BayWa r.e.

r.e.think energy

Anstehende Änderungen im IT-Sicherheitsgesetz 3.0 und KRITIS Dachgesetz

Agenda

1. Vorstellung
2. IT-Sicherheitsgesetz 3.0
3. KRITIS Dachgesetz

1

Vorstellung

Vorstellung Mohamed Harrou

- Jahrgang 1982, verheiratet, zwei Kinder
- Ausbildung zum Industrieelektroniker
- Weiterbildung zum Automatisierungstechniker und Technischer Betriebswirt
- Seit 2012 in der Erneuerbare Energien Branche
- Von Anfang an im SCADA Bereich
- Aktuell Teamleiter Globales SCADA Team
- Mitarbeit in Gremien beim BSW, BWE, dena und FGW im Bereich Cyber Security

Vernetzen wir uns auf LinkedIn!

Vorstellung
BayWa r.e. Data Services GmbH

BayWa r.e. Data Services unterstützt seine Kunden im Bereich der Erneuerbaren mit datenbasierten Diensten

- BayWa r.e. Data Services GmbH ist eine global agierende Tochter der BayWa r.e. AG
- Wir bieten SCADA, Leitstellen- und Überwachungs-dienstleistungen, IT-Sicherheit, Daten Analysen und Dienstleistungen zur Software Implementierung an
- Unser Team aus erfahrenen SCADA Engineers bietet Dienstleistungen zu SCADA, Kommunikation und IT-Sicherheit an
- Unterstützung von internen und externen Kunden bei Wind und PV-Anlagen in jedem Projektstatus

Hinweis/Disclaimer

Der folgende Vortrag stellt keine Rechtsberatung dar, sondern nur die Meinung des Autors, wie eine Ausgestaltung des Gesetzes aussehen könnte.

Beide Gesetze befinden sich in der Erstellungsphase und sind somit als „Work in Progress“ anzusehen. Änderungen aller Art sind nicht auszuschließen. Dieser Vortrag bezieht sich auf den aktuell bekannten Status, Stand 11.10.2023.

2

IT-Sicherheitsgesetz 3.0

Gesetz/Verordnung/Richtline – Eine Einordnung

NIS2-Richtline

- Richtline der EU
- Novellierung der NIS-Richtline (Update)
- Gibt den Rahmen für nationale Gesetze vor
- Die NIS2-Richtline muss bis zum 14.10.2024 in allen Staaten der EU in nationales Recht umgesetzt werden

IT-Sicherheitsgesetz

- Nationales Gesetz bzw. nationale Umsetzung der NIS2-Richtline in Deutschland
- Gibt teilweise vor, wer betroffen ist
- Definiert Rechte/Pflichten/Strafen
- Ist ein Artikelgesetz d. h. es werden verschiedene Gesetze (z. B. BS-Gesetz) geändert und alle relevanten Paragraphen werden im IT-Sicherheitsgesetz zusammengefasst
- Verabschiedung voraussichtlich Q1-2023

KRITIS Verordnung

- Legt fest, welche Sektoren betroffen sind
- Legt Schwellwerte fest

Wer ist von der neuen Gesetzgebung betroffen?

Nach IT-Sicherheitsgesetz 3.0/NIS2

- Betreiber Kritischer Anlagen (BKA)
  - Definition in der KRITIS Verordnung
- Besonders wichtige (BWU) und wichtige Unternehmen (WU) aus definierten Sektoren
  - Energie ist Teil dieser Sektoren
  - Mittlere Unternehmen (wichtig):
    - 50 – 249 Mitarbeiter **ODER** bis zu >10 Mio. Euro Jahresumsatz **UND** bis zu >10 Mio. Euro Bilanz
  - Große Unternehmen (besonders Wichtig):
    - Ab 250 Mitarbeiter **ODER** >50 Mio. Umsatz **UND** >43 Mio. Bilanz

Nach KRITIS Verordnung

(aktuelle Verordnung, Änderungen möglich)

- Erzeugungsanlagen (am Netzverknüpfungspunkt)
  - Schwarzstartfähig: Jede
  - Bereitstellung von Primärregelleistung: ab 36 MW
  - Alle anderen: Ab 104 MW
  - Anlagen zur Bündelung und Steuerung elektrischer Leistung: ab 104 MW

Beispiele betroffener Unternehmen [1/2]

PV oder Windpark mit >104 MW Leistung

Zählt als kritische Infrastruktur, die SPV ist registrierungspflichtig und muss alle Anforderungen des Gesetzes befolgen. Bei einer SPV bedeutet dies u. a. Einsatz zertifizierter Komponenten in wichtigen Bereichen und Lieferantenmanagement.

Technischer Betriebsführer

Wenn die Mitarbeiter des Unternehmens auf insg. 104 MW Leistung regelnd zugreifen können, fällt das Unternehmen unter das Gesetz. Dabei ist es egal ob man 104 MW auf einmal (Red Button) oder nach-einander schalten kann.

Beispiele betroffener Unternehmen [2/2]

Die Sache mit der Bilanzsumme …

Eine SPV hält eine Anlage auf der Bilanz. Am Tag 1 der Unternehmensgründung, beträgt der Wert der Anlage 100% des Kaufpreises. Dieser Wert sinkt jährlich durch festgelegte Abschreibungen bis auf 0€ Buchwert. Wenn eine Anlage für >43 Mio. Euro gekauft wird, und einen Umsatz >50M€ p.a. ist die SPV bzw. der Besitzer der SPV registrierungspflichtig bzw. fällt unter das IT-Sicherheitsgesetz.

Betreiber von Wind und PV-Analgen

Wenn das Unternehmen die Schwellwerte für Mitarbeiter, Umsatz oder Bilanzsumme überschreitet, fällt es in den Geltungsbereich des Gesetzes. Kennzahlen der SPVs werden angerechnet.

Pflichten betroffener Unternehmen [1/2]

Registrierung (BKA, BWU, WU)

Unternehmen und Betreiber müssen sich selbst identifizieren und beim BSI melden. Es erfolgt keine Ansprache durch das BSI! Unternehmen haben drei Monate Zeit, nach der Feststellung sich zu melden. (Betreiber kritischer Infrastrukturen müssen dies unverzüglich bzw. am nächsten Werktag machen).

Umsetzung von „Risikomanagementmaßnahmen“ (BKA, BWU, WU)

- Einführung eines ISMS – Informations-Sicherheits-Management-System. Ein Management System zum Erfassen, koordinieren und Umsetzen aller Maßnahmen zur Einhaltung der Ziele „Störungen der Verfügbarkeit, Integrität, Authentizität und Vertraulichkeit“ der relevanten Systeme. Ähnlich eines QM-Management Systems nach ISO 9001
- Maßnahmen zur Aufrechterhaltung des Betriebs (Backups, Krisen- und Notfallvorsorge)
- Sicherheit der Lieferkette
- Sicherheitsmaßnahmen bei Erwerb von IT-Produkten und Dienstleistungen
- Konzepte zur Bewertung der Sicherheitsmaßnahmen
- Schulungen zur Cybersicherheit
- Einsatz von Kryptografie und Verschlüsselung
- „Sicherheit des Personals“ (evtl. sind hier Sicherheitsüberprüfungen des Personals gemeint)
- Multi Faktor Authentifizierung

Pflichten betroffener Unternehmen [2/2]

System zur Angriffserkennung (BKA)

Betreiber Kritischer Infrastrukturen müssen zusätzlich ein System zur Angriffserkennung (IDS – Intrusion Detection System) implementieren.

Nachweise (BKA)

Die erfolgreiche Umsetzung der „Risikomanagementmaßnahmen“ muss beim BSI nachgewiesen werden. Dies erfolgt durch ein Audit eines zugelassenen Auditors, eine Zertifizierung ist nicht Pflicht. Der erste Nachweis muss drei Jahre nach der Registrierung erfolgen, anschließend alle drei Jahre.

Meldepflichten (BKA, BWU, WU)

Betroffene Unternehmen müssen IT-Sicherheitsvorfälle umgehend (max. 24h) an das BSI melden. Die Erstmeldung muss nicht vollständig sein und kann nachträglich ergänzt werden.

Informationsaustausch (BKA, BWU)

Die Teilnahme an der Plattform zum Informationsaustusch des BSI (BSIP) ist Pflicht.

Besondere Pflichten für Geschäftsführer

Billigung und Überwachung der Maßnahmen (BKA, BWU, WU)

Der Geschäftsführer von betroffenen Unternehmen ist verpflichtet, die Einhaltung der „Risikomanagementmaßnahmen“ zu überwachen und diese zu billigen.
~~Die Beauftragung eines Dritten für diese Aufgaben ist nicht zulässig!~~

Persönliche Haftung (BKA, BWU, WU)

Der Geschäftsführer haftet nicht mehr persönlich wie in den vorherigen Gesetzestexten benannt. Er kann auch nicht mehr vom BSI entlassen werden. Das entbindet nicht von der Sorgfaltspflicht z. B. nach §98 AktG.

Regelmäßige Schulungen (BKA, BWU, WU)

Geschäftsführer müssen regelmäßig an Cyber Security Schulungen teilnehmen.

Einsatz zertifizierter Produkte

Produkte, Dienste und Prozesse (BKA, BWU, WU)

Kritische Anlagen, wichtige und besonders wichtige Unternehmen dürfen bestimmte Produkte, Dienste und Prozesse nur einsetzen, wenn diese eine gültige Cybersicherheitszertifizierung haben. Welche (IKT) Produkte, Dienste und Prozesse davon betroffen sein werden, wird in einer separaten Verordnung festgehalten.

Kritische Komponenten (KA)

Der Betreiber einer kritischen Infrastruktur muss kritische Komponenten dem Innenministerium melden. Welche Komponenten als kritisch einzustufen sind, erfolgt in einem separaten Gesetz, bisher liegt ein solches nur für die ITK-Branche vor (Lex Huawei – 5G Netze).

Das Innenministerium kann den Einsatz bestimmter Komponenten untersagen.

Zuständigkeiten

Wichtige und besonders wichtige Unternehmen

Das BSI ist für wichtige Unternehmen sowie besonders wichtige Unternehmen zuständig, die in Deutschland niedergelassen sind.

Betreiber kritischer Infrastrukturen

Für kritische Anlagen, die auf deutschem Hoheitsgebiet betrieben werden bzw. deren Betreiber, ist das BSI ebenfalls verantwortlich.

Befugnisse des BSI

- Überprüfung der Umsetzung der Anforderungen (BKA)
- Anweisungen zur Verhütung oder Behebung von Vorfällen (BKA, BWU)
- Verbindliche Anweisungen zur Umsetzung von Verpflichtungen (BKA, BWU, WU)
- Unterrichtung von Personen und Unternehmen (BKA, BWU, WU)
- Forderung einer Kontaktperson (BKA, BWU, WU)
- Entzug der Zulassung bei Nichteinhaltung der Vorschriften (KA, BU)

Sanktionen und Bußgelder

Allgemein

Die Strafe richtet sich nach betroffenen Unternehmen und dem Tatbestand aus. Der neue Bußgeldkatalog orientiert sich an den Strafen der DSGVO. Es werden hier nur die Höchststrafen aufgelistet.

Wichtige Unternehmen

Höchststrafe:
2 Mio. Euro

Besonders wichtige Unternehmen

Höchststrafe:
7 Mio. Euro oder 1,4%
des globalen Umsatzes vom Vorjahr

Betreiber kritischer Infrastrukturen

Höchststrafe:
10 Mio. Euro oder 2%
des globalen Umsatzes vom Vorjahr

Timeline IT-Sicherheitsgesetz 3.0 (geplant)

Erster Referentenentwurf

Zweiter Referenten-entwurf

Dritter Referentenentwurf (Diskussionspapier)

Verkündung des Gesetzes

Inkrafttreten

01 02 03 04 05 06 07 08 09 10 11 12

2023

01 02 03 04 05 06 07 08 09 10 11 12

2024

3

KRITIS Dachgesetz

Ziele und betroffene Unternehmen

Ziele des Gesetzes

Ziel dieses Gesetzes ist es die Resilienz der kritischen Infrastrukturen zu verbessern.

Betroffene Unternehmen

- Betroffen sein sollen die Betreiber Kritischer Infrastrukturen wie in der KritisV geregelt
- Die bisherige KritisV soll durch eine Verordnungs-ermächtigung ersetzt werden, die für das IT-Sicherheits-gesetz und für das Kritis-Dachgesetz gültig sein soll
- Besonders wichtige Unternehmen und wichtige Unternehmen sind nicht betroffen

Pflichten betroffener Unternehmen [1/4]

Registrierung

Betreiber kritischer Infrastrukturen müssen diese am nächsten Werktag nach bekannt werden registrieren. Es gibt nur eine Registrierungsstelle für betroffene nach IT-Sicherheitsgesetz und Kritis-Dachgesetz. Zudem muss eine Kontaktperson benannt werden.

Risikoanalyse

Neun Monate nach der Erstregistrierung und anschließend alle vier Jahre müssen Risikoanalysen durchgeführt werden.

Risiken können u. a. sein:

- Unfälle
- Naturkatastrophen
- Gesundheitliche Notlagen (Corona)
- Hybride Bedrohungen
- Feindliche Bedrohungen
- Terrorismus

Pflichten betroffener Unternehmen [2/4]

Alle Maßnahmen müssen dokumentiert werden.

Resilienz Maßnahmen

Betroffene Unternehmen müssen „geeignete und verhältnismäßige“ Maßnahmen ergreifen, um die Resilienz der betroffenen Infrastruktur zu gewährleisten. Dabei soll der „Stand der Technik“ eingehalten werden.

Maßnahmen können u.a. sein:

- Maßnahmen, die erforderlich sind um das Auftreten von Vorfällen verhindern
- Angemessener physischer Schutz der kritischen Anlagen
- Reaktion und Abwehr und Begrenzung der Folgen von Vorfällen
- Wiederherstellung nach Vorfällen
- Angemessenes Sicherheitsmanagement für eigenes Personal und externe Dienstleister
- Schulungen, Übungen für Personal

Pflichten betroffener Unternehmen [3/4]

Mögliche Maßnahmen, um die Resilienz zu erhöhen

Um die voran genannten Maßnahmen zu erreichen, sollen die Betreiber folgende Maßnahmen berücksichtigen:

- Verhindern von Vorfällen
- Physischer Schutz
- Reaktion auf Vorfälle
- Wiederherstellung nach Vorfällen
- Personalsicherheit
- Schulungen für Mitarbeiter

Einsatz kritischer Komponenten

Wie auch im IT-Sicherheitsgesetz vorgesehen, soll auch im Kritis-Dachgesetz der Einsatz bestimmter Komponenten reguliert werden. Der Paragraph ist aktuell noch leer.

Pflichten betroffener Unternehmen [4/4]

Nachweise

Alle Maßnahmen müssen in einem Resilienz Plan dargestellt werden. Dieser Plan muss dem BBK alle zwei Jahre „auf geeigneter Weise“ nachgewiesen werden. Der Nachweis **kann** durch Audits erfolgen.

Bei Zweifeln kann das BBK selbst eine Überprüfung vornehmen.

Meldungen

Betreiber müssen „erhebliche“ Störungen innerhalb von 24 Stunden an eine gemeinsame Meldestelle von BSI und BBK melden. Spätestens nach einem Monat muss ein ausführlicher Bericht vorgelegt werden.

Bußgelder

Allgemein

Bußgelder sind geplant aber aktuell noch nicht definiert.

Timeline Kritis-Dachgesetz (geplant)

Erster Referentenentwurf

Verabschiedung

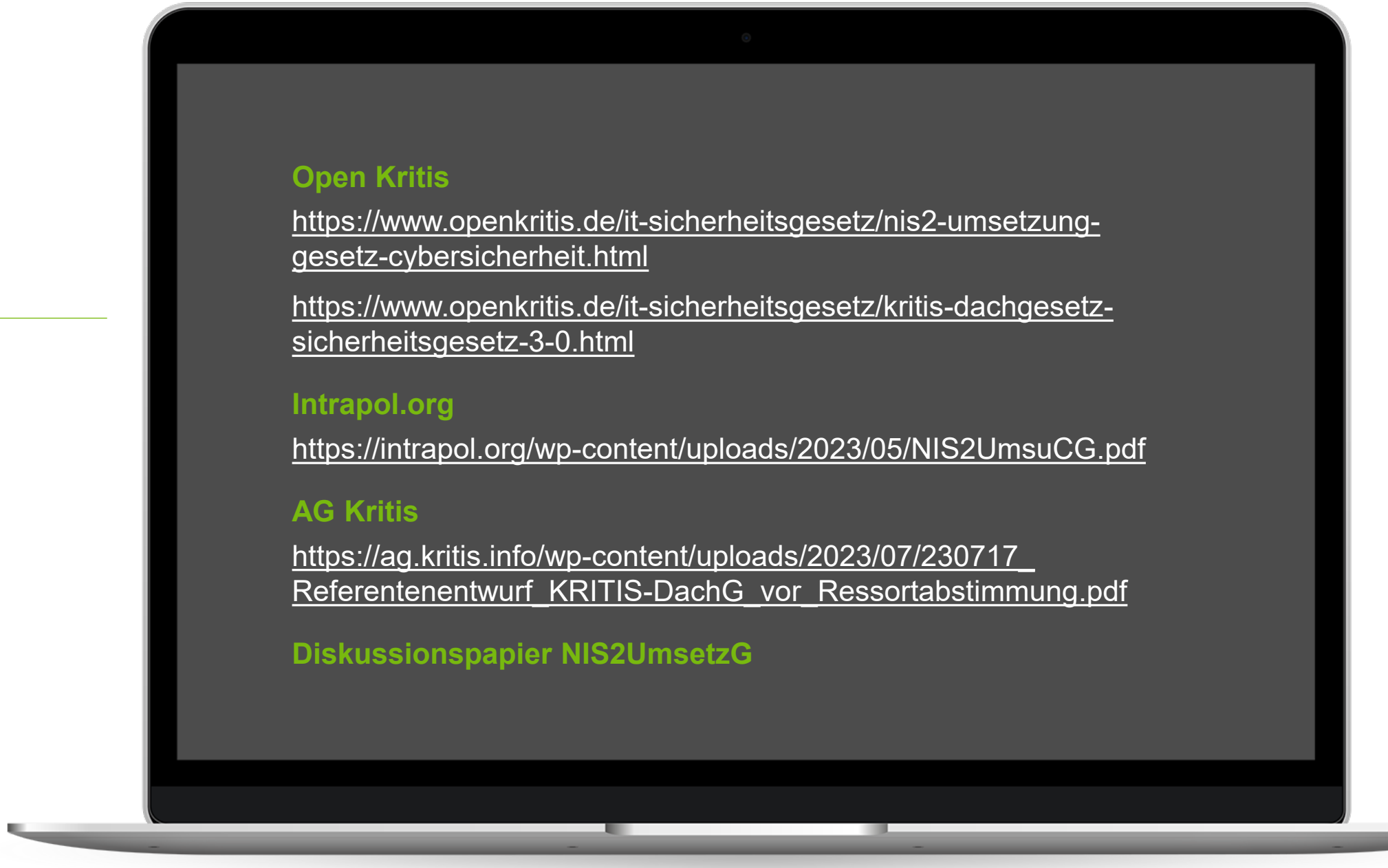
Inkrafttreten

Nachliefern Rechtsverordnung

01 02 03 04 05 06 07 08 09 10 11 12 | 01 02 03 04 05 06 07 08 09 10 11 12

2023 | 2024

Quellen


Open Kritis
https://www.openkritis.de/it-sicherheitsgesetz/nis2-umsetzung-gesetz-cybersicherheit.html
https://www.openkritis.de/it-sicherheitsgesetz/kritis-dachgesetz-sicherheitsgesetz-3-0.html
Intrapol.org
https://intrapol.org/wp-content/uploads/2023/05/NIS2UmsuCG.pdf
AG Kritis
https://ag.kritis.info/wp-content/uploads/2023/07/230717_Referentenentwurf_KRITIS-DachG_vor_Ressortabstimmung.pdf
Diskussionspapier NIS2UmsetzG

Vielen Dank

Mohamed Harrou

Head of Global SCADA
Mohamed.Harrou@baywa-re.com

Copyright