllt werden

Anders als beim KRITIS-Dachgesetz gelten die Pflichten nach NIS2 bereits seit dem Inkrafttreten am 6. Dezember 2025. Die Registrierung hätte bis zum 6. März 2026 erfolgt sein müssen. Es gibt keine mehrjährige Umsetzungsphase für die eigentlichen Sicherheitsanforderungen. Unternehmen, die in den Anwendungsbereich fallen, müssen die gesetzlichen Anforderungen daher grundsätzlich bereits erfüllen.

I. KRITIS-Dachgesetz

Was ist das KRITIS-Dachgesetz?

Das KRITIS-Dachgesetz setzt die europäische CER-Richtlinie um und soll die Widerstandsfähigkeit kritischer Infrastrukturen gegen Ausfälle und Störungen stärken. Erfasst werden insbesondere Risiken durch Sabotage, Terroranschläge, Naturkatastrophen, Stromausfälle, Lieferkettenstörungen oder Personalausfälle.

Die Lebensmittelwirtschaft gehört ausdrücklich zu den erfassten kritischen Sektoren.

1) Ist damit jedes Agrarhandelsunternehmen automatisch betroffen ist?

Nein. Die Zugehörigkeit zum Sektor Ernährung allein reicht nicht aus.

Entscheidend ist, ob das Unternehmen eine **kritische Anlage** betreibt und damit eine **kritische Einrichtung** darstellt. Maßgeblich ist dabei vor allem die Bedeutung für die Versorgung der Bevölkerung. Als Orientierungswert nennt der Gesetzgeber eine Versorgung von mehr als 500.000 Menschen; im Lebensmittelbereich entspricht dies ungefähr 434.500 Tonnen Lebensmitteln pro Jahr.

Unterscheide:
Kritische Anlage = die Infrastruktur.

Kritische Einrichtung = das Unternehmen, das diese Infrastruktur betreibt.

Beispiel:
Das Silo ist die kritische Anlage, der Silobetreiber ist die kritische Einrichtung.

2) Welche Agrarhändler sind typischerweise nicht betroffen?

Beispiel:
Getreidehändler mit Bürostandort, Vertrieb, Warenhandel, Außendienst, Auftragsabwicklung **aber ohne** Silos, Lagerhäuser, Umschlaganlagen, Verarbeitungsanlagen, Hafenanlagen.

In diesen Fällen spricht viel dafür, dass keine kritische Anlage betrieben wird.

3) Welche Agrarhändler können betroffen sein?

Agrarhändler mit z. B. großen Getreidehafenterminalen, großdimensionierten Silokomplexen, für die Lebensmittelversorgung besonders wichtigen Lagerstandorten, BLE-Lagerhaltung, zentralen Umschlaganlagen mit hoher Versorgungsrelevanz.

Hier sollte eine Einzelfallprüfung erfolgen.

4) Welche Pflichten haben KRITIS-Betreiber?

Betroffene Unternehmen müssen insbesondere:

- sich registrieren und eine 24/7 erreichbare Kontaktstelle nennen,
- Risiken analysieren und Risikomanagement-Maßnahmen ergreifen (näheres dazu hier),

- erhebliche Störungen melden.

Die Geschäftsleitung trägt hierfür eine besondere Verantwortung.

5) Müssen Zäune, Schranken oder Pförtneranlagen errichtet werden?

Nicht automatisch. Das Gesetz schreibt keine bestimmten Sicherheitsmaßnahmen vor.

Vielmehr gilt ein sogenannter „All-Gefahren-Ansatz". Das Unternehmen muss seine individuellen Risiken bewerten und daraus angemessene Maßnahmen ableiten. Genannt werden beispielsweise:

- Zugangsschutz, Objektschutz, Notfallorganisation, Ersatzversorgung, Schutz vor Sabotage, Sicherung von Lieferketten

6) Was bedeutet das für ein reines Handelshaus?

Ein Agrarhändler mit z. B. lediglich Büros, Telefonanlage, ERP-System, Handels- und Verwaltungsfunktionen muss regelmäßig keine Hochsicherheitsmaßnahmen errichten.

Falls das Unternehmen überhaupt unter das Gesetz fallen sollte, könnten je nach Risikolage beispielsweise ausreichen:

- geregelte Zutrittsrechte, Schlüsselmanagement, Besucherkonzept, Notfallhandbuch, Alarmierungs- und Kommunikationspläne

7) Wohin müssen erhebliche Störungen gemeldet werden?

Betreiber kritischer Anlagen müssen erhebliche Störungen an die vom Bundesamt für Bevölkerungsschutz und Katastrophenhilfe (BBK) und dem Bundesamt für Sicherheit in der Informationstechnik (BSI) gemeinsam eingerichtete Meldestelle melden.

Die Meldung muss:

- unverzüglich, spätestens jedoch innerhalb von 24 Stunden nach Kenntnis des Vorfalls, erfolgen,
- bei andauernden Vorfällen aktualisiert werden und
- spätestens einen Monat nach Kenntnis des Vorfalls durch einen ausführlichen Bericht ergänzt werden.

Das BKK schreibt auf seiner Homepage: Die Verpflichtung zur Meldung von Vorfällen ist an die Registrierung gekoppelt und gilt erst zehn Monate nach erfolgter Registrierung als Betreiber kritischer Anlagen (vgl. § 8 Abs. 7 KRITISDachG). **Zurzeit** besteht **noch keine Meldepflicht** da sich die konkretisierende Rechtsverordnung zur Bestimmung kritischer Anlagen gem. § 4 Abs. 3 und § 5 Abs. 1 KRITISDachG noch in Erarbeitung und Abstimmung befindet.

8) Welche Vorfälle sind meldepflichtig?

Meldepflichtig sind erhebliche Störungen, die die Erbringung der kritischen Dienstleistung beeinträchtigen oder gefährden können. Das Gesetz verlangt insbesondere Angaben zu:

- Art und Ursache des Vorfalls,

- Anzahl der Betroffenen,
- Dauer oder voraussichtlicher Dauer,
- betroffenem geografischen Gebiet sowie
- möglichen Auswirkungen auf die Versorgungssicherheit.

9) Wie analysiere ich Risiken und erstelle einen Resilienzplan?

Bei dem genannten „All-Gefahren-Ansatz“ werden nicht nur klassische Sicherheitsrisiken betrachtet, sondern sämtliche Gefahren, die die Leistungserbringung beeinträchtigen könnten. Dazu gehören insbesondere:

- Naturereignisse, Stromausfälle, technische Defekte, Sabotage, Ausfall wichtiger Dienstleister, Lieferkettenstörungen, Personalausfälle.

Für einen Agrarhändler kann eine Risikoanalyse beispielsweise in 3 Schritten erfolgen.

Schritt 1: Kritische Prozesse bestimmen
Welche Tätigkeiten müssen unbedingt funktionieren?

Beispiele: Warenwirtschaftssystem, Vertragsmanagement, Rechnungsstellung, Zahlungsverkehr, Disposition, Kommunikation mit Kunden und Lieferanten

Schritt 2: Kritische Ressourcen identifizieren
Wovon hängen diese Prozesse ab?

Beispiele: Büroräume, Server, Cloud-Dienstleister, Telefonanlage, Internetanschluss, Schlüsselpersonen

Schritt 3: Risiken bewerten
Was kann ausfallen?

Beispiele: Cyberangriff auf ERP-System, Brand im Büro, Stromausfall, Ausfall des Rechenzentrums, Ausfall eines wichtigen Mitarbeiters

10) Für ein typisches Agrarhandelsunternehmen könnte ein Resilienzplan folgende Gliederung haben:

1. **Unternehmensbeschreibung**
   Standorte, Tätigkeiten, Ansprechpartner
2. **Risikoanalyse**
   s. oben - identifizierte Gefahren, Eintrittswahrscheinlichkeit, Schadensausmaß
3. **Schutzmaßnahmen**
   Zutrittsregelungen, Datensicherung, Notstromversorgung (falls erforderlich), Vertretungskonzepte, Zweitzugang zum Internet
4. **Krisenorganisation**
   Krisenteam, Alarmierungskette, Kommunikationswege, Notfallkontakte

5. **Wiederanlaufplanung**
   Prioritäten nach einem Ausfall, Wiederherstellung von IT-Systemen, Ersatzarbeitsplätze

11) Fristen nach dem KRITIS-Dachgesetz

Entgegen einer vielfach anzutreffenden Darstellung wurde die Frist zur Registrierung nach dem KRITIS-Dachgesetz nicht pauschal verlängert. Vielmehr wurde die ursprünglich diskutierte allgemeine Registrierungsfrist durch eine an die Einstufung als kritische Einrichtung anknüpfende Fristenregelung ersetzt. Entscheidend ist heute nicht mehr ein einheitlicher Stichtag für alle Unternehmen, sondern der Zeitpunkt, zu dem eine Einrichtung als kritische Anlage identifiziert wird.

Nach der derzeitigen Systematik des KRITIS-Dachgesetzes gilt eine ereignisbezogene Fristenkette:

- **Registrierung:** Betreiber kritischer Anlagen müssen sich innerhalb von drei Monaten nach ihrer Einstufung bzw. Identifizierung registrieren.
- **Risikoanalyse:** Innerhalb von neun Monaten nach der Registrierung ist eine All-Gefahren-Risikoanalyse durchzuführen. Diese muss physische, organisatorische und sonstige Risiken berücksichtigen.
- **Resilienzplan:** Anschließend sind die erforderlichen Resilienzmaßnahmen zu planen, zu dokumentieren und umzusetzen. Dafür gibt es im Gesetz keine konkrete Frist.
- **Meldepflichten:** Erhebliche Störungen der kritischen Dienstleistung sind innerhalb von 24 Stunden den zuständigen Behörden zu melden. Hierfür müssen Unternehmen entsprechende Prozesse bereits im Vorfeld einrichten.

12) Wo finde ich weitere Informationen zum KRITIS-Dachgesetz?

Die wichtigsten offiziellen Stellen sind:

- das Bundesamt für Bevölkerungsschutz und Katastrophenhilfe (BBK), das für die Umsetzung des KRITIS-Dachgesetzes zuständig ist,
- das Bundesamt für Sicherheit in der Informationstechnik (BSI), soweit Melde- und Registrierungsverfahren betroffen sind.

II. NIS2 und das BSI-Gesetz

Was ist NIS2?

NIS2 ist die europäische Cybersicherheitsrichtlinie. Sie wurde in Deutschland über das BSI-Gesetz umgesetzt und soll Unternehmen besser gegen Cyberangriffe schützen.

Während das KRITIS-Dachgesetz vor allem die **physische Sicherheit** betrifft, konzentriert sich NIS2 auf die **IT-Sicherheit**.

1) Welche Risiken stehen hier im Mittelpunkt?

Hackerangriffe, Ransomware, Datenverlust, Phishing, Ausfall von Warenwirtschaftssystemen, Ausfall von Handelssystemen, Manipulation von Lieferketten

2) Wer ist betroffen?

Anders als beim KRITIS-Dachgesetz kommt es häufig nicht auf bestimmte Anlagen an, sondern auf das Unternehmen selbst.

Besonders **relevant** sind: **Unternehmensgröße, Mitarbeiterzahl, Umsatz, Tätigkeit** in einem regulierten Sektor. Es gibt zwei Kategorien: wichtige und besonders wichtige Einrichtungen.

Der Sektor **Lebensmittel** (Produktion Verarbeitung und Vertrieb) gehört grundsätzlich zum Anwendungsbereich. Die Zahl der betroffenen Unternehmen ist deutlich größer als beim klassischen KRITIS-Recht.

3) Was sind wichtige und besonders wichtige Einrichtungen?

Als „wichtige Einrichtungen“ gelten typischerweise mittlere und größere Unternehmen bestimmter Wirtschaftssektoren, darunter auch der Sektor Ernährung. Dazu zählen unter anderem Lebensmittelunternehmen, wenn sie die relevanten Größenschwellen überschreiten (s. nächste Frage).

Besonders wichtige Einrichtungen

„Besonders wichtige Einrichtungen“ sind Unternehmen aus Sektoren mit besonders hoher Kritikalität, beispielsweise Energie, Verkehr, Gesundheit oder digitale Infrastrukturen. Daneben zählen **auch Betreiber kritischer Anlagen** nach dem KRITIS-Dachgesetz zu dieser Kategorie.

4) Kann ein Agrarhändler betroffen sein?

Ja: Ein Unternehmen aus dem Sektor Lebensmittel gelten grundsätzlich als **wichtige Einrichtung**, wenn sie mindestens die Größe eines mittleren Unternehmens erreichen.

Dies ist regelmäßig der Fall bei:

- mindestens **50 Beschäftigten** oder
- mehr als **10 Millionen Euro Jahresumsatz** und mehr als **10 Millionen Euro Bilanzsumme**.

Auch ohne Silos oder Lagerhäuser kann eine Betroffenheit nach NIS2 vorliegen.

Eine Einstufung als **besonders wichtige Einrichtung** kommt regelmäßig bei Großunternehmen in Betracht.

Die Schwellen liegen bei:

- mindestens **250 Beschäftigten** oder
- mehr als **50 Millionen Euro Jahresumsatz** und mehr als **43 Millionen Euro Bilanzsumme**.

Besonders wichtige Einrichtung ist man auch, wenn man in den Anwendungsbereich des KRITIS-Dachgesetzes (vgl. oben Teil I) fällt.

5) Sind auch Futtermittelunternehmen betroffen?

Aus unserer Sicht spricht vieles dafür, dass die Futtermittelproduktion nicht vom Sektor „Lebensmittel“ im Sinne der NIS2-Regelungen erfasst wird. Die maßgeblichen Vorschriften verweisen auf die Begriffsbestimmungen der Verordnung (EG) Nr. 178/2002. Dort wird ausdrücklich zwischen Lebensmittelunternehmen und Futtermittelunternehmen unterschieden.

Eine abschließende rechtliche Bewertung ist jedoch derzeit nicht möglich. Aus den bislang bekannten behördlichen Auslegungshilfen ergibt sich keine eindeutige Aussage der zuständigen Stellen zu dieser Frage. Da die Versorgung mit Futtermitteln mittelbar auch für die Lebensmittelversorgung von Bedeutung ist, kann eine abweichende Auslegung nicht vollständig ausgeschlossen werden. Bis zu einer klarstellenden behördlichen oder gerichtlichen Einordnung verbleibt daher eine gewisse Rechtsunsicherheit.

6) Unterscheiden sich die Pflichten von „wichtigen Einrichtungen" und „besonders wichtigen Einrichtungen"?

Überraschenderweise kaum.

Beide Kategorien müssen grundsätzlich dieselben Anforderungen an das Cyber-Risikomanagement erfüllen. Dazu gehören insbesondere:

- Risikomanagement für IT-Systeme,
- Notfall- und Krisenmanagement,
- Incident-Response-Prozesse,
- Datensicherung und Wiederherstellung,
- Lieferkettensicherheit,
- Zugriffskontrollen,
- Schulung von Mitarbeitern,
- Meldung erheblicher Sicherheitsvorfälle,
- Registrierung beim BSI.

Der wesentliche **Unterschied liegt** daher nicht in den Pflichten, sondern **in der staatlichen Aufsicht** und den **Sanktionen.**

7) Wie unterscheiden sich die behördlichen Kontrollen?

Bei **wichtigen Einrichtungen** erfolgt die Aufsicht grundsätzlich reaktiv.

Das bedeutet:

- Das BSI wird meist erst tätig, wenn es Hinweise auf Verstöße oder Sicherheitsvorfälle gibt.
- Regelmäßige Vor-Ort-Prüfungen sind nicht der Regelfall

Besonders wichtige Einrichtungen unterliegen einer intensiveren und proaktiven Aufsicht.

Das BSI kann beispielsweise Nachweise anfordern, Audits verlangen, Vor-Ort-Kontrollen durchführen, Sicherheitsprüfungen veranlassen

8) Muss jedes Unternehmen eine eigene IT-Abteilung haben?

Nein. Die Anforderungen müssen jedoch angemessen erfüllt werden.

Ein mittelständischer Agrarhändler kann viele Maßnahmen auch gemeinsam mit:

- externen IT-Dienstleistern, Rechenzentren, Softwareanbietern oder Managed-Service-Providern umsetzen.

9) Welche Pflichten treffen Agrarhändler?

Die Pflichten sind gesetzlich detailliert vorgegeben (u. a. in den §§ 30ff des BSI-Gesetzes). Für den Agrarhandel zentral sind drei Themen:

a) IT-Sicherheits- und Risikomanagementpflichten

Maßnahmen des Risikomanagements sollen den Stand der Technik einhalten, die einschlägigen europäischen und internationalen Normen berücksichtigen und müssen auf einem gefahrenübergreifenden Ansatz beruhen. Die Maßnahmen müssen zumindest Folgendes umfassen:

1. Risikoanalyse und Sicherheit der Informationssysteme
2. Bewältigung von Sicherheitsvorfällen
3. Aufrechterhaltung des Betriebs (Backup, Disaster Recovery, Krisenmanagement)
4. Sicherheit der Lieferkette
5. Sicherheit bei Erwerb, Entwicklung und Wartung
6. Konzepte zur Bewertung der Wirksamkeit der Risikomanagement-Maßnahmen
7. Grundlegende Cyberhygiene und Schulungen
8. Konzepte zur Verwendung von Kryptografie
9. Personalsicherheit, Zugangskontrollen, Anlagenmanagement

10. Multi-Faktor-Authentifizierung, kontinuierliche Authentifizierung, gesicherte Sprach-/Video-/Textkommunikation

b) Meldepflichten bei IT-Sicherheitsvorfällen

Bei erheblichen Vorfällen gelten strenge Fristen:

- **innerhalb von 24 Stunden**: Frühwarnmeldung
- **innerhalb von 72 Stunden**: detaillierte Meldung
- **innerhalb eines Monats**: Abschlussbericht

c) Registrierungspflicht

Betroffene Unternehmen müssen sich beim **BSI registrieren**.

- Frist: grundsätzlich **innerhalb von 3 Monaten nach Betroffenheit**
- Für bestehende Unternehmen bedeutet dies: 3 Monate nach Inkrafttreten des Gesetzes am 6.12.2025, also: **bis 6. März 2026** (keine Übergangsfrist)

13) Wichtig aus Unternehmenssicht

Die Pflicht richtet sich ausdrücklich an die **Geschäftsleitung** (Organverantwortung, Schulungspflicht). Dies ist der wohl folgenreichste Unterschied zur bisherigen Cybersicherheitsregulierung. Die NIS2-Richtlinie verpflichtet die Leitungsorgane, die Risikomanagement-Maßnahmen zu billigen, ihre Umsetzung zu überwachen und an regelmäßigen Schulungen teilzunehmen. Diese Pflicht lässt sich nicht vollständig delegieren: Auch wenn die operative Umsetzung an einen CISO oder IT-Dienstleister ausgelagert wird, bleibt die Aufsichtsverantwortung bei Geschäftsführung und Vorstand.

Das deutsche Umsetzungsgesetz greift diese Vorgabe auf und macht die Leitungsebene bei Pflichtverletzungen haftbar. Für Unternehmen bedeutet das: **Cybersicherheit ist keine reine IT-Frage mehr, sondern ein Thema der Unternehmensführung mit dokumentierten Vorstandsbeschlüssen**.

14) Checkliste zur Umsetzung der NIS2-Anforderungen

☐ Prüfen, ob das Unternehmen unter die NIS2-Vorgaben fällt (Branche und Unternehmensgröße)

☐ Erforderliche Registrierung beim BSI fristgerecht vornehmen

☐ Risiken für die Informations- und IT-Sicherheit ermitteln und dokumentieren

☐ Angemessene technische und organisatorische Schutzmaßnahmen umsetzen

☐ Verfahren für den Umgang mit Sicherheitsvorfällen festlegen und Meldewege definieren

☐ Sichere Anmeldeverfahren (z. B. Mehrfaktor-Authentisierung) einsetzen

☐ Sicherheitsanforderungen an Dienstleister und Lieferanten berücksichtigen und dokumentieren

☐ Regelmäßige Sensibilisierung und Schulung der Beschäftigten durchführen

☐ Zuständigkeiten und Überwachungsaufgaben der Geschäftsleitung festhalten